UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

CLASIFICACIÓN DE RIESGOS Y AMENAZAS CIBERNÉTICAS PARA LA SEGURIDAD NACIONAL MEXICANA EN EL SIGLO XXI

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN CIENCIAS POLÍTICAS Y ADMINISTRACIÓN PÚBLICA (OPCIÓN: CIENCIA POLÍTICA)

PRESENTA:

ANTONIO HERNÁNDEZ ALEJO

DIRECTOR:

DR. MANUEL QUIJANO TORRES

Ciudad Universitaria, CD. MX., 2021

El ser humano es, por naturaleza, un Animal Político.

ARISTÓTELES

AGRADECIMIENTOS

A mi madre y a mi padre, por brindarme su apoyo en todo momento a pesar de las adversidades. Queridos mamá y papá, considero que no existen palabras suficientes para agradecerles todo lo que soy y todo lo que tengo, por ese motivo quiero dedicarles con todo mi corazón el presente trabajo de investigación, ya que sin ustedes no tendría razón de ser.

A mis hermanos Eduardo y Araceli; a mis sobrinos Sebastián y Francisco; a mis primos Diego, Ángel, Fernanda, Luis, Alejandra, Martín, Viridiana, Rosa, Elena y Miguel; a mis tíos José Luis (QEPD), Amelia (QEPD), Martín, Luisa, Mario, Juana, Gloria y Margarita; a mis abuelos Juan (QEPD), Celia (QEPD) y Juana (QEPD). Querida familia, les agradezco por estar presentes en cada uno de los momentos de mi vida, tanto en las buenas como en las malas.

A mi alma máter la Universidad Nacional Autónoma de México, en especial al Colegio de Ciencias y Humanidades Plantel Azcapotzalco; a la Escuela Nacional de Lenguas, Lingüística y Traducción; así como a la Facultad de Ciencias Políticas y Sociales. Querida UNAM, te agradezco por todo lo que me has concedido a lo largo de diez años desde que ingresé por primera vez a tus aulas; por todas las amistades que hice, por todas las experiencias que tuve y por todas las enseñanzas aprendidas. Me retiro de tus aulas con la promesa de poner en lo alto tu nombre y el de México.

A quienes me ofrecieron su amistad de manera incondicional: Leonardo Sánchez Peña, Javier De Jesús Leal, Pedro Alvarado Zainos, Gilda Sánchez Fuentes, Yesenia Velázquez Román, Camila Retana Gutiérrez, Viridiana Valdez Vilchis, Fernanda García Tlapanco, Linda Palomo Victoria, Josselyn Flores Gálvez, Laura Reyes De Gaona, Daniela Álvarez García, Lizette Pérez Castillo, Lidia Moreno Hernández, Reina De Gaona Barón, Aura Patiño Muciño, Salvador Ojeda Espinosa y Armando Sánchez Ramírez. Queridos amigos y amigas, quiero agradecerles por todos los momentos que hemos compartido juntos, por todos los consejos que me han dado y por formar parte de esta travesía llamada vida.

A

Reyna Alejo Márquez

Antonio Hernández Sánchez

A la memoria de

Amelia Alejo Márquez

José Luis Solís González

ÍNDICE

INTRODUCCIÓN

Desde la Constitución Política de los Estados Unidos Mexicanos de 1917 hasta la actualidad la Nación mexicana enfrenta circunstancias internas y externas que ponen en peligro la integridad, estabilidad y permanencia del Estado. En el siglo XXI el Estado mexicano afronta el surgimiento de una nueva clase de antagonismos generados por las Tecnologías de la Información y la Comunicación (TIC) que atentan contra la seguridad de la nación.

Los antagonismos para la seguridad nacional que derivan de las TIC reciben el prefijo *Ciber* o el adjetivo *Cibernética* ya que están presentes en el *Ciberespacio* el cual se describe como un dominio virtual derivado de la convergencia entre sistemas informáticos y redes de telecomunicaciones. Los sectores público, privado y social del Estado dependen de ambos elementos por lo cual son vulnerables ante riesgos y amenazas cibernéticas.

En consecuencia aparece la *Ciberseguridad* o *Seguridad Cibernética* como dimensión de la *Seguridad Nacional* cuyo objeto de estudio consiste en determinar las acciones pertinentes para salvaguardar los factores tecnológico (hardware y software) y humano (usuarios) del Estado. El primero atiende los componentes físico y lógico de las TIC mientras que el segundo considera la interacción entre individuos, sociedades y naciones.

En ese sentido el estudio de la Ciberseguridad como asunto de Seguridad Nacional se divide en una parte técnica y en otra política cuya comprensión requiere de las categorías de la Ciencia Política. El objeto de la Ciencia Política, en palabras de Cicerón, consiste en "ver los caminos a veces sinuosos que atraviesan los Estados, con el fin de que, una vez sabido adonde tienden los acontecimientos, poder detenerlos o prevenirlos".[1]

[1] Marco Tulio Cicerón, *La república/Las leyes*, Madrid, Ediciones Akal, 2017, p. 107.

Por ese motivo el presente trabajo de investigación propone un modelo de clasificación de riesgos y amenazas cibernéticas para la seguridad nacional mexicana en el siglo XXI. En la investigación convergen referentes teóricos y prácticos de la Ciencia Política, la Administración Pública y la Informática para explicar cada uno de los conceptos en lo general y en lo particular sin dejar de lado la naturaleza política del objeto de estudio.

La hipótesis de la investigación sostiene que en el siglo XXI las Tecnologías de la Información y la Comunicación generan riesgos y amenazas que atentan contra la seguridad del individuo, la familia, la sociedad, las instituciones e inclusive del Estado. Por lo tanto es indispensable contar con un modelo de clasificación que permita dimensionar los antagonismos cibernéticos para la seguridad nacional con el propósito de detenerlos o prevenirlos.

El objetivo general consiste en establecer un modelo de clasificación de riesgos y amenazas cibernéticas para la seguridad nacional mexicana. Para lograrlo se determinan tres objetivos específicos: 1) fijar las bases teórico-conceptuales de la Seguridad Nacional y la Ciberseguridad; 2) diagnosticar el estado que guarda la ciberseguridad a nivel nacional e internacional en la actualidad; 3) definir la agenda de riesgos y amenazas en la materia.

En el primer capítulo “Seguridad Nacional y Ciberseguridad: Marco teórico-conceptual” se emplean conceptos de la Ciencia Política y la Administración Pública para definir los medios y los fines del Estado como razón de ser de la Seguridad Nacional y por ende de la Ciberseguridad. La primera se define con base en los fundamentos de la teoría política y administrativa; la segunda parte de las nociones básicas de la Informática.

La definición conceptual de la Seguridad Nacional se construye a partir de la teoría aristotélica y maquiavélica junto las interpretaciones de la Ley de Seguridad Nacional, el Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional, el Programa para la Seguridad Nacional y la Agenda Nacional de Riesgos. La definición de la Ciberseguridad se compara con las definiciones establecidas en la Estrategia Nacional de Ciberseguridad.

En el segundo capítulo “El estado de la ciberseguridad en el siglo XXI” se exponen las problemáticas asociadas con las TIC más recurrentes a nivel nacional e internacional en el transcurso del nuevo milenio. Para describir los contextos interno y externo se consideran tanto el Informe Global de Riesgos como el Índice Global de Ciberseguridad para determinar el grado de vulnerabilidad en el que se encuentran las naciones.

Si bien existen numerosos casos reportados desde inicios del nuevo milenio, comenzando con el denominado “Efecto 2000” o “Y2K” como precursor del enfoque de la ciberseguridad como asunto de seguridad nacional, tan sólo se abordan aquellos cuyos efectos trascienden lo tecnológico. Con base en los incidentes descritos en los ámbitos interno y externo se exponen de manera individual los más significativos para la seguridad de uno o más Estados.

Por último, en el tercer capítulo “Clasificación de riesgos y amenazas cibernéticas” se propone un modelo de clasificación con el que se define la agenda de los principales antagonismos cibernéticos a partir de las características que se determinaron en los dos capítulos anteriores. El modelo contempla la síntesis política, administrativa y tecnológica de las definiciones conceptuales del primer capítulo junto con los casos del segundo.

La clasificación tiene el propósito de conocer la dimensión política de riesgos y amenazas asociadas con las Tecnologías de la Información y la Comunicación que atentan contra la seguridad del individuo, la familia, la sociedad, las instituciones y del Estado mexicano para poder detenerlos o prevenirlos. Además sirve como propuesta de instrumento de análisis político para el estudio de la Ciberseguridad como asunto de Seguridad Nacional en México.

En resumen, la presente investigación es un estudio político-administrativo en el que se sientan las bases de la Seguridad Nacional y la Ciberseguridad; se diagnostica el estado que guarda la ciberseguridad en México y el mundo; se clasifican los riesgos y las amenazas cibernéticas. En especial porque el uso de las TIC puede beneficiar o perjudicar a los sectores público, privado y social que constituyen el Estado mexicano.

1. SEGURIDAD NACIONAL Y CIBERSEGURIDAD: MARCO TEÓRICO-CONCEPTUAL

1.1 Sobre el concepto de Seguridad Nacional

El concepto de Seguridad Nacional ha tenido múltiples interpretaciones en la teoría y en la práctica debido a la ambigüedad del término. No obstante se trata de un asunto de origen político ya que encuentra su razón de ser en el Estado que se define como "la sociedad política y jurídicamente organizada que se integra por tres elementos básicos: Territorio, Población y Gobierno y cuyo propósito es la procuración del bien común".[2]

En otras palabras, el Estado es la forma de organización política en la que un gobierno ejerce su autoridad sobre una población en un territorio determinado. Tiene como objetivos mitigar la escasez y el conflicto social por medio de las instituciones públicas, privadas y sociales que procuran los mínimos de bienestar: alimentación, salud, educación, trabajo, vivienda, comunicaciones y transporte, energía, ecología, seguridad pública y procesos de justicia.[3]

Para garantizar el bienestar común de la sociedad el Estado asume la rectoría de los asuntos públicos en beneficio esencial de los gobernados antes que de los gobernantes. En el *Libro Primero* de la *Retórica* Aristóteles menciona que las materias de deliberación política, en orden a la seguridad, son: 1) la adquisición de recursos; 2) la guerra y la paz; 3) la defensa del territorio; 4) las importaciones y exportaciones y 5) la legislación.[4]

---

[2] Manuel Quijano Torres, "El Estado supranacional y la administración pública", *Revista Buen Gobierno*, núm. 23, México, Fundación Mexicana de Estudios Políticos y Administrativos A.C., julio-diciembre, 2017, p. 85.

[3] Manuel Quijano Torres, "El concepto y su contexto", clase presentada en el curso *Seguridad Nacional*, México, FCPyS-UNAM, 15 de agosto de 2017.

[4] Aristóteles, *Retórica*, Madrid, Editorial Gredos, 2015, pp. 60-63.

Los cinco objetos de deliberación se traducen en asuntos de Estado ya que son condiciones necesarias para salvaguardar el territorio, la población y la forma de gobierno. La adquisición de recursos junto con las importaciones y exportaciones contribuyen al bienestar de la población; la guerra y la paz junto con la defensa del territorio conllevan a la protección de las fronteras; la legislación asegura la forma de gobierno establecida.

Nicolás Maquiavelo a diferencia de Aristóteles establece en el *Capítulo XII* de *El príncipe* como fundamentos de todos los Estados, tanto nuevos como antiguos o mixtos, sólo dos aspectos: las buenas leyes y las buenas armas.[5] Las primeras tienen que ser apropiadas para la forma de organización política adoptada mientras que las segundas tienen que ser propias y no auxiliares, mercenarias o mixtas para que actúen bajo el mando del gobernante.

De acuerdo con Maquiavelo las leyes y las armas son "razones de Estado" ya que garantizan la supervivencia de los elementos básicos del Estado. Por una parte las leyes contribuyen al resguardo de la forma de gobierno monárquica o republicana por lo que tiene que examinarse la organización política establecida; por otra parte las armas permiten la defensa del territorio, en ambos casos el gobernante requiere de la virtud y/o la fortuna.[6]

En general los asuntos de Estado procuran la continuidad de la organización política, jurídica y administrativa por medio de los intereses nacionales: la defensa nacional, la protección nacional, la estabilidad nacional, el desarrollo nacional, la reforma del Estado y la administración del proyecto de nación.[7] A su vez se clasifican con base en el nivel de relevancia para el Estado en intereses vitales, intereses críticos e intereses serios:

[5] Nicolás Maquiavelo, *El príncipe/Discursos sobre la primera década de Tito Livio (Selección)*, Madrid, Editorial Gredos, 2014, p. 40.
[6] *Ibid.*, pp. 3-89.
[7] Mario Santos Caamal, *La globalización de la seguridad nacional*, México, CESNAV-SEMAR, 2002, p. 217.

Intereses vitales. Aquellos que garantizan la supervivencia de un Estado-nación, está en juego el territorio, población o independencia nacional.

Intereses críticos. Aquellos en donde no está en juego la supervivencia del Estado, no afectan intereses vitales de momento, pero de alguna manera a largo plazo podrían presentar un problema para la supervivencia del Estado.

Intereses serios. Aquellos que no afectan los intereses de primer o segundo orden, pero los esfuerzos nacionales deben encaminarse a garantizar el bienestar común.[8]

En términos político-administrativos los intereses nacionales se sostienen con la ayuda de cuatro pilares institucionales que garantizan la Seguridad Nacional: política interior, política exterior, política económica y política social.[9] La Seguridad Nacional es una responsabilidad del Estado que deriva en tres competencias clave: seguridad externa, seguridad interna e inteligencia en sus vertientes estratégica, táctica y operativa.[10]

En ese sentido la seguridad de la nación es una condición que conlleva a la seguridad del individuo, la familia, la sociedad, el Estado y las instituciones públicas, privadas y sociales mediante la definición de la agenda de riesgos y amenazas.[11] En el *Libro Quinto* de la *Política* Aristóteles expone las causas que ponen en peligro al Estado en general y en particular a cada uno de los regímenes políticos, así como los medios de conservación.

De manera general señala que la desigualdad numérica y proporcional entre las distintas partes y clases sociales de una nación es la causa principal que genera inestabilidad política, social y económica en los Estados. La desigualdad tiene lugar en el Estado cuando se imponen los intereses de uno de los sectores de la sociedad por encima de los intereses nacionales ya que se deja de lado la procuración del bienestar común.[12]

---

[8] Leonardo Curzio Gutiérrez, “Seguridad interna y externa”, ponencia presentada en el diplomado *Seguridad nacional: escenarios estratégicos de fin de siglo*, INAP, 8 de julio de 1988.
[9] Manuel Quijano Torres, *op. cit.*, pp. 91-95.
[10] Mario Santos Caamal, *op. cit.*, p. 221.
[11] Manuel Quijano Torres, *op. cit.*, p. 92.
[12] Aristóteles, *Política*, Madrid, Editorial Gredos, 2014, pp. 195-199.

De manera particular menciona que cada forma de gobierno: Monarquía, Aristocracia, República, Democracia, Oligarquía y Tiranía está expuesta a sufrir cambios en la organización del Estado como consecuencia de circunstancias internas y externas que dan paso a las revoluciones. Las revoluciones son conflictos entre los diversos sectores de la sociedad que pueden derivar en un régimen donde prevalece el interés común o el interés sectorial.[13]

Para Aristóteles la Constitución Política es el único medio de conservación del Estado ya que determina la organización política, jurídica y administrativa, así como los principios políticos que rigen la relación entre gobernantes y gobernados. De igual manera para Maquiavelo la Constitución es el medio de preservación ya que establece las condiciones necesarias para mantener la integridad, estabilidad y permanencia del Estado.

La dualidad maquiavélica aplicada en los asuntos de Estado (leyes-armas), así como en las formas de gobierno (monarquía-república) también se utiliza para designar la organización del Estado entre los notables y el pueblo. Los primeros son los pocos poseedores de bienes internos y externos mientras que los segundos son los muchos desposeídos de bien alguno por lo que el gobernante se instaura como mediador entre ambas partes.[14]

En el *Libro Tercero* de los *Discursos sobre la primera década de Tito Livio* Maquiavelo menciona sobre las razones de Estado que “cuando hay que resolver acerca de su salvación, no cabe detenerse por consideraciones de justicia o de injusticia, de humanidad o de crueldad, de gloria o de ignominia”.[15] De tal manera que la Seguridad Nacional está vinculada con la “razón de Estado” ya que ambas tienen como finalidad la seguridad y defensa del Estado-nación.[16]

---

[13] Patricio Marcos Giacoman, *Diccionario de la democracia: Diccionario clásico y literario de la democracia antigua y moderna. Vol. II*, México, Editorial Palibrio, 2012, p. 637.
[14] Nicolás Maquiavelo, *op. cit.*, 2014, pp. 32-34.
[15] *Ibid.*, 2014, p. 351.
[16] Emilio Vizarretea Rosales, *Poder y seguridad nacional*, México, SEMAR-CESNAV/Senado de la República, 2013, pp. 187-248.

A pesar de las diferencias entre Aristóteles y Maquiavelo ambos coinciden en la constitución política como el factor fundamental para la seguridad del Estado. La constitución es el eje rector de cualquier nación motivo por el que también se denomina proyecto nacional ya que determina la conducción política de los asuntos públicos hacia el interior y hacia el exterior, así como la relación entre las distintas partes y clases sociales.

Con base en las categorías aristotélicas y maquiavélicas se deduce que a partir del conocimiento de los principios histórico-políticos de la Constitución se identifican los medios de conservación y las causas de corrupción del Estado como organización política que antepone los intereses generales por encima de los particulares. Por ese motivo la Seguridad Nacional se convierte en un asunto primordialmente político cuyo principio y fin es la seguridad del Estado.

El Estado como organización política, jurídica y administrativa es la entidad que asume la responsabilidad de procurar la seguridad de la nación por medio de políticas de Estado y de gobierno en los que intervienen los sectores público, privado y social. Las acciones para garantizar la seguridad nacional se comprenden como “razones de Estado” y se realizan con base en cuatro apartados institucionales: interior, exterior, económico y social.

Si bien las definiciones conceptuales tienden a evolucionar con el transcurso del tiempo es importante reflexionar sobre su naturaleza ya que de ella depende que sean llevadas de la teoría a la práctica. Aun cuando existe una amplia brecha temporal con el momento actual las propuestas teórico-conceptuales permanecen vigentes toda vez que permiten comprender cuestiones políticas trascendentales como la Seguridad Nacional.

En resumen, el origen y causa de la Seguridad Nacional se encuentra en la seguridad y defensa del Estado como condición y organización política. Si bien dicho término es de reciente adopción gubernamental y académica se puede afirmar que desde las pequeñas ciudades-Estado de la antigüedad hasta los enormes Estados-nacionales de la actualidad han llevado a cabo medidas para garantizar la seguridad interior y exterior.

1.1.1 La Seguridad Nacional en México

La Seguridad Nacional en México surge con la consolidación del Estado mexicano a principios del siglo XX al establecer la Constitución Política de los Estados Unidos Mexicanos de 1917 como proyecto nacional. Desde la consumación del proceso de independencia en 1821 el país pasó por un periodo de inestabilidad ante la ausencia de un proyecto que permitiera organizar política, jurídica y administrativamente los sectores de la sociedad mexicana.

La Constitución Política de 1917 es la ley fundamental que determina la organización política: Ejecutivo, Legislativo y Judicial; jurídica: Leyes y Normas; administrativa: Federal, Estatal y Municipal del Estado, así como la relación entre los sectores público, privado y social. Se divide en una parte dogmática del artículo 1º al 38 donde residen los derechos fundamentales y en otra orgánica del artículo 39 al 136 en la que radica la organización del Estado mexicano.

Para Roger Bartra la seguridad nacional en México es protegida por los ideales del "nacionalismo revolucionario" expresados en los 136 artículos de la Carta Magna de 1917.[17] Para José Luis Piñeyro los artículos constitucionales que procuran la seguridad son: 3º de la educación, 27 de la seguridad pública, 31 de las obligaciones de los mexicanos, 89 de las facultades y obligaciones del presidente, 90 de la administración pública federal y 123 del trabajo.[18]

Lo cierto es que la administración pública de la Constitución por parte del sector público como mediador entre los sectores privado y social generó una fase de estabilidad política, social y económica desde 1917. No obstante, a partir de esa fecha se han presentado diversas problemáticas del contexto interno y externo que han puesto en peligro la seguridad nacional mexicana.

---

[17] Marco Antonio López Valdez, *La seguridad nacional en México: interferencias y vulnerabilidades*, México, Editorial Porrúa/Universidad Anáhuac-México-Norte, 2006, pp. 1-2.

[18] Roger Bartra, "Nacionalismo revolucionario y seguridad nacional", *En busca de la seguridad perdida: aproximaciones a la seguridad nacional mexicana*, México, Siglo XXI Editores, 2009, pp. 146-171.

Por ese motivo cuando se hace referencia a la Seguridad Nacional en México cabe preguntarse *¿qué es lo que se debe proteger y defender? ¿para qué? ¿cómo? ¿con qué?*.[19] Las respuestas a tales preguntas serán necesarias para determinar igualmente *¿de qué se debe proteger y defender?* ya que no sólo es relevante tomar en consideración los fines y los medios, también se requiere identificar los factores que impiden la realización del objetivo.

¿Qué proteger y defender? El Artículo 3 de la *Ley de Seguridad Nacional* de 2005 y el Artículo 3 del *Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional* de 2006 estipulan que los intereses permanentes de la Seguridad Nacional de México son las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado mexicano:

I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;
II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;
III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;
IV. El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y
VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.[20] [21]

[19] Marco Antonio Bandala López, "La política de seguridad y defensa del Estado mexicano: componentes más importantes", *La seguridad nacional integral de México: diagnósticos y propuestas*, México, SEMAR-CESNAV/SEDENA-UDEFA, 2013, pp. 299-303
[20] Cámara de Diputados, *Ley de Seguridad Nacional*, [en línea], 25 pp., México, 20 de mayo de 2021, Dirección URL: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac_200521.pdf, [consulta: 30 de junio de 2021].
[21] Diario Oficial de la Federación, *Reglamento para la coordinación de acciones ejecutivas en materia de Seguridad Nacional*, [en línea], México, 29 de noviembre de 2006, Dirección URL: http://dof.gob.mx/nota_detalle.php?codigo=4938925&fecha=29/11/2006, [consulta: 30 de junio de 2021].

¿Para qué? Para asegurar la continuidad de los ideales del proyecto nacional contenidos en los 136 artículos constitucionales de la Carta Magna de 1917. Con base en las categorías políticas de Aristóteles y Maquiavelo se comprende que la naturaleza de la seguridad nacional mexicana se encuentra en el resguardo de la República como forma de gobierno y sus principios histórico-políticos establecidos en el Título Segundo Capítulo I de la Constitución:

> **Artículo 39.** La soberanía nacional reside esencial y originariamente en el pueblo. Todo poder público dimana del pueblo y se instituye para beneficio de éste. El pueblo tiene en todo tiempo el inalienable derecho de alterar o modificar la forma de su gobierno.
>
> **Artículo 40.** Es voluntad del pueblo mexicano constituirse en una república representativa, democrática, laica y federal, compuesta por Estados libres y soberanos en todo lo concerniente a su régimen interior, y por la Ciudad de México, unidos en una federación establecida según los principios de esta ley fundamental.
>
> **Artículo 41.** El pueblo ejerce su soberanía por medio de los Poderes de la Unión, en los casos de la competencia de éstos, y por los de los Estados y la Ciudad de México, en lo que toca a sus regímenes interiores, en los términos respectivamente establecidos por la presente Constitución Federal y las particulares de cada Estado y de la Ciudad de México, las que en ningún caso podrán contravenir las estipulaciones del Pacto Federal.[22]

¿Cómo? Promoviendo las condiciones necesarias para asegurar los fines y los medios del Estado por medio de planes de Estado y de gobierno dirigidos por el sector público y apoyados por los sectores privado y social. Los primeros están vinculados con el bien común para el individuo, la familia y la sociedad mientras que los segundos están relacionados con la supervivencia de los elementos básicos del Estado: Territorio, Población y Gobierno.[23]

---

[22] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*, [en línea], 354 pp., México, 28 de mayo de 2021, Dirección URL: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf, [consulta: 30 de junio de 2021].
[23] Mario Santos Caamal, *op. cit.*, p. 221.

¿Con qué? Con acciones políticas, jurídicas y administrativas apoyadas por las instituciones públicas, privadas y sociales del Estado encargadas de atender los apartados interno, externo, económico y social mejor conocidas como "razones de Estado" ya que sostienen los intereses nacionales. Considerando las respuestas a cada una de las preguntas se da por sentado que la Seguridad Nacional en México es un asunto político que se define como:

> La condición en la que la mayoría de las partes y clases sociales de la nación tiene garantizados por el gobierno los mínimos de bienestar mediante decisiones de Estado, es decir, la Seguridad Nacional se refiere a las acciones de conjunto de los sectores público, privado y social. Es una situación de seguridad frente a riesgos y amenazas internas o externas, reales o potenciales que atentan contra la reproducción del individuo, la familia, la sociedad, la nación y sus instituciones.[24]

Para los fines del presente trabajo de investigación la Seguridad Nacional se comprende con base en la teoría política, la legislación nacional y la ley en la materia como la condición que permite salvaguardar los principios histórico-políticos de la nación establecidos en la Constitución Política. La seguridad nacional se genera cuando los sectores público, privado y social actúan en conjunto con la intención de favorecer los intereses nacionales.

¿De qué proteger y defender? La Ley de Seguridad Nacional y el Reglamento clasifican los antagonismos para la seguridad nacional mexicana en Riesgos y Amenazas. De ambos documentos se desprenden el *Programa para la Seguridad Nacional* y la *Agenda Nacional de Riesgos* cuyo propósito es definir los desafíos para la integridad, estabilidad y permanencia del Estado mexicano.

En términos político-administrativos tanto el *Programa para la Seguridad Nacional* como la *Agenda Nacional de Riesgos* han formado parte de la política de seguridad nacional del Estado mexicano. Hasta el momento sólo se han realizado dos versiones del programa mientras que la agenda se actualiza anualmente con la diferencia de que su contenido es de carácter confidencial.

[24] Manuel Quijano Torres, *op. cit*.

Por una parte, el *Programa para la Seguridad Nacional 2009-2012* establece un objetivo general del que derivan dos objetivos específicos y trece líneas estratégicas:

Objetivo general. Mantener la integridad, la estabilidad y la permanencia del Estado Mexicano, a través de la anulación de las amenazas y la desactivación de riesgos que puedan impactar dichos atributos.

Objetivo específico 1. Fortalecer estructuralmente al Sistema de Seguridad Nacional.

Líneas estratégicas:

- Impulsar el incremento de las capacidades de las instancias de Seguridad Nacional;
- Establecer un sistema integral de información para la preservación de la Seguridad Nacional;
- Desplegar un trabajo integral y sistemático de inteligencia y alerta temprana;
- Promover el desarrollo del marco jurídico para la Seguridad Nacional en respuesta a desafíos y necesidades, e
- Impulsar la cooperación internacional en materia de Seguridad Nacional, regional, hemisférica e internacional.

Objetivo específico 2. Atender integralmente las amenazas que ponen en peligro la Seguridad Nacional, así como aquellos riesgos definidos como prioritarios que pudieran llegar a vulnerarla.

Líneas estratégicas:

- Profundizar el conocimiento en torno a amenazas y riesgos específicos vía la generación de inteligencia;
- Incidir, a través de políticas públicas, sobre factores que desempeñan un papel crítico en la génesis de amenazas y de riesgos;
- Acotar vulnerabilidades existentes frente a amenazas y riesgos;
- Anticipar y limitar amenazas y riesgos por la vía de la contrainteligencia;
- Desalentar la planeación o realización de actos que constituyan una amenaza o un riesgo emprendiendo acciones de corte disuasivo;
- Blindar contra amenazas y riesgos a través de la instrumentación de acciones de protección;

- Reaccionar con pertinencia y oportunidad para hacer frente a amenazas y riesgos que han perdido su carácter potencial al concretarse en los hechos,
- Limitar el daño actuando para mitigar impactos adversos derivados de amenazas y riesgos o, en su caso, controlar efectos.[25]

Por otra, el *Programa para la Seguridad Nacional 2014-2018* establece dos grandes objetivos estratégicos de los que derivan seis objetivos específicos y veinte líneas estratégicas:

> **Objetivo estratégico 1.** 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.
>
> **Objetivo específico 1.1.** Desarrollar e implementar los fundamentos normativos y operativos que dan sustento al funcionamiento del Sistema de Seguridad Nacional para permitir una atención integral de los temas que forman parte de su agenda con una perspectiva multidimensional.
>
> **Líneas estratégicas:**

- Consolidar el marco jurídico del Sistema de Seguridad Nacional para fortalecer las capacidades de las instituciones y autoridades del Estado mexicano.
- Desarrollar los sistemas y programas que sustentan el funcionamiento del Sistema de Seguridad Nacional.
- Diseñar e implementar un modelo de profesionalización y certificación en materia de Seguridad Nacional.

> **Objetivo específico 1.2.** Articular la información y las inteligencias especializadas del Estado mexicano mediante el establecimiento y operación del Sistema Nacional de Inteligencia, a fin de potenciar la generación de inteligencia estratégica para la Seguridad Nacional.
>
> **Líneas estratégicas:**

[25] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2009-2012*, [en línea], México, 20 de agosto de 2009, Dirección URL: https://dof.gob.mx/nota_detalle.php?codigo=5106082&fecha=20/08/2009, [consulta: 30 de junio de 2021].

- Establecer el Sistema Nacional de Inteligencia por medio del desarrollo de mecanismos que permitan su integración y operación como parte del Sistema de Seguridad Nacional.
- Desarrollar una Doctrina Nacional de Inteligencia para la Seguridad Nacional que unifique los criterios y las fases del ciclo de inteligencia en los órganos de inteligencia civiles y militares del Estado mexicano.

Objetivo específico 1.3. Desarrollar y divulgar la Cultura de Seguridad Nacional del Estado mexicano, para contribuir al conocimiento colectivo sobre el tema.

Líneas estratégicas:

- Diseñar esquemas para desarrollar y divulgar la cultura de Seguridad Nacional entre autoridades coadyuvantes del Sistema de Seguridad Nacional y la sociedad civil.

Objetivo estratégico 2. Asegurar que la política de Seguridad del Estado mexicano adopte una perspectiva multidimensional mediante la coordinación de las autoridades e instituciones competentes, para favorecer así la consecución de los objetivos e intereses nacionales.

Objetivo específico 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.

Líneas estratégicas:

- Actualizar bajo una perspectiva multidimensional los temas que serán considerados en la Agenda Nacional de Riesgos y en los esquemas de coordinación de acciones para su atención integral.
- Desarrollar una política de Estado en materia de seguridad cibernética y ciberdefensa, para proteger y promover los intereses y objetivos nacionales.

Objetivo específico 2.2. Fortalecer la capacidad de respuesta de las Fuerzas Federales para contribuir tanto al mantenimiento de la Seguridad Interior como a las tareas de Defensa Exterior de la Federación.

Líneas estratégicas:

- Impulsar las reformas legales necesarias para dar sustento a la actuación de las Fuerzas Armadas en actividades de Seguridad Interior.
- Fortalecer la arquitectura institucional y la capacidad de respuesta de las Fuerzas Federales en materia de seguridad y defensa.
- Consolidar los esquemas de coordinación entre las autoridades federales y locales en materia de Seguridad Interior.
- Fortalecer las capacidades militares y navales de la nación a través de la adopción de equipamiento adecuado y tecnología actualizada.
- Fomentar la preparación del personal militar y naval, así como la mejora continua del sistema de formación y educación de las Fuerzas Armadas.
- Desarrollar y probar mecanismos de continuidad de operaciones de las instalaciones estratégicas nacionales, a fin de elevar su nivel de resiliencia y la provisión de bienes y servicios públicos esenciales para la población.

Objetivo específico 2.3. Contribuir al mantenimiento de un entorno internacional estable que favorezca los intereses y objetivos nacionales del Estado mexicano.

Líneas estratégicas:

- Fortalecer el desarrollo fronterizo y regional como elemento de la política de Seguridad Nacional del Estado mexicano.
- Gestionar la agenda migratoria desde una perspectiva integral que incluya acuerdos con países expulsores de migrantes.
- Promover acciones de cooperación en materia de seguridad internacional con un enfoque multidimensional.
- Impulsar acciones encaminadas al cumplimiento de instrumentos internacionales en materia de no proliferación y desarme.
- Impulsar iniciativas en foros multilaterales para contribuir a la Seguridad Nacional e internacional desde una perspectiva multidimensional.
- Fortalecer las capacidades del Estado en las fronteras y puertos a efecto de ordenar flujos comerciales y migratorios.[26]

[26] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2014-2018*, [en línea], México, 30 de abril de 2014, Dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014, [consulta: 30 de junio de 2021].

1.1.1.1 Riesgos

En materia de Riesgos para la Seguridad Nacional el *Programa para la Seguridad Nacional 2009-2012* determina lo siguiente:

> Para efectos del presente Programa, riesgo a la Seguridad Nacional es aquel antagonismo a la Seguridad Nacional que no teniendo el carácter de amenaza conforme a la Ley, implica 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, cuya presencia pudiera poner en entredicho el desarrollo nacional.
>
> Los riesgos a la Seguridad Nacional se contrarrestan mediante la aplicación de políticas públicas, establecidas en el Plan Nacional de Desarrollo, evitando que den lugar a la conformación de amenazas a la Seguridad Nacional, mismas que obligarían a emplear recursos extraordinarios de la fuerza del Estado para su atención.[27]

El artículo 26 párrafo IV constitucional menciona que "al desarrollo económico nacional concurrirán, con responsabilidad social, el sector público, el sector social y el sector privado, sin menoscabo de otras formas de actividad económica que contribuyan al desarrollo de la Nación".[28] Por lo cual, se deduce que los Riesgos son condiciones que perjudican a los sectores que constituyen al Estado mexicano ya sea de manera

En la primera versión del Programa los Riesgos para la Seguridad Nacional de México son los siguientes:

Conflictos políticos y sociales. Como se menciona en la teoría política la persistencia de conflictos internos de índole política y social entre las distintas partes y clases sociales de una nación genera inestabilidad que puede derivar en todo tipo de expresiones violentas.

[27] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2009-2012*.
[28] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*.

Pérdida de cohesión social. La falta de unidad entre los sectores público, privado y social es indicativa de la ausencia de medidas destinadas a garantizar el bienestar común por lo que no se están generando las condiciones necesarias para garantizar la seguridad nacional.

Dinámicas migratorias. La frontera norte con Estados Unidos y la frontera sur con Belice y Guatemala convierten al país en el lugar propicio para el flujo de mercancías y para el tránsito de personas de diversa procedencia cuyas intenciones pudieran poner en entredicho a alguno de los sectores.

Pandemias y epidemias. Las pandemias de gripe A(H1N1) de 2009-2010 y la de COVID-19 de 2019 han demostrado la capacidad de impacto de los virus en las actividades de todos los sectores al grado de paralizar cualquier interacción a nivel nacional e internacional.

Medio ambiente y calentamiento global. Los desastres naturales, como consecuencia del cambio climático, no sólo provocan pérdidas materiales y humanas también ponen en entredicho el desarrollo nacional al afectar los recursos naturales necesarios para procurar los mínimos de bienestar.

Desequilibrios en el desarrollo nacional. La administración pública del proyecto nacional requiere de la participación de los sectores público, privado y social por lo que la exclusión de alguno conllevaría a la desigualdad entre las partes y clases sociales de la nación.

En materia de Riesgos para la Seguridad Nacional el *Programa para la Seguridad Nacional 2014-2018* determina lo siguiente:

> Probabilidad de que en un lapso determinado se produzcan daños a los intereses nacionales debido a la interacción de fenómenos políticos, económicos y sociales con la intervención de agentes no estales o desastres de origen natural o antropogénico. Se trata de una condición que pone a prueba la capacidad de respuesta de la nación y que puede ser potenciada por sus vulnerabilidades.[29]

[29] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2014-2018*.

En ese sentido los Riesgos son condiciones que perjudican los intereses nacionales que son “elementos constitutivos del Estado mexicano (conformados por la población, la soberanía y el territorio nacionales, así como por el orden constitucional, el gobierno y la democracia) que resultan indispensables para su consolidación y viabilidad”.[30] De tal manera que ponen en peligro los elementos básicos del Estado: Territorio, Población y Gobierno.

En la segunda versión del Programa los Riesgos para la Seguridad Nacional de México son los siguientes:

Desastres naturales y pandemias. Como se mencionó con anterioridad los desastres naturales son eventos relacionados con el medio ambiente que afectan un territorio y una población determina mientras que las pandemias ponen en peligro la población de una o varios países.

Fronteras, mares y flujos migratorios irregulares. Las fronteras terrestres, marítimas y aéreas son espacios vulnerables del territorio nacional por excelencia debido a la complejidad que representa el establecimiento de puntos de control de acceso en los límites territoriales.

Por lo tanto, a partir de las definiciones propuestas en ambos programas y tomando en consideración las clasificaciones ya mencionadas se concluye lo siguiente con respecto a los riesgos para la seguridad nacional mexicana:

- Son condiciones internas o externas.
- Son generados por situaciones y/o fenómenos políticos, económicos y sociales.
- Son influenciados por agentes no estatales y por desastres de tipo natural o antropogénico.
- Afectan primordialmente a los sectores público, privado y social encargados de procurar el desarrollo nacional.

[30] *Ídem*.

1.1.1.2 Amenazas

Con base en el Artículo 5 de la *Ley de Seguridad Nacional* las *Amenazas* para la Nación mexicana son:

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 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;
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos; y
XIII. Actos ilícitos en contra el fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales.[31]

En cuestión de *Amenazas* para la Seguridad Nacional el *Programa para la Seguridad Nacional 2009-2012* establece lo siguiente:

[31] Cámara de Diputados, *Ley de Seguridad Nacional*.

> Para efectos del presente Programa, amenaza a la Seguridad Nacional es un fenómeno intencional generado por el poder de otro estado, o por agentes no estatales contemplados en el artículo 5 de la Ley, cuya característica es una voluntad hostil y deliberada que pone en peligro de vulneración particularmente grave a los intereses permanentes tutelados por la Seguridad Nacional, en parte o en todo el país, y cuestionan la existencia del mismo Estado. Es por ello que el fin último es prevenir, disuadir o enfrentar las amenazas que ponen en peligro al Estado Mexicano.[32]

En la primera versión del Programa las Amenazas para la Seguridad Nacional de México son las siguientes:

Delincuencia organizada. El Artículo 2º de la *Ley Federal contra la Delincuencia Organizada* la define como:

> Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada:

I. Terrorismo
II. Acopio y tráfico de armas
III. Tráfico de personas
IV. Tráfico de órganos
V. Corrupción de personas menores de dieciocho años
VI. Delitos en materia de trata de personas
VII. Delitos en materia de secuestro
VIII. Contrabando y su equiparable
IX. Delitos en materia de hidrocarburos
X. Delitos contra el ambiente[33]

[32] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2009-2012*.
[33] Cámara de Diputados, *Ley Federal contra la Delincuencia Organizada*, [en línea], 41 pp., México, 20 de mayo de 2021, Dirección URL: http://www.diputados.gob.mx/LeyesBiblio/pdf/101_200521.pdf, [consulta: 30 de junio de 2021].

Narcotráfico. El narcotráfico en México ha representado una amenaza para la seguridad nacional debido a la injerencia de los cárteles de la droga en distintas instituciones encargadas de la procuración y administración de justicia en cada uno de los órdenes de gobierno.

Grupos armados. El surgimiento de grupos guerrilleros en el transcurso del siglo XX y de grupos de autodefensas a principios del siglo XXI han sido muestra de la existencia de movimientos armados resultantes de la persistencia de conflictos políticos y sociales internos.

Terrorismo. El Artículo 139 del *Código Penal Federal* lo define como:

> A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos, o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, intencionalmente realice actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.
>
> Al que acuerde o prepare un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional.[34]

Vulnerabilidades en fronteras. La gran extensión territorial, las condiciones geográficas desfavorables, la vecindad con Estados Unidos, Belice y Guatemala, así como la ausencia de puntos de control en los límites territoriales convierten a las fronteras en los lugares ideales para las amenazas antes mencionadas.

En cuestión de *Amenazas* para la Seguridad Nacional el *Programa para la Seguridad Nacional 2014-2018* establece lo siguiente:

---

[34] Cámara de Diputados, *Código Penal Federal*, [en línea], México, 332 pp., 01 de junio de 2021, Dirección URL: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_010621.pdf, [consulta: 30 de junio de 2021].

> Acto generado por el poder de otro Estado, o por actores no estatales, que puede vulnerar de modo particularmente grave las aspiraciones, intereses y objetivos nacionales del Estado mexicano. Las amenazas pueden ser tradicionales o emergentes.[35]

En la segunda versión del Programa las Amenazas para la Seguridad Nacional de México son las siguientes:

Delincuencia Organizada Trasnacional. Las organizaciones del crimen y la delincuencia de origen nacional y extranjero han adquirido una mayor capacidad de expansión como resultado de la globalización.

Ciberseguridad. Las Tecnologías de la Información y la Comunicación (TIC) han significado un gran avance para la Nación mexicana y también han supuesto un desafío ya que han dado paso a la aparición de riesgos y amenazas.

Terrorismo y armas de destrucción masiva. Si bien la nación mexicana no enfrenta alguno de los dos problemas de manera directa puede ser utilizada como plataforma de tránsito o asilo de entidades terroristas.

Por lo tanto, a partir de las definiciones propuestas en ambos programas, así como del catálogo establecido en la ley sobre las características que poseen las amenazas a la seguridad nacional mexicana podrían sacarse las siguientes consideraciones al respecto:

- Son actos generados por otro Estado o por entidades no estatales las cuales pueden actuar colectiva o individualmente.
- Se pueden dividir en tradicionales y emergentes; las primeras son las que han prevalecido sin importar las circunstancias del entorno y las segundas son las que han surgido de situaciones específicas.
- Afectan total o parcialmente a las aspiraciones, objetivos e intereses nacionales.

[35] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2014-2018*.

1.2 Sobre el concepto de Ciberseguridad

El concepto de *Ciberseguridad* ha tenido diversas interpretaciones en la teoría y en la práctica debido al vínculo que tiene con las Tecnologías de la Información y la Comunicación (TIC). No obstante, se afirma que la Ciberseguridad como dimensión tecnológica de la Seguridad Nacional se convierte en un asunto político.

Por consiguiente, la seguridad cibernética ha sido entendida prioritariamente como parte del campo de estudio de la técnica. Sin embargo, para lograr una aproximación concisa del término será necesario tomar en consideración ambas perspectivas tanto la técnica como la política.

Para empezar, acorde con Arturo García Hernández, el estudio de la ciberseguridad requiere de aproximaciones interdisciplinarias, sobre todo destaca su importancia como asunto de Seguridad Informática y de Seguridad Nacional.[36] En consecuencia, será necesario analizar la primera bajo la óptica tecnológica y la segunda desde la política.

Por una parte, la seguridad informática atañe a los componentes tangibles (*hardware*) e intangibles (*software*) que conforman a las llamadas Tecnologías de la Información y Comunicación (TIC). Por otra, la seguridad nacional comprende las decisiones que deberán ser tomadas con respecto al uso de las TIC para beneficio del Estado, así como las acciones perjudiciales que puedan derivar de ellas.[37]

Desde el punto de vista técnico, las TIC "permiten el manejo electrónico de la información en una variedad de formas y que facilitan distintas formas de comunicación".[38] Ellas están constituidas por dos soportes: el físico y el lógico; en el primero se encuentran las tecnologías de captura, las de almacenamiento, las de procesamiento y las de comunicación de toda clase de información.

---

[36] Arturo García Hernández, *CiberMéxico: voluntades y acciones en el ciberespacio*, Ius Literatus, México, 2018, pp. 36-38.
[37] *Ídem*.
[38] Cees J. Hamelink, *La ética del ciberespacio*, Siglo XXI Editores, México, 2015, p. 24.

En el segundo se incluyen los sistemas operativos, las aplicaciones y los programas, los cuales se catalogan con base en su intencionalidad. Si su objetivo es permitir el buen funcionamiento del *hardware*, es decir, de cualquier dispositivo digital se les denomina simplemente *software*; si está diseñado para afectar parcial o totalmente los soportes físico y/o lógico, entonces se les asigna el nombre de software malicioso o *malware*.[39]

La suma de ambos soportes, junto con la conectividad de la internet, han constituido un "espacio virtual", es decir, intangible. A esa nueva dimensión se le ha dado el nombre de *Ciberespacio* como referencia del lugar al que sólo es posible acceder con el apoyo de la infraestructura tecnológica capaz de conectarse a la red de redes, entre las cuales se encuentran las siguientes:

1. Computadoras digitales (desde laptops hasta sistemas expertos);
2. Redes que conectan teléfonos y faxes mediante sistemas electrónicos digitales;
3. Sistemas de transporte operados en forma digital (como automóviles, trenes, aviones y elevadores);
4. Sistemas de control operados digitalmente, como aquellos que son usados en procesos químicos, cuidado de la salud o para proveer energía;
5. Aparatos operados en forma digital, como relojes, hornos de microondas y videograbadoras;
6. Robots operados en forma digital que corren, en forma independiente, sistemas automáticos.[40]

En el mundo digital, a diferencia del mundo real, el tiempo y el espacio no están determinados, motivo por el cual se vuelve casi imposible indicar el momento y el lugar precisos en el que se realiza una acción. Así mismo, para interactuar en él es necesario el uso de dispositivos electrónicos capaces de compartir el mismo lenguaje de tipo digital basado en el código binario (0 y 1).

[39] Eduardo Suárez Vázquez, "Software malicioso (Malware). Historia y evolución", *Revista del Centro de Estudios Superiores Navales*, núm. 2, vol. 28, México, SEMAR-CESNAV, abril-junio, 2007, pp. 48-56.
[40] Cees J. Hamelink, *op. cit.*, pp. 22-23.

Es así como la ciberseguridad, desde el enfoque de la seguridad informática, radica en "el conjunto de procesos destinados a proteger la disponibilidad, la privacidad y la integridad de los datos [e información], sea de personas o instituciones".[41] En ese caso, las medidas deben estar encaminadas a garantizar el aseguramiento de los sistemas de información y las redes de telecomunicaciones.

Desde la perspectiva política, las Tecnologías de la Información y Comunicación, así como sus elementos físicos y virtuales han contribuido "tanto en beneficio de la paz como para hacer la guerra".[42] De acuerdo con la intencionalidad, el uso y aprovechamiento de las nuevas tecnologías ha permitido beneficiar o perjudicar la seguridad del Estado afectando a la integridad territorial y/o a la estabilidad política.

En primer lugar, el espacio cibernético se ha transformado en el sitio de interacción entre individuos, sociedades y naciones. En él han pasado a realizarse gran parte de las actividades políticas, económicas y sociales, "desde actividades cotidianas hasta operaciones especializadas".[43] Por lo cual, se ha convertido en la nueva quinta dimensión junto con los espacios estratégicos terrestre, marítimo, aéreo y radioeléctrico.[44]

En ese sentido, lo *ciber* se presenta como parte integrante de los límites territoriales de cualquier nación desde el cual puede ser vulnerado por alguna otra entidad. No obstante, debido a las características técnicas antes mencionadas, resulta inviable establecer en ese sitio divisiones políticas que determinen el margen de acción tanto de actores estatales como no estatales transformándola en la frontera más insegura de todas las anteriores.

---

[41] Hugo D. Scolnik, *Qué es la seguridad informática*, México, Ediciones Culturales Paidós, 2016, p. 19.
[42] María Cristina Rosas, "Ciberespacio, crimen organizado y seguridad nacional", *Revista del Centro de Estudios Superiores Navales*, núm. 3, vol. 32, México, SEMAR-CESNAV, julio-septiembre, 2011, p. 5.
[43] Mario Gómez Sánchez, "Prólogo", *CiberMéxico: voluntades y acciones en el ciberespacio*, México, Ius Literatus, 2018, p. 15.
[44] Emilio Vizarretea Rosales, *op. cit.*, p. 56.

En segundo lugar, las tecnologías digitales han incidido principalmente en los modos de producción de las naciones favoreciendo el crecimiento y el desarrollo. Autores como Alvin Toffler han denominado al momento actual *tercera ola*[45], como referencia de la importancia que han tenido la innovación y el desarrollo tecnológicos, en secuencia con la *segunda ola*, basada en la industria, y en la *primera ola*, sostenida en la agricultura.

En la denominada tercera ola, la principal materia prima de los servicios digitales ha sido la información[46]. Ésta puede ser de todo tipo y puede suponer un peligro para la estabilidad del Estado de acuerdo con el grado de criticidad y sensibilidad del contenido. Es así como la información resulta fundamental para la toma de decisiones políticas, las cuales conlleven a la consecución de las aspiraciones, objetivos e intereses nacionales.

Por consiguiente, en el primer caso, la integridad de la frontera digital deberá procurarse a través de los elementos que la soportan: el físico y el lógico. En el segundo, la estabilidad dependerá mayoritariamente del aseguramiento de la información política, económica y social tanto de los ciudadanos como de las instituciones del Estado capturada, almacenada, procesada y comunicada por las tecnologías digitales.

De esa forma la ciberseguridad, desde el enfoque de la seguridad nacional, reside en procurar el resguardo de lo que Norbert Wiener designa "interacción *humano-máquina*",[47] es decir, se deben tomar en consideración tanto los dispositivos tecnológicos como quienes los utilizan pudiendo ser desde los gobernados hasta los gobernantes. Para lograrlo, se deben emplear medidas preventivas y reactivas destinadas sobre todo a procurar al Estado.

[45] Alvin Toffler, *La tercera ola*, Barcelona, Plaza y Janes Editores, 2000, pp. 25-30.
[46] Fundación Telefónica, *Ciberseguridad, la protección de la información en un mundo digital*, Barcelona, Editorial Ariel, 2016, pp. 1-8.
[47] Norbert Wiener, *Cibernética y sociedad*, Buenos Aires, Editorial Sudamericana, 1958, p. 16.

1.2.1 La Ciberseguridad en México

En México, el concepto de *Ciberseguridad* adquiere cada día mayor relevancia como asunto de seguridad nacional. Algunas aproximaciones se han generado desde los ámbitos tecnológico en cuanto a la Seguridad Informática y la Seguridad de la Información y jurídico con respecto a la promulgación de un marco regulatorio.[48]

Uno de los primeros intentos por definir dicho término se realizó en la *Estrategia Nacional de Ciberseguridad* (ENCS) de 2017. Si bien, en el PSN 2014-2018 ya se había abordado el tema en cuestión no fue sino hasta el surgimiento de la Estrategia cuando finalmente se atendió de manera integral al fenómeno cibernético a través de un objetivo general, el cual es:

> Fortalecer 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.[49]

Para lograr el objetivo general se decretaron dentro de la estrategia cinco objetivos estratégicos, los cuales comprenden el conjunto de entornos a resguardar con el apoyo de la tecnología:

Sociedad y derechos. Como parte integrante de los sectores del desarrollo nacional, el sector social comprende el más numeroso de los tres por encima del público y el privado. Como base de la pirámide del desarrollo, resultará vital la protección de sus actividades en el mundo virtual.

---

[48] Edgar Iván Espinosa, "Hacia una estrategia nacional de ciberseguridad en México", *Revista de Administración Pública*, núm. 1, vol. L, México, INAP A.C., enero-abril, 2015, p. 118.

[49] Gobierno de México, *Estrategia Nacional de Ciberseguridad*, [en línea], México, 31 pp., 13 de noviembre de 2017, Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf, [consulta: 30 de junio de 2021].

Economía e innovación. El crecimiento y desarrollo económicos son dos pilares fundamentales de la nación ya que contribuyen a la justa distribución del ingreso y la riqueza. Para ello, son importantes las entidades e instituciones financieras y monetarias cuyas actividades se realizan con ayuda de las TIC.[50]

Instituciones públicas. El sector público es el más importante ya que tiene bajo su cargo las áreas estratégicas de la nación. El óptimo funcionamiento de ellas reside mayoritariamente en el resguardo tanto de la información reservada y confidencial como de los medios que la contienen.

Seguridad pública. La seguridad pública, como antesala de la seguridad nacional, previene la amplificación de ciertas problemáticas, sobre todo las que puedan afectar a la integridad física y moral de las personas, así como su patrimonio en el entorno cibernético.

Seguridad nacional. La identificación de los principales riesgos y amenazas cibernéticas para la seguridad nacional mexicana contribuirá al mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano mediante la aplicación de políticas de Estado y de gobierno en la materia.

De acuerdo con la Estrategia, la ciberseguridad en México se vuelve un asunto de Estado toda vez que incide en cuestiones primordiales como la sociedad, la economía, las instituciones, así como las seguridades pública y nacional. Para lo cual ofrece una definición multidimensional desde la perspectiva gubernamental como:

> Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.[51]

[50] OEA/CNBV, *Estado de la ciberseguridad en el sistema financiero mexicano*, [en línea], 98 pp., Dirección URL: http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf, [consulta: 30 de junio de 2021].
[51] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.

2. EL ESTADO DE LA CIBERSEGURIDAD EN EL SIGLO XXI

2.1 Contexto internacional

De acuerdo con el *Informe Global de Riesgos 2021*, elaborado por el Foro Económico Mundial, los principales problemas tecnológicos a nivel internacional han sido la concentración del poder digital, la desigualdad digital, las fallas de ciberseguridad y los daños en la infraestructura de las TIC. El informe establece dos escalas de medición de diez posiciones cada una para valorarlos en términos de probabilidad e impacto.

El informe posicionó en la escala de probabilidad la concentración del poder digital en la sexta posición, la desigualdad digital en la séptima y las fallas de ciberseguridad en la novena; en cuestión de impacto los daños en la infraestructura de las TIC se ubicaron en el décimo lugar.[52] Cada una de las cuatro incidencias ha representado un riesgo para la seguridad de los sectores público, privado y social que constituyen el Estado.

Desde el enfoque del Derecho Internacional, el uso perjudicial de las TIC se ha catalogado en tres figuras jurídicas: los Ciberataques, el Ciberespionaje y el Ciberterrorismo.[53] El primero se toma en cuenta como el equivalente tecnológico de un ataque armado en el cual se hace uso de la fuerza mientras que el segundo y el tercero son considerados como tipos de ofensas que pueden ser efectuados por agentes de diversa procedencia.[54]

---

[52] Foro Económico Mundial, *Informe Global de Riesgos 2021*, [en línea], 97 pp., 15 de enero de 2020, Dirección URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf, [consulta: 30 de junio de 2021].

[53] Alejandra Morán Espinosa; Abraham Alejandro Servín Caamaño; Oscar Alquicira Gálvez, "TIC (Internet) y ciberterrorismo", *Revista Seguridad. Cultura de prevención para TI*, núm. 23, México, UNAM-DGTIC, marzo-abril, 2015, pp. 25.

[54] *Ibid.*, pp. 26-28.

En ese sentido, los ataques cibernéticos se han colocado como las amenazas más recurrentes para la ciberseguridad de las naciones en el presente milenio. De manera general, se les denomina como "la acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información (ICI), las Infraestructuras de Información Esenciales (IIE), así como la seguridad de las personas".[55]

De manera progresiva, han sido técnicamente más sofisticados, más frecuentes y graves ante el incremento de dispositivos digitales globalmente interconectados. Por ese motivo "pueden ser considerados uso de la fuerza nacional o internacional"[56] en función del contexto de la acción, el actor o actores que intervinieron, el objetivo establecido y la ubicación de origen.

Por otra parte, con base en el informe de riesgos, el robo de datos personales y de información confidencial contenidos en sistemas informáticos ha representado otra de las problemáticas tecnológicas internacionales. Para garantizar las interacciones de la sociedad de la información y el conocimiento se vuelve indispensable asegurar su integridad, disponibilidad y confidencialidad.

En ese panorama ha cobrado relevancia la seguridad de la información tanto a nivel individual como organizacional, ya sea público o privado. Para las personas se procura el derecho a la privacidad pretendiendo mantener a salvo la identidad digital de los usuarios de las TIC mediante la protección de sus datos e información personales de entidades no autorizadas.

Para las organizaciones públicas y privadas se previenen las filtraciones masivas de información confidencial cuyos protagonistas se identifican con el movimiento "hacktivista". El *hacktivismo* (acrónimo de *hacker* y *activismo*) se ha designado como un movimiento político-social motivado por la búsqueda de libertad de expresión en la red, así como de acceso a todo tipo de información.

[55] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.
[56] Alejandra Morán Espinosa; Abraham Alejandro Servín Caamaño; Oscar Alquicira Gálvez, *op. cit.*, pp. 27-28.

Con respecto a la seguridad de la información de los probables robos o fugas han surgido dos posturas contrarias; por un lado, se encuentran los simpatizantes de la libertad en el mundo digital cuya ideología está plasmada en dos documentos: el *Manifiesto Hacker*[57] de 1986 y la *Declaración de Independencia del Ciberespacio*[58] de 1996. En el otro extremo están los partidarios de la intervención gubernamental a través de la regulación global del ciberespacio.

El primer bando está conformado esencialmente por *Hackers*[59] tanto individuales como grupales. La gran mayoría de ellos mantienen ocultas sus identidades debido al anonimato que permite la internet, por lo cual ha resultado complicado diferenciar entre las intenciones de quienes sólo buscan privacidad y quienes realizan actividades delictivas.

El segundo está constituido por integrantes de los sectores público y privado entre los que destacan las instituciones gubernamentales, así como corporaciones empresariales respectivamente.[60] A diferencia de la otra facción, los defensores de la segunda muestran sus identidades reales en calidad del gobierno o la compañía que representan.

Sin embargo, ambas posturas han sido malversadas en algunos de sus puntos que las han desviado de su objetivo primordial. Para comenzar, la libertad del ciberespacio, al convertirse en libertinaje, ha ocasionado el surgimiento de los llamados "cuatro jinetes del info-Apocalipsis": el lavado de dinero, la venta de drogas, el terrorismo y la pornografía infantil,[61] las cuales se han visto fortalecidas por la falta de regulación de la red y han representado la parte "oscura".

---

[57] Galvy Ilvey Cruz Valencia, "Hacktivismo: ¿delito o comunicación ciudadana?", *Revista Seguridad. Cultura de prevención para TI*, núm. 12, México, UNAM-DGTIC, diciembre-enero, 2011-2012, p. 29.
[58] John Perry Barlow, *Declaración de Independencia del Ciberespacio*, [en línea], 08 de febrero de 1996, Dirección URL: https://www.eff.org/cyberspace-independence, [consulta: 30 de junio de 2021].
[59] El termino *Hacker* posee múltiples connotaciones. De manera general, "se designa con este término, a la persona que conoce a fondo el funcionamiento y operación de equipos de cómputo, sin tener necesariamente fines maliciosos".
[60] Cees J. Hamelink, *op. cit.*, pp. 7-8.
[61] Julian Assange, *Cypherpunks: la libertad y el futuro de internet*, México, Editorial Planeta Mexicana, 2013, p. 105.

Por otra parte, cuando los controles gubernamentales y corporativos rebasan los límites entre lo íntimo, lo privado y lo público se genera el dilema entre la seguridad y la libertad. Entendiendo lo primero como "el ámbito de los pensamientos de cada cual",[62] lo segundo como "el ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales"[63] y lo tercero como "la libre accesibilidad de los comportamientos y decisiones de las personas en sociedad".[64]

Por ejemplo, la decisión del gobierno ha pretendido anteponer la seguridad de los sectores público y privado por encima de las libertades individuales del sector social con el incremento de las medidas de vigilancia en las redes de telecomunicaciones.[65] Por ese motivo, el margen de acción de la ciberseguridad debe mantenerse en un punto medio donde no prevalezca una sobre otra.

Asimismo, en el mismo ámbito se encuentra la figura jurídica del *Ciberespionaje*. El auge en el uso masivo e intensivo de las tecnologías digitales ha provocado que dicha ofensa haya dejado de ser propia de los gobiernos para ser realizada progresivamente por cualquiera sin la necesidad de tener un conocimiento profundo sobre el funcionamiento de tales herramientas tecnológicas, desde simples usuarios hasta corporativos industriales. Aquél consiste en:

> Obtener, saber o copiar la información confidencial o clasificada de forma no autorizada de un equipo de destino mediante el uso de sistemas tecnológicos de información y redes para obtener una ventaja militar, política o económica, lo cual nos indica que el perpetrador puede ser de distintos indoles, como son: particulares, es decir individuos, competidores en un mercado determinado, por ejemplo, en el mercado comercial, grupos militares, de insurgencia, etc., o gobiernos.[66]

---

[62] Ernesto Garzón Valdés, *Lo íntimo, lo privado y lo público*, INAI-Cuadernos de transparencia 06, México, 2015, p. 14.
[63] *Ibid.*, p. 16.
[64] *Ídem.*
[65] Julian Assange, *op. cit.*, pp. 39-53.
[66] Alejandra Morán Espinosa; Abraham Alejandro Servín Caamaño; Oscar Alquicira Gálvez, "TIC (Internet) y ciberterrorismo – III", *Revista Seguridad Cultura de prevención para TI*, núm. 25, México, UNAM-DGTIC, julio-agosto, 2015, p. 34.

Por último, se encuentran las afectaciones a los soportes físicos y lógicos que integran a las Infraestructuras Críticas de Información (ICI), a las Infraestructuras de Información Esenciales (IIE) y a las Infraestructuras Críticas del Estado (ICE) las cuales han supuesto una situación de vulnerabilidad para los Estados dependientes de ellas. Las conductas encaminadas a afectarlas se entenderán como *Ciberterrorismo* siempre que:

- Actúen con violencia
- Hagan uso del terror
- Se valgan de cualquier medio ilícito
- Atenten contra las personas
- Produzcan miedo psicológico
- Generen impacto trasnacional[67]

Del mismo modo, en el panorama de ciberseguridad a nivel internacional han comenzado a presentarse una serie de cambios de las tendencias en materia tecnológica. Entre las más importantes pueden citarse la creación de las criptomonedas, el *ransomware* como método de extorsión, el robo de datos personales, la promulgación del Reglamento General de Protección de Datos de la Unión Europea, así como la aplicación progresiva de la inteligencia artificial.[68]

La gravedad de esos fenómenos tecnológicos ha llevado a una gran cantidad de países a implementar una serie de medidas legales, técnicas, institucionales, formativas y cooperativas contenidas en una estrategia de ciberseguridad.[69] Ésta se ha vuelto necesaria ante las consecuencias resultantes de algunas de las problemáticas que han tenido mayor impacto en lo que va del nuevo milenio y que se explican a continuación.

---

[67] *Ibid.*, pp. 35-36.

[68] Panda Security, *2018 in cybersecurity: the experts talk*, [en línea], 43 pp., 27 de noviembre de 2018, Dirección URL: https://www.pandasecurity.com/emailhtml/1909-Ebook-Pandalabs-Sans/1810-the%20experts%20talk-ES.PDF, [consulta: 30 de junio de 2021].

[69] Unión Internacional de Telecomunicaciones, *Guía para la elaboración de una estrategia nacional de ciberseguridad*, [en línea], 76 pp., Dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf, [consulta: 30 de junio de 2021].

2.1.1 Estonia (2007)

El 27 de abril de 2007 tuvo lugar en Estonia, una nación ubicada en el noroeste europeo, uno de los primeros ataques informáticos a gran escala con consecuencias palpables para la política y la economía de aquel país. La agresión estuvo precedida por una gran cantidad de movilizaciones por parte de una mayoría de la población de habla rusa ante la decisión del gobierno de trasladar el "Monumento para los Libertadores de Tallin" a las afueras de la capital.

La ofensiva inició un día después de los disturbios generados en la ciudad con el colapso de las páginas web de organismos públicos y entidades privadas mediante la saturación del tráfico de internet provocada por el envío masivo de solicitudes de acceso y pedidos automáticos.[70] Ese acontecimiento provocó la inutilización prolongada de los servicios públicos que dependen del uso de la red.

De acuerdo con los resultados de las investigaciones efectuadas por las autoridades responsables, los ataques fueron perpetrados desde Rusia, específicamente desde la capital y presuntamente desde la sede de gobierno conocida como "Kremlin".[71] No obstante, aun con esos indicios, resultó complicado determinar que efectivamente había sido el gobierno ruso el responsable.

Las principales consecuencias de ese acontecimiento fueron, primeramente, el agravamiento de la situación iniciada por la remoción del monumento soviético al haber un aumento en la tensión política y social interna. De igual manera, se produjo un clima de inestabilidad económica al verse impedidos todos los sectores del uso de los servicios financieros.

---

[70] Damien McGuiness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país", [en línea], *bbc.com*, 6 de mayo de 2017, Dirección URL: https://www.bbc.com/mundo/noticias-39800133, [consulta: 30 de junio de 2021].

[71] Ricardo Martínez de Rituerto, "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y en la UE", [en línea], *elpais.com*, 18 de mayo de 2007, Dirección URL: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html, [consulta: 30 de junio de 2021].

Sin embargo, aunque Estonia forma parte de la Organización del Tratado del Atlántico Norte (OTAN), ésta se vio impedida de invocar el ejercicio del derecho de legítima defensa individual previsto en el Artículo 5 del Tratado del Atlántico Norte[72] ya que no se consideraba un ataque físico convencional. Esa situación ha llevado al cuestionamiento sobre el uso de las TIC como factores de posibles *casus belli*, es decir, "motivos de guerra".[73]

A causa de lo acontecido en el país báltico, los ministros de defensa de la OTAN reconocieron en junio de 2016 al ciberespacio como dominio operacional militar ante el surgimiento de una nueva amenaza capaz de poner en peligro la seguridad de cualquiera de los Estados miembros.[74] Los ciberataques han tomado gran significación a tal grado que dicho organismo internacional las ha catalogado al mismo nivel que las armas químicas, biológicas, radiológicas y nucleares.

Si bien, las tecnologías digitales no fueron por sí solas las causantes de provocar tal coyuntura, en combinación con otros factores presentes en el entorno político y social demostraron su capacidad para desatar y agravar las problemáticas ya existentes. Asimismo, evidenciaron la dificultad para reconocer el origen y la identidad de los agresores con la finalidad de ejercer responsabilidades tanto políticas como jurídicas.

Por lo tanto, el caso estonio ha puesto en evidencia lo trascendental que resulta la ciberseguridad como asunto de seguridad nacional toda vez que ésta fue vulnerada con el apoyo de las Tecnologías de la Información y Comunicación. Principalmente, se diría que fue víctima de un intento de desestabilización interna de origen probablemente externo, el cual posee las características de un nuevo método para hacer la guerra sin las repercusiones que conlleva un conflicto armado.

---

[72] Organización del Tratado del Atlántico Norte, *Tratado del Atlántico Norte*, [en línea], 4 de abril de 1949, Dirección URL: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es, [consulta: 30 de junio de 2021].

[73] Edgar Iván Espinosa, *op. cit.*, p. 116.

[74] Lillian Ablon, *et al.*, *Operationalizing Cyberspace as a Military Domain. Lessons for NATO*, [en línea], 42 pp., Dirección URL: https://www.rand.org/pubs/perspectives/PE329.html, [consulta: 30 de junio de 2021].

2.1.2 Assange y Snowden (2010-2013)

A principios de la segunda década del siglo XXI, entre los años 2010 y 2015, ocurrieron dos de los sucesos más trascendentales en cuestión de ciberseguridad a nivel internacional. El primero sucedió durante el transcurso del año 2010 cuando la organización internacional *WikiLeaks* realizó una filtración masiva de documentos clasificados pertenecientes en su mayoría a los Departamentos de la Defensa y de Estado de los Estados Unidos.[75]

Dicha organización, al mando del programador y activista australiano Julian Assange, puso en evidencia dos aspectos importantes. Primeramente, demostró la facilidad con la que cualquier país puede ser vulnerado en sus sistemas de información; posteriormente, dio cuenta de los actos de espionaje cibernético que han estado llevando a cabo los gobiernos, especialmente el estadounidense.

El segundo suceso tuvo lugar entre los años 2013 y 2015 cuando el exanalista de la Agencia de Seguridad Nacional, Edward Snowden, filtró un conjunto de documentos que mostraban la existencia de una red de vigilancia global realizada por la alianza internacional *Five Eyes*. Ésta se encuentra integrada por las agencias de inteligencia de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos.[76]

Los documentos revelaban el uso de *spyware*, es decir, software espía especializado en la intercepción indiscriminada de telecomunicaciones radiales y satelitales por parte de los miembros de dicho tratado en contra de países aliados y rivales.[77] La importancia del caso Snowden radicaba en evidenciar las actividades de espionaje cibernético que han estado realizando diversos países.

---

[75] David Leigh y Luke Harding, *WikiLeaks y Assange: un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*, México, Editorial Deusto, 2011, pp. 233-250.
[76] Glenn Greenwald, *Snowden: sin un lugar donde esconderse*, Barcelona, Ediciones B, 2014, pp. 213-258.
[77] Adolfo Arreola García, *Ciberespionaje: la puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de Estados Unidos*, México, Siglo XXI Editores/Universidad Anáhuac, 2015, pp. 111-116.

Las filtraciones realizadas por Julian Assange y Edward Snowden dejaron en claro que el elemento más importante en cualquier sistema de ciberseguridad es el factor humano antes que el tecnológico.[78] Ambos demostraron intencionalmente la importancia que han comenzado a tomar los individuos especializados en las TIC en la era digital, sobre todo como nuevos actores de la escena política internacional en cuestión de seguridad nacional.

Asimismo, dichos protagonistas han quedado envueltos en una encrucijada política para las sociedades y para los gobiernos ya que mientras las primeras los han dotado de autoridad al legitimar sus acciones los segundos los han catalogado indistintamente como amenazas del ciberespacio, lo cual ha llevado a un enfrentamiento gobernantes-gobernados. En cierto sentido, se han transformado en "nuevo Mesías de la prensa para algunos, ciberterroristas para otros".[79]

Por otro lado, a diferencia de los ataques cibernéticos tradicionales que involucran el uso de *software* y *hardware*, las fugas de información requieren mayoritariamente de la participación de los miembros de la organización objetivo. Para llevar a cabo las filtraciones, Assange se valió de la colaboración de la exanalista de inteligencia del ejército estadounidense Chelsea Manning mientras que Snowden se sirvió de su pertenencia a la NSA.

Por ese motivo, se torna necesario definir la situación política y jurídica de tales actores. Especialmente porque en el plano futuro se tiene previsto que las filtraciones masivas de información confidencial contenida en servidores informáticos sean cada vez más recurrentes porque "siempre habrá demasiada gente con acceso a demasiada información como para detener las filtraciones masivas. En el futuro habrá más Assanges y más Snowdens".[80]

---

[78] Pablo Rodríguez Canfranc, *Profesiones digitales 2. Ciberseguridad, protegiendo la información vulnerable*, Madrid, Fundación Telefónica, 2019, p.

[79] Alan Rusbridger, "Introducción", *WikiLeaks y Assange: un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*, México, Editorial Deusto, 2011, pp. 15-26.

[80] Julian Assange, *Cuando Google encontró a WikiLeaks*, Buenos Aires, Editorial Capital Intelectual, 2014, p. 211.

2.1.3 *WannaCry* (2017)

El último gran incidente cibernético a escala mundial tuvo lugar el 12 de mayo de 2017 cuando inicialmente se vieron afectados los equipos informáticos del Servicio Nacional de Salud de Inglaterra (*NHS*, por sus siglas en inglés). De acuerdo con los primeros reportes informativos, el percance se debió a la propagación de un software malicioso llamado *WannaCry*, con lo cual quedaron suspendidos los servicios médicos temporalmente.[81]

Posteriormente, *WannaCry* se esparció en España donde afectó a empresas tales como *Telefónica*, *Iberdrola*, *Gas Natural*, entre otras.[82] Al igual que en la nación inglesa, los servicios provistos por aquéllas se mantuvieron interrumpidos momentáneamente. Asimismo, más de 150 países alrededor del mundo mencionaron haber sido afectados de manera directa o indirecta en sus sistemas dependientes de la red de redes.[83]

De forma similar a lo sucedido en Estonia, resultó casi imposible señalar algún responsable individual o colectivo de la creación y propagación del *malware* lo cual llevó a que algunos gobiernos se culparan entre ellos en cuanto a su autoría. Sin embargo, las autoridades de los Estados Unidos, específicamente el Buró Federal de Investigaciones (*FBI*, por sus siglas en inglés), convinieron en apuntar a la participación del hacker norcoreano Park Jin Hyok.

---

[81] s/a, "Ciberataque afecta a sistema de salud en Inglaterra", [en línea], México, *eluniversal.com.mx*, 12 de mayo de 2017, Dirección URL: https://www.eluniversal.com.mx/articulo/mundo/2017/05/12/ciberataque-afecta-sistema-de-salud-en-inglaterra, [consulta: 30 de junio de 2021].

[82] s/a "Ataque informático en España afecta a Telefónica, Iberdrola y Gas Natural", [en línea], México, *eluniversal.com.mx*, 12 de mayo de 2017, Dirección URL: https://www.eluniversal.com.mx/articulo/mundo/2017/05/12/ataque-informatico-en-espana-afecta-telefonica-iberdrola-y-gas-natural, [consulta: 30 de junio de 2021].

[83] Bruno Toledano, "El ciberataque con el virus WannaCry se extiende a nivel mundial", [en línea], Madrid, *elmundo.es*, 12 de mayo de 2017, Dirección URL: https://www.elmundo.es/tecnologia/2017/05/12/5915e99646163fd8228b4578.html, [consulta: 30 de junio de 2021].

Las diferencias entre lo ocurrido en Estonia en 2007 y en prácticamente todo el mundo en el 2017 no sólo son cuantitativas sino cualitativas. En un periodo de diez años ambos acontecimientos han ejemplificado la evolución de los ciberataques en cuestión de devastación y sofisticación. “Si bien no es el tipo de malware que afecte a la mayor cantidad de usuarios, por sus características es uno de los que más preocupación causa”.[84]

Desde el punto de vista técnico, *WannaCry* es un software malicioso perteneciente a la categoría *ransomware* cuya finalidad es “bloquear el acceso a los dispositivos electrónicos o codificar los archivos en ellos”.[85] Una vez que ha logrado su cometido, el atacante exige a la parte perjudicada cierta cantidad de dinero virtual o *bitcoins* en un periodo limitado para “liberarlo”, por lo cual resulta una especie de secuestro de información.

Utilizado en una escala reducida, se diría que el uso general del *ransomware* conlleva una motivación primordialmente económica. No obstante, empleado en un nivel amplio conllevaría una aplicación política ya que “este tipo de amenazas tienden a enfocarse menos en los datos y más en impedirle a la víctima el uso de su dispositivo y los servicios que facilita”.[86] Eso permite a cualquiera ejercer presión sobre las entidades gubernamentales de algún país, como en el caso de Estonia.

Por lo tanto, se diría que *WannaCry* ha marcado un antes y un después en cuestión de ciberseguridad y de seguridad nacional toda vez que su creación responde a generar un impacto global indiscriminado. Tanto aquél como *Stuxnet*[87] han evidenciado la importancia que han adquirido los códigos maliciosos como nuevas armas para hacer la guerra.

---

[84] Camilo Gutiérrez Amaya y Miguel Ángel Mendoza, “Tendencias 2018: el costo de nuestro mundo conectado”, *Revista Seguridad Cultura de prevención para TI*, núm. 31, México, UNAM-DGTIC, mayo-junio, 2018, p. 19.

[85] Policía Federal, *Glosario de términos en ciberseguridad*, [en línea], México, 4 de julio de 2018, Dirección URL: https://www.gob.mx/policiafederal/articulos/glosario-de-terminos-en-ciberseguridad?idiom=es, [consulta: 30 de junio de 2021].

[86] Camilo Gutiérrez Amaya y Miguel Ángel Mendoza, *op. cit.*, p. 19.

[87] Stuxnet es el nombre de otro código malicioso que fue creado en el 2010 para afectar los sistemas de Supervisión, Control y Adquisición de Datos (*SCADA*, por sus siglas en inglés).

2.2 Contexto nacional

Acorde con el *Índice Global de Ciberseguridad* de 2020, elaborado por la Unión Internacional de Telecomunicaciones, México se posicionó en el lugar 52 a nivel mundial sobre un ranking de 182 posiciones. A nivel regional fue ubicado en el 4º lugar detrás de Brasil, Canadá y Estados Unidos quienes obtuvieron la tercera, segunda y primera posición respectivamente. En aquél se consideraron cinco pilares: Legal, Técnico, Organizacional, Formación y Cooperación.[88]

Por otra parte, el informe de la OEA *Tendencias de Seguridad Cibernética en América Latina y el Caribe* indicó que las entidades más afectadas por incidentes cibernéticos en México fueron, en orden porcentual, las organizaciones académicas (39%), las instituciones gubernamentales (31%), las entidades del sector privado (26%) y otras entidades (4%). Los ataques más denunciados fueron por uso de malware, phishing, hackeos, así como intrusiones en los sistemas.[89]

Por último, el *17º Estudio sobre los Hábitos de los Usuarios de Internet en México*, realizado por la Asociación de Internet MX muestra que, hasta el 2020, el número de usuarios de internet en México se encontraba en 86.8 millones de personas con una penetración del 76.3% entre la población mayor a 6 años. De igual forma, señala que para conectarse a la red el 92% cuenta con smartphone, el 45.2% tiene computadora, el 24.4% utiliza SmartTV y el 14.4% mediante tablet.[90]

---

[88] Unión Internacional de Telecomunicaciones, *Índice Global de Ciberseguridad 2020*, [en línea], 172 pp., Dirección URL: https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020, [consulta: 30 de junio de 2021].

[89] Organización de los Estados Americanos/Symantec, *Tendencias de seguridad cibernética en América Latina y el Caribe*, [en línea], 100 pp., Dirección URL: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-225/14, [consulta: 30 de junio de 2021].

[90] Asociación de Internet MX, *17º Estudio sobre los hábitos de los usuarios de internet en México 2019*, [en línea], 26 pp., México, 06 de mayo de 2021, Dirección URL: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v15%20Publica.pdf, [consulta: 30 de junio de 2021].

Con base en las estadísticas se diría que en México se ha generado una desproporción entre el crecimiento de las TIC y el establecimiento de medidas legales, técnicas, organizacionales, formativas y cooperativas.[91] Por ese motivo, se ha dicho que existe una crisis de ciberseguridad "que se ha ido agudizando ante la falta de una política unificada que coordine los esfuerzos implementados por algunas dependencias gubernamentales y la iniciativa privada".[92]

Para algunos especialistas, como Edgar Iván Espinosa, una de las carencias más importantes del Estado mexicano en materia de ciberseguridad ha sido la ausencia de una clasificación de los principales riesgos y amenazas cibernéticas para la seguridad nacional mexicana.[93] Sobre todo, porque el desconocimiento de ese tipo de antagonismos impide la implementación de medidas preventivas y reactivas entendidas en tanto políticas de Estado como de gobierno.

A pesar de no existir tal clasificación, dicho autor identifica como peligros más relevantes a la *Ciberdelincuencia*, al *Ciberespionaje* y al *Hacktivismo*. A cada una de las problemáticas las vincula con una naturaleza distinta; a la primera le atribuye una causa económica al ser la obtención de dinero su objetivo primordial, al segundo lo relaciona con motivos políticos al estar asociada a la obtención de información y a la ultima la considera una mezcla de ambos.

En el caso de la ciberdelincuencia, a pesar de estar relacionada con la seguridad pública, le otorga el rango de antagonismo a la seguridad de la nación toda vez que incide en todos los sectores del desarrollo nacional. Se le define como las "actividades que llevan a cabo individuo(s) realiza(n) que utilizan como medio o como fin las Tecnologías de la información y comunicación"[94], las cuales abarcan desde las que van en contra de la información como de las personas.

---

[91] Unión Internacional de Telecomunicaciones, *The ITU National Cybersecurity Strategy Guide*, [en línea], 122 pp., Dirección URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf, [consulta: 30 de junio de 2021].

[92] Edgar Iván Espinosa, *op. cit.*, p. 115.

[93] *Ibid.*, p. 117.

[94] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.

En el sector público, el mayor número de incidencias cibernéticas se han presentado en el sistema financiero. Según el informe de la OEA y la CNBV *Estado de la ciberseguridad en el sistema financiero mexicano*, el 100% de las entidades e instituciones pertenecientes a ese ámbito resultaron afectadas, de las cuales el 56% fue por *malware*, el 47% por *phishing* y el 31% por violación de políticas de escritorio limpio. Además, reportó que el 19% sufren ataques por malware diariamente.[95]

En el sector privado, las afectaciones más relevantes hacia las empresas y organizaciones han sido los ataques por *ransomware*, los ataques por inyección SQL (*Structured Query Language*), los ataques de día cero y los ataques de denegación de servicio (*DoS*, por sus siglas en inglés).[96] En el sector social, los daños que más han sufrido los usuarios son el *phishing*, el software espía, así como la ingeniería social.

En cuanto al ciberespionaje, éste se ha convertido en una de las tácticas más recurrentes entre las naciones. Debido al área de influencia geopolítica de México con respecto a otros países, sobre todo con Estados Unidos, el país se ha vuelto proclive al padecimiento de esa clase de incidentes tal como lo evidenciaron las filtraciones de Edward Snowden donde se mostró cómo fueron espiados los expresidentes Felipe Calderón Hinojosa y Enrique Peña Nieto.[97]

Por último, el hacktivismo se ha presentado como un suceso inesperado para los ámbitos nacional e internacional ya que ha emergido como respuesta individual y colectiva mayoritariamente del sector social ante diversas circunstancias políticas, económicas y sociales.[98] Por ese motivo, resulta necesario conocer algunas de las incidencias más significativas para la ciberseguridad nacional en el siglo XXI con la finalidad de determinar las causas y las entidades que los originaron.

---

[95] OEA/CNBV, *op. cit*.
[96] Pablo Rodríguez Canfranc, *op. cit*.
[97] Cámara de Diputados, *Gaceta Parlamentaria*, [en línea], México, Jueves 24 de octubre de 2013, Dirección URL: http://gaceta.diputados.gob.mx/Black/Gaceta/Anteriores/62/2013/oct/20131024-VII/Proposicion-9.html, [consulta: 30 de junio de 2021].
[98] M. Á. Bastenier, "Hacktivismo", [en línea], *elpaís.com*, 30 de noviembre de 2010, Dirección URL: https://elpais.com/internacional/2010/11/30/actualidad/1291071624_850215.html, [consulta: 30 de junio de 2021].

2.2.1 *Pegasus* (2017)

Para comenzar, el 11 de febrero de 2017, el laboratorio interdisciplinario canadiense *The Citizen Lab* realizó un reporte titulado *Bitter Sweet* donde denunciaba la presunta adquisición y uso de spyware por parte de algunas entidades del gobierno federal mexicano, principalmente de las encargadas de la seguridad y la procuración de justicia. La investigación está conformada por ocho apartados en los cuales se describe la forma en la que supuestamente fueron espiadas algunas personas.

De acuerdo con la primera parte, entre el 20 de abril y el 17 de agosto de 2016, los afectados fueron los activistas Alejandro Calvillo y Luis Encarnación, así como el científico Simón Barquera quienes impulsaban el establecimiento de un impuesto a las bebidas azucaradas.[99] Después, en la segunda parte se menciona que, desde enero de 2015 hasta agosto de 2016, los perjudicados fueron algunos periodistas como Carmen Aristegui y Carlos Loret de Mola.

Luego, la tercera parte dice que, entre los meses de junio y julio de 2016, los perjudicados fueron los políticos panistas Ricardo Anaya Cortés, Roberto Gil Zuarth y Fernando Rodríguez Doval. Enseguida, en la cuarta parte se menciona que, a principios de marzo de 2016, los afectados fueron los miembros del Grupo Interdisciplinario de Expertos Independientes (GIEI) quienes investigaban el caso de los estudiantes desaparecidos en Ayotzinapa en 2014.

Posteriormente, la quinta parte menciona que el programa fue dirigido, entre los meses de septiembre y octubre de 2015, en contra de los abogados Karla Michel Salas y David Peña quienes representaban a las familias de mujeres asesinadas. También, en la sexta sección se describe cómo fueron vigilados los integrantes de la organización civil *Mexicanos Contra la Corrupción y la Impunidad*, entre los que destaca su director, Claudio X. González.

[99] The Citizen Lab, *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, [en línea], Toronto, 11 de febrero de 2017, Dirección URL: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/, [consulta: 30 de junio de 2021].

En la séptima parte se señala que, en el mes de mayo de 2017, los objetivos fueron los periodistas Ismael Bojórquez y Andrés Villareal los cuales investigaban casos sobre crimen organizado. Por último, el reporte concluye con el caso de la periodista Griselda Triana, esposa del periodista asesinado Javier Cortez Cárdenas, dando un total de 25 personas que mencionaron presuntamente haber sido espiadas a través de la intrusión del spyware en sus teléfonos inteligentes.

El programa utilizado recibe el nombre *Pegasus* y ha sido creado por la empresa israelí *NSO Group Technologies* dedicada al desarrollo de tecnología "para ayudar a las agencias del gobierno a detectar y prevenir el terrorismo y el crimen".[100] Con base en los lineamientos de la compañía, los productos que desarrolla son de uso exclusivo de las agencias de inteligencia gubernamentales, así como de las fuerzas del orden.

Técnicamente, *Pegasus* entraría en la categoría de "software malicioso cuyo objetivo es la obtención de información en el equipo infectado y enviarlo al atacante".[101] El programa puede recopilar toda clase de información y quien lo utilice puede dirigirlo mediante mensaje SMS o correo electrónico a cualquier dispositivo digital (hardware) capaz de conectarse a internet sin importar el sistema operativo (software) utilizado.[102]

Políticamente, su uso por parte de los gobiernos ha llevado a la discusión filosófica-política entre la seguridad y la libertad. Si bien, ha sido creado con la intención de contribuir a las autoridades encargadas de garantizar el orden, la seguridad y la justicia, también puede ser utilizado contrariamente a su finalidad interfiriendo en la intimidad y privacidad del usuario de las TIC ocasionando que pueda ser considerado "arma de doble filo".

---

[100] NSO Group, *About us*, [en línea], Dirección URL: https://www.nsogroup.com/about-us/, [consulta: 30 de junio de 2021].
[101] Eduardo Suárez Vázquez, *op. cit.*, p. 52.
[102] s/a, "12 claves para entender qué es el spyware Pegasus y cómo funciona", [en línea], México, *expansion.mx*, 19 de junio de 2017, Dirección URL: https://expansion.mx/tecnologia/2017/06/19/12-claves-para-entender-que-es-el-spyware-pegasus-y-como-funciona, [consulta: 30 de junio de 2021].

2.2.2 Banco de México (2018)

Posteriormente, entre los meses de abril y mayo de 2018, “cinco bancos detectaron operaciones a través de las cuales se hicieron transferencias a cuentas ‘fantasma’”.[103] En orden cronológico, todo comenzó a partir del 27 de abril cuando los bancos comerciales Banorte y Citibanamex reportaron haber presentado fallas en el Sistema de Pagos Electrónicos Interbancarios (SPEI) en el momento en el que los usuarios intentaron realizar transferencias electrónicas.[104]

Hasta ese momento el Banco de México, en tanto institución encargada del sistema de pagos electrónicos, mantenía su postura respecto a lo sucedido al declarar que se trataba de problemas operativos propios del sistema y no de algún tipo de ataque cibernético o intento de hackeo. Sin embargo, tanto las entidades afectadas como sus usuarios continuaron presentando fallos el 30 de abril con respecto a la rapidez e inmediatez de las transacciones.[105]

A partir de esa fecha, el banco central había tomado como una primera medida preventiva el uso de un modo alternativo al original utilizado por el sistema electrónico. De esa manera, se obligaba a la mayoría de los intermediarios financieros a utilizarlo, desde los que resultaron perjudicados directa o indirectamente hasta los que no sufrieron percance alguno.[106]

---

[103] s/a, “Por hackeo a SPEI, Banxico crea dirección de Ciberseguridad”, [en línea], México, *excelsior.com.mx*, 15 de mayo de 2018, Dirección URL: https://www.excelsior.com.mx/nacional/por-hackeo-a-spei-banxico-crea-direccion-de-ciberseguridad/1238972, [consulta: 30 de junio de 2021].

[104] s/a, “Banxico descarta afectación a clientes por falla en sistemas de pagos de bancos”, [en línea], México, *expansión.mx*, 27 de abril de 2018, Dirección URL: https://expansion.mx/empresas/2018/04/27/citibanamex-y-banorte-reportan-fallas-en-sus-sistemas-de-pago, [consulta: 30 de junio de 2021].

[105] s/a, “Las fallas en transferencias vía SPEI continúan, según usuarios”, [en línea], México, *expansión.mx*, 30 de abril de 2018, Dirección URL: https://expansion.mx/empresas/2018/04/30/las-fallas-en-transferencias-via-spei-continuan-segun-usuarios, [consulta: 30 de junio de 2021].

[106] Adrián Estañol, “Más bancos se desconectan temporalmente del SPEI”, [en línea], México, *expansión.mx*, 11 de mayo de 2018, Dirección URL: https://expansion.mx/empresas/2018/05/10/mas-bancos-se-desconectan-temporalmente-del-spei, [consulta: 30 de junio de 2021].

No fue sino hasta el 14 de mayo cuando finalmente el gobernador del Banco de México, Alejandro Díaz de León, informó a través de audioconferencia que las incidencias presentadas habían sido a causa de un ataque cibernético. Asimismo, destacó que la agresión había sido identificada, contenida y mitigada; aunque no se detalló oficialmente la suma exacta sustraída por los atacantes, algunas fuentes comentaron que la cantidad rondaba entre los 300 y 400 millones de pesos.[107]

De manera específica, el problema se generó en el servicio de transferencias del Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México y la banca comercial, cuya finalidad es la de funcionar como plataforma digital para enviar y recibir pagos de manera electrónica. Al igual que en otras situaciones de la misma naturaleza, resultó complicado deslindar responsabilidades en tanto se desconociera el origen y la identidad de los atacantes.

Aunque el ataque fue perpetrado mayormente con el apoyo de las tecnologías digitales también fue indispensable la participación de agentes individuales. Posteriores investigaciones efectuadas por la Fiscalía General de la República (FGR) demostrarían la participación de un grupo delictivo detrás de ése y otros robos cibernéticos entre 2018 y 2019.[108]

Cabe mencionar que, como resultado de ese acontecimiento, la autoridad bancaria central decidió implementar como medida institucional la creación de una Dirección de Ciberseguridad.[109] Si bien, a pesar de que dicha medida está enfocada en garantizar la protección de la información y sus procesos en el medio financiero, no tiene alcance significativo en cuestión de seguridad nacional.

---

[107] s/a, “Banxico confirma ciberataque y dice que el monto está por definirse”, [en línea], México, *expansión.mx*, 14 de mayo de 2018, Dirección URL: https://expansion.mx/economia/2018/05/14/banxico-confirma-ciberataque-y-dice-que-el-monto-esta-por-definirse, [consulta: 30 de junio de 2021].

[108] Arturo Ángel, “Fiscalía identifica a presuntos responsables de ciberataques contra bancos”, [en línea], México, *animalpolitico.com*, 17 de marzo de 2019, Dirección URL: https://www.animalpolitico.com/2019/03/fiscalia-responsables-ciberataques-bancos/, [consulta: 30 de junio de 2021].

[109] Banco de México, *Estrategia de Ciberseguridad del Banco de México*, [en línea], 5 pp., México, 17 de mayo de 2018, Dirección URL: https://www.banxico.org.mx/spei/d/%7BA578961B-C965-33AD-0A8A-BFE6D6FE9669%7D.pdf, [consulta: 30 de junio de 2021].

2.2.3 Petróleos Mexicanos (2019)

Para finalizar, el tercer percance se presentó a principios del sexenio del presidente Andrés Manuel López Obrador. El incidente se dio a conocer mediante un comunicado de prensa emitido por Petróleos Mexicanos (PEMEX), en la cual informaba que el día 10 de noviembre de 2019 "recibió intentos de ataques cibernéticos que fueron neutralizados oportunamente, afectando el funcionamiento a menos del 5% de los equipos personales de cómputo".[110]

De acuerdo con información no oficial, proporcionada a través de los medios de comunicación, el hackeo consistió en el "secuestro de datos" contenidos en algunos de los servidores computacionales de la empresa productiva del Estado. Tal acción fue concretada con el apoyo de un programa malicioso presuntamente llamado *DoppelPaymer*, el cual forma parte de la categoría *ransomware* especializada en afectar la disponibilidad de la información.[111]

La naturaleza del ataque cibernético aparentemente fue de tipo económica ya que los presuntos cibercriminales habían exigido la cantidad de 565 bitcoins (dinero virtual) equivalente a 5 millones de dólares aproximadamente para liberar la información secuestrada de los equipos infectados. No obstante, la titular de la Secretaría de Energía, institución responsable de la subsidiaria, informó que la entidad no estaba dispuesta a pagar el monto solicitado.[112]

---

[110] Petróleos Mexicanos, "Pemex opera con normalidad", [en línea], México, *Boletines nacionales*, 11 de noviembre de 2019, Dirección URL: https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx, [consulta: 30 de junio de 2021].

[111] Rodrigo Riquelme, "Hackeo a Pemex puede considerarse como un delito de extorsión", [en línea], México, *eleconomista.com.mx*, 13 de noviembre de 2019, Dirección URL: https://www.eleconomista.com.mx/tecnologia/Hackeo-a-Pemex-puede-considerarse-como-un-delito-de-extorsion-20191113-0095.html, [consulta: 30 de junio de 2021].

[112] Karol García, "Pemex no pagará rescate a hackers tras ciberataque: Rocío Nahle", [en línea], México, *eleconomista.com.mx*, 13 de noviembre de 2019, Dirección URL: https://www.eleconomista.com.mx/empresas/Pemex-no-pagara-rescate-a-hackers-tras-ciberataque-Rocio-Nahle-20191113-0064.html, [consulta: 30 de junio de 2021].

Posteriormente, el titular de la Secretaría de Seguridad y Protección Ciudadana aseguró que "prácticamente de inmediato se desactivó, no se registran pérdidas porque afortunadamente alcanzó un porcentaje menor y equipos que no contenían información relevante y estratégica de Pemex".[113] Cabe destacar que la paraestatal forma parte de las áreas estratégicas que están bajo la autoridad del sector público, uno de los sectores del desarrollo nacional.[114]

De manera particular, el ciberataque fue dirigido al área administrativa de la compañía mediante el uso de un código malicioso afectando principalmente la red informática y forzando a dejar inhabilitados equipos de cómputo en todo el país. Con base en las declaraciones de las autoridades responsables, el percance no tuvo consecuencias palpables ni considerables para la nación tales como afectaciones al abasto de gasolina o a la infraestructura petrolera.

Aunque en un principio se mencionó que el percance había sido lanzado desde el exterior de la institución, fuentes alternas no descartaron el hecho de que pudo haberse originado premeditadamente desde el interior. Independientemente de la veracidad de esas afirmaciones, lo cierto es que quedó demostrada la susceptibilidad de los sistemas informáticos y las redes de telecomunicaciones estratégicas ante ataques cibernéticos.

El caso Pemex, al igual que los anteriores mencionados, han demostrado la capacidad adquirida por las nuevas tecnologías para vulnerar al Estado mexicano en cada uno de sus sectores. El presente suceso ha sido muestra de ello ya que se ha sumado al conjunto de sectores estratégicos del país perjudicados técnica, económica, social y, sobre todo, políticamente mediante las TIC.

---

[113] Forbes, "Hackeo a Pemex no afectó ni registró daños a información estratégica: funcionarios", [en línea], México, *Forbes.com.mx*, 14 de noviembre de 2019, Dirección URL: https://www.forbes.com.mx/hackeo-a-pemex-no-afecto-ni-registro-danos-a-informacion-estrategica-funcionarios/, [consulta: 30 de junio de 2021].

[114] Con base en el artículo 25 párrafo V constitucional, el sector público, representado por el Gobierno Federal, mantendrá la propiedad y el control sobre los organismos y las empresas productivas del Estado en lo concerniente a la planeación y el control del sistema eléctrico nacional, al servicio público de transmisión y distribución de energía eléctrica, así como a la exploración y extracción de petróleo y otros hidrocarburos.

Los seis incidentes antes referidos, tanto los internacionales como los nacionales, han sido sólo algunos de los ejemplos más representativos de la ciberseguridad como asunto de seguridad nacional en el siglo XXI. Cada uno de ellos ha puesto en evidencia que "no existe una solución universal que nos proteja para siempre porque los atacantes evolucionan y continuamente aparecen nuevas técnicas que derrotan a los mecanismos de protección".[115]

En primer lugar, en ninguno de los casos ha sido posible señalar, hasta el momento, algún responsable material y/o intelectual al cual imputar jurídica y políticamente por llevar a cabo tales acciones. Si bien, existen ciertos indicios que llevan a suponer la identidad de los probables responsables, éstos no han sido suficientes para determinar de manera fehaciente su participación.

En segundo lugar, el estado de la ciberseguridad en el mundo y en México ha reflejado que la mayoría de los países que dependen de las tecnologías digitales han sufrido en mayor o menor medida algún percance. Independientemente de los niveles de seguridad, de las medidas adoptadas y de las capacidades técnicas de una nación, siempre que se valga del uso de los sistemas computacionales estará vulnerable a ser atacada.

Por último, la investigación y el desarrollo tecnológicos motivados por los intereses de algunos gobiernos, así como de las corporaciones afines, han sido los principales factores que han contribuido a la evolución de las tecnologías de la información y comunicación. Sin embargo, esas acciones también han llevado al surgimiento de nuevas problemáticas asociadas a ese ámbito.

Por ese motivo, resulta necesario llevar a cabo un análisis político que permita identificar y realizar una clasificación de los peligros más relevantes que se han presentado y de los que puedan surgir como resultado de esas dinámicas cambiantes. Lo anterior con la finalidad de conocer el tipo de medida necesaria que se debe aplicar para contrarrestarlos, ya sea como medida preventiva o como medida reactiva.

[115] Hugo D. Scolnik, *op. cit.*, p. 27.

3. CLASIFICACIÓN DE RIESGOS Y AMENAZAS CIBERNÉTICAS

3.1 Riesgos cibernéticos

Desde la perspectiva gubernamental, la *Agenda Nacional de Riesgos* (ANR) ha sido el documento guía de la política de seguridad del Estado Mexicano en cuanto a la clasificación de riesgos. Para su elaboración toma como referencia los acontecimientos de los entornos nacional e internacional, así como las aportaciones de las instituciones que integran el Consejo de Seguridad Nacional, de forma que:

> Es un producto de inteligencia y un instrumento prospectivo que identifica riesgos y amenazas a la seguridad nacional, la probabilidad de su ocurrencia, las vulnerabilidades del Estado frente a fenómenos diversos y las posibles manifestaciones de los mismos.[116]

La ANR se caracteriza por ser un documento confidencial cuyo contenido sólo es accesible para la institución que lo realiza, es decir, para el Centro Nacional de Inteligencia (CNI). Por lo cual, el conocimiento de la metodología, de los procesos generales y específicos que conlleva su realización, así como los elementos que logra identificar anualmente se mantienen bajo reserva.

Por ello, para la formulación de una clasificación de los principales antagonismos vinculados con el ambiente cibernético se retomarán los elementos mencionados tanto en la teoría política como en la legislación nacional vigente. Primeramente, a partir de las aproximaciones realizadas de los conceptos de Seguridad Nacional y Ciberseguridad se establecerán los fines que se buscan alcanzar.

---

[116] Centro Nacional de Inteligencia, *¿Qué es la Agenda Nacional de Riesgos?*, [en línea], México, 18 de febrero de 2020, Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/535128/Agenda_Nacional_Riesgos.pdf, [consulta: 30 de junio de 2021].

Por una parte, se ha dicho que la naturaleza de la Seguridad Nacional se encuentra en el resguardo del Estado, es decir, de la organización política establecida, ya que de ella derivan los intereses, las aspiraciones y los objetivos nacionales. Específicamente, es posible asegurarlo garantizando su integridad, estabilidad y permanencia a través de medidas preventivas y reactivas entendidas como políticas de Estado y de gobierno. De esa forma quedó definida como:

> La situación en la que la mayoría de los sectores y grupos sociales de una nación tienen garantizadas por su gobierno sus necesidades culturales y materiales vitales mediante decisiones de Estado. Es decir, la Seguridad Nacional se refiere a las acciones de conjunto de las instancias de dicho Estado (sectores público, privado y social). Es una situación de seguridad frente a amenazas y/o retos internos o externos, reales o potenciales que atenten contra la reproducción de la nación, de la sociedad, de la familia, del individuo y de sus instituciones.[117]

Por otra parte, la Ciberseguridad es la dimensión tecnológica de la seguridad nacional cuya causa primera es la protección del binomio *humano-máquina*, es decir, tanto del factor humano como del técnico. Con respecto al primero, lo que se debe resguardar es la disponibilidad, privacidad e integridad de su información y datos personales; en cuanto al segundo, se deben procurar los elementos físicos (hardware) y lógicos (software) que los soportan. Quedando definida como:

> Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.[118]

Posteriormente, se tomarán en cuenta las características que constituyen tanto a los riesgos como a las amenazas con la finalidad de relacionarlos con los acontecimientos más recurrentes y con mayor impacto en materia tecnológica que han ocurrido en el transcurso del nuevo milenio a nivel nacional e internacional. En el caso de los Riesgos, se mencionó con anterioridad que poseían las siguientes propiedades:

---

[117] Manuel Quijano Torres, *op. cit.*, 15 de agosto de 2017.
[118] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.

- Son condiciones internas o externas.
- Son generados por situaciones y/o fenómenos políticos, económicos y sociales.
- Son influenciados por agentes no estatales y por desastres de tipo natural o antropogénico.
- Afectan principalmente al desarrollo nacional en sus tres sectores: público, privado y social.

En primera instancia, se les denominará *Riesgos cibernéticos* por estar asociados con dinámicas tecnológicas que llegan a combinarse con situaciones políticas, económicas y sociales. Al ser la tecnología una invención eminentemente de la humanidad tendrá que tomarse en cuenta como un fenómeno de origen antropogénico, es decir, que sólo el ser humano es capaz de generarlo.

Por otra parte, se les considerará con tal denominación cuando su presencia en el entorno nacional tenga repercusiones negativas en el corto, mediano o largo plazo para alguno o para todos los elementos involucrados en el desarrollo nacional. Cabe señalar que éste es el factor que permite procurar la estabilidad política de la nación ya que con ella es posible atender el equilibrio de otros sectores como el económico y el social.

Con base en los atributos antes mencionados se establecería la clasificación dividiendo entre riesgos cibernéticos *Internos* y *Externos*; los primeros serán aquellos que se desarrollan como producto de las dinámicas internas mientras que los segundos serán el resultado de las acciones de otros países. Lo que se pretende con esa división es dimensionar y priorizar en orden de atención las situaciones que serán posteriormente expuestas.

Con respecto a la temporalidad de los casos, sólo se va a tomar en cuenta el tiempo transcurrido del siglo XXI (2000-2020), sobre todo porque los riesgos tienden a desenvolverse a lo largo de los años. Si bien, el objetivo no es la realización de un catálogo exhaustivo de todos los antagonismos a la seguridad nacional, lo que se busca es identificar y clasificar las circunstancias que es importante atender de forma urgente y necesaria.

3.1.1 Internos

3.1.1.1 Tácticas en proceso

A la hora de hablar de la seguridad y defensa nacionales resulta necesario hacer hincapié en dos conceptos trascendentales que no pueden ser entendidos el uno sin el otro en una relación dialéctica: la táctica y la estrategia. Mientras que la primera está enfocada en "la capacidad logística del uso de recursos",[119] la segunda "es vital para determinar los fines de toda empresa y establecer los medios para alcanzarlos"[120] en una suerte del todo y sus partes.

A lo largo de la historia, diversos autores de distintas épocas, tanto de occidente como de oriente, la han abordado como asunto de Estado. En primer lugar, en el Capítulo III de *El arte de la guerra*, el general chino Sun Tzu (544-496 a. n. e.) destaca que en la guerra "lo mejor de lo mejor no consiste en ganar cien batallas de cada cien; lo mejor de lo mejor consiste en vencer al enemigo sin luchar"[121] y esto sólo se consigue mediante la estrategia planeada.

Después, en el Libro I de *Del arte de la guerra*, Nicolás Maquiavelo (1469-1527) indica que "el principal objetivo de quien inicia una guerra es poder librar una batalla decisiva contra su enemigo, una que le proporcione la victoria"[122]. Para lograrla propone una serie de acciones que deben ser consideradas y realizadas por el general al mando, aunque no las menciona se comprende que hace referencia a la táctica y a la estrategia.

---

[119] Manuel Quijano Torres, "El modelo de planeación estratégica", clase presentada en el Curso *Seguridad Nacional*, México, Facultad de Ciencias Políticas y Sociales, UNAM, 22 de agosto de 2017.

[120] Emilio Vizarretea Rosales, "Sobre el discurso estratégico (primera parte)", *Revista del Centro de Estudios Superiores Navales*, N° 3, Vol. 34, México, SEMAR-CESNAV, julio-septiembre, 2013, pp. 7-8.

[121] Sun Tzu, *El arte de la guerra*, Madrid, Alianza Editorial, 2014, p. 89.

[122] Nicolás Maquiavelo, *op. cit.*, 2009, p. 117.

Por último, en el Libro III del tratado *De la Guerra*, el general prusiano Carl Von Clausewitz (1780-1831) define la Estrategia como "el uso del combate para los fines de la guerra".[123] Desde el punto de vista del militar, el establecimiento de una estrategia adecuada no sólo a la teoría sino también a los hechos, así como a los fines y los medios repercute en el éxito que pueda obtener un príncipe o un general en un conflicto bélico. De tal manera que:

> tiene que fijar a todo el acto bélico una meta que corresponda al objetivo del mismo, es decir, desarrolla el plan de guerra y enlaza con ese objetivo la serie de acciones que deben conducir al mismo, o sea, hace los diseños de las distintas campañas y dispone en ellas los distintos combates.[124]

Si bien, tanto el término como la definición hacen referencia a circunstancias estrictamente militares, hoy día se ha generalizado su uso para designar las medidas enfocadas a atender problemáticas prioritarias como la ciberseguridad. Muestra de ello ha sido la progresiva importancia que se le ha dado a la implementación de una estrategia nacional por parte del gobierno.

En el caso mexicano, la necesidad de implementarla responde a las necesidades por entender y atender política, económica y administrativamente el fenómeno cibernético ante el inminente avance y evolución de las tecnologías digitales. Un primer documento de trabajo fue realizado en el año 2017 en un proceso colaborativo entre diferentes actores: gobiernos, sector privado, comunidad técnica, sociedad civil y academia.

Sin embargo, aunque el documento de trabajo logró evolucionar a un Plan Nacional con miras a la Agenda 2030, la Estrategia no tuvo mayor trascendencia que en el papel a pesar de contar con una estructura definida. Las dificultades se presentaron, entre otras cosas, en cuanto a la administración estratégica al no concretarse aspectos como la logística, la planificación, así como la instrumentación de las reformas político-administrativas necesarias.

---

[123] Carl von Clausewitz, *De la Guerra*, Madrid, La esfera de los libros, 2015, p. 39.
[124] *Ídem*.

De esa manera quedaron inconclusas ciertas puntualizaciones referentes a un modelo de planeación de estratégica que contemple el proceso, la estrategia, las disposiciones, el comando, la maniobra y la infiltración.[125] Si bien, fue redactado correctamente en la teoría, estuvo mal planeado para ejecutarse en la práctica al no corresponder los fines con los medios.

La ausencia de una Estrategia Nacional de Ciberseguridad se considera como Riesgo cibernético interno al ser una condición propia del país, ya que es el gobierno federal, mediante los poderes Ejecutivo, Legislativo y Judicial, el responsable de ejecutar las políticas públicas en la materia. El principal riesgo cibernético para el desarrollo nacional de esa situación es que "al no tener una estrategia, la infraestructura crítica del país está a merced del crimen".[126]

La importancia de protegerlas radica en que se encuentran "relacionadas con la provisión de bienes y prestación de servicios públicos esenciales"[127] por lo que se verían afectados indistintamente los sectores público, privado y social en cuanto a la realización de sus actividades cotidianas llevando a una posible inestabilidad interna. Sobre todo, porque "México no está listo para resistir un ataque cibernético masivo"[128] como menciona Fernando Gutiérrez Cortés.

Por lo tanto, debido a que "ningún país está listo para enfrentar un ciberataque masivo"[129] resulta urgente y necesario implementar una estrategia nacional de ciberseguridad. No obstante, un aspecto que debe ser contemplado es que cualquier medida o acción que se busque llevar a cabo debe responder a la realidad política, económica y social de la nación.

---

[125] Manuel Quijano Torres, *op. cit.*, 22 de agosto de 2017.
[126] José Reyez, "Gobierno de México, sin estrategia ante ataques cibernéticos", [en línea], México, *contralinea.com.mx*, 5 de mayo de 2019, Dirección URL: https://www.contralinea.com.mx/archivo-revista/2019/05/05/gobierno-de-mexico-sin-estrategia-ante-ataques-ciberneticos/, [consulta: 30 de junio de 2021].
[127] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.
[128] Gonzalo Monterrosa, "VII. México, indefenso ante ciberataques Ed. 506", [en línea], México, *contralinea.com.mx*, 18 de septiembre de 2016, Dirección URL: https://www.contralinea.com.mx/archivo-revista/2016/09/18/mexico-indefenso-ante-ciberataques/, [consulta: 30 de junio de 2021].
[129] *Ídem*.

3.1.1.2 Digitalización de la sociedad

En diciembre de 1977 los investigadores franceses Simon Nora y Alain Minc publicaron, por encargo de su gobierno, un informe titulado *La informatización de la sociedad*. En él desarrollaron las ventajas y desventajas que traería consigo la *telemática* (acrónimo de *telecomunicación* e *informática*) donde destacaba que el cambio más importante se daría en las relaciones de poder internacional debido a la interdependencia que generaría.[130]

En el origen, se diría que "la convergencia tecnológica de la informática y las telecomunicaciones mejora la calidad de vida y propicia el ambiente adecuado para la integración y el desarrollo nacional".[131] Principalmente porque ha permitido la eficacia y la eficiencia en el acceso y prestación de servicios públicos por parte del gobierno tanto a la población como a las empresas.

En ese sentido, se podría argumentar que las tecnologías de la información y comunicación han pasado a formar parte de los medios para alcanzar políticamente cierto grado de independencia, ya sea parcial o totalmente. Eso se debe fundamentalmente a que en la era digital "las TIC nos hacen competitivos [económicamente] a nivel mundial".[132]

Sin embargo, así como han traído beneficios para la nación también han generado perjuicios en contra de ella derivados de la dependencia hacia su uso. Uno de los principales que se puede señalar es el hecho de que progresivamente todo tipo de actividades han comenzado a realizarse con su apoyo, desde las más provechosas hasta las más improductivas.

---

[130] Simon Nora y Alain Minc, *La informatización de la sociedad*, México, Fondo de Cultura Económica, 1981, p. 18.

[131] Edwin A. Arreola Rueda, "La informática, internet y la economía en México a principios del siglo XXI", *Estudios Políticos*, México, FCPYS-UNAM, núm. 7, enero-abril, 2006, p. 43.

[132] José de Jesús Vázquez Gómez, "Amenazas y riesgos a la seguridad nacional en el ciberdominio", *Seguridad y defensa en el ciberespacio*, México, SEMAR-CESNAV, 2015, p. 390.

De acuerdo con estimaciones realizadas por la firma internacional *Deloitte*, se espera que en el transcurso del año 2020 se alcance en México la cifra de 200 millones de dispositivos conectados a internet.[133] Considerando que, con base en el Censo de Población y Vivienda 2020, la población total del país se encuentra aproximadamente en 126, 014, 024 millones de habitantes[134] quiere decir que habrá 1,5 dispositivos digitales por persona.

Dichas cifras muestran, en primer lugar, el crecimiento exponencial que han tenido y tendrán las tecnologías digitales como herramientas de uso cotidiano, en segundo, que prácticamente todo el país se encuentra expuesto a ser víctima de ciberataques de cualquier tipo. Eso quiere decir que a medida que crezca descontroladamente el número de aparatos conectados a internet también aumentará el número de incidentes relacionados con ellos.

En ese caso, el riesgo se presenta en el momento en el que, de mantenerse esa tendencia en el largo plazo sin que se implementen mecanismos de protección técnicos y jurídicos, puedan dar pie al surgimiento de distintas amenazas donde los ciberataques han demostrado ser los más recurrentes. Especialmente porque el uso de esas tecnologías terminará abarcando todos los aspectos de los sectores público, privado y social.

Uno de los principales factores a considerar en cuanto a la creciente dependencia en las TIC es el *Internet de las cosas* cuyo concepto hace referencia a la idea de que todos los objetos electrónicos puedan conectarse a internet. Cabe señalar que no sólo se hace referencia a los dispositivos portátiles como los teléfonos inteligentes o las tabletas electrónicas sino a cualquiera con las capacidades técnicas para tener acceso a la red.

---

[133] Carlos Nuel, "Esperan 200 millones de dispositivos conectados en México para 2020", [en línea], 20 de junio de 2018, Dirección URL: https://www.xataka.com.mx/legislacion-y-derechos/esperan-200-millones-de-dispositivos-conectados-en-mexico-para-finales-del-2020. [consulta: 30 de junio de 2021].

[134] Instituto Nacional de Estadística y Geografía, *Censo de Población y Vivienda 2020*, [en línea], Dirección URL: https://www.inegi.org.mx/programas/ccpv/2020/#Resultados_generales, [consulta: 30 de junio de 2021].

Una de las consecuencias más graves de ese fenómeno tecnológico ha sido que poco a poco otros objetos electrónicos, que no estaban contemplados en un principio, han sido incorporados con funciones de interconectividad desde automóviles hasta electrodomésticos. En cierto sentido se diría que actualmente "no hay más automóviles, ni aviones, ni audífonos sino computadoras con cuatro ruedas, computadoras con alas y computadoras que mejoran tu audición".[135]

Es importante recordar que tanto en el caso de Estonia como en el de *WannaCry* la capacidad de impacto de los ciberataques estuvo relacionada con la cantidad de actividades que dependían de la internet. Mientras que en el primero los perjudicados fueron los servicios públicos de una sola nación, en el segundo fueron tanto servicios públicos como privados de más de un país.

Ante esa situación cabría preguntarse si "se está causando un mal o haciendo más vulnerable a un Estado, en lugar de proporcionarle el esperado beneficio".[136] Sobre todo, porque cada aparato conectado a la red de internet implica una ventana de vulnerabilidad para el gobierno, para la sociedad o para las empresas que puede ser aprovechada por cualquier entidad.

Sin embargo, eso no quiere decir que el Estado mexicano tenga que mantenerse al margen de la investigación y el desarrollo tecnológicos ya que, como se dijo al principio, pueden repercutir benéficamente en términos de productividad, competitividad y, sobre todo, de ciberseguridad. Así como son los medios ideales para procurar la integridad, estabilidad y permanencia del Estado también pueden perjudicarlo.

Por lo tanto, es de suma relevancia mantener un equilibrio al interior del país entre el crecimiento tecnológico y el establecimiento de estrategias de seguridad enfocadas en la materia con la finalidad de prevenir y responder ante las posibles y probables problemáticas. Especialmente porque es una tendencia que se mantendrá al alza en el siglo XXI.

---

[135] Julian Assange, *op cit.*, pp. 50-52.
[136] José de Jesús Vázquez Gómez, *op. cit.*, p. 390.

3.1.2 Externos

3.1.2.1 *Deep web*

En el mundo interconectado del siglo XXI el espacio cibernético se ha transformado en el sitio de reunión de individuos, sociedades, empresas e inclusive gobiernos. Hoy día no existe entidad alguna que no se encuentre inmerso en él en cada una de sus actividades cotidianas ya sea con la ayuda de medios convencionales como las computadoras personales o por medios inusuales como los vehículos particulares.

A causa de las ventajas que ofrece ha representado el entorno ideal para la realización de las actividades políticas, económicas y sociales de una nación por lo que "se ha constituido como una nueva ágora",[137] es decir, el lugar donde se congregan los ciudadanos de un Estado. Sin embargo, el primero a diferencia del segundo tiene la particularidad de no contar con una estructura físicamente visible debido a su naturaleza virtual, es decir, intangible.

Otro de los aspectos a destacar es el de la convivencia ya que mientras en el mundo real se tiene la certeza de la identidad de las personas en el mundo digital se complica conocer la del otro. Eso se debe a que las interacciones en la realidad se llevan a cabo cara a cara y en la virtualidad con el apoyo de un intermediario digital.

Aún con esas diferencias antes descritas existen ciertas similitudes, por ejemplo, tanto en el mundo tangible como en el intangible se han estado realizando actividades lícitas e ilícitas. No obstante, las leyes que pueden ser aplicables en un ambiente material resulta complicado ejecutarlas en uno inmaterial por las siguientes razones.

---

[137] Laura Coronado Contreras, *La regulación global del ciberespacio*, México, Editorial Porrúa/Universidad Anáhuac, 2017, p. 123.

En primer lugar, la naturaleza virtual y global del ciberespacio dificulta la imposición de delimitaciones territoriales por parte de las entidades gubernamentales. Especialmente por la disparidad en las legislaciones de los Estados que les impide implementar una regulación global al surgir dudas como ¿quién o quiénes lo van a regular? ¿cómo lo van a hacer? y ¿a partir de dónde?

En segundo lugar, cuando se habla de ese dominio sólo se hace referencia a la parte visible y no a la parte oculta o, como se le ha denominado, "profunda". Técnicamente, lo que se conoce como Internet puede dividirse en internet superficial e internet profundo;[138] el primero es aquel donde cualquier usuario común puede tener acceso y el segundo donde se requiere de conocimientos especializados para entrar.

En la parte visible de internet, o lo que Google ve, se encuentran las páginas web de acceso generalizado como buscadores, redes sociales, etc. En la parte invisible, o lo que Google no ve, se haya todo el contenido encriptado, es decir, oculto para los usuarios comunes y cuyo acceso sólo es posible mediante el uso de programas especiales.[139]

A la "parte oscura" de la red se le ha dado el nombre de *Internet profunda* o *Deep Web* haciendo referencia a todo el contenido, tanto lícito como ilícito, que no se muestra en los motores de búsqueda convencionales como Google. Su origen es militar y fue creado por el laboratorio de Investigación Naval de Estados Unidos con la finalidad de lograr el anonimato total.[140]

Cabe señalar que gran parte de los productos y servicios que se ofrecen en la *Deep Web* son considerados ilegales por la mayoría de las legislaciones. Entre algunas de las actividades que se llevan a cabo en ese sitio se encuentran los ya citados "cuatro jinetes del info-apocalipsis" a los cuales se les puede añadir la trata de personas y el tráfico de órganos.

---

[138] Pere Cervantes y Oliver Tauste, *Internet negro: el lado oscuro de la red*, México, Paidós, 2016, pp. 223-224.
[139] *Ibid.*, pp. 23-24.
[140] *Ibid.*, p. 223.

De cierta forma, la internet profunda ha tomado el papel de un mercado negro digital al que pueden acudir individuos de cualquier parte del mundo ya sea para adquirir o para ofrecer artículos o actividades ilícitas. Los pilares técnicos que la conforman son los programas PGP (*Pretty Good Privacy*), las monedas virtuales, los sistemas de reputación y el *Escrow* o depósito fiduciario.[141]

El mercado negro virtual, al igual que su versión física, representa un peligro para el desarrollo nacional. Políticamente, se presenta como un lugar sin leyes aplicables por sus características técnicas; económicamente, se utiliza dinero sin algún control o respaldo institucional público o privado; socialmente, se distribuye y se promueve material perjudicial para la sociedad.

En ese sentido, por ser una condición tecnológica que pone en riesgo al desarrollo nacional y, por ende, a la seguridad de la nación, la internet profunda se presenta como riesgo cibernético. Además, es una dimensión externa ya que al no estar sujeta a la soberanía de país alguno puede hacerse proclive a la participación de entidades internacionales.

De igual manera, se le considera un antagonismo a la seguridad de la nación mexicana toda vez que sus dimensiones técnicas le permiten albergar un gran número de participantes entre los cuales pueden encontrarse algunas amenazas. De acuerdo con algunas estimaciones, el tamaño del internet profundo es seiscientas veces mayor al internet superficial.[142]

Si bien, aunque desde su creación la internet ha actuado "como un lienzo sobre el cual hemos pintado imágenes negativas y positivas"[143] no por ello deben descartarse sus aportaciones. Como se ha mencionado con anterioridad, todo aquello relacionado con las tecnologías de la información y comunicación puede utilizarse con un doble propósito.

---

[141] *Ibid.*, pp. 227-231.

[142] Antonio Castañeda Solís, "La Deep web y el anonimato en el ciberespacio", *Seguridad y defensa en el ciberespacio*, México, SEMAR-CESNAV, 2015, p. 25.

[143] Jamie Bartlett, *La red oculta: ciberterrorismo, pornografía infantil, mercado del asesinato y demás ilícitos en Internet*, México, Paidós, 2017, p. 17.

3.1.2.2 Carrera ciberarmamentista

En el periodo comprendido de 1947 a 1991, durante el transcurso del conflicto político-ideológico entre los bloques occidental y oriental conocido como Guerra Fría, uno de los peligros latentes para ambos bandos era la carrera armamentista. Ésta consistió fundamentalmente en el desarrollo, innovación, perfeccionamiento e incremento de las capacidades bélicas ofensivas y defensivas de un Estado o Alianza de Estados como la OTAN y el Pacto de Varsovia.

La particularidad del fenómeno científico-tecnológico radicaba en la extensión que se le estaba dando progresivamente hacia otros ámbitos fuera de los sistemas de armamento convencional. El mayor ejemplo se encuentra en el surgimiento de las denominadas armas de destrucción masiva cuyos máximos exponentes han sido catalogados como armamento nuclear, radiológico, biológico y químico.[144]

Algunas de las características de esa clase de armamento es que su uso no está dirigido hacia un objetivo específico por lo que puede tener efectos devastadores sobre las personas, en la infraestructura, así como en el medio ambiente.[145] Por ese motivo, su desarrollo por parte de los Estados implica un riesgo para la seguridad de las naciones toda vez que su utilización puede llevar a una destrucción mutua asegurada.

Ante esa situación cabría preguntarse si las tecnologías de la información y comunicación, así como los elementos derivados de ellas pueden ser utilizados con finalidades bélicas. Por ello, resulta necesario analizar el tratamiento que se les ha dado por parte de agentes estatales y no estatales en el transcurso del nuevo milenio con la finalidad de determinar sus posibles efectos destructivos.

---

[144] Lillian Ablon, *et al.*, *op. cit*.

[145] Ramón García Gibson, “Armas de destrucción masiva”, [en línea], México, *Forbes.com.mx*, 2 de septiembre de 2013, Dirección URL: https://www.forbes.com.mx/armas-de-destruccion-masiva/, [consulta: 30 de junio de 2021].

Para comenzar, tanto la internet superficial como la profunda fueron creadas a partir de necesidades militares. La primera tiene sus orígenes en el año 1969 con la creación de la *Red de la Agencia de Proyectos de Investigación Avanzada* por encargo del Departamento de Defensa de Estados Unidos; la segunda se remonta al año 1994 con la creación de la *Invisible Web* por encargo del laboratorio de Investigación Naval del mismo país.[146] [147]

A causa del contexto histórico-político en el cual fueron concebidas se diría que toda la internet ha sido un producto derivado de la carrera armamentista del siglo XX. Por ese motivo no se descarta que siga manteniendo ese mismo curso en los albores del siglo XXI ante la inminente necesidad por parte de algunos Estados de mantenerse a la vanguardia bélica, sobre todo en aquellos donde persisten conflictos externos e internos.

Otra de las causas que lleva a pensar en el inicio de una carrera ciberarmamentista en el nuevo milenio ha sido el carácter castrense que se le ha dado al ciberdominio. Organismos militares internacionales como la Organización del Tratado del Atlántico Norte (OTAN) lo han reconocido como uno de sus ámbitos operacionales lo que ha generado que sus miembros integrantes hayan comenzado a desarrollar capacidades cibernéticas.[148]

Desde el punto de vista de Karl Greenfield "la carrera cibernética no consiste sólo en herramientas, sino también en estrategias para espiar, censurar y ganar fuerza en el ciberespacio".[149] Para otros autores como Rob Pritchard las capacidades cibernéticas desarrolladas por los Estados pueden dividirse en ofensivas y defensivas según el propósito.

---

[146] Internet Society, *Breve historia de internet*, [en línea], Dirección URL: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/, [consulta: 30 de junio de 2021].

[147] Pere Cervantes y Oliver Tauste, *op. cit.*, p. 223.

[148] Lillian Ablon, *et al.*, *op. cit*.

[149] Lucía Blasco, "¿Cuáles son los países que tienen más armas cibernéticas", [en línea], *bbc.com*, 31 de julio de 2017, Dirección URL: https://www.bbc.com/mundo/noticias-40631138, [consulta: 30 de junio de 2021].

Por una parte, las capacidades ofensivas pueden ser realizadas tanto por gobiernos como por delincuentes; dentro de ellas se encuentran la vigilancia electrónica, las acciones de hackeo, así como el uso de malware. Por otro, las capacidades defensivas son las que pueden llevar a cabo los sectores público, privado y social; en ellas se encuentran las estrategias de ciberseguridad, así como la formación de cuerpos especializados.[150]

Uno de los casos que ha demostrado la capacidad destructiva que han adquirido los programas informáticos sofisticados es el de *Stuxnet*, considerado la primera ciberarma en el mundo. Ese malware fue responsable en el 2010 de dañar la central y el complejo nucleares de Irán, el cual fue presuntamente creado por el gobierno estadounidense en colaboración con el israelí debido a la complejidad de su elaboración.[151] Algunas de las características que se pueden citar son:

- No requieren proximidad física del atacante a la víctima
- Son fáciles de ocultar
- Pueden ser difíciles de atribuir al atacante (estatal o no estatal)
- Requieren fallas en su víctima o no funcionan en absoluto
- Son considerablemente más variadas que las municiones convencionales
- Tienden a tener consecuencias inesperadas
- No tienen usos legítimos[152]

Por lo tanto, la carrera ciberarmamentista se presenta como riesgo cibernético externo al presentarse como una condición del entorno internacional que incide en la seguridad de la nación. Sobre todo, porque las ciberarmas han demostrado tener la misma o una mayor capacidad de impacto que el armamento convencional afectando tanto a la integridad territorial como a la estabilidad interna.

---

[150] *Ídem*.

[151] Sal Emergui, “Israel y EEUU crearon el virus que dañó el programa nuclear iraní”, [en línea], *elmundo.es*, 16 de enero de 2011, Dirección URL: https://www.elmundo.es/elmundo/2011/01/16/internacional/1295180388.html, [consulta: 30 de junio de 2021].

[152] Anahiby Becerril Gil, “La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio”, *Revista de Administración Pública*, núm. 1, vol. 54, México, Instituto Nacional de Administración Pública A.C., enero-abril, 2019, p. 129.

3.2 Amenazas cibernéticas

En cuanto a la clasificación de amenazas a la seguridad nacional mexicana se refiere, la Ley de Seguridad Nacional ha sido el documento en el que se han plasmado algunas disposiciones. Desde su publicación en el Diario Oficial de la Federación en el 2005 hasta el momento del presente trabajo (2020) ha reconocido un total de trece antagonismos. Todos hacen referencia a las acciones que pueden ejecutar agentes estatales y no estatales.

No obstante, uno de los mayores problemas es que ninguno de los puntos establecidos especifica las entidades que pueden generarlas, así como la dimensión de la seguridad nacional a la que pertenecen: económica, alimentaria, tecnológica, ambiental, societal o humana.[153] La falta de precisión temática en el listado impide atribuir responsabilidades políticas, así como competencias institucionales con respecto al ámbito de aplicación.

Uno de los primeros acercamientos al establecimiento de una tipificación de amenazas cibernéticas fue mostrado en el 2019 en una iniciativa de decreto promovida por la senadora de Morena por Baja California Jesús Lucía Trasviña Waldenrath por la cual se buscaba, entre otras cosas, expedir una Ley de Seguridad Informática. De acuerdo con la iniciativa propuesta, se considerará como amenazas a la Seguridad Informática:

I. Cuando se tenga acceso deliberado e ilegítimo dentro de un sistema informático, con la intención de obtener datos personales.
II. La interceptación deliberada e ilegítima a través de medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas y un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informáticos que sirva como medio de transporte de dichos datos informáticos.

[153] Diario Oficial de la Federación, *Programa para la Seguridad Nacional 2014-2018*.

III. Actos tendientes a consumar espionaje, sabotajes, terrorismo, rebelión, traición a la patria, a través del ciberespacio;

IV. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación a los activos de información, así como a los activos de las Tecnologías de Información y la Comunicación;

V. Actos que impidan a las autoridades actuar contra la ciberdelincuencia;

VI. Actos que tiendan a dar usos indebidos a los datos informáticos y personales, así como los relativos al tráfico en un sistema informático o dentro del internet;

VII. Actos tendientes para obstaculizar o bloquear actividades de inteligencia o contrainteligencia dentro de la ciberdefensa, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos;

VIII. Actos tendientes para destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos a través de internet.

IX. Actos deliberados e ilegítimos que dañen, borren, deterioren, alteren o supriman datos informáticos, contenidos dentro de los sistemas informáticos del Estado y particulares.

X. La producción, venta, obtención para su utilización, importación, difusión u otra forma de las Tecnologías de Operación, en atención a los derechos de autor vigentes en la materia.[154]

Si bien, aunque la iniciativa expone de forma específica cada uno de los peligros derivados de las tecnologías de la información y comunicación sólo se enfoca en el entorno de la Seguridad Informática relegando todos los aspectos tecnológicos y humanos que involucra la Ciberseguridad Nacional. Asimismo, toma como referente legal el Código Penal Federal en lugar del Programa para la Seguridad Nacional o inclusive la propia Ley de Seguridad Nacional.

[154] Jesús Lucía Trasviña Waldenrath, *Iniciativa con Proyecto de Decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se Expide la Ley de Seguridad Informática*, [en línea], 25 pp., México, 27 de marzo de 2019, Dirección URL: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf, [consulta: 30 de junio de 2021].

Por ese motivo, para la creación de una clasificación de amenazas cibernéticas a la seguridad nacional mexicana adecuada al presente trabajo se tomarán los mismos aspectos que en el apartado de Riesgos cibernéticos. Es necesario recalcar que se les dará esa denominación por estar asociados con el entorno de las Tecnologías de la Información y Comunicación con la finalidad de diferenciarlos de las otras dimensiones.

Además, se retomarán las características antes referidas que conforman a las amenazas para vincularlas con las situaciones más recurrentes en materia tecnológica que han tenido incidencia directa en los sectores del desarrollo nacional. Asimismo, para establecer los que puedan generar perjuicio en contra de la integridad, estabilidad y permanencia del Estado mexicano. Con respecto a las amenazas, se determinaron las siguientes características:

- Son actos generados por otro Estado o por entidades no estatales las cuales pueden actuar colectiva o individualmente.
- Se pueden dividir en tradicionales y emergentes donde las primeras son aquellas que han prevalecido independientemente de las circunstancias del contexto y las segundas son las que han surgido de situaciones específicas del entorno.
- Afectan total o parcialmente a las aspiraciones, objetivos e intereses nacionales.

A partir de esas atribuciones se dirá que son acciones realizadas por agentes identificables entendidos como gobiernos, empresas y sociedades. De igual manera, pueden llevarse a cabo individual o colectivamente entendiendo la participación de una sola entidad o de un conjunto de las mencionadas.

Por otra parte, la división establecida se realizará en Amenazas Tradicionales y Emergentes. Las primeras serán aquellos comportamientos hostiles que han prevalecido en el transcurso de la historia y sólo se han trasladado al entorno cibernético; las segundas serán aquellas acciones resultantes de comportamientos inesperados cuya presencia ha sido reciente.

3.2.1 Tradicionales

3.2.1.1 Ciberdelincuencia

Desde el punto de vista de Steven Angerthal, las Organizaciones Criminales Trasnacionales (OCT) “actualmente representan la mayor amenaza para la seguridad nacional que encara el Estado mexicano y lo seguirá siendo en el futuro previsible”.[155] Eso se debe primordialmente a la progresiva dimensión operativa que han adquirido no sólo en cuestiones geográficas de tipo nacional e internacional sino en cuanto a la clase de actividades realizadas.

De igual manera, los Programas para la Seguridad Nacional de los periodos 2009-2012 y 2014-2018 ponen a la delincuencia organizada como la principal amenaza al Estado mexicano. Ambos documentos determinaron que esa problemática ha dejado de ser competencia de la seguridad pública para pasar a la seguridad nacional en cuanto a las capacidades adquiridas para vulnerar la soberanía y el orden constitucional.

La causa fundamental de colocarla en el rango de asunto de Estado se debe a que su presencia en el entorno ha impedido en mayor o menor medida la gobernabilidad de la nación. Especialmente, ha incidido en cada uno de los órdenes de gobierno: federal, estatal y municipal de las instituciones responsables de la seguridad y procuración de justicia a través de la cooptación de sus miembros.

Cabe destacar que cuando se hace referencia a la delincuencia organizada no sólo se alude al narcotráfico sino a las diferentes actividades sancionadas por las diversas legislaciones internacionales y nacionales. Esas disposiciones se encuentran en el caso mexicano en la *Ley Federal contra la Delincuencia Organizada*.

[155] Steven Argenthal, “El futuro de la seguridad nacional”, *La seguridad nacional integral de México: diagnósticos y propuestas*, México, SEMAR-CESNAV, 2013, p. 317.

Con el surgimiento de las nuevas tecnologías digitales, parte o gran parte de las actividades ilícitas han pasado a realizarse en el mundo virtual conformando una dimensión distinta que les ha dado el nombre de Ciberdelincuencia Organizada. Con base en el tratado internacional denominado *Convenio sobre Ciberdelincuencia* de 2001, elaborado por el Consejo de Europa, ese fenómeno tecnológico se divide en los siguientes cuatro apartados:

I. Ofensas contra la confidencialidad, integridad, y disponibilidad de datos y sistemas informáticos (hackeo, phishing, espionaje, intercepción, DoS).
II. Ofensas relativas a los contenidos (pornografía infantil, extremismo, apuestas, spam);
III. Ofensas mediante el uso de computadoras (fraude, falsificación, robo de identidad), y
IV. Ofensas contra los derechos de autor y la propiedad intelectual (piratería).[156]

Al igual que su contraparte del mundo real, la ciberdelincuencia organizada ha alcanzado un rango similar como asunto de Estado toda vez que su presencia global y local ha tenido incidencias a gran escala. La más significativa se ha presentado en lo económico ya que le ha costado al mundo un aproximado de 600 mil millones de dólares al año a comparación de los 3 mil millones de dólares que le cuesta a México en cuestión de daños informáticos.[157]

En cierto sentido, se diría que tanto la delincuencia como su contraparte cibernética han tenido una motivación sustancialmente económica ya que tiene como principal objetivo la obtención ilegal de recursos monetarios. Dentro de las operaciones que se han llevado a cabo mediante las TIC se encuentran desde las más simples como las extorsiones telefónicas hasta las más complejas como el lavado de dinero y los fraudes electrónicos.[158]

---

[156] Edgar Iván Espinosa, *op. cit.*, p. 123.
[157] James Lewis, "Economic Impact of Cybercrime – No Slowing Down", [en línea], Dirección URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf, [consulta: 30 de junio de 2021].
[158] Elma del Carmen Trejo García, *et al.*, *Regulación Jurídica de Internet*, México, Centro de Documentación, Información y Análisis-Cámara de Diputados, 2006, pp. 22-26.

Sin embargo, sus motivaciones no sólo han sido económicas sino inclusive políticas y sociales. Si bien, a pesar de que gran parte de las afectaciones han sido dirigidas en contra del apartado financiero de los sectores público y privado, también han resultado perjudicados los integrantes del sector social. El ejemplo más claro de esa situación se ha visto reflejado en la difusión de pornografía infantil la cual ha generado anualmente un aproximado de 34 mil millones de dólares.[159]

En cuanto al apartado político, el peligro más grande que ha representado ha sido con respecto a su estructura organizacional ya que las tecnologías de la información y comunicación le han permitido pasar de una relación jerárquica formal a un fluido sistema en red. Esa configuración les ha permitido a esos grupos ser "simultáneamente omnipresentes e intangibles, ubicuos e invisibles, están en todas partes y en ninguno".[160]

Al estar estructuradas en forma de red, significa que sus integrantes (nodos) pueden ser desde simples individuos hasta empresas y compañías de más de un país por lo que sus acciones difícilmente pueden ser rastreadas. De igual forma, es importante destacar que el ámbito operacional de la ciberdelincuencia organizada se encuentra tanto en el internet superficial como en el internet profundo, en mayor medida en el segundo que en el primero por sus propiedades anónimas.

Por lo tanto, la ciberdelincuencia organizada se considera una amenaza cibernética a la seguridad nacional mexicana toda vez que sus acciones y motivaciones han sido las más reiteradas y las de mayor impacto para la estabilidad interna en el presente siglo. Además, se le considera tradicional por estar asociada a un comportamiento que ha sido continuamente atendido por los Estados la cual sólo ha cambiado el plano de operaciones de uno real a uno digital.

---

[159] s/a, "México ocupa primer lugar mundial en difusión de pornografía infantil", [en línea], México, *elsoldemexico.com.mx*, 21 de agosto de 2017, Dirección URL: https://www.elsoldemexico.com.mx/mexico/sociedad/mexico-ocupa-primer-lugar-mundial-en-difusion-de-pornografia-infantil-242048.html#, [consulta: 30 de junio de 2021].

[160] Phil Williams, "Redes trasnacionales de delincuencia", *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el hacktivismo*, Madrid, Alianza Editorial, 2003, pp. 91-93.

3.2.1.2 Ciberguerra

La guerra, en tanto conflicto armado, ha evolucionado a lo largo de los años desde sus fines hasta sus medios. Lo único que ha conservado a pesar de las distintas transformaciones han sido sus motivaciones bélicas, económicas y políticas donde las primeras siempre han estado, y estarán, subordinadas a las segundas al grado de decir que "la guerra no es sólo un acto político, sino un verdadero instrumento político, una ejecución del mismo por otros medios".[161]

La definición más acertada de ese fenómeno político-militar ha sido la establecida en el Libro I del tratado *De la guerra* como "un acto de violencia para obligar al contrario a hacer nuestra voluntad".[162] La violencia requerida para llevar a cabo ese acto "se arma con los inventos de las artes y las ciencias"[163] ya que es el medio para lograr el fin que resulta en imponer al enemigo nuestra voluntad. Algunos de los rasgos comunes que las han caracterizado a todas son:

- Coexistencia de grupos incompatibles
- Existencia de posturas polarizadas
- Sometimiento o destrucción del otro
- Provocar daño al otro
- Están organizadas e institucionalizadas
- Tienen reglas propias
- Implican gran parte de la sociedad[164]

Además, se debe agregar que las formas de la guerra han cambiado en función del contexto político presente. Para autores como Lind, Nighengale, Schmitt, Sutton y Wilson los tipos de guerra se pueden dividir por generaciones; para D.J. Hanle esa clasificación se lleva a cabo por las habilidades predominantes de cada era y para Alvin Toffler por olas productivas.

---

[161] Carl von Clausewitz, *op. cit.*, p. 31.
[162] *Ibid.*, p. 17.
[163] *Ídem*.
[164] Miguel del Nogal Tomé, *Guerra psicológica*, México, Alfaomega Grupo Editor, 2016, p. 23.

Para los primeros la guerra se divide en primera generación o clásica, segunda generación o industrial de bajas, tercera generación o de maniobras y cuarta generación o no convencional. El segundo la entiende en era medieval (físicas), era neoclásica (organizacionales), principios de la era moderna (técnicas), finales de la era moderna (administrativas) y era nuclear (sociales). Para el último, en primera ola agraria, segunda ola industrial y tercera ola de información.[165]

De acuerdo con esas preposiciones, la ciberguerra como dimensión tecnológica de la guerra se inscribiría, por una parte, en la cuarta generación ya que se libra en un ambiente (ciberespacio) y mediante instrumentos (ciberarmas) distintos a los convencionales; por otra, se establecería en la era nuclear por las habilidades de la sociedad de la información y el conocimiento. Por último, se asentaría en la tercera ola por estar asociada con las tecnologías digitales.

En ese sentido, se diría que la guerra cibernética antes que ser una problemática de índole tecnológica resulta ser una de naturaleza política toda vez que conserva sus principios, medios y finalidades bélicas. Sobre todo, porque mantiene su objetivo de funcionar como enlace entre dos entidades opuestas donde una busca someter a otra a partir de la fuerza.

Una de las situaciones más graves a nivel internacional es que en la actualidad nadie está a salvo de la ciberguerra debido a la continua inmersión tecnológica que han tenido todos los países del globo. Casos como los de Kosovo (1999), Taiwán (2003), Estonia (2007), Georgia (2008), Irán (2010), Canadá (2011), Medio Oriente (2012) y Estados Unidos (2013) sólo son algunos de los ejemplos que mayor relevancia han tenido en el presente siglo.[166]

---

[165] Manuel Ignacio Balcázar Villarreal, “Inteligencia de fuentes abiertas: cómo implementar la mejor opción para las agencias gubernamentales en la era de las redes sociales”, *Inteligencia estratégica en el contexto mexicano*, México, Plaza y Valdés Editores/Instituto Tecnológico de Estudios Superiores de Monterrey, 2012, pp. 93-96.

[166] Rosa Jiménez Cano, “Nadie está a salvo de esta ciberguerra”, [en línea], *elpais.com*, 10 de diciembre de 2010, Dirección URL: https://elpais.com/diario/2010/12/10/sociedad/1291935601_850215.html, [consulta: 30 de junio de 2021].

Uno de los aspectos a destacar es que el ciberespacio se está transformando en "un escenario estratégico, operacional y táctico"[167] para los próximos conflictos interestatales. Ejemplos de ello han sido el reconocimiento internacional de ese entorno como "el quinto dominio de la guerra",[168] la creación de grupos operativos militares especializados en el entorno[169], así como de programas y dispositivos con capacidades destructivas similares al armamento convencional, como los drones.

Si bien, aunque México todavía no ha sido víctima de una agresión de esa naturaleza no se descarta el hecho de que en el futuro próximo resulte perjudicada debido a su posicionamiento geopolítico con Estados Unidos y Canadá, a su creciente dependencia en las TIC por parte de los sectores público, privado y social, así como la falta de medidas preventivas y reactivas. Por ello se presenta como un peligro potencial en el nuevo milenio.

En suma, la ciberguerra se considera como amenaza cibernética toda vez que forma parte de una acción que puede ser llevada a cabo por Estados ya sea sólo por uno o por todo un conjunto de ellos. De igual manera, porque "es una forma de guerra que interrumpe, sino destruye, los sistemas de información y comunicaciones"[170] del país, especialmente las infraestructuras críticas de información y las de información esencial que contribuyen al desarrollo nacional.

Por último, se atribuye como tradicional debido a que "desde que el hombre es hombre ha habido guerras, y a menos que el género humano se trastocase en divino es indudable que el fenómeno bélico seguirá existiendo entre los pueblos".[171] Por lo cual, mientras exista la necesidad de imponer la voluntad de uno sobre el otro a través de la violencia la guerra se mantendrá vigente y se llevará a cabo por los mecanismos existentes.

---

[167] Milena Elizabeth Realpe Díaz y Jorge Darwin Guevara Guerrero, "La ciberguerra, una amenaza a la seguridad y defensa nacional", *Seguridad y defensa en el ciberespacio*, México, SEMAR-CESNAV, 2015, p. 296.

[168] *Ibid.*, p. 295.

[169] El caso más significativo es el del Cibercomando de Estados Unidos perteneciente al Departamento de la Defensa creado el 23 de junio de 2009.

[170] Anahiby Becerril Gil, *op. cit.*, p. 133.

[171] Patricio Marcos, *Lecciones de política*, Editorial Nueva Imagen, México, 1990, p. 148.

3.2.1.3 Ciberespionaje

El espionaje, al igual que la guerra, ha sufrido transformaciones en el transcurso del tiempo, particularmente en la forma de llevarlo a cabo por los Estados debido a la mutabilidad de los contextos político y tecnológico. Sin embargo, a diferencia del conflicto bélico cuya motivación es principalmente política, en el espionaje puede ser de varias clases: militar, político, económico, ideológico e industrial de acuerdo con el objetivo establecido.[172]

De manera general, esa acción puede ser definida como "acechar, observar disimuladamente lo que se hace o se dice"[173] y puede ser realizada a través de los medios materiales y humanos disponibles. Es posible rastrear sus orígenes desde la antigüedad al estar vinculada con los de la guerra y, por ende, con los de las primeras comunidades políticas ante su necesidad por saber "lo que hay detrás de la colina", es decir, todo lo referente al enemigo.[174]

La relación entre una y otra se debe a que, como menciona Sun Tzu en el Capítulo 13 de *El arte de la guerra*, "es precisamente conociendo con anticipación como cualquier señor inteligente y cualquier general sabio podrían vencer en toda acción y obtener egregios logros".[175] Y ese entendimiento previo del contrincante sólo es posible mediante la obtención de información producto del espionaje.

En cierto sentido, se puede describir como una actividad cuyo objetivo ha sido desde siempre el conocimiento previo de las fortalezas y debilidades de una entidad tenida como contraria a los intereses propios. No obstante, la característica que la ha diferenciado de cualquier otra es su naturaleza secreta y encubierta ya que quienes la ejercen lo hacen con la finalidad de evitar alertar al adversario.

---

[172] Domingo Pastor Petit, *Diccionario del espionaje*, Plaza y Janes, S.A. Editores, Barcelona, 1971, p. 83.
[173] *Ídem*.
[174] Juan Carlos Herrera Hermosilla, *Breve historia del espionaje*, Ediciones Nowtilus, Madrid, 2012, p. 13.
[175] Sun Tzu, *op. cit.*, p. 138.

En el contexto del siglo XXI, una de las problemáticas con respecto al espionaje ha sido su relación con la inteligencia ya que tanto en la teoría como en la práctica han sido utilizados como sinónimos. Aunque ambas comparten un carácter confidencial se diferencian en que el primero se reconoce como amenaza y la segunda se considera como medio para procurar al Estado y se define como:

> Información especializada que tiene como propósito aportar insumos a los procesos de toma de decisiones relacionados con el diseño y ejecución de la estrategia, las políticas y las acciones en materia de Seguridad Nacional.[176]

De igual manera, la inteligencia es considerada en tanto proceso (ciclo de inteligencia) y como institución (servicio de inteligencia). Mientras que el primero es una serie que se compone de cinco etapas: planeación, recolección, procesamiento y análisis, difusión y explotación, así como retroalimentación[177] el segundo tiene como atribución operar el sistema de inteligencia para la seguridad nacional.

En el panorama actual, la seguridad de los datos e información se vuelve un asunto de Estado ya que tanto las actividades de inteligencia como de espionaje de todos los países han pasado a desarrollarse en la virtualidad. Sobre todo, porque los sistemas informativos y las redes de telecomunicaciones "a diferencia de la electricidad no transmiten una corriente inerte, sino información, es decir, poder".[178]

Sin embargo, aunque la información genera cierto tipo de poder, no toda promueve el mismo tipo de poder; más bien se diría que la información conduce al conocimiento y mediante un uso adecuado puede lograr poder.[179] Por lo cual, resulta fundamental para la nación proteger aquella que pueda ser vital para sus intereses ya que será la más vulnerable ante actos de ciberespionaje.

---

[176] Centro Nacional de Inteligencia, "¿Qué es la inteligencia?", [en línea], México, 18 de febrero de 2020, Dirección URL: https://www.gob.mx/cni/documentos/que-es-la-inteligencia, [consulta: 30 de junio de 2021].
[177] Centro Nacional de Inteligencia, "Ciclo de inteligencia", [en línea], México, 18 de febrero de 2020, Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/535136/Ciclo_Inteligencia.pdf, [consulta: 30 de junio de 2021].
[178] Simon Nora y Alain Minc, *op. cit.*, p. 18.
[179] Emilio Vizarretea Rosales, *op. cit.*, p. 52.

En ese sentido, el ciberespionaje como vertiente tecnológica del espionaje, resulta un peligro toda vez que tanto en la realidad como en la virtualidad conserva sus características y motivaciones. En el caso mexicano algunas de ellas se dieron en el contexto de las filtraciones masivas realizadas por Assange y Snowden donde evidenciaban la injerencia de Estados Unidos mediante sus agencias.

En el nuevo milenio es posible mencionar dos de esas operaciones efectuadas por el vecino del norte: *Whitetamale* y *Flatliquid*. La primera corresponde a la intrusión en los sistemas y comunicaciones de varios funcionarios de la entonces Secretaría de Seguridad Pública en el 2009. En la segunda se logró sustraer del correo del entonces presidente de México Felipe Calderón Hinojosa alrededor de 260 documentos en el 2010.[180]

Aunque el espionaje cibernético pudiera parecer de los antagonismos menos agresivos, lo cierto es que se presenta como el de mayores consecuencias políticas. Por una parte, se demuestra que instituciones clave como la Presidencia de la República pueden ser vulneradas; por otra, la información sustraída puede ser utilizada tanto por agencias extranjeras como por grupos delincuenciales internos con fines perjudiciales para los intereses nacionales.

Por esos motivos, el ciberespionaje se considera amenaza cibernética a la seguridad nacional mexicana en el sentido que es un acto que puede ser generado por agentes estatales a través de instituciones de inteligencia militares y civiles o por agentes no estatales mediante el uso de programas conocidos como spyware. La mayor amenaza se presenta en cuanto puede ser robada información de carácter confidencial por su valor estratégico.

Por último, se le considera una amenaza tradicional por la antigüedad de su ejecución ya que no es posible entender el ciberespionaje sin el espionaje. Siempre que exista la necesidad por parte de cualquier comunidad por saber “lo que hay detrás de la colina” será necesario llevar a cabo la recolección de información por cualquier medio físico o electrónico.

[180] Edgar Iván Espinosa, *op. cit.*, p. 126.

3.2.2 Emergentes

3.2.2.1 Ciberterrorismo

A partir del 11 de septiembre de 2001 el panorama de la seguridad internacional en el siglo XXI cambiaría radicalmente a raíz de los atentados efectuados en contra del complejo de edificios comerciales *World Trade Center*, así como sobre la sede del Departamento de la Defensa de los Estados Unidos *El Pentágono*. El resultado más significativo de ese hecho sería la conformación de una nueva amenaza de carácter global: el terrorismo.[181]

A pesar de haber sido reconocida en tanto amenaza a la seguridad de las naciones en el nuevo milenio, todavía no existe una definición que sea aceptada internacionalmente, lo cual se debe en parte a las motivaciones políticas y económicas que lo rodean. Sin embargo, algunas legislaciones nacionales han determinado ciertas características que lo configuran, por ejemplo, en el artículo 139 del Código Penal Federal donde lo estipula como:

> A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos, o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, intencionalmente realice actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.[182]

[181] María Cristina Rosas, "Seguridad pública y seguridad nacional en México: los desafíos" en *La seguridad internacional en el siglo XXI: retos y oportunidades para México*, UNAM-FCPYS, México, 2010, p. 35.
[182] Cámara de Diputados, *Código Penal Federal*.

El efecto más notable de esa problemática con respecto a la seguridad de los Estados ha sido la modificación que ha ejercido sobre el paradigma de seguridad en sus cinco niveles: internacional, hemisférica, regional, binacional y nacional.[183] Sobre todo porque sus implicaciones han logrado "traspasar fronteras" geográficas tanto físicas como virtuales, lo cual les ha permitido trasladarse al mundo digital recibiendo el nombre de Ciberterrorismo.

De manera general, el ciberterrorismo puede entenderse como la convergencia entre el ciberespacio y el terrorismo.[184] En ese sentido, se diría que son las acciones anteriormente estipuladas en la legislación vigente con la única diferencia que son realizadas mediante las tecnologías de la información y comunicación, especialmente de la internet ya que a través de ella los grupos terroristas pueden tener una mayor comunicación entre sí.

Si bien, todavía "no existen pruebas concretas de que los terroristas estén preparados para utilizar Internet como medio para provocar graves daños"[185] no se debe descartar el hecho de que progresivamente diversos bienes y servicios están haciendo uso de la red, especialmente los servicios financieros.[186] Para México, ese hecho implica una vulnerabilidad que puede ser aprovechada por grupos de esa índole con la finalidad de conseguir algún objetivo político.

Por lo tanto, el Ciberterrorismo se considera una amenaza cibernética a la seguridad nacional ya que corresponde a un acto que puede ser ejercido principalmente por entidades extranjeras. De igual manera, sus acciones representan un peligro en el sentido que tienen incidencias perjudiciales sobre los medios necesarios para el desarrollo nacional. Por último, es emergente porque tanto su parte física como virtual han sido resultado de una situación inesperada.

---

[183] Manuel Ignacio Balcázar Villareal, *op. cit.*, p. 91.
[184] Dorothy E. Denning, "Activismo, hacktivismo y ciberterrorismo: Internet como instrumento de influencia en la política exterior", *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*, Madrid, Alianza Editorial, 2003, pp. 302-303.
[185] *Ibid.*, p. 305.
[186] Adolfo Arreola García, *op. cit.*, p. 10.

3.2.2.2 Hacktivismo

El 8 de enero de 1986 el informático Loyd Blankeship publicó el *Manifiesto hacker* el cual pretendía ser una guía para los hackers en el que justifica el uso de la tecnología para la libertad. Por otra parte, el 8 de febrero de 1996 el activista John Perry Barlow presentó la *Declaración de independencia del ciberespacio* en el que defendía, entre otras cosas, la invalidación de cualquier término legal de propiedad, expresión, identidad, etc., en ese sitio.[187]

Ambos documentos, con diez años de distancia uno del otro, sentarían las bases de una de las mayores dificultades para la ciberseguridad de las naciones: el hacktivismo. El hacktivismo (acrónimo de *hacker* y *activismo*) hace referencia a dos situaciones propias del siglo XXI; mientras que la primera alude a los individuos con conocimientos técnicos en las tecnologías digitales la segunda describe una forma de organización y manifestación social.

De cierta forma, el hacktivismo se describiría como una acción social organizada de libre manifestación mediante las tecnologías digitales como lo afirmaban sus ideólogos. Sin embargo, en el fondo se ha presentado mediante acciones directas encaminadas a generar presión social sobre alguna entidad. Muestra de ese comportamiento ha sido el incremento en el uso de las redes sociales como medios digitales de comunicación y también de coerción.[188]

De acuerdo con Dorothy E. Denning, el hacktivismo se puede definir como "la unión de la 'piratería electrónica' (hacking) con el activismo".[189] Para ella, esa actitud es básicamente una especie de desobediencia civil electrónica la cual sólo traslada los medios utilizados en el mundo real para ejercerlos en el digital dividiéndolas en cuatro tipos de actividades:

[187] John Perry Barlow, *op. cit*.
[188] Gonzalo Monterrosa, *op. cit*.
[189] Dorothy E. Denning, *op. cit.*, p. 286.

- Sentadas y bloqueos virtuales;
- Bombas de correo electrónico automatizadas;
- Sabotajes a la web y allanamiento informático, y
- Virus y gusanos informáticos.

Con las primeras se busca bloquear el acceso a páginas web a través de la saturación del sitio; con las segundas se trata de impedir el uso del correo electrónico; con los terceros se desea la eliminación de sitios completos de internet, así como el robo de la información contenida y con los últimos se pretende causar daños a los sistemas informáticos.[190] Esas circunstancias han demostrado el poder que han adquirido los hacktivistas en internet.

En los albores del siglo XXI, el hacktivismo ha evolucionado a tal grado que han alcanzado el rango de organización internacional siendo el caso de *Anonymous* el más conocido. Dicha asociación, formada en el 2003, ha tenido como característica el hecho de no tener un líder identificable y que sus acciones son globales por lo que pueden dirigir alguna de esas cuatro agresiones en contra de cualquier sitio web del mundo.

Si bien, sus actividades han estado encaminadas a atacar páginas de internet gubernamentales, también han dirigido sus acciones en contra de los sistemas de transacciones de bancos públicos y privados ocasionando pérdidas considerables. Para Edgar Iván Espinosa, esa actitud se presenta como amenaza para México debido a "lo compleja que resulta su neutralización, debido a su estructura acéfala, su red de apoyo internacional y su capacidad operativa perfeccionada".[191]

Por lo tanto, es menester considerarla como amenaza cibernética a la seguridad nacional mexicana ya que es una acción ejecutada por agentes no estatales entendidos en organizaciones como Anonymous o por individuos como Assange y Snowden. Por último, se clasifica como emergente por ser una circunstancia emergida del contexto político y tecnológico actual.

[190] *Ibid.*, pp. 286-302.
[191] Edgar Iván Espinosa, *op. cit.*, p. 129.

3.2.2.3 Ciberataques

En el proceso de transformación tecnológica nacional e internacional ha quedado demostrado que una de las consecuencias más significativas de ese fenómeno ha sido el traslado de los comportamientos humanos, y por tanto políticos, del mundo real al mundo digital. Actividades como la delincuencia organizada, la guerra, el espionaje, el terrorismo y el activismo han dejado en claro la dimensión tecnológica que han adquirido en los últimos veinte años del nuevo siglo.

Los factores que han interrelacionado a cada una de esas acciones políticas han sido los ciberataques cuyas motivaciones dependen de la intención que se busca generar en el afectado ya sea una máquina o una persona. Se le puede definir como la "acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas".[192]

En un mundo cada vez más interconectado a la red de internet mediante dispositivos convencionales y no convencionales, así como el incremento de las instalaciones de provisión de bienes y de prestación de servicios que dependen de ella cualquier nación se vuelve completamente vulnerable a recibir ataques de todo tipo. Con base en el objetivo pueden catalogarse como ciberdelincuencia organizada, ciberguerra, ciberespionaje, ciberterrorismo y hacktivismo.

Desde el punto de vista de Arturo García Hernández, los ataques cibernéticos se clasifican en función de la entidad que los ejecuta ya que "no todos tienen el mismo objetivo ni nivel de recursos disponibles".[193] Para él, quienes las ejecutan, se denominan ciberatacantes y se dividen en cuatro apartados: Hackers solitarios, Grupos hacktivistas, Hackers de la delincuencia organizada y Hackers Estado-nación.

[192] Gobierno de México, *Estrategia Nacional de Ciberseguridad*.
[193] Arturo García Hernández, "La cultura de ciberseguridad", *Revista Seguridad en América*, N° 106, México, Seguridad en América, enero-febrero, 2018, p. 61.

Los primeros están asociados con conductas individuales aparentemente sin motivación alguna; los segundos se relacionan con comportamientos grupales con inclinaciones hacia una tendencia política o ideológica; los terceros están vinculados con grupos delictivos de origen nacional o trasnacional y los últimos son actitudes hostiles por parte de las naciones. Como es posible observar, cada uno de ellos se relaciona con alguna de las disposiciones antes señaladas.

Para poder asociar los ciberataques en relación con los perpetradores y sus intenciones se debe realizar una evaluación del contexto en el que se desarrolló, el probable actor que la pudo haber perpetrado, el objetivo hacia el cual fue dirigido y su probable ubicación de origen.[194] Ello con la intención de determinar si representa un peligro para la integridad, estabilidad y permanencia del Estado y para saber la clase de medida preventiva o reactiva que se necesita implementar.

En México, como se ha mencionado con anterioridad, prácticamente no ha existido sector alguno que no haya sido perjudicado mediante un ciberataque en mayor y menor medida. Tanto para los enemigos internos como los externos, los ataques cibernéticos representan una ventaja para afectar parcial o totalmente a la nación por sus características de organización rápida y sistemática; al alcance de sus afectaciones y a la variedad de opciones de herramientas, tiempo y objetivos.[195]

En ese sentido, los ciberataques se presentan como una amenaza cibernética a la seguridad nacional de México ya que son acciones ejercidas por agentes individuales y colectivos tanto internos como externos con miras a "socavar las funciones de un sistema o red de computadoras"[196] de valor estratégico por su contribución al desarrollo nacional. Asimismo, se les considera emergentes debido a su vínculo con las nuevas tecnologías digitales.

[194] Alejandra Morán Espinosa; Oscar Alquicira Gálvez; Abraham Alejandro Servín Caamaño; "TIC (Internet) y ciberterrorismo-II", *Revista Seguridad. Cultura de prevención para TI*, N° 24, México, UNAM-DGTIC, junio-julio, 2015, p. 27.
[195] Anahiby Becerril Gil, *op. cit.*, p. 131.
[196] *Ibid.*, p. 132.

CONCLUSIONES

En primer lugar la relación entre la Ciencia Política y la Seguridad Nacional consiste en comprender los acontecimientos histórico-políticos por los que atraviesan los Estados a nivel nacional e internacional con la finalidad de detenerlos o prevenirlos. De igual manera considera la organización política, jurídica y administrativa del Estado con la consigna de conservarla en el tiempo ante riesgos y amenazas que atentan contra los sectores de la nación.

La Ciencia Política es la disciplina clave para comprender los cambios de régimen político que sufren los Estados tanto antiguos como modernos que son los objetivos de lo que en la actualidad se entiende como Seguridad Nacional. Por lo cual, con base en esas afirmaciones y con lo expuesto en el primer apartado del trabajo se estaría confirmando la naturaleza y el origen políticos del concepto más allá de la multidimensionalidad que se le ha asignado.

En el caso de la Seguridad Nacional ha quedado claro que no se puede abordar sin haber comprendido políticamente al Estado ya que en él encuentra su razón de ser y sus finalidades. Para ello resulta necesario identificar su origen y causa tanto teórica como práctica los cuales, como se ha establecido en el principio, han sido procurar el bien común de las distintas partes y clases sociales que constituyen el Estado.

Por ese motivo se diría que independientemente de la multidimensionalidad de la Seguridad Nacional su esencia no deja de ser política toda vez que tiene como objetivo de estudio el mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano. Por lo tanto, la ciberseguridad en tanto dimensión tecnológica de aquélla antes que ser considerada un asunto de índole técnica se presenta como uno de tipo político.

Si se trasladan esas cuestiones teórico-conceptuales a la realidad nacional se estaría diciendo que la seguridad nacional mexicana radica en el resguardo de sus principios histórico-políticos los cuales se encuentran fundamentados en cada uno de los artículos de la Constitución Política de los Estados Unidos Mexicanos. En cada uno de ellos se encuentran las disposiciones para proteger las instituciones del Estado mexicano, desde la Familia hasta la Presidencia de la República.

En segundo lugar debe destacarse el hecho de que las Tecnologías de la Información y Comunicación se han presentado como un suceso que no había estado contemplado en algún texto político y/o jurídico nacional o internacional. No fue sino hasta principios del siglo XXI que fue considerado como una problemática de atención global ya que impactaba en aspectos críticos de los Estados como los sectores público, privado y social.

En el caso mexicano esa circunstancia había resultado problemática toda vez que los primeros estudios se basaban en aproximaciones realizadas desde la técnica y ocasionalmente desde la perspectiva económica, pero muy pocas veces desde la política. No obstante, como se ha demostrado con las diversas situaciones presentadas a nivel internacional y nacional ha quedado claro que es una condición que debe ser atendida desde la Ciencia Política.

Algunos de los trabajos citados en la investigación han dado muestra de que en años recientes la ciberseguridad ha cobrado gran relevancia como asunto de seguridad nacional en México. En ellos no sólo se destacan aspectos como los riesgos y las amenazas existentes en el espacio cibernético sino también de la oportunidad que representan para la nación mexicana en tanto actor global.

Cabe destacar que la presente investigación tiene por objeto demostrar que, así como existen beneficios derivados de la innovación y el desarrollo tecnológicos también conllevan ciertos peligros ya que las herramientas digitales no son en sí mismas el peligro sino el uso que se les pueda dar. La clasificación realizada ha demostrado que la mayor parte de los retos que enfrenta el Estado mexicano ya habían existido con anterioridad tan sólo han mudado sus acciones al ciberespacio.

En tercer lugar ha quedado claro el continuo avance que han tenido, tienen y tendrán los dispositivos interconectados mediante la red de internet lo que probablemente muestre en un futuro muy cercano otro tipo de aparatos electrónicos con la misma capacidad. Sobre todo, porque hablando de la tecnología no se tiene una certeza bien definida de lo que pueda suceder derivado de su invención y de uso dual cívico-militar.

Por lo cual es necesario poner énfasis en el hecho de que por la existencia de esas problemáticas existentes en el dominio digital la nación mexicana no debe rechazar su uso ya que le permiten contribuir al correcto desarrollo nacional de sus sectores: público, privado y social. El buen equilibrio de esos tres elementos permite la consolidación interna y externa evitando la existencia de conflictos derivando en un clima de inestabilidad.

Si bien las tecnologías digitales no comprenden un riesgo y/o una amenaza para la integridad territorial del Estado mexicano se debe destacar que el ciberespacio puede comprenderse como parte de él junto con las dimensiones terrestre, marítima y aérea. Además, se debe destacar que en la virtualidad resulta complicado establecer delimitaciones políticas primordialmente por sus propiedades siendo un lugar vulnerable a cualquier ataque.

A partir de la creación del modelo se confirma la hipótesis planteada ya que se demuestra que en el siglo XXI las TIC generan riesgos y amenazas que atentan contra la seguridad del individuo, la familia, la sociedad, las instituciones e inclusive del Estado. El modelo resultante clasifica los antagonismos con base en cada una de las dimensiones política, económica, social y militar.

Finalmente, la Ciberseguridad se presenta como un asunto que debe ser analizado desde el enfoque de la Seguridad Nacional, al ser éste un concepto perteneciente fundamentalmente a la Ciencia Política debe ser entendido a partir de ella. Aunque el prefijo *ciber* le otorga una característica técnica al término debe ser analizado y comprendido a partir de las dos perspectivas en el sentido de que el medio es la Tecnología mientras que el fin es la Política.

REFERENCIAS

Bibliográficas:

- Aguayo Quezada, S., & Bagley, B. M. (1990). *En busca de la seguridad perdida: aproximaciones a la seguridad nacional mexicana*. México: Siglo XXI Editores.
- Aristóteles. (2015). *Política*. Madrid: Editorial Gredos.
- Aristóteles. (2015). *Retórica*. Madrid: Editorial Gredos.
- Arquilla, J., & Ronfeldt, D. (2003). *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. Madrid: Alianza Editorial.
- Arreola García, A. (2015). *Ciberespionaje: la puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de Estados Unidos*. México: Siglo XXI Editores/Universidad Anáhuac.
- Assange, J. (2013). *Cypherpunks: la libertad y el futuro de internet*. México: Editorial Planeta Mexicana.
- Assange, J. (2014). *Cuando Google encontró a WikiLeaks*. Buenos Aires: Capital Intelectual.
- Bartlett, J. (2017). *La red oculta: ciberterrorismo, pornografía infantil, mercado del asesinato y demás ilícitos en Internet*. México: Paidós.
- Centro de Estudios Superiores Navales. (2014). *El área de influencia de México desde una visión geopolítica*. México: SEMAR-CESNAV.
- Centro de Estudios Superiores Navales. (2015). *Seguridad y defensa en el ciberespacio*. México: SEMAR-CESNAV.
- Centro de Estudios Superiores Navales. (2017). *Inteligencia estratégica: retos y oportunidades para México*. México: SEMAR-CESNAV.
- Cervantes, P., & Tauste, O. (2016). *Internet negro: el lado oscuro de la red*. México: Paidós.
- Cicerón, M. T. (2017). *La república/Las leyes*. Madrid: Ediciones Akal.
- Clarke, R. A. (2011). *Guerra en la red: los nuevos campos de batalla*. Barcelona: Ariel.
- Coronado Contreras, L. (2017). *La regulación global del ciberespacio*. México: Editorial Porrúa.
- Curzio, L. (2007). *La seguridad nacional de México y la relación con Estados Unidos*. México: UNAM-CISAN.

- Del Nogal Tomé, M. (2016). *Guerra psicológica*. México: Alfaomega Grupo Editor.
- Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Madrid: Editorial Ariel.
- García Hernández, A. (2018). *CiberMéxico: voluntades y acciones en el ciberespacio*. México: Ius Literatus.
- Garzón Valdés, E. (2015). *Lo íntimo, lo privado y lo público*. México: INAI-Cuadernos de Transparencia.
- Greenwald, G. (2014). *Sin un lugar donde esconderse*. Barcelona: Ediciones B.
- Hamelink, C. J. (2015). *La ética del ciberespacio*. México: Siglo XXI Editores.
- Herrera Hermosilla, J. C. (2012). *Breve historia del espionaje*. Madrid: Ediciones Nowtilus.
- International Telecommunications Union. (2018). *Global Cybersecurity Index (GCI) 2018*. Ginebra: ITUPublications.
- Leigh, D., & Harding, L. (2011). *WikiLeaks y Assange un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*. Barcelona: Deusto.
- Lewis, J. (2018). *Economic impact of cybercrime - No slowing down* -. California: McAfee.
- López Valdez, M. A. (2006). *La seguridad nacional en México: interferencias y vulnerabilidades*. México: Editorial Porrúa/Universidad Anáhuac.
- Maquiavelo, N. (2009). *Del arte de la guerra*. Madrid: Editorial Minerva.
- Maquiavelo, N. (2010). *El príncipe*. Madrid: Alianza Editorial.
- Maquiavelo, N. (2014). *Discursos sobre la primera década de Tito Livio*. Madrid: Editorial Gredos.
- Marcos, P. (1990). *Lecciones de política*. México: Nueva Imagen.
- Nora, S., & Minc, A. (1981). *La informatización de la sociedad*. México: Fondo de Cultura Económica.
- Organización de los Estados Americanos y Symantec. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe*. Washington, D.C.
- Panda Security. (2018). *2018 in cybersecurity: the experts talk*. Panda Security.
- Pastor Petit, D. (1971). *Diccionario del espionaje*. Barcelona: Plaza y Janes, S. A. Editores.
- Rosas, M. C. (2010). *La seguridad internacional en el siglo XXI: retos y oportunidades para México*. México: UNAM-FCPYS.

- Rosas, M. C. (2013). *Repensando la seguridad nacional de México*. México: SEMAR-CESNAV/UNAM/CEOP.
- Sarmiento Beltrán, Á. E. (2013). *La seguridad nacional integral de México: diagnósticos y propuestas*. México: SEMAR-CESNAV.
- Scolnik, H. D. (2016). *Qué es la seguridad informática*. México: Ediciones Culturales Paidós.
- Sun Tzu. (2014). *El arte de la guerra*. Madrid: Alianza Editorial.
- Tello Peón, J. E., Laborde Carranco, A. A., & Villarreal Díaz, M. (2012). *Inteligencia estratégica en el contexto mexicano*. México: Plaza y Valdés Editores/Instituto Tecnológico de Estudios Superiores de Monterrey.
- Toffler, A. (2000). *La tercera ola*. Barcelona: Plaza y Janes.
- Trejo García, E. C. (2006). *Regulación jurídica de internet*. México: Centro de Documentación, Información y Análisis-Cámara de Diputados.
- Wiener, N. (1958). *Cibernética y sociedad*. Buenos Aires: Editorial Sudamericana.
- World Economic Forum. (2019). *The global risk report 2019*. Ginebra: World Economic Forum.

Hemerográficas:

- Arreola García, A. (2019). Desafíos a las estrategias de ciberseguridad en América. *Revista del Centro de Estudios Superiores Navales*, 40(4), 28 pp.
- Arreola Rueda, E. A. (2006). La informática, internet y la economía en México a principios del siglo XXI. *Estudios Políticos* (7), 30 pp.
- Becerril Gil, A. (2019). La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio. *Revista de Administración Pública*, LIV (1), 34 pp.
- Cruz Valencia, G. I. (2012). Hacktivismo: ¿delito o comunicación ciudadana? *Revista Seguridad. Cultura de prevención para TI* (12), 6 pp.
- Espinosa, E. I. (2015). Hacia una estrategia nacional de ciberseguridad en México. *Revista de Administración Pública*, L (1), 31 pp.
- García Hernández, A. (2018). La cultura de ciberseguridad. *Seguridad en América* (106), 3 pp.
- Gutiérrez Amaya, C., & Mendoza, M. Á. (2018). Tendencias 2018: el costo de nuestro mundo conectado. *Revista Seguridad. Cultura de prevención para TI* (31), 6 pp.

- Lyne, J. (2016). Internet de las Cosas (IoT). *OUCH!*, 2 pp.
- Morán Espinosa, A., Servín Caamaño, A. A., & Alquicira Gálvez, O. (2015). TIC (internet) y ciberterrorismo. *Revista Seguridad. Cultura de prevención para TI* (23), 3 pp.
- Morán Espinosa, A., Servín Caamaño, A. A., & Alquicira Gálvez, O. (2015). TIC (internet) y ciberterrorismo - II. *Revista Seguridad. Cultura de prevención para TI* (24), 4 pp.
- Morán Espinosa, A., Servín Caamaño, A. A., & Alquicira Gálvez, O. (2015). TIC (internet) y ciberterrorismo - III. *Revista Seguridad. Cultura de prevención para TI* (25), 5 pp.
- Quijano Torres, M. (2017). El Estado supranacional y la administración pública. *Revista Buen Gobierno*, 28 pp.
- Rosas, M. C. (2011). Ciberespacio, crimen organizado y seguridad nacional. *Revista del Centro de Estudios Superiores Navales*, 3, 13 pp.
- Suárez Vázquez, E. (2007). Software malicioso (Malware). Historia y evolución. *Revista del Centro de Estudios Superiores Navales*, 28(2).
- Vizarretea Rosales, E. (2013). Sobre el discurso estratégico (primera parte). *Revista del Centro de Estudios Superiores Navales*, 34(3), 15 pp.
- Vizarretea Rosales, E. (2013). Sobre el discurso estratégico (segunda parte). *Revista del Centro de Estudios Superiores Navales*, 34(4), 19 pp.
- Vizarretea Rosales, E. (2016). Nueva inteligencia y ciberseguridad. *Revista del Centro de Estudios Superiores Navales*, 37(1), 34 pp.

Electrónicas:

- Ángel, A. (17 de marzo de 2017). “Fiscalía identifica a presuntos responsables de ciberataques contra bancos”. Obtenido de *Animal Político*: https://www.animalpolitico.com/2019/03/fiscalia-responsables-ciberataques-bancos/
- Asociación de Internet MX. (1 de agosto de 2019). *15 Estudio sobre los Hábitos de los Usuarios de Internet en México 2019*. Obtenido de https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

- Banco de México. (2018). *Estrategia de Ciberseguridad del Banco de México*. Obtenido de https://www.banxico.org.mx/spei/d/%7BA578961B-C965-33AD-0A8A-BFE6D6FE9669%7D.pdf
- Barlow, J. P. (8 de febrero de 1996). "A Declaration of the Independence of Cyberspace". Obtenido de *Electronic Frontier Foundation*: https://www.eff.org/cyberspace-independence
- Bastenier, M. Á. (30 de noviembre de 2010). "Hacktivismo". Obtenido de *El País*: https://elpais.com/internacional/2010/11/30/actualidad/1291071624_850215.html
- Blasco, L. (31 de julio de 2017). "¿Cuáles son los países que tienen más armas cibernéticas?" Obtenido de *BBC Mundo*: https://www.bbc.com/mundo/noticias-40631138
- Cámara de Diputados. (29 de noviembre de 2006). *Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional*. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/regla/n18.pdf
- Cámara de Diputados. (24 de octubre de 2013). *Gaceta Parlamentaria*. Obtenido de http://gaceta.diputados.gob.mx/Black/Gaceta/Anteriores/62/2013/oct/20131024-VII/Proposicion-9.html
- Cámara de Diputados. (8 de noviembre de 2019). *Código Penal Federal*. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/9_081119.pdf
- Cámara de Diputados. (8 de noviembre de 2019). *Ley de Seguridad Nacional*. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac_081119.pdf
- Cámara de Diputados. (8 de noviembre de 2019). *Ley Federal contra la Delincuencia Organizada*. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/101_081119.pdf
- Centro Nacional de Inteligencia. (1 de diciembre de 2018). *¿Qué es la Inteligencia?* Obtenido de: https://www.gob.mx/cms/uploads/attachment/file/272832/Qu__es_la_inteligencia.pdf
- Centro Nacional de Inteligencia. (1 de diciembre de 2018). *Ciclo de inteligencia*. Obtenido de: https://www.gob.mx/cms/uploads/attachment/file/233665/ciclo-inteligencia.pdf
- Emergui, S. (16 de enero de 2011). "Israel y EEUU crearon el virus que dañó el programa nuclear iraní". Obtenido de *El Mundo*: https://www.elmundo.es/elmundo/2011/01/16/internacional/1295180388.html

- Forbes Staff. (14 de noviembre de 2019). “Hackeo a Pemex no afectó ni registró daños a información estratégica: funcionarios”. Obtenido de *Forbes México*: https://www.forbes.com.mx/hackeo-a-pemex-no-afecto-ni-registro-danos-a-informacion-estrategica-funcionarios/
- García Gibson, R. (2 de septiembre de 2013). “Armas de destrucción masiva”. Obtenido de *El País*: https://www.forbes.com.mx/armas-de-destruccion-masiva/
- García, K. (13 de noviembre de 2019). “Pemex no pagará rescate a hackers tras ciberataque: Rocío Nahle”. Obtenido de *El Economista*: https://www.eleconomista.com.mx/empresas/Pemex-no-pagara-rescate-a-hackers-tras-ciberataque-Rocio-Nahle-20191113-0064.html
- Gobierno de México. (20 de agosto de 2009). *Programa para la seguridad nacional 2009-2012*. Obtenido de https://dof.gob.mx/nota_detalle.php?codigo=5106082&fecha=20/08/2009
- Gobierno de México. (2013). *Programas sectoriales 2013-2018*. Obtenido de http://inafed.gob.mx/es/inafed/inafed_programas_operacion_sectoriales
- Gobierno de México. (30 de abril de 2014). *Programa para la seguridad nacional 2014-2018*. Obtenido de http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014
- Gobierno de México. (12 de julio de 2017). *Documento de trabajo Hacia una Estrategia Nacional de Ciberseguridad*. Obtenido de https://www.gob.mx/cms/uploads/attachment/file/239446/Documento_de_trabajo_ENCS_v0.pdf
- Gobierno de México. (13 de noviembre de 2017). *Estrategia Nacional de Ciberseguridad*. Obtenido de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
- Gobierno de México. (1 de diciembre de 2018). *¿Qué son las amenazas y los riesgos a la seguridad nacional?* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/443055/Agenda_Nacional_de_Riesgos.pdf
- International Telecommunications Union. (Septiembre de 2011). *ITU National Cybersecurity Strategy Guide*. Obtenido de https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

- Internet Society. (1977). *Breve historia de internet*. Obtenido de https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/
- Jiménez Cano, R. (10 de diciembre de 2010). “Nadie está a salvo de esta ciberguerra”. Obtenido de *El País*: https://elpais.com/diario/2010/12/10/sociedad/1291935601_850215.html
- Martínez de Rituerto, R. (18 de mayo de 2007). “Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE”. Obtenido de *El País*: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html
- McGuiness, D. (6 de mayo de 2017). “Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país”. Obtenido de *BBC Mundo*: https://www.bbc.com/mundo/noticias-39800133
- Monterrosa, G. (18 de septiembre de 2016). “VII. México, indefenso ante ciberataques Ed. 506”. Obtenido de *Contralinea*: https://www.contralinea.com.mx/archivo-revista/2016/09/18/mexico-indefenso-ante-ciberataques/
- NSO Group. (2019). *About us*. Obtenido de https://www.nsogroup.com/about-us/
- Nuel, C. (8 de mayo de 2017). “Esperan 200 millones de dispositivos conectados en México para finales del 2020”. Obtenido de *Xataka*: https://www.xataka.com.mx/legislacion-y-derechos/esperan-200-millones-de-dispositivos-conectados-en-mexico-para-finales-del-2020
- Organización del Tratado del Atlántico Norte. (4 de abril de 1949). *Tratado del Atlántico Norte*. Obtenido de https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es
- Petróleos Mexicanos. (11 de noviembre de 2019). *Pemex opera con normalidad*. Obtenido de https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx
- Policía Federal. (4 de julio de 2018). *Glosario de términos en Ciberseguridad*. Obtenido de https://www.gob.mx/policiafederal/articulos/glosario-de-terminos-en-ciberseguridad?idiom=es
- RAND Corporation. (junio de 2009). *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*. Obtenido de https://www.rand.org/pubs/perspectives/PE329.html

- Reyez, J. (5 de Mayo de 2019). “Gobierno de México, sin estrategia ante ataques cibernéticos”. Obtenido de *Contralínea*: https://www.contralinea.com.mx/archivo-revista/2019/05/05/gobierno-de-mexico-sin-estrategia-ante-ataques-ciberneticos/
- Riquelme, R. (13 de noviembre de 2019). “Hackeo a Pemex puede considerarse como un delito de extorsión”. Obtenido de *El Economista*: https://www.eleconomista.com.mx/tecnologia/Hackeo-a-Pemex-puede-considerarse-como-un-delito-de-extorsion-20191113-0095.html
- Rodríguez Canfranc, P. (05 de Febrero de 2019). *Profesiones digitales 2. Ciberseguridad: protegiendo la información vulnerable*. Obtenido de: https://www.fundaciontelefonica.com.mx/publicaciones/pagina-item-publicaciones/itempubli/651/
- s/a. (19 de junio de 2017). “12 claves para entender qué es el spyware Pegasus y cómo funciona”. Obtenido de *Expansión*: https://expansion.mx/tecnologia/2017/06/19/12-claves-para-entender-que-es-el-spyware-pegasus-y-como-funciona
- s/a. (12 de mayo de 2017). “Ataque informático en España afecta a Telefónica, Iberdrola y Gas Natural”. Obtenido de *El Universal*: https://www.eluniversal.com.mx/articulo/mundo/2017/05/12/ataque-informatico-en-espana-afecta-telefonica-iberdrola-y-gas-natural
- s/a. (12 de mayo de 2017). “Ciberataque afecta a sistema de salud en Inglaterra”. Obtenido de *El Universal*: https://www.eluniversal.com.mx/articulo/mundo/2017/05/12/ciberataque-afecta-sistema-de-salud-en-inglaterra
- s/a. (21 de agosto de 2017). “México ocupa primer lugar mundial en difusión de pornografía infantil”. Obtenido de *El Sol de México*: https://www.elsoldemexico.com.mx/mexico/sociedad/mexico-ocupa-primer-lugar-mundial-en-difusion-de-pornografia-infantil-242048.html
- s/a. (27 de abril de 2018). “Banxico descarta afectación a clientes por falla en sistemas de pagos de bancos”. Obtenido de *Expansión*: https://expansion.mx/empresas/2018/04/27/citibanamex-y-banorte-reportan-fallas-en-sus-sistemas-de-pago
- s/a. (30 de abril de 2018). “Las fallas en transferencias vía SPEI continúan, según usuarios”. Obtenido de *Expansión*: https://expansion.mx/empresas/2018/04/30/las-fallas-en-transferencias-via-spei-continuan-segun-usuarios

- s/a. (11 de mayo de 2018). “Más bancos se desconectan temporalmente del SPEI”. Obtenido de *Expansión*: https://expansion.mx/empresas/2018/05/10/mas-bancos-se-desconectan-temporalmente-del-spei
- s/a. (14 de mayo de 2018). “Banxico confirma ciberataque y dice que el monto está por definirse”. Obtenido de *Expansión*: https://expansion.mx/economia/2018/05/14/banxico-confirma-ciberataque-y-dice-que-el-monto-esta-por-definirse
- s/a. (15 de mayo de 2018). “Por hackeo a SPEI, Banxico crea dirección de Ciberseguridad”. Obtenido de *Excelsior*: https://www.excelsior.com.mx/nacional/por-hackeo-a-spei-banxico-crea-direccion-de-ciberseguridad/1238972
- The Citizen Lab. (11 de febrero de 2017). *Bittersweet: Supporters of Mexico’s Soda Tax Targeted with NSO Exploit Links*. Obtenido de https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/
- Toledano, B. (12 de mayo de 2017). “El ciberataque con el virus WannaCry se extiende a nivel mundial”. Obtenido de *El Universal*: https://www.elmundo.es/tecnologia/2017/05/12/5915e99646163fd8228b4578.html
- Trasviña Waldenrath, J. L. (27 de Marzo de 2019). *Gaceta del Senado*. Obtenido de: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf
- Unión Internacional de Telecomunicaciones. (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad. Participación estratégica en la ciberseguridad.* Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf