RAP

REVISTA DE ADMINISTRACIÓN PÚBLICA

148

Volumen LIV, No. 1
(enero-abril 2019)

Ciberseguridad Nacional

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.
SECCIÓN MEXICANA DEL INSTITUTO INTERNACIONAL DE CIENCIAS ADMINISTRATIVAS

Instituto Internacional de Ciencias Administrativas

64 Años al servicio de México

ISSN: 0482-5209 www.inap.org.mx
Instituto Nacional de Administración Pública, A.C.
Km. 14.5, Carretera Federal México-Toluca No. 2151
Col. Palo Alto, 05110, Cuajimalpa, D.F., México
Tel. 5081-2657, e-mail: contacto@inap.org.mx

RAP

REVISTA DE ADMINISTRACIÓN PÚBLICA

148

Volumen LIV, No. 1
(enero-abril 2019)

Ciberseguridad Nacional

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.
SECCIÓN MEXICANA DEL INSTITUTO INTERNACIONAL DE CIENCIAS ADMINISTRATIVAS

64 Años al servicio de México

© Instituto Nacional de Administración Pública, A.C.
Km. 14.5 Carretera Federal México-Toluca No. 2151
Col. Palo Alto, C.P. 05110, Delegación Cuajimalpa
México, Distrito Federal
Teléfono (55) 50 81 26 57
http://www.inap.org.mx
contacto@inap.org.mx

ISSN 0482-5209

Publicación periódica
Registro número 102 1089
Características 210241801

Certificado de licitud de título número 2654
Certificado de licitud de contenido número 1697

Las opiniones expresadas en esta revista son estrictamente responsabilidad de los autores. La RAP, el INAP o las instituciones a las que están asociados no asumen responsabilidad por ellas.

Se autoriza la reproducción total o parcial de los artículos, citando la fuente, siempre y cuando sea sin fines de lucro.

CONSEJO DIRECTIVO 2017-2020

Carlos Reta Martínez
Presidente

Luis Humberto Fernández Fuentes
Vicepresidente para Asuntos Internacionales

Ricardo Uvalle Berrones
Vicepresidente

José de Jesús Jiménez Hernández
Vicepresidente para los IAPs de los Estados, 2019-2020

CONSEJEROS

José Ángel Gurría Treviño
Roberto Padilla Domínguez
Arturo Núñez Jiménez
Omar Guerrero Orozco
Carlos Almada López
Julián Alfonso Olivas Ugalde
Alejandro Romero Gudiño
Jorge Tamayo Castroparedes
Elena Jeannetti Dávila
Eber Omar Betanzos Torres
Soraya Pérez Munguía
María de Jesús Alejandro Quiroz
Jorge Francisco Márquez Montes
Fernando Pérez Correa Fernández del Castillo
Raúl Martínez Almazán
Manuel Quijano Torres

CONSEJO DE HONOR

Luis García Cárdenas
Ignacio Pichardo Pagaza
Adolfo Lugo Verduzco
José Natividad González Parás
Alejandro Carrillo Castro
José R. Castelazo

IN MEMORIAM

Gabino Fraga Magaña
Gustavo Martínez Cabañas
Andrés Caso Lombardo
Raúl Salinas Lozano

FUNDADORES

Francisco Apodaca y Osuna
José Attolini Aguirre
Enrique Caamaño Muñoz
Antonio Carrillo Flores
Mario Cordera Pastor
Daniel Escalante Ortega
Gabino Fraga Magaña
Jorge Gaxiola Zendejas
José Iturriaga Sauco
Gilberto Loyo González
Rafael Mancera Ortiz
Antonio Martínez Báez
Lorenzo Mayoral Pardo
Alfredo Navarrete Romero
Alfonso Noriega Cantú
Raúl Ortiz Mena
Manuel Palavicini Piñeiro
Álvaro Rodríguez Reyes
Jesús Rodríguez y Rodríguez
Raúl Salinas Lozano
Andrés Serra Rojas
Catalina Sierra Casasús
Ricardo Torres Gaitán
Rafael Urrutia Millán
Gustavo R. Velasco Adalid

COMITÉ EDITORIAL

Diego Barría Traverso	Universidad de Santiago de Chile
Jorge Culebro Moreno	Universidad Autónoma Metropolitana Unidad Cuajimalpa
Mauricio Dussauge Laguna	Centro de Investigación y Docencia Económicas
Maximiliano García Guzmán	Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México
Roberto Padilla Domínguez	Instituto Nacional de Administración Pública
Fernando Pérez	Universidad de Córdoba
Adriana Plasencia Díaz	Instituto Nacional de Administración Pública
Diana Vicher García	Instituto Nacional de Administración Pública
Héctor Zamitiz García	Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México

DIRECTOR DEL NÚMERO
Alejandro Pisanty

REVISTA DE ADMINISTRACIÓN PÚBLICA

148

Volumen LIV, No. 1
(enero – abril 2019)

Ciberseguridad Nacional

ÍNDICE

Presentación 13
Carlos Reta Martínez

Introducción 17
Alejandro Pisanty Baruch

CIBERSEGURIDAD NACIONAL

Ciberseguridad: estado de la cuestión en América Latina 23
Jimena Moreno González
María Mercedes Albornoz
María Solange Maqueo Ramírez

Esfera ética del ciberconflicto 47
Mario Vignettes

Inteligencia y ciberseguridad nacional 79
María José Rodríguez Rodríguez

La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio 113
Anahiby Becerril Gil

Seguridad de la información en instituciones de educación superior de México 149
Rafael Espinosa García
Guillermo Morales Luna

DNSChain y Namecoin: Una mirada a la revolución del DNS 189
Salvador Camacho Hernández

Tecnología cuántica y Ciberseguridad 209
Salvador E. Venegas Andraca

Atlas de riesgos para la Seguridad Nacional Cibernética en México 231
Carlos Estrada Nava

Ciberseguridad y la gobernanza multistakeholder 263
Fátima Cambronero

Regímenes para la ciberseguridad 301
Alejandro Pisanty

ANÁLISIS

Las constituciones locales mexicanas durante la Cuarta Transformación: un análisis prospectivo 341
Eduardo de Jesús Castellanos Hernández

La evolución del pensamiento sobre la "administración pública" a la luz de los clásicos: un breve recorrido histórico (siglo XVI al siglo XX) 365

José Joel Peña Llanes

Indicaciones para los colaboradores 403

Revista de Administración Pública

INAP

Presentación

Uno de los propósitos fundamentales de la RAP es servir como instrumento de difusión de los avances desarrollados en nuestras disciplina, así como espacio de resonancia de los debates que se suscitan en función del surgimiento de problemas públicos que necesitan atención.

En este sentido, el presente número de la revista está dedicado a la exploración conceptual y al análisis de las implicaciones que representa la conversión digital de la administración pública. En efecto, como toda tecnología, la adopción de las tecnologías de la información y comunicación (TICs) supone la aceptación de ventajas y de peligros de los cuales se debe ser consciente.

El empleo de las TICs es un tema que ha sido abordado extensamente por la literatura de nuestra disciplina. Una muestra de ello es el desarrollo de temas como el gobierno electrónico o e-government, y posteriormente el gobierno abierto. Este último incluso dio lugar a una agenda internacional de promoción de reformas institucionales tendientes a promover la participación ciudadana por medio del escrutinio de la información pública. En el INAP mismo se han editado diversas publicaciones sobre estos asuntos.

La digitalización de la administración pública tiende a profundizarse aún más en el futuro cercano. Ahora los retos que se plantean tienen que ver con la adopción de la inteligencia artificial y la robótica en el proceso de gestión y toma de decisiones.

En esta oportunidad, convencidos de la necesidad de explorar los temas de frontera, la RAP está dedicada a la cuestión de la ciberseguridad nacional. Cabe señalar que con esto se profundiza de manera convergente en dos temas que han sido de interés constante para nuestro Instituto. Por un lado, el de las TICs, ya referido, y pot el otro, el de la seguridad nacional. En este caso, contamos con una especialización y una maestría sobre inteligencia para la seguridad nacional.

En efecto, el presente número aborda el ámbito del ciberespacio desde una perspectiva de la seguridad nacional. En este esfuerzo académico han colaborado 13 destacados especialistas en la materia, ya sea desde la academia o desde la práctica profesional, en 10 artículos en donde se analizan las diversas aristas de la ciberseguridad: desde las cuestiones tecnológicas, hasta las éticas, pasando por aquellas pertinentes para la gobernanza.

Agradezco la colaboración de cada uno de los especialistas por atender a la convocatoria por ensamblar este valioso y pertinente número. En particular reconozco la labor de coordinación de este esfuerzo por parte del Dr. Alejandro Pisanty, destacado profesor de nuestros programas académicos en línea.

De acuerdo con diversas investigaciones y encuestas realizadas por firmas nacionales e internacionales, México es uno de los países que han estado sujetos a ataques cibernéticos. Por ejemplo, de acuerdo con la encuesta *The Impossible Puzzle of Cybersecurity* conducida por Sophos, 82 por ciento de las empresas mexicanas afirmaron haber sido vulnerables durante 2018. Le siguen Francia con 82 por ciento y la India con 76. No es casual, por su parte, que Japón sólo reportó un 24 por ciento. En el caso particular de la administración pública, un botón de muestra lo constituye la Comisión Federal de Electricidad (CFE), la cual, entre diciembre y abril pasados reportó haber sufrido 4, 205 ataques.

El número se completa con la publicación de dos artículos que nutren nuestra sección abierta, la cual se pone a disposición de nuestros investigadores y especialistas en el servicio público a partir de este número.

Estoy convencido, que como ha sucedido con los diversos números que la RAP ha publicado, el presente está destinado a convertirse en un material de consulta obligada para todo aquel interesado en los desafíos que plantea la conversión tecnológica y digital en el gobierno y la administración pública.

Carlos Reta Martínez
Presidente del INAP

Revista de Administración Pública

INAP

Introducción

El presente número de la Revista de Administración Pública es producto de una invitación del Dr. Carlos Reta Martínez, Presidente del INAP, quien ha tenido la visión de observar que la Ciberseguridad es un tema emergente con múltiples ángulos relevantes para la Administración Pública, Siguiendo su gentil invitación a coordinar esta edición, tanto el Instituto como este autor hicimos amplia convocatoria a autores y temas, con el resultado que hoy ponemos en manos de los lectores.

La ciberseguridad, como se discute en los artículos aquí contenidos, es un tema emergente, sujeto a vaivenes de atención, nomenclatura y enfoques, y que a través de ellps va estableciendo algunos paradigmas, al menos en la escala de una década, a la vez que se renueva constantemente. Tema multidisciplinario por excelencia, nuestra fortuna en esta convocatoria nos ha atraído autores expertos –no hablo acerca de mí– y dotados de una profunda visión ética y pragmática a la vez. Las vidas profesionales de nuestras autoras y autores se han enriquecido con sus actividades tanto académicas como profesionales, con intercambios de ideas vigorosos y actuaciones públicas en cargos de decisión sujetos a fuertes presiones. Su reflexión nutrida por la multidisciplina nos deja un panorama amplio y variado. Sin duda habrá otras perspectivas y experiencias que tomar en cuenta, que exceden la capacidad de este volumen, y serán bienvenidas hacia el futuro, pero no me cabe duda de que les debemos ya una visión panorámica de gran riqueza.

La convocatoria, como lo reflejan los artículos aquí contenidos, solicitó a los autores escribir sobre ciberseguridad en tanto ciberseguridad nacional. En el trabajo de coordinación y en la revisión editorial se contempló la diversidad de definiciones existentes para ciberseguridad y los conceptos relacionados, atendiendo a la perspectiva de los autores, pidiendo siempre observar el objetivo a tratar: la ciberseguridad nacional. Las esferas de la seguridad informática –personal, pública– se intersectan con la seguridad nacional y así han sido contempladas.

Jimena Moreno, Mercedes Albornoz y Solange Maqueo nos ofrecen una revisión comparada de la cuestión de ciberseguridad en los países de América Latina, sobre todo desde el punto de vista de la legislación y la práctica legal, complementada con observaciones sobre la práctica gubernamental. Esta visión comparativa de una realidad rápidamente cambiante será de utilidad para quienes estudian y responden a iniciativas de ley y proyectos de regulación, tanto como para quienes deben buscar los marcos legales para la acción en el ámbito operativo.

Mario Vignettes estudia la esfera ética del ciberconflicto. A partir de una revisión de los marcos relevantes en el pensamiento ético, permite alimentar el análisis y la toma de decisiones en diversas posiciones, como la preventiva, la defensiva y la ofensiva, en el conflicto en el ciberespacio. Conviene recordar que el conflicto en el ciberespacio no se restringe exclusivamente a este ámbito virtual; los actores del ciberconflicto son seres humanos y sus organizaciones, y las consecuencias del ciberconflicto se traducen, al menos potencialmente, en daños o defensa a las personas y sus activos físicos. El texto de Vignettes deberá ser estudiado por años como un marco para el pensamiento, la planeación y la acción en este campo.

María José Rodríguez extrae de su profundo conocimiento y experiencia un análisis sólido de la intersección entre ciberseguridad, a nivel nacional, e inteligencia. A partir del reconocimiento de la inteligencia como una necesidad vital de los Estados y un recorrido por los desafíos del ciberespacio a la seguridad nacional, revisa documentos y estrategias en la intersección de ciberseguridad nacional e inteligencia en varios países, incluyendo la Estrategia Nacional de Ciberseguridad de México. Concluye con un

planteamiento que debe ser tomado en cuenta por el Estado mexicano hacia el futuro.

Anahiby Becerril revisa también los ámbitos de intersección de ciberseguridad y seguridad nacional, a partir de una llamada de atención sobre la vitalidad y actualidad de los riesgos originados en el ciberespacio. De forma sistemática recorre los tipos de armas y ataques cibernéticos y ubica como especial foco de atención la guerra informacional. Una revisión del estado del arte de algunas defensas, entre ellas las basadas en técnicas de Inteligencia artificial, lleva a un llamado –en el que coinciden casi todas las contribuciones de esta colección– a que el Estado mexicano propicie la investigación en ciencia y tecnología conducentes a mejores capacidades de defensa del interés nacional.

Rafael Espinosa y Guillermo Morales revisan la situación de seguridad de la información en las instituciones de educación superior en México. Estas instituciones han sido y seguirán siendo nodales para la seguridad informática en todos sus niveles; fueron las primeras en contar con recursos computacionales y de red abiertos al mundo y por ello las primeras en recibir ataques informáticos, y en formar organizaciones y recursos humanos competentes para enfrentarlos exitosamente. El desarrollo de capacidades, que va más allá de las competencias técnicas de los individuos y debe llevar a un ecosistema robusto de ciberseguridad, pasa inexorablemente por las universidades. Futuras estrategias de ciberseguridad harán bien –y más: deberán– acercarse nuevamente a estas fecundas raíces.

Salvador Camacho nos abre a perspectivas recientes en el uso del sistema de nombres de dominio de Internet (DNS) como vehículo y objetivo de ataques lesivos a la ciberseguridad nacional, y a técnicas –entre ellas algunas basadas en tecnologías *Blockchain*– para dar seguridad al DNS sin interferir en el activo comercio y uso de los nombres de dominio. El artículo orienta al impacto en seguridad nacional a futuro para México y –él también– llama a fortalecer el desarrollo tecnológico y el de capacidades.

Salvador Venegas toma uno de los temas de mayor visión a futuro en ciberseguridad: la computación cuántica. Esta disciplina, que ve días de febril desarrollo ahora y hacia el futuro, puede permitir formas inéditas e insospechadas de

protección de la información mediante criptografía cuántica y, del otro lado de la moneda, puede proveer a los atacantes de una capacidad de descifrado de esquemas criptográficos que puede derrotar a cualquier defensa no cuántica. Si bien la computación cuántica enfrenta todavía desafíos formidables –es posible lograr coherencia con números muy pequeños de *qubits*– el desarrollo de su ciencia y de la tecnología en tanto software y simulaciones de dispositivos es rico y prometedor. Como otras disciplinas basadas en software, enfrenta barreras de entrada mucho menores que la producción de dispositivos y debe ser abordada de manera decisiva. Su dependencia de una formación matemática sólida y actual exige la formación de personal y laboratorios que, si se inician a tiempo y en la escala adecuada, y con apoyo suficiente, ágil y oportuno, puede proveer una envolvente avanzada a la estrategia nacional en materia de ciberseguridad, tanto al sector público como al privado, y a su colaboración. Hacerlo tendrá un costo relativamente bajo y sobre todo muy inferior al de no hacerlo.

Carlos Estrada Nava presenta y justifica la necesidad de establecer un atlas de riesgos de ciberseguridad para México, como una tarea de gran escala a la vez que urgente. Para ello provee taxonomías útiles e información actualizada del entorno geopolítico de la ciberseguridad, y un inventario de los grandes pasos hacia una estrategia de ciberseguridad que se han presentado en el país, así como de iniciativas recientes propuestas en el ámbito legislativo. Sin duda habrá controversias sobre algunos de los conceptos expresados por el autor, como en todos los demás artículos, las cuales serán bienvenidas para dar madurez al debate público informado en esta crucial materia.

Fátima Cambronero aborda un tema crucial para la ciberseguridad nacional: absorber eficazmente las lecciones aprendidas en más de veinte años de evolución y práctica de la gobernanza de Internet mediante mecanismos, acuerdos e instituciones multisectoriales o "multistakeholder", que no están maniatadas por las restricciones del esquema multilateral o intergubernamental propio de las relaciones internacionales (y lo complementan con agilidad, relevancia, y participación de los actores relevantes en formas eficaces). Formula convincentemente la tesis de que las decisiones

y acciones de carácter estratégico en ciberseguridad, en particular la nacional, sólo podrán alcanzar la eficacia y la capacidad de respuesta que el entorno cambiante exige si son multisectoriales y estructuradas en forma que pueda producir los resultados deseados.

Finalmente, en el artículo de quien suscribe esta introducción, Alejandro Pisanty, se discuten aspectos problemáticos de la definición de ciberseguridad y de su intersección con la seguridad nacional. El énfasis en entender las conexiones con el delito cibernético y la actividad de actores subnacionales y no nacionales conduce a una discusión de los regímenes aplicables, multilateral, multistakeholder, y un híbrido o régimen ecléctico vigente en la actualidad al que se propone reconocer en su naturaleza específica. El artículo termina con un análisis de los juegos que las potencias juegan para apalancar su acción entre regímenes y llama al Estado mexicano a hacer conciencia de éstos y operar en función de ese conocimiento en beneficio del interés nacional.

Agradezco al INAP y en particular al Dr. Carlos Reta Martínez la invitación, a la que ha sido una gratísima tarea de coordinar el presente número de la RAP. Que me fuera planteado el reto de contribuir de esta manera a la magna tarea del INAP ha sido singularmente honroso. También han sido invaluables las discusiones con algunos de los autores y autoras. La Facultad de Química de la UNAM, mi alma mater y lugar-ancla, a través de su Departamento de Física y Química Teórica, otorgó incondicionalmente su apoyo a la realización de este proyecto; llegue a él mi agradecimiento a través de nuestro Jefe de Departamento el Dr. Jesús Hernández Trujillo. Un agradecimiento a los revisores de los artículos, contribución insustituible. A cada una y uno de las autoras y autores mi reconocimiento y agradecimiento por la calidad profesional y humana, la dedicación, la paciencia y el brillante resultado de sus trabajos.

Alejandro Pisanty
Director del Número 148 de la RAP

Revista de Administración Pública

INAP

Ciberseguridad: estado de la cuestión en América Latina

Jimena Moreno González, María Mercedes Albornoz, María Solange Maqueo Ramírez

Resumen: El desarrollo tecnológico tiene un fuerte y creciente impacto en las relaciones económicas y sociales a nivel mundial y regional. Esto también se verifica en América Latina. Las actividades que se llevan a cabo en Internet implican la transmisión de información que puede ser objeto de ciberataques, afectando la seguridad de los Estados, de las empresas y de los individuos. Por ello se requiere adoptar acciones para prevenir y mitigar riesgos, así como para recuperarse rápidamente de las vulneraciones sufridas. La ciberseguridad constituye actualmente uno de los desafíos más acuciantes. Por eso, el objetivo de este artículo consiste en introducir la problemática de la ciberseguridad desde una perspectiva regional e interdisciplinaria que permita apreciar el estado de la cuestión en América Latina e identificar posibles líneas de análisis, a fin de sentar las bases sobre las cuales se puedan generar propuestas susceptibles de tener un impacto positivo en la práctica.

Palabras clave: Ciberseguridad, Ciberataque, Ciberresiliencia, América Latina. Interdisciplinariedad.

Cybersecurity: State of the question in Latin America

Abstract: Technological development has a strong and growing impact on economic and social relations worldwide and regionally. This is also verified in Latin America. The activities carried out on the Internet involve the transmission of information that may be subject to cyberattacks, affecting the security of States, companies and individuals. Therefore, it is necessary to adopt actions to prevent and mitigate risks, as well as to recover quickly from the violations suffered. Cybersecurity is currently one of the most pressing challenges. Therefore, the objective of this article is to introduce the problem of cybersecurity from a regional and interdisciplinary perspective that allows us to appreciate the state of the issue in Latin America and identify possible lines of analysis, in order to lay the foundations on which they can generate proposals that can have a positive impact on practice.

Keywords: Cybersecurity, Cyber-attack, Cyber-resilience, Latin America. Interdisciplinarity

Fecha de recepción: 14 de septiembre de 2018
Fecha de aceptación: 16 de octubre de 2018

Revista de Administración Pública

INAP

Ciberseguridad: estado de la cuestión en América Latina

Jimena Moreno González *
María Mercedes Albornoz **
María Solange Maqueo Ramírez ***

Introducción

La ciberseguridad constituye actualmente uno de los desafíos más acuciantes de los Estados, las empresas y los individuos a nivel global. Los países latinoamericanos no son ajenos a este fenómeno. Por eso, el objetivo de este artículo consiste en introducir la problemática de la ciberseguridad desde una perspectiva regional que permita apreciar el estado de la cuestión en América Latina e identificar posibles líneas de análisis, a fin de sentar las bases sobre las cuales se puedan generar propuestas susceptibles de tener un impacto positivo en la práctica. Justamente, la formulación de las mismas es parte de la misión del Centro de Política Digital para América

* Profesora asociada de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE), afiliada al Centro LATAM Digital. Maestra en Dirección Internacional, Instituto Tecnológico Autónomo de México (ITAM).

** Profesora investigadora de la División de Estudios Jurídicos del CIDE, afiliada al Centro LATAM Digital. Doctora en Derecho, Université de Paris II, Panthéon-Assas (Francia).

*** Directora y profesora investigadora de la División de Estudios Jurídicos del CIDE, afiliada al Centro LATAM Digital. Doctora en Derecho, Universidad de Salamanca (España).

Latina (Centro LATAM Digital)[1], alojado en el Centro de Investigación y Docencia Económicas (CIDE), con el apoyo del *International Development Research Center* (IDRC).

En primer lugar, se destacará la relevancia del tema (I), para inmediatamente después identificar y analizar la noción de ciberseguridad (II). A continuación, se examinará la situación de la ciberseguridad en Latinoamérica (III), se insistirá en la necesidad de adoptar un enfoque interdisciplinario a fin de abordar su estudio en el futuro y se identificará una serie de posibles ejes temáticos (IV). Finalmente, se presentará un breve apartado de conclusiones.

I. Relevancia del tema

La sociedad de la información y la era digital representan oportunidades muy importantes para el desarrollo de los países y para el pleno ejercicio de los derechos humanos. En efecto, Internet representa más del 3% del PIB mundial.[2] Por otra parte, se registra un constante aumento del uso de Internet a nivel global.[3] Sólo en América Latina[4], el 56% de sus habitantes usaron Internet en 2016[5], lo que significa que hubo un aumento del 36% en una década[6]. Esto implica que existe un consenso sobre la necesidad de redoblar esfuerzos para reducir la brecha digital, aumentar la conectividad y disminuir el analfabetismo digital.

La tendencia mundial se encamina hacia un aumento de la dependencia con respecto a las Tecnologías de la

1 Sitio web del Centro LATAM Digital: http://centrolatam.digital/ (último acceso: 09/08/2018).

2 David Abusaid *et al.*, *Perspectiva de ciberseguridad en México,* McKinsey & Company, junio 2018, p. 7. Disponible en: http://consejomexicano.org/multimedia/1528987628-817.pdf (último acceso: 09/08/2018).

3 De 2000 a 2018 se registró un crecimiento de usuarios de Internet del 1052% a nivel mundial. *Internet World Stats. Usage and Population Statistics*. Disponible en: https://internetworldstats.com/stats.htm (último acceso: 09/08/2018).

4 Cuando en el presente artículo se hace referencia a América Latina o Latinoamérica, se entiende que también está incluido el Caribe.

5 Edwin Fernando Rojas y Laura Poveda, *Estado de la banda ancha en América Latina y el Caribe 2017*, Santiago, Naciones Unidas, 2018, p. 5. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf (último acceso: 09/08/2018).

6 *Ídem*.

Información y de la Comunicación (TIC). De ahí que la ciberseguridad se haya convertido en unos de los retos más desafiantes que actualmente enfrentan los Estados y haya sido incluida en las agendas nacionales de muchos países como un tema estratégico, ya que, entre otras cuestiones, involucra la seguridad nacional.[7]

Es importante mencionar que, en América Latina, el costo del cibercrimen oscila entre los US$ 15,000 y US$ 30,000 millones de dólares[8]. En este contexto, se incrementa la vulnerabilidad de las personas, de las empresas, de las instituciones y de los Estados, ante el surgimiento de amenazas de naturaleza cibernética. Así, "[m]ás usuarios, más dispositivos y sistemas, más redes y más servicios representaron más oportunidades y beneficios para más personas. Sin embargo, también significaron más amenazas y vulnerabilidades, más víctimas y mayores costos financieros y de otros tipos".[9]

II. Noción de ciberseguridad

En términos generales, "[l]a ciberseguridad es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque".[10] Tales acciones pretenden reducir

7 Véase Nicholas Burns y Jonathon Price (eds.), *Securying Cyberspace. A New Domain for National Security,* Washington D.C., The Aspen Institute, 2012. Daniela Danca, "The National and International Cyber Security Dimension", en *European Social Fund, International Conference Law Between Modernization and Tradition. Implications for the Legal, Political, Administrative and Public Order Organization, Bucarest, 21 al 23 de abril de 2015*, Bucarest, Editura Hamangiu, 2015, pp. 653-658.

8 James Lewis, *Economic Impact of Cybercrime. No Slowing Down*, McAfee y Center for Strategic and International Studies (CSIS), 2018, p. 7. Disponible en: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email (último acceso: 09/08/2018).

9 Organización de los Estados Americanos y Symantec, *Tendencias de Seguridad Cibernética en América Latina y el Caribe*, Washington D.C., OEA, junio de 2014, p. 7. Disponible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf (último acceso: 09/08/2018).

10 David Abusaid *et al.*, *Perspectiva de ciberseguridad en México,* McKinsey & Company, junio 2018, p. 21.

vulnerabilidades, pero no alcanzan a erradicarlas[11]. Si bien éste es el objetivo común de la ciberseguridad, no existe consenso sobre los alcances jurídicos, políticos y técnicos de su definición[12], ni sobre los mecanismos para su implementación, toda vez que varían de manera significativa entre los países, a pesar de que el ciberespacio es intrínsecamente global.

Lo anterior implica pensar la seguridad en términos de colaboración y cooperación en el intercambio de información a nivel nacional e internacional, además de entablar estrategias comunes para prevenir ataques, resolver problemas y enfrentar las posibles amenazas, reduciendo las probabilidades de que se materialicen. Sin embargo, el concepto y las estrategias de seguridad no son cuestiones meramente técnicas[13], sino que están fuertemente relacionadas con las situaciones específicas que se enfrentan de manera local o regional. Esto incluye las características culturales, éticas y políticas de cada lugar; por tanto, la ciberseguridad debe responder a retos concretos de manera local, además de ser interoperable y compatible a nivel internacional[14].

En este sentido, es necesario generar un significado amplio de lo que se entiende por seguridad y las características del ciberespacio. La visión de seguridad debe capturar la problemática que implica el desarrollo de las tecnologías y el intercambio masivo de información. Desde un punto de vista técnico, el concepto de seguridad

11 Véase Lior Tabansky, "Israel´s Cyber Security Policy, Local Response to the Global Cybersecurity Risk", en Metodi Hadji-Janev y Mitko Bogdanoski (eds.), *Handbook of Research on Cybersociety and National Security in the Era of Cyber Warfare*, Hershey, IGI Global, 2016, p. 476.

12 Daniel Álvarez Valenzuela y Francisco Vera Hott, "Ciberseguridad y derechos humanos en América Latina", en Agustina Del Campo (comp.), *Hacia una Internet libre de censura II*: *Perspectivas en América Latina*, Ciudad Autónoma de Buenos Aires, Universidad de Palermo, 2017, p. 38. Disponible en: https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf (último acceso: 09/08/2018).

13 James A. Lewis, "Harnessing Leviathan: Internet Governance and Cybersecurity", en Nicholas Burns y Jonathon Price (eds.), *Securing Cyberspace. A New Domain for National Security,* Washington, D.C., The Aspen Institute, 2012, p. 118.

14 Viorel Coroiu, "Conceptual Dimensions of Cyber Security", *European Journal of Public Order and National Security*, volumen II, número 7, 2015, p. 18.

de la información "puede resumirse en la preservación de la tríada de confidencialidad, integridad y disponibilidad de la información de un sistema"[15]. Por otro lado, "el ciberespacio se caracteriza por la ausencia de fronteras, el dinamismo y su anonimidad"[16], lo que hace indispensable una efectiva cooperación internacional entre los países y las organizaciones. Hablar de ciberseguridad supone también enfrentar las amenazas, los riesgos y la capacidad de acción y de reacción de los ciberataques que incluyen el ciberterrorismo, el ciberespionaje, el cibercrimen, entre otros, y que pueden venir desde hackers aislados, organizaciones criminales o, incluso, involucrar la participación de los Estados.

Al diseñar una política de ciberseguridad es necesario tener en cuenta la gestión de riesgos y la ciberresiliencia. La primera "implica una aproximación racional y proporcionada al tema, y promueve el uso de herramientas técnicas apropiadas para gestionar los riesgos dentro del ciberespacio"[17]. La segunda consiste en la capacidad de los sectores público, privado y de la sociedad para mantenerse seguros de forma sostenida en el tiempo, para tomar decisiones inmediatas con información veraz y para recuperarse rápidamente de vulneraciones sufridas[18].

Más allá de los debates que se presentan en la literatura en torno al concepto de ciberseguridad, es necesario entender que, en la práctica, "es un fenómeno complejo, sistémico y multifactorial que involucra diferentes aspectos como la seguridad de las redes estatales, privadas, infraestructuras críticas, prevención de delitos, educación, buenas prácticas, alianzas público-privadas, relaciones internacionales y un largo etcétera"[19].

15 Daniel Álvarez Valenzuela y Francisco Vera Hott, "Ciberseguridad y derechos humanos en América Latina", p. 42.

16 Ioana Martin, "Cyber Security Strategies - An Overview", *International Journal of Information Security and Cybercrime*, volumen 4, número 1, 2015, p. 33.

17 Daniel Álvarez Valenzuela y Francisco Vera Hott, "Ciberseguridad y derechos humanos en América Latina", p. 44.

18 David Abusaid *et al.*, *Perspectiva de ciberseguridad en México,* McKinsey & Company, junio 2018, p. 22.

19 Daniel Álvarez Valenzuela y Francisco Vera Hott, "Ciberseguridad y derechos humanos en América Latina", p. 54.

III. La ciberseguridad en Latinoamérica

Latinoamérica está enfocando sus esfuerzos en la seguridad cibernética e introduciéndola en su agenda como un tema principal. Sin embargo, tales esfuerzos han sido desarticulados, por lo que persiste un desequilibrio en la situación de cada país, tanto en términos de desarrollo como de implementación de políticas de seguridad cibernética.

El Informe Ciberseguridad 2016[20], elaborado por el Observatorio de la Ciberseguridad en América Latina y el Caribe, es un reporte que, mediante el uso de 49 indicadores, mide el grado o nivel de madurez de la capacidad de seguridad cibernética. El modelo, desarrollado por el Centro Global de Capacidad sobre Seguridad Cibernética (Oxford), cuenta con cinco dimensiones: política, sociedad, educación, legislación y tecnología y cinco niveles de madurez para cada indicador: inicial, formativo, establecido, estratégico y dinámico[21].

Lo primero que evalúa el Informe es el desarrollo de la estrategia nacional de seguridad cibernética oficial o documentada en cada país. Para ello, se considera que una estrategia nacional *integral* de seguridad cibernética "identifica los intereses y roles de una gama de actores que contribuyen a, tienen la responsabilidad de o se ven afectadas [*sic*] por la seguridad cibernética [,] con el propósito de crear un marco coordinado y cohesionado"[22]. Los cinco niveles de madurez que se proponen en esta área son los mencionados más arriba, cuyas explicaciones se reproducen textualmente a continuación:

1. **INICIAL**: no hay evidencia de la existencia de una estrategia nacional de seguridad cibernética;

20 Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*, Organización de los Estados Americanos y Banco Interamericano de Desarrollo, 2016. Este informe es el resultado de la colaboración entre el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford. Disponible para su descarga a partir de: https://publications.iadb.org/handle/11319/7449?locale-attribute=es (último acceso: 09/08/2018).

21 *Ibidem*, p. XIII.

22 *Ibidem*, p. 124.

si existe un componente cibernético, puede ser responsabilidad de uno o más departamentos del gobierno; ha comenzado un proceso para el desarrollo sin consultar a los interesados.

2. **FORMATIVO**: se ha articulado un esquema de una estrategia nacional de seguridad cibernética construido sobre la base de la consulta del gobierno; se han establecido procesos de consulta para los grupos de interés clave, posiblemente con asistencia internacional.
3. **ESTABLECIDO**: se ha establecido una estrategia de seguridad cibernética nacional; se ha acordado un mandato específico para consultar a todos los sectores y la sociedad civil; se utilizan tendencias históricas y datos para planificar; una cierta comprensión de los riesgos y amenazas de seguridad cibernética nacional impulsa la creación de capacidades a nivel nacional.
4. **ESTRATÉGICO**: la estrategia de seguridad cibernética nacional se implementa con conocimiento por parte de múltiples partes interesadas en todo el gobierno; se confirman los procesos de revisión y renovación de la estrategia; se llevan a cabo ejercicios cibernéticos regulares de escenario y en tiempo real; planes estratégicos de seguridad cibernética impulsan la creación de capacidad y las inversiones en seguridad; se han establecido procesos de medición y métricas, los cuales se implementan y sirven de base para la toma de decisiones.
5. **DINÁMICO**: la estrategia de seguridad cibernética se revisa continuamente para adaptarse a los cambiantes entornos sociopolíticos, de amenazas y tecnológico, impulsando el proceso de toma de decisiones de múltiples partes interesadas; se llevan a cabo medidas de transparencia y de fomento de la confianza (TCBM, por sus siglas en inglés) para garantizar la inclusión y la contribución continua de todos los interesados, incluido el mejoramiento de la asociación público-privada, la sociedad en general y los aliados internacionales.[23]

23 *Ídem.*

Del total de países reportados, resulta relevante destacar que ninguno se encuentra en una etapa estratégica ni dinámica (4 y 5). De hecho, el nivel de desarrollo de la estrategia nacional de seguridad cibernética oficial o documentada es, en la mayoría de los casos, inicial; en algunos casos es formativo y sólo una minoría es establecido, tal como se indica a continuación. La presente tabla permite apreciar en cuál de estos tres niveles se encontraban los 32 países estudiados en 2016 [24].

Nivel Inicial (17 países)	**Nivel Formativo (10 países)**	**Nivel Establecido (5 países)**
1. Antigua y Barbuda 2. Bahamas 3. Barbados 4. Belice 5. Bolivia 6. Ecuador 7. El Salvador 8. Granada 9. Guatemala 10. Guyana 11. Haití 12. Honduras 13. Nicaragua 14. República Dominicana 15. Saint Kitts y Nevis 16. Santa Lucía 17. Venezuela	1. Argentina 2. Brasil 3. Chile 4. Costa Rica 5. Dominica 6. México 7. Paraguay 8. Perú 9. San Vicente y las Granadinas 10. Surinam	1. Colombia 2. Jamaica 3. Panamá 4. Trinidad y Tobago 5. Uruguay

Las conclusiones principales del Informe[25] relevantes para efectos del presente documento, son reportadas a continuación. Asimismo, cuando ello sea pertinente, se irá

24 *Ibidem*., pp. 48-111.
25 *Ibidem*, p. 115.

agregando información actualizada al mes de agosto de 2018.

- Aunque los gobiernos reconocen la importancia de asegurar un acceso asequible a las TIC, la penetración de Internet en América Latina es muy baja todavía[26]. A 2016, ésta era de menos del 50% en aproximadamente la mitad de la región.[27] Se estima que para 2019, la penetración de usuarios de Internet suba al 60.9%[28].
- La adopción de una estrategia nacional de seguridad cibernética es un elemento fundamental del compromiso de un país en este ámbito[29]. Hasta 2016 inclusive, los países de la región que habían adoptado estrategias de seguridad cibernética eran: Brasil, Colombia, Jamaica, Panamá, Trinidad y Tobago y Uruguay, mientras que otros (como Argentina, Antigua y Barbuda, Bahamas, Costa Rica, El Salvador, Haití, México, Paraguay, Perú), se encontraban avanzando hacia la articulación de estrategias de ciberseguridad[30]. Según el Repositorio de Estrategias Nacionales de Seguridad de la Unión Internacional de Telecomunicaciones[31], los Estados latinoamericanos que actualmente cuentan con estrategias o políticas nacionales de ciberseguridad son: Brasil, Colombia, Chile y Uruguay. Con respecto al referido Informe de 2016 se agrega Chile[32]. Asimismo, debe sumarse México a la lista[33]. Finalmente, cabe mencionar que en

26 *Ídem*.
27 *Ídem*.
28 Statista, *Internet usage in Latin America. Statistics & Facts*. Disponible en: https://www.statista.com/topics/2432/internet-usage-in-latin-america/ (último acceso: 09/08/2018).
29 Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*, p. 115.
30 *Ídem*.
31 International Telecommunications Union, *National Strategies Repository*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx (último acceso: 09/08/2018).
32 Desde 2017, Chile cuenta con una Política Nacional de Ciberseguridad. Disponible en: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf (último acceso: 09/08/2018).
33 En efecto, en 2017 fue aprobada la Estrategia Nacional de Ciberseguridad de México. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (último acceso: 09/08/2018).

Honduras se está discutiendo un controvertido proyecto de ley que contiene una Estrategia Nacional de Ciberseguridad[34].

- Dado que la población desconoce los riesgos y vulnerabilidades ligados al uso de las TIC, es necesario que los gobiernos informen y sensibilicen a la ciudadanía al respecto[35].
- Como el establecimiento de asociaciones público-privadas confiables y de mecanismos formales de intercambio de información es limitado en Latinoamérica, la colaboración entre los actores clave ha disminuido[36].
- La capacidad de respuesta a las crisis o a incidentes en materia de seguridad informática, así como las posibilidades de abordar las amenazas cibernéticas, son limitadas en los países de América Latina en general[37]. No obstante, algunos de ellos, como Colombia, ya cuentan con iniciativas maduras para atender incidentes del gobierno y del sector privado[38].
- Los esfuerzos para desarrollar marcos legales integrales para combatir la delincuencia cibernética están en marcha en toda la región. Hasta 2016, sólo República Dominicana y Panamá se habían adherido al Convenio de Budapest sobre la ciberdelincuencia, del 23 de noviembre de 2001[39]. Hoy por hoy, ya se han sumado Argentina, Chile, Costa Rica y Paraguay; a Colombia y Perú sólo les queda pendiente ratificar este instrumento

34 *Ley nacional de ciberseguridad y medidas de protección ante los actos de odio y discriminación en internet y redes sociales,* Proyecto presentado por el diputado Marcos Bertilio Paz Sabillón, con modificaciones efectuadas por la Comisión Especial, 8 de febrero de 2018, http://congresonacional.hn/wp-content/uploads/2018/02/DICTAMEN-LEY-DE-CIBERSEGURIDAD-I.pdf (último acceso: 09/08/2018).

35 Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*, p. 115.

36 *Ídem.*

37 *Ídem.*

38 *Ídem.*

39 Convenio de Budapest, traducción al español avalada por el Consejo de Europa, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c (último acceso: 09/08/2018).

internacional[40], lo que demuestra que los países latinoamericanos están cada vez más dispuestos a tomar medidas frente al problema de la ciberdelincuencia.

IV. Interdisciplinariedad y ejes temáticos o líneas de investigación sugeridas

Se considera fundamental abordar la ciberseguridad a través de un enfoque interdisciplinario que tome en cuenta aspectos o herramientas propias de disciplinas como la ingeniería, la economía, las políticas públicas y el derecho (por mencionar tan sólo algunas).

A continuación, se procede a identificar algunos ejes temáticos o líneas de investigación relacionados con la ciberseguridad que podrían ser considerados para su análisis, a fin de contribuir a la formulación de políticas públicas integrales en la materia.

IV. 1. Perspectiva internacional

En la perspectiva internacional es necesario considerar, específicamente, tres temas relevantes: 1) jurisdicción, 2) derecho aplicable y 3) cooperación internacional.

IV.1.a) Jurisdicción

El surgimiento de Internet y el carácter transnacional de esta nueva tecnología desafían la tradicional noción de jurisdicción, concebida para un mundo dividido en Estados y fuertemente ligada al territorio. Ante la ausencia de un tribunal internacional competente, cuando se produce una vulneración a la ciberseguridad, se ha de recurrir a las autoridades de algún Estado. El problema es identificar cuál sería el Estado cuyos tribunales estarían dotados de competencia para decidir la controversia.

40 Convenio de Budapest, tabla de firmas y ratificaciones, actualizado al 09/08/2018. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=GLngzb88 (último acceso: 09/08/2018).

Se trata de una cuestión compleja y delicada porque, dadas las características propias de Internet y de los ciberataques (especialmente la dificultad de localizarlos), hay que decidir a qué elemento del caso se le da prevalencia para atribuir jurisdicción. Por ejemplo: el lugar de comisión del ciberataque, o aquél de donde proviene o donde se inicia, el lugar donde sus efectos se producen, o uno de los lugares donde se sufre el daño. ¿Qué sucedería si no se contara con elementos suficientes para ligar la conducta a un Estado concreto? ¿Y si los efectos de un ciberataque se expandieran a varios Estados? ¿Acaso habría jurisdicción concurrente?

El Derecho Internacional en general, y el Derecho Internacional Privado en particular, disponen de herramientas que pueden ser de utilidad en la búsqueda de respuestas a estas preguntas. En el Convenio de Budapest, el artículo 22 establece que cada Estado Parte adoptará las medidas necesarias para afirmar su jurisdicción cuando el delito haya sido cometido en su territorio, o bien por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar de comisión o si ningún Estado tiene competencia territorial respecto del mismo. Adicionalmente, al permitir que los Estados no excluyan otros principios de atribución de jurisdicción en determinadas situaciones, se les confiere cierta libertad para adoptar criterios acordes con su propia tradición y marco jurídico[41].

IV.1.b) Derecho aplicable

A la cuestión de determinar la autoridad competente en materia de ciberataques se suma otra, íntimamente relacionada con aquélla: la del derecho aplicable. Se trata de averiguar qué normas jurídicas utilizará el tribunal que resulte competente para resolver el caso.

El punto de partida es la ausencia de normas jurídicas de carácter global que regulen la ciberseguridad. Hoy por hoy la regulación es escasa. Sin embargo, hay un instrumento internacional de *hard law*, el ya aludido Convenio de Budapest, que obliga a los Estados Parte a adoptar medidas

41 Cristos Velasco San Martín, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Valencia, Editorial Tirant lo Blanch, 2012, p. 95.

legislativas con cierto piso mínimo de contenido común (por ejemplo, tipificando determinadas conductas como delitos).

Adicionalmente, entiende que sería interesante analizar si, cuando una autoridad debe resolver conflictos jurídicos surgidos a raíz de vulneraciones a la ciberseguridad, debería aplicar invariablemente el derecho sustantivo del foro, o si cabría la posibilidad de aplicar derecho extranjero y, en su caso qué derecho extranjero.

Asimismo, hay que tener en cuenta que las autoridades también podrían adoptar una postura flexible, adecuada a los tiempos que corren y, cuando en virtud de la materia y de las circunstancias del caso corresponda, utilizar normas de *soft law* tales como las contenidas en lineamientos, guías de mejores prácticas, principios, etc. Al hablar de derecho aplicable, no debe perderse de vista que las empresas –especialmente, los grupos de empresas transnacionales– cuentan ya con normas y protocolos corporativos en esta materia. Finalmente, aquí se encuadraría también la aplicación de resoluciones no vinculantes emitidas por la Organización de las Naciones Unidas para luchar contra la utilización de las TIC con fines delictivos, para crear una cultura mundial de seguridad cibernética y para proteger infraestructuras de información esenciales[42].

IV.1. c) Cooperación internacional

Las vulneraciones a la ciberseguridad generan problemas jurídicos que, en la gran mayoría de los casos, estarán vinculados con diversos Estados. La propia naturaleza de Internet contribuye a que esto sea así. Al tratarse de conflictos transfronterizos o incluso de carácter global, resulta a todas luces insuficiente pretender prevenir su aparición, o solucionarlos una vez que se han producido, con la intervención de las autoridades de un solo país, porque éstas tienen un ámbito de competencia y actuación delimitado por sus fronteras.

En este contexto, adquiere suma importancia la cooperación entre Estados. Nótese que el Convenio de Budapest dedica

42 Cristos Velasco San Martín, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, p. 79.

un capítulo completo (el Capítulo III, integrado por trece artículos) a la cooperación internacional.

Además, se considera que es necesario estimular la colaboración de otros actores públicos y privados relevantes, tales como universidades, empresas, organizaciones de la sociedad civil y agencias de seguridad[43]. En suma, sin reforzar los mecanismos de cooperación internacional, la batalla contra los ciberataques estará perdida de antemano.

IV.2. Derechos humanos

Es importante identificar las áreas de relación, compatibilidad y/o tensión entre ciberseguridad y derechos humanos. Por un lado, la ciberseguridad puede ayudar a garantizar los derechos, dependiendo de cómo se la conciba. Por otro lado, las medidas que se adopten en aras de fortalecer la seguridad cibernética podrían atentar contra los derechos humanos[44] si son injustificadas, inadecuadas, innecesarias, o desproporcionadas.

Estos problemas están siendo objeto de análisis en distintos sistemas de protección de derechos humanos (universal, regionales y nacionales). Por eso es importante que estos conflictos se piensen desde la perspectiva latinoamericana, atendiendo a los contextos jurídicos, políticos y sociales propios de la región. Al respecto, es necesario considerar, por lo menos, los derechos humanos a la vida privada, la protección de datos personales, la libertad de expresión e información y la libertad de asociación.

IV.3. Educación digital

Es necesario que existan políticas públicas que incluyan la educación digital como eje transversal para abordar el tema de ciberseguridad. La seguridad en las redes debería ser contenido prioritario en los programas educativos. Se

43 José Carlos Hernández, *Estrategias Nacionales de Ciberseguridad en América Latina*, Granada, Grupo de Estudios en Seguridad Internacional (GESI), 2018. Disponible en: http://www.seguridadinternacional.es/?q=es/print/1335 (último acceso: 09/08/2018).

44 Véase Daniel Álvarez Valenzuela y Francisco Vera Hott, "Ciberseguridad y derechos humanos en América Latina", p. 53.

requiere comprender e integrar las tecnologías al proceso de enseñanza y aprendizaje, tomando en cuenta las necesidades y particularidades de los diversos contextos sociales, culturales y económicos. De este modo, se podrá sensibilizar acerca de cómo prevenir que las personas, las empresas, los gobiernos, sean víctimas de vulneraciones a la seguridad y de cómo actuar ante los riesgos inherentes al aumento de la conectividad y la dependencia con respecto a las nuevas tecnologías[45]. Se debe procurar crear una verdadera cultura de ciberseguridad[46].

Diferentes iniciativas de sensibilización, como las que han comenzado a surgir en algunos países de América Latina y que han ayudado a construir una comprensión compartida de la importancia de la seguridad cibernética, también pueden conducir a la acción. Dos claros ejemplos de esto son: la campaña "La seguridad de la información comienza por ti"[47] de Venezuela y la campaña internacional Stop.Think.Connect[48].

IV.4. Economía digital

La economía digital se ha convertido en un motor de crecimiento e inclusión para las industrias, las empresas y los Estados y ha modificado la forma en la que se intercambian bienes y servicios a nivel global. El desarrollo de la inteligencia artificial, Internet de las cosas, el comercio electrónico y la innovación son indispensables para seguir generando economías más dinámicas. Sin embargo, sin políticas específicas que impulsen el desarrollo de

45 Véase Adolfo Arrieta y Donicer Montes, "Alfabetización digital: uso de las TIC's más allá de una formación instrumental y una buena infraestructura", *Revista Colombiana de Ciencia Animal*, volumen 3, número 1, 2011, p. 182.

46 Un informe reciente de la European Union Agency for Network and Information Security (ENISA), define la cultura de la ciberseguridad de las organizaciones como "el conocimiento, las creencias, percepciones, actitudes, suposiciones, normas y valores de la gente acerca de la ciberseguridad y cómo éstos se manifiestan en el comportamiento de la gente con respecto a las tecnologías de la información". ENISA, *Cyber Security Culture in organisations*, 2017, p. 7. Disponible para su descarga desde: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (último acceso: 09/08/2018).

47 Campaña lanzada por VenCERT, que es el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela. Sitio web: http://www.vencert.gob.ve/es-ve/ (último acceso: 09/08/2018).

48 Más sobre la campaña en su sitio web: https://www.stopthinkconnect.org (último acceso: 09/08/2018).

plataformas que ayuden a prevenir, dar respuesta oportuna y eficaz a los ciberataques en las transacciones comerciales, financieras y de robo de identidad, los esfuerzos para seguir creciendo por esta vía se verán mermados.

"Para prosperar en la economía de Internet del futuro, los países, negocios e incluso trabajadores deberán ser ágiles y poder aprender rápidamente. En una economía global caracterizada por la velocidad del cambio, la brecha digital evolucionará y posiblemente se profundizará simplemente en función de la capacidad de mantenerse al día con la tecnología."[49] En este sentido, la ciberseguridad enfrentará nuevos retos para generar ambientes seguros en los que se desarrolle esta economía.

IV.5. Regulación y autorregulación

Dada la vertiginosa velocidad a la que se producen los cambios tecnológicos, legislar en materia de ciberseguridad constituye un gran desafío. Sin embargo, se considera indispensable emprender esta ardua tarea, tanto por parte de los Estados como por parte de diferentes actores del ámbito privado.

En este sentido, es fundamental abordar, por lo menos, los siguientes temas: la propiedad intelectual, las patentes y los derechos de autor, las telecomunicaciones, la protección de datos personales y la competencia económica. Asimismo, a través de una política fiscal que incluya estímulos apropiados, se debe impulsar la innovación y el desarrollo de tecnología que sirva para prevenir y mitigar amenazas a la seguridad cibernética.

De modo adicional, en lo atinente a la autorregulación, se estima necesario avanzar en cuanto a la utilización de instrumentos tales como certificaciones, mejores prácticas, protocolos internacionales, y normas corporativas vinculantes.

49 Internet Society, *Caminos Hacia Nuestro Futuro Digital. 2017 Internet Society Global Internet Report*, p.86. Disponible en: https://future.internetsociety.org/wp-content/uploads/2017/12/2017-Internet-Society-Global-Internet-Report-Caminos-Hacia-Nuestro-Futuro-Digital-EsFull-v1e.pdf (último acceso: 09/08/2018).

Finalmente, corresponde tener presente que una de las discusiones más importantes en el debate académico es el que se refiere a si la ciberseguridad es un bien público, o no lo es[50]. Esta definición es fundamental para poder regular la materia de forma integral.

IV.6. Gobernanza de Internet

Con respecto a la gobernanza de Internet, es necesario incorporar al análisis el enfoque de múltiples actores interesados, la adopción de mejores prácticas y recomendaciones no vinculantes, así como el estudio y la implementación de mecanismos ágiles y efectivos para la solución de controversias. La *Agenda de Túnez para la Sociedad de la Información* adoptada por la Cumbre Mundial sobre Sociedad de la Información (Ginebra 2003 – Túnez 2005) ha definido la gobernanza de Internet como: "[el] desarrollo y [la] aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet"[51].

Mary Ellen O´Connell[52] señala que la perspectiva que han decidido adoptar los gobiernos que tienen estrategias de seguridad más establecidas, implica que Internet sea protegida a través de la fuerza militar (de manera análoga a las estrategias seguidas en la época de la Guerra Fría). No obstante, esto va en contra de los objetivos de gobernanza de Internet y, sobre todo, de la participación de múltiples partes interesadas. Es por ello que se debe propiciar la regulación de Internet desde una aproximación pacífica. En efecto, *"[t]he motto should be: a good cyber defence is good cyber defence"*.[53]

50 Véase Nathan Alexander Sales, "Regulating Cyber-Security", *Northwestern University Law Review*, volume 107, número 4, 2013, pp. 1503-1568.

51 Cumbre Mundial sobre Sociedad de la Información, *Agenda de Túnez para la Sociedad de la Información*, WSIS-05/TUNIS/DOC/6(Rev.1)-S, 28 de junio de 2006, punto 34. Disponible en: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html (último acceso: 09/08/2018).

52 Mary Ellen O'Connell, "Cyber Security without Cyber War", *Journal of Conflict & Security Law* volumen 17, número 2, 2012, pp.187-209.

53 Mary Ellen O'Connell, "Cyber Security without Cyber War", p. 209.

IV.7. Perspectiva sancionatoria

Dentro de la perspectiva sancionatoria, es preciso abordar: los tipos penales, la responsabilidad de los Estados, la responsabilidad de los particulares, el poder sancionatorio de los Estados y la cooperación internacional.

Asimismo, se entiende que la regulación de la ciberseguridad debe darse a través de un cambio de paradigma legal. La forma en la que actualmente se la regula, básicamente pretende penalizar la conducta. Es decir, en el sistema normativo penal se tipifica ciertas conductas que implican vulneración de la ciberseguridad y se les atribuye sanciones.

Quedarse con el enfoque sancionador resulta insuficiente. Sería una opción muy limitada. Por el contrario, se considera que el tema de la ciberseguridad ha de ser abordado con un enfoque más amplio que incluya la prevención, la cooperación en el intercambio de información entre empresas privadas, entre empresas públicas y privadas, y con el gobierno. Los posibles ataques a los sistemas pueden poner a un Estado o a varios Estados simultáneamente, en una zona de alta vulnerabilidad. Por ejemplo, una intromisión al sistema financiero, bancario, de telecomunicaciones, de energía eléctrica, o el *hackeo* de información confidencial de las empresas privadas y de sus clientes, o bien de instituciones gubernamentales, puede tener repercusiones graves para la estabilidad de un país.

Conclusiones

En los tiempos que corren, es indispensable que los Estados de América Latina consideren la ciberseguridad como un asunto prioritario. El riesgo de vulneración cibernética es alto y va en aumento. Ello tiene repercusiones económicas negativas para los gobiernos y las empresas. Por eso se requiere la adopción de una actitud proactiva de parte de múltiples actores públicos y privados, que se traduzca en medidas concretas para prevenir y mitigar las amenazas, así como para actuar de manera efectiva cuando se produzca un incidente, recuperándose rápidamente.

En esta contribución se ha identificado una serie (enunciativa, no limitativa) de posibles perspectivas, ejes temáticos o líneas de investigación para el estudio de

la ciberseguridad: perspectiva internacional, derechos humanos, educación digital, economía digital, regulación y autorregulación, gobernanza de Internet y perspectiva sancionatoria. La problemática relativa a la ciberseguridad involucra cuestiones diversas y complejas, por lo que su análisis debe ser abordado propiciando un diálogo interdisciplinario. Así, será posible identificar las vías de acción más adecuadas para que los países latinoamericanos hagan frente a esta nueva realidad.

BIBLIOGRAFÍA

Abusaid, David *et al*, *Perspectiva de ciberseguridad en México,* McKinsey & Company, junio 2018, Disponible en: http://consejomexicano.org/multimedia/1528987628-817.pdf (último acceso: 29/06/2018).

Álvarez Valenzuela, Daniel y Vera Hott, Francisco, "Ciberseguridad y derechos humanos en América Latina", en Agustina Del Campo (comp.), *Hacia una Internet libre de censura II*: *Perspectivas en América Latina*, Ciudad Autónoma de Buenos Aires, Universidad de Palermo, 2017, pp. 37-63. Disponible en: https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf (último acceso: 08/08/2018).

Arrieta, Adolfo y Montes, Donicer, "Alfabetización digital: uso de las TIC's más allá de una formación instrumental y una buena infraestructura", *Revista Colombiana de Ciencia Animal*, volumen 3, número 1, 2011, pp. 180-197.

Burns, Nicholas y Price, Jonathon (eds.), *Securying Cyberspace. A New Domain for National Security,* Washington D.C., The Aspen Institute, 2012.

Chile, *Política Nacional de Ciberseguridad*, 2017. Disponible en: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf (último acceso: 09/08/2018).

Convenio de Budapest sobre la ciberdelincuencia, del 23 de noviembre de 2001, tabla de firmas y ratificaciones, actualizado al 09/08/2018. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/

treaty/185/signatures?p_auth=GLngzb88 (último acceso: 09/08/2018).

Convenio de Budapest sobre la ciberdelincuencia, del 23 de noviembre de 2001. Traducción al español avalada por el Consejo de Europa, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c (último acceso: 09/08/2018).

Coroiu, Viorel, "Conceptual Dimensions of Cyber Security", *European Journal of Public Order and National Security*, volumen II, número 7, 2015, pp. 17-20.

Cumbre Mundial sobre Sociedad de la Información, *Agenda de Túnez para la Sociedad de la Información*, WSIS-05/TUNIS/DOC/6(Rev.1)-S, 28 de junio de 2006. Disponible en: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html (último acceso: 09/08/2018).

Danca, Daniela, "The National and International Cyber Security Dimension", en *European Social Fund, International Conference Law Between Modernization and Tradition. Implications for the Legal, Political, Administrative and Public Order Organization, Bucarest, 21 al 23 de abril de 2015*, Bucarest, Editura Hamangiu, 2015, pp. 653-658.

European Union Agency for Network and Information Security (ENISA), *Cyber Security Culture in organisations*, 2017. Disponible para su descarga desde: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (último acceso: 09/08/2018).

Hernández, José Carlos, *Estrategias Nacionales de Ciberseguridad en América Latina*, Granada, Grupo de Estudios en Seguridad Internacional (GESI), 2018. Disponible en: http://www.seguridadinternacional.es/?q=es/print/1335 (último acceso: 09/08/2018).

Honduras. *Ley nacional de ciberseguridad y medidas de protección ante los actos de odio y discriminación en internet y redes sociales,* Proyecto presentado por el diputado Marcos Bertilio Paz Sabillón, con modificaciones efectuadas por la Comisión Especial, 8 de febrero de 2018. http://congresonacional.hn/wp-content/uploads/2018/02/DICTAMEN-LEY-DE-CIBERSEGURIDAD-I.pdf (último acceso: 09/08/2018).

International Telecommunications Union, *National Strategies Repository*, https://www.itu.int/en/ITU-D/

Cybersecurity/Pages/National-Strategies-repository.aspx (último acceso: 09/08/2018).

Internet Society, *Caminos Hacia Nuestro Futuro Digital. 2017 Internet Society Global Internet Report*. Disponible en: https://future.internetsociety.org/wp-content/uploads/2017/12/2017-Internet-Society-Global-Internet-Report-Caminos-Hacia-Nuestro-Futuro-Digital-EsFull-v1e.pdf (último acceso: 09/08/2018).

Internet World Stats. Usage and Population Statistics. Disponible en: https://internetworldstats.com/stats.htm (último acceso: 03/07/2018).

Lewis, James, *Economic Impact of Cybercrime. No Slowing Down*, McAfee y Center for Strategic and International Studies (CSIS), 2018. Disponible en: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email (último acceso: 09/08/2018).

Martin, Ioana, "Cyber Security Strategies - An Overview", *International Journal of Information Security and Cybercrime*, volumen 4, número 1, 2015, pp. 33-40.

México, *Estrategia Nacional de Ciberseguridad*, 2017. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (último acceso: 09/08/2018).

O'Connell, Mary Ellen, "Cyber Security without Cyber War", *Journal of Conflict & Security Law* volume 17, número 2, 2012, pp. 187-209.

Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*, Organización de los Estados Americanos y Banco Interamericano de Desarrollo, 2016. Disponible para su descarga a partir de: https://publications.iadb.org/handle/11319/7449?locale-attribute=es (último acceso: 08/08/2018).

Organización de los Estados Americanos y Symantec, *Tendencias de Seguridad Cibernética en América Latina y el Caribe*, Washington D.C., OEA, junio de 2014. Disponible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf (último acceso: 03/07/2018).

Rojas, Edwin Fernando y Poveda, Laura, *Estado de la banda ancha en América Latina y el Caribe 2017*, Santiago, Naciones Unidas, 2018. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf (último acceso: 29/06/2018).

Sales, Nathan Alexander, "Regulating Cyber-Security", *Northwestern University Law Review*, volume 107, número 4, 2013, pp. 1503-1568.

Statista, *Internet usage in Latin America. Statistics & Facts*. Disponible en: https://www.statista.com/topics/2432/internet-usage-in-latin-america/ (último acceso: 09/08/2018).

Stop.Think.Connect. Disponible en: https://www.stopthinkconnect.org (último acceso: 09/08/2018).

Tabansky, Lior, "Israel´s Cyber Security Policy, Local Response to the Global Cybersecurity Risk", en Metodi Hadji-Janev y Mitko Bogdanoski (eds.), *Handbook of Research on Cybersociety and National Security in the Era of Cyber Warfare*, Hershey, IGI Global, 2016, pp. 475-494.

Velasco San Martín, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Valencia, Editorial Tirant lo Blanch, 2012.

Venezuela, VenCERT, Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela. Sitio web: http://www.vencert.gob.ve/es-ve/ (último acceso: 09/08/2018).

Revista de Administración Pública

INAP

Esfera ética del ciberconflicto

Mario Vignettes

Resumen: Es necesario iniciar en México el debate de los límites éticos de la ciberseguridad ante la vertiginosa dinámica del mundo digital y la postura estratégica que están adoptando Estados, empresas e individuos alrededor del mundo.

Parte de este debate consiste en explorar la relación que existe entre la ciberseguridad y la ética desde la postura consecuencialista. Para este propósito se utilizan dos constructos básicos: la ciberdefensa activa y el ciberconflicto. Se plantean dos dilemas éticos fundamentales y se sugieren criterios básicos para superarlos. Finalmente se ofrecen cinco conclusiones generales. Esta colaboración es de carácter exploratorio y de ninguna manera puede esperarse respuestas definitivas a cuestionamientos tan profundos como las consecuencias éticas del uso de ciberarmas.

Palabras clave: Ciberdefensa, Medidas Activas, Dilema Ético, Ciberconflicto

Ethical sphere of cyber conflict

Abstract: It is necessary to start in Mexico the debate on the ethical limits of cybersecurity in the face of the vertiginous dynamics of the digital world and the strategic position that

states, companies and individuals are adopting around the world.

Part of this debate is to explore the relationship between cybersecurity and ethics from the consequentialist position. Two basic constructs are used for this purpose: active cyber defense and cyber conflict. Two fundamental ethical dilemmas arise and basic criteria are suggested to overcome them. Finally, five general conclusions are offered. This collaboration is exploratory in nature and in no way can definitive answers to such deep questions as the ethical consequences of the use of cyber weapons be expected.

Keywords: Cyber Defense, Active Measures, Ethical Dilemma, Cyber Conflict

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 16 de febrero de 2019

Revista de Administración Pública

INAP

Esfera ética del ciberconflicto

Mario Vignettes*

1. Enfoque y orientación

México es uno de los países más atacados del mundo desde el ciberespacio. Ello tiene consecuencias negativas en muchos ámbitos y niveles. Es necesario asumir que en el futuro, México requerirá adoptar medidas activas para reforzar la postura de ciberseguridad actual, lo cual implicará una revolución en la cultura estratégica nacional, lo que incluye plantearse y resolver dilemas éticos insólitos para nuestra sociedad.

A partir de los conceptos de ciberdefensa activa y ciberconflicto, se explora la relación entre la ciberseguridad y la ética desde la postura consecuencialista, porque la tradicional postura normativista es incapaz de caracterizar los dilemas que plantea una defensa activa en el ciberespacio. Las conclusiones que se ofrecen son de naturaleza provisional y quizá insuficientes, pero tienen el mérito de abril el debate nacional en la materia.

* Doctor en Derecho por la Facultad de Derecho de la UNAM. Diplomado en Ejercicio Jurisdiccional y Justicia Constitucional impartido por la Suprema Corte de Justicia de la Nación. Integra la planta docente del Instituto Nacional de Administración Pública (INAP) desde 2005. Ejerció profesionalmente la Inteligencia de Estado entre 1995 y 2018. Actualmente es Consultor en evaluación de riesgos y control de crisis.

El ciberespacio

El ciberespacio es un "ámbito intangible, de naturaleza global, soportado por TIC, que es utilizado para la interacción entre individuos y entidades públicas y privadas"[1] o dicho de otro modo, es un entorno "informativo evolutivo, interconectado, vagamente acotado que utiliza métodos de comunicación tecnológicamente gestionados por programas [que] almacenan, transportan, interpretan y median información a través de los dominios virtual y físico, interactuando con comunicación, información, y con elementos cognitivos y sociales"[2]. Permea la vida individual y social con creciente importancia y con repercusiones aún ambiguas.

Lo que sabemos es que su naturaleza ubicua hace obsoleto el concepto de frontera nacional, ya que el ciberespacio comprende a "todas las redes del mundo y cualquier cosa conectada a, o controlada por esas redes"[3]. Ello obliga a replantear las tradicionales categorías analíticas útiles para estudiar la geopolítica. Además, el ciberespacio cruza también las fronteras domésticas con los dispositivos cuyo uso harán realidad los "hogares inteligentes" y con ello, un monitoreo permanente y voluntario de los usuarios-consumidores-ciudadanos.

Precisamente por ello es indispensable contar con una definición de ciberseguridad. La Unión Internacional de Telecomunicaciones señala:

> "Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación,

1 Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

2 David Ormrod y Benjamin Turnbull, "The Cyber conceptual framework for developing a military doctrine", Defence Studies, 2016 Vol. 16, No. 3, Routledg, pp. 208 y 281. El gobierno federal mexicano lo concibe como "Realidad virtual o simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo", Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

3 R. A. Clarke y R. K. Knake, "Cyber war: The next threat to national security and what to do about it, New York, Harperd Collins, 2012, citado en David Ormrod et al., Op cit., p. 284.

> prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
> Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.
> La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio, y la confidencialidad"[4]

El Gobierno Federal mexicano utiliza la siguiente:

> "Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno"[5]

Ninguna incluye la noción "bien público" asociada a la definición de Ciberseguridad. Como toda clase de seguridad, ésta debe ser el desenlace virtuoso de una estrategia gubernamental comprensiva que guíe efectivamente a las instancias gubernamentales, pero sobre todo a la sociedad civil organizada (empresas, universidades, tanques de pensamiento) y a los usuarios individuales.

4 Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es, citado en Enrique Francisco Galindo Ceballos, La seguridad cibernética en el nuevo entorno operativo, Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, p. 186.

5 Gobierno Federal, Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

El ambito ético

Para efectos del este ensayo es necesario delimitar el alcance de tres términos que son contiguos, pero de ninguna manera sinónimos, a saber:

- Axiología es una disciplina filosófica enfocada en la "Teoría de los Valores". Estudia críticamente los valores éticos y estéticos, así como los "disvalores" que se asocian a aquellos. Por tanto, tiene un fuerte sentido teórico y didáctico.
- Moral es una técnica de control social que se caracteriza por ser: heterónoma, abstracta, unilateral y no coercitiva. Estas dos últimas características señalan su diferencia con el Derecho. La moral depende fuertemente del contexto social por lo que en un lugar y una época determinada, cierta conducta individual o colectiva puede ser calificada de inmoral por otra sociedad que se encuentre alejada en el espacio o en el tiempo. La moral está formada por usos y costumbres, es decir, la repetición de actos a través del tiempo que se consideran necesarios o imperiosos para alcanzar algún fin práctico. Por tanto, tiene un fuerte sentido deontológico y colectivo.
- Ética es una disciplina práctica centrada en la conducta humana y en la toma de decisiones en los ámbitos personal o profesional. A lo largo de la historia, se han definido dos grandes posturas que abordan esta disciplina:
  a) La deontológica, que postula que la ética es el estudio del fin de las conductas humanas y de la valoración de los medios para lograrlos. Esta postura, también llamada ´ética normativa´, es la más antigua y cercana a la axiología ya que tiende a considerar que los estándares éticos son absolutos y trascienden a toda circunstancia social o histórica, lo que marca una diferencia sustancial con la moral. Con base en este punto de vista, algunas profesiones o empresas establecen Códigos Éticos[6]. Desde el mismo

6 Esta postura tiene la ventaja de concentrar los «valores compartidos que guían la manera en que un individuo (y una organización) se comporta, y define una cultura institucional». Christopher E. Bailey, "The Intelligence Comunity ethos: a closely regulated profession", v. 3, n. 2, Autumn–Winter, 2012, p. 54. Disponible en: http://journals.fcla.edu/ijie/article/view/83453.

enfoque, el Poder Ejecutivo Federal adoptó un Código de Ética de los servidores públicos federales que incluye reglas de integridad[7] lo cual, sin duda, es meritorio en la medida en que sea conocido y practicado.

b) La consecuencialista, que sostiene que un acto particular es éticamente correcto o incorrecto, juzgando sus consecuencias reales[8]. Esta familia de escuelas éticas está arraigada en la tradición filosófica del utilitarismo. La diferencia más notable con la posición deontológica es que afirma que los estándares éticos son relativos en el tiempo y en el espacio, están vinculados a las circunstancias particulares del tomador de decisiones que designa como 'agente'.

Si bien ambos abordajes tienen cualidades, las características de la de ciberespacio no permiten, como se argumentará más adelante, estudiar con provecho el tema desde la ética deontológica.

2. Globalización y Ciberseguridad

El telón de fondo de cualquier comentario responsable sobre ciberseguridad es la realidad que plantea la globalización. Para Adda, la globalización se caracteriza por la progresiva unificación de los mercados mundiales de bienes, servicios y capitales, así como por una creciente integración mundial de la producción, lo cual genera el debilitamiento de las fronteras físicas y reglamentarias que traban la acumulación a escala mundial del capital[9]. Frente a esta realidad es que todo Estado soberano debe proyectar su poder nacional en promoción de sus intereses nacionales. Sin embargo,

> "Lo que hace a la globalización un componente nuevo y esencial de la seguridad internacional contemporá-

7 Código de Ética de los Servidores Públicos del Gobierno Federal, las Reglas de Integridad para el Ejercicio de la Función Pública, DOF del 20 de agosto de 2015, consultado el 10 de agosto de 2018, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5404568&fecha=20/08/2015

8 Es decir, no futuras, previstas, intentadas o deseadas; independientemente de las intenciones de su autor.

9 Cfr. Adda Jacques: La Globalización de la Economía, Editorial Sequitur, Madrid, 1999, p. 203.

> nea son las cada vez más complejas condiciones bajo las cuales los actores internacionales ejercen poder"[10].

Entre esas complejas condiciones debe contarse la esfera ética del ejercicio de poder, particularmente en el ciberespacio. Tras casi tres lustros, sigue siendo válida la reflexión de Kay en el sentido de que es muy difícil concluir con exactitud la forma en que la globalización impacta a la seguridad. Postula que:

> "Si la seguridad es la búsqueda por la ausencia o la mengua de riesgos en un mundo anárquico, la globalización debe incrementar o decrementar los resultados de seguridad. Si la seguridad es vista como una búsqueda particular de las naciones-Estados para proveerse de defensa, entonces la globalización también propicia tanto retos como oportunidades"[11].

Enfoquémonos en los retos. El 44% de los 9,500 ejecutivos de empresas que contestaron la encuesta sobre el Estado Global de la Seguridad de la Información 2018[12] afirman carecer de información sobre una estrategia de seguridad digital. Por otra parte, durante el primer semestre de 2018 se registraron 5.9 mil millones de ataques de a nivel mundial, es decir un 102% que en el mismo periodo de 2017, lo cual marca una tendencia mundial preocupante. Pero en México esos ataques se incrementaron en un 215% en el mismo periodo[13]. De hecho existen estudios que señalan a México como el "tercer país más vulnerado y con mayor índice de ataques a nivel mundial, únicamente detrás de Estados Unidos y el Reino Unido"[14]. Está claro que México enfrenta una variedad de ciberamenazas que han sido agrupadas en tres categorías, a saber:

10 Cfr. Sean Kay: "Globalization, Power, and Security", Security Dialogue vol. 35, no. 1. March 2004, p. 11.
11 Sean Kay, Op. cit., p. 10.
12 Christopher Castelli, Revitalizing privacy and trust in a data-driven world, Key findings from GSISS 2018 PWC, consultado el 21 de Agosto de 2018, disponible en https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf
13 Omar Ortega, "México, la tercera nación con más ciberataques en el mundo", El Financiero, 30 de julio de 2018, p. 42. Cita al Reporte Semestral de Ciberseguridad de SonicWall. Disponible en: http://www.elfinanciero.com.mx/tech/mexico-la-tercer-nacion-con-mas-ciberataques-en-el-mundo
14 Ibid.

> "...la ciberdelincuencia, especialmente el robo, el fraude y la difusión de pornografía infantil. La segunda es el ciberespionaje de Estados Unidos, Rusia, China e Irán, quienes buscan extraer información política, económica y comercial, sobre todo en materia energética. En tercer lugar está el desafío de de colectivos *hacktivistas* como *Anonymous*, los cuales poseen las capacidades necesarias para irrumpir en los sistemas del Estado e imponer sus agendas"[15]

Igualmente claro es que la sociedad civil requiere mucha mayor información respecto de tales amenazas, a juzgar por su comportamiento cotidiano. Un indicador de esa displicencia es que durante 2017 el sistema financiero mexicano se abstuvo de presentar denuncias de ciberdelitos[16].

El telón de fondo de lo anterior son los principios de política exterior con que el Ejecutivo Federal de México conduce las relaciones y que están señalados en la fracción X del artículo 89 constitucional.

> "Si bien la coherencia interna de estos principios fue una sólida base de acción en la etapa previa a la globalización, estos principios sin duda se convierten en limitaciones concretas a una participación más activa en la seguridad hemisférica, pues estaban fundados en una visión internacional en la que los Estados-naciones eran los actores centrales de las relaciones internacionales. Sin embargo, la configuración internacional ha cambiado de manera acelerada: las nuevas amenazas internacionales salen de la esfera de los Estados, el incremento de los intercambios a través de la telecomunicaciones y los flujos financieros atraviesan las fronteras virtualmente, la delincuencia organizada opera en redes con frecuencia articuladas con los poderes económicos y políticos de diversos

15 Edgar Iván Espinosa, Hacia una estrategia nacional de ciberseguridad en México, Revista de Administración Pública No. 136, Volumen L, Nº 1, (enero-abril 2015), INAP, México, p. 143.

16 Jeanette Leyva, "Bancos no acostumbran denunciar ciber delitos: PGR", El Financiero, 22 de agosto de 2018, p. 11.

países, factores ante los cuales la doctrina de política exterior, no está preparada para responder"[17].

El panorama concreto de la ciberseguridad en México ya ha sido diagnosticado a profundidad por expertos nacionales. Remitimos al lector a ensayos sólidos que describen detalladamente el esfuerzo del gobierno federal en materia de ciberseguridad[18], que plantean un inventario de acciones que deben ser asumidas por gobiernos, empresas y la sociedad civil para 2022[19] o bien que instan al establecimiento de un cibercomando plenamente operativo a partir del concepto de ciberdefensa[20].

De hecho, el Objetivo Sectorial 2 del Programa Sectorial de Defensa Nacional 2013-2018 denominado "Fortalecer el Sistema de Inteligencia Militar", tiene entre sus indicadores el 4 "Impulsar el desarrollo de la cuarta dimensión de operaciones militares denominada "ciberespacio", mediante la creación de un Centro de Operaciones del Ciberespacio". Ello se justifica porque "…se requiere desarrollar las capacidades de defensa y seguridad en la cuarta dimensión de operaciones denominada 'Ciberespacio', mediante la creación de un organismo, con instalaciones, equipo y personal adecuados, con el objeto de proteger y asegurar las Tecnologías de la Información y Comunicaciones de la SEDENA y en su caso, la red de infraestructura crítica nacional."[21] SEDENA debe replantear su postura a este respecto.

3. El ciberconflicto

La coyuntura revelada por los datos estadísticos citados, justifica examinar nociones que son arcanas a la sociedad

17 Raúl Benítez Manaut y Georgina Sánchez: Avances y Límites de la participación de México en la Seguridad Hemisférica en el Siglo XXI en "Cooperación y conflicto en las Américas. Seguridad Hemisférica: Un largo y sinuoso camino"; María Cristina Rosas (coordinadora); UNAM – Centro de Estudios de Defensa Hemisférica; México; 2003; pp. 167 y 168.

18 Enrique Francisco Galindo Ceballos, Op. cit., pp. 181 a 198.

19 Alejandro Pisanty, Algunos rasgos del futuro de las agendas digitales nacionales: el caso de México, Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, pp. 13 a 43.

20 Edgar Iván Espinosa, Op. cit. pp. 115 a 146.

21 Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

y la cultura estratégica mexicanas como ciberdefensa. Ignorar el cúmulo de amenazas de las que México es blanco en el ciberespacio, simplemente no es una opción.

El Estado mexicano entiende por ciberdefensa el "conjunto de acciones, recursos y mecanismos del Estado en materia de Seguridad Nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional"[22]. Este concepto no está definido en documentos oficiales mexicanos, pero si el de infraestructuras críticas de información, es decir, "Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia"[23]

Algunas de ellas son de uso dual y merecerían también protección bajo el concepto de ciberdefensa, piénsese en "… una amplia variedad de sistemas guiados por computadora, como la red del sistema de posicionamiento global satelital (GPS por sus siglas en ingles), e infraestructura de energía, comunicaciones, de agua potable o sanitaria, o bien sistemas de refinamiento petrolero o químico." [24]

La defensa se justifica por la necesidad práctica a cargo del Estado –en este caso México– de prevenir, acotar y responder a los ataques de adversarios o enemigos. Por tanto, su noción simétrica es la de ciberataque, concebido como "acciones deliberadas para alterar, desordenar, engañar, degradar o destruir sistemas o redes de cómputo o la información y/o programas residentes en o que están siendo

22 Gobierno Federal, Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

23 ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, en su versión publicada en el DOF, 2 de febrero de 2016.

24 Randall R. Dipert, The Ethics of Cyberwarfare, Journal of Military Ethics, Vol. 9, No. 4, 2010, p. 390. Se refiere a M. Walzer, Just and Unjust War, 4th ed., Basic Books, New York, 2006, pp. 144 a 151.

trasmitidos en esos sistemas o redes"[25] Todo administrador de sistemas y redes, públicas o privadas, es responsable de la defesa pasiva de las mismas. Esa es la premisa del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).

Según Randall R. Dipert "Si los ataques entre entidades políticas están suficientemente 'extendidos' entonces hablamos de ciberguerra"[26]. Según este autor es una cuestión de intensidad y de intensión. Empero, el término "guerra" tradicionalmente denota el uso de fuerza letal contra humanos en el marco de un conflicto armado entre comunidades políticas. La noción popular de ciberguerra se aleja de algunos de estos elementos. Por ello, en el medio estadounidense empieza a generalizarse el uso de "guerra kinética"[27] para implicar el efecto físico de la presión (proyectil, convencional o nuclear) o el fuego (explosión, convencional o nuclear) sobre humanos o estructuras y distinguirla así, de otras formas de agresión que no implican movimiento de fuerzas físicas como la guerra psicológica, la guerra económica, la guerra criptográfica, guerra electrónica, guerra sónica o la ciberguerra[28].

Ciberconflicto parece más adecuado para describir el contexto y las consecuencias de los ciberataques, y no por ello restarles peso a su impacto negativo que puede clasificarse desde la desobediencia civil hasta el terrorismo, lo cual no es menor. El ciberconflicto implica que un agente,

25 William A. Owens Kenneth Dam y Herbert S. Lin (ed.) Technology, Policy, law and Ethics regarding US adquisition and Use of Cyberattack Capabilities, The National Academy Press, Washington DC, 2009 citado en David Danks Y Joseph H. Danks, "The Moral Permissibility of Automated Responses During Cyberwar", Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 25.

26 Randall R. Dipert, The Ethics..., p. 397. Se ha sugerido la siguiente definición de ciberguerra "... el uso de computadoras para entorpecer las actividades de un país enemigo, especialmente el ataque deliberado de sistemas de comunicación" W. H. Boothby, , Oxford University Press, Oxford, 2012 citado en David Ormrod et al., Op. cit., p. 288.

27 Timothy Noah, Birth of a Washington Word, When warfare gets "kinetic", Slate, Noviembre de 2002, consultado el 5 de Agosto de 2018, disponible en: http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html

28 Para un estudio de la ciberguerra desde el Derecho Internacional Público remitimos al lector a María Pilar Llorens. Los desafíos del uso de la fuerza en el ciberespacio, Anuario Mexicano de Derecho Internacional, vol. XVII, enero-diciembre, UNAM, 2017, pp. 785 a 816.

individual o colectivo de forma autónoma o patrocinada, pero siempre voluntaria, explota "la infraestructura de red digital y la información contenida en ella, o impacta en los beneficios proporcionados por los sistemas de información enlazados en red, como parte de una ofensiva ideológica dirigida al gobierno, a la población, o a la industria de la nación".[29]

Lógicamente, el elemento definitorio del ciberconflicto es el instrumento por el que se causa daño, que en el ciberespacio es la ciberarma y que puede generar alteración, desórdenes, engaño, degradación o destrucción de sistemas o información. La dificultad inicia a partir de que no existe consenso internacional sobre lo que implica y denota exactamente ese término.

Una definición provisional define ciberarma como un "código de computadora que es usado, o diseñado para ser usado con el propósito de amenazar o causar daño físico, funcional o mental a estructuras, sistemas o seres vivientes", que incluye además dos dimensiones psicológicas, a saber: a) la intención del perpetrador de amenazar o de causar daño a un blanco, y b) la anticipación con la que el perpetrador anuncia su uso y su daño potencial[30]. Por su naturaleza incorpórea, toda ciberarma cuenta con una arquitectura peculiar que, al día de hoy, integra tres capas de ofensivo, a saber:

1. "Software de reconocimiento o espionaje para determinar la naturaleza o debilidad del sistema, y para impactarlo de forma única (en vez de, digamos, también dañar sistemas de información civiles).
2. "Software de producción de daño que altere de forma dañosa el comportamiento del del enemigo o que produzca otros efectos indeseables, incluyendo posiblemente muertes o daño físico a sistemas. Estas son las bombas lógicas o ciber en sí mismas.

29 G. Szentgali, The NATO policy on cyber defence: the road so far, Academic & Applied Research in Military Science (AARMS), No. 12, 2013, citado en David Ormrod et al., Op. cit., p. 289.

30 Thomas Rid y Peter McBurney, Cyber-Weapons, The RUSI Journal, Febrero de 2012, pp. 7 y 8, consultado el 10 de agosto, disponible en https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354

3. "Software de evaluación de daños que determinen la efectividad del de producción de daño."[31]

Pero no toda ciberarma es letal en el sentido literal de la palabra. Puede ser repelida antes de que produzca daño al ser "filtrada" por el sistemablanco o bien, ser removida y puesta en cuarentena al tiempo que el daño puede ser acotado reiniciando el sistema atacado con los datos existentes antes del ataque, acciones que pueden tomar desde microsegundos hasta semanas. Entonces, "Desde el punto de vista del uso ofensivo de la ciberarma, esto las hace armas de cuya efectividad disminuye rápidamente"[32] Por tanto podrían clasificarse en ciberarmas de grado civil y de grado militar. Para este último caso, existen tres categorías de blancos, a saber:

> "Primero, las ciberarmas pueden impactar e inhabilitar a las principales cadenas de comando, específicamente a las de comando y control; de comunicación y de recolección de información, así como a las de comunicación de órdenes precisas para maniobrar, defender, o atacar. Los datos de comando y control, podrían ser bloqueados alterados, o podría insertarse falsos informes u órdenes. La mayoría de las organizaciones militares modernas han endurecido sus canales de comunicación (tales como embeber, poner escudos o proteger de otras formas los cables eléctricos y ópticos), instalando esquemas de encripción elaborados, y sistemas redundantes.
> Segundo, las armas o los sistemas de armas pueden resultar inoperantes por un tiempo o incluso saboteados físicamente por mensajes falsos o intrusiones en los sistemas de información que los controlan; en caso extremo, podrían ser dirigidos por un enemigo para atacar un blanco falso.
> Finalmente, las ciberarmas pueden impactar la infraestructura de uso conjunto, esto es, sistemas y estructuras tanto para uso civil como militar, o incluso blancos civiles con la finalidad de desmoralizar, debilitar, o confundir al ejército enemigo y al liderazgo civil."[33]

31 Randall R. Dipert, The Ethics..., p. 391.
32 Ibid.
33 Randall R. Dipert, The Ethics..., pp. 389 y 390.

Pero este esfuerzo, aún incipiente, de definición y clasificación puede llevar a la falsa conclusión de que hay una comprensión cabal de las ciberarmas. Muy por el contrario, "los mecanismos mediante los cuales las ciberarmas mueven y afectan a las computadoras no son bien comprendidas, y uno puede imaginarse efectos ubicuos incluso peores a los de las armas químicas, que no son deseados pero que, sin embargo, afectan a áreas relativamente limitadas"[34] Esto es un dato cardinal para la esfera ética del ciberconflicto, ya que abre espacios de incertidumbre enormes.

Dos características que definen al ciberconflicto deben tenerse presentes: a) la ciberseguridad es cara en tanto que la acción ofensiva es comparativamente barata, lo que pone en desventaja a Estados y empresas frente a los perpetradores que van desde el individuo hasta los Estados patrocinadores de ciberataques y, b) los efectos laterales no deseados pueden ser más letales que el propio ciberataque y ser adecuadamente anticipados es particularmente difícil.[35]

Considerando lo anterior, generar inteligencia es aún más complicado. Empero, hacerlo es la respuesta racional de Estados y grandes empresas para acotar la incertidumbre que siembra el ciberconflicto. Ello llevará a una revolución dentro del mundo de la inteligencia porque las misiones se centrarán particularmente sobre: a) la configuración de la red de cómputo del adversario, b) la planeación del ciberataque, y c) el autor del ciberataque. La ubicación de los sistemas afectados es mucho menos importante[36]. Ello implica que la respuesta a esa clase específica de amenazas no se circunscribe al ciberespacio. Por el contrario, tiene un contexto social, un sustrato organizacional, un impacto económico y soporte en alguna red personal.

Otro género de dificultades surgen con las diferentes posturas estratégicas que puedan adoptar los blancos. La defensa o protección pasiva de la propia infraestructura e información, de los sistemas y su operatividad no parecen

34 Edward T. Barrett, Warfare in a New Domain: The Ethics of Military Cyber-Operations, Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 10.
35 Cfr. Randall R. Dipert, The Ethics..., p. 385.
36 Cfr. David Ormrod et al., op. cit., p. 289.

plantear mayores desafíos legales. Pero la postura de defensa activa, es decir las ciberoperaciones ofensivas, aún es debatida legalmente.

El argumento estrictamente legal es que el Derecho Internacional Público estipula que los civiles y los objetos civiles no deben ser 'objeto de ataque', porque un ataque kinético se define como el uso de fuerza que causa muerte, lesiones, daños, y destrucción. Sin embargo, un arma no letal deja de lado el uso de la fuerza como en el caso de sistemas de denegación activa (*active denial system* –ADS– por sus siglas en inglés) por tanto es lícito y ético usarlo contra perpetradores civiles[37].

Sin embargo, detrás de esta justificación están las suposiciones no comprobadas de que las ciberarmas no fallan y de que pueden contenerse las repercusiones de los cibertaques. Por supuesto, estos aspectos tienen sin cuidado a los perpetradores pero son necesaria materia de deliberación en las esferas militares y gubernamentales ya que los sistemas o los datos de civiles inocentes, pudiesen ser destruidos o inhabilitados por una respuesta activa. Ante una catástrofe informática desatada por una medida activa que sea percibida como injusta por el público, el Estado responsable podría ver mermada su base de apoyo público "sin importar cuan valioso sea al objetivo político"[38]

La posibilidad de que un ciberataque tenga repercusiones físicas similares a las de un ataque kinético, aún son escasas, pero no improbables. Por tanto, el "uso de la fuerza" en defensa propia, previsto en el artículo 51 de la Carta de las Naciones Unidas parece un fundamento endeble para normar la realidad que implica el cúmulo de ciberataques en las modalidades y niveles actuales, es decir, por ahora la justificación de estricto derecho de una defensa activa por parte de un Estado parece inoperante. Ello abre la posibilidad de explorar una justificación de orden ético partiendo de un abordaje alejado del normativismo.

37 Cfr. Edward T. Barrett, Op. cit., p. 11.

38 Charles J. Dunlap Jr., Some Reflections on the Intersection of Law and Ethics in Cyber War, Air & Space Power Journal, January-February 2013, pp. 27 y 28.

5. Ética consecuencialista[39]

El utilitarismo no está exento de detractores que con variado éxito, refutan sus posiciones más conocidas como el hedonismo. Sin embargo, desde Jeremy Bentham (1748-1832) o John Stuart Mill (1806-1873), el utilitarismo ha evolucionado dando origen, entre otras, a la ética consecuencialista que debe ser juzgada por sus méritos propios, y no en el marco del utilitarismo.

Ahora bien, hay posturas consecuentalistas que arrojan saldos absurdos, que no se revisan aquí en obvio de espacio y tiempo. Por ello, este ensayo se guía por el consecuencialismo evaluativo que establece que la calificación ética de una decisión debe basarse únicamente en el valor de las consecuencias realmente provocadas, sin considerar las características no evaluables de las consecuencias. Este enfoque ético distingue entre 'agente' que es el ser humano que realiza una acción y por tanto que toma una decisión, y el 'observador' que es todo aquel que reconoce una acción o decisión ajena, participe o no de sus consecuencias.

Para la mayoría de los consecuencialistas el valor de una consecuencia se identifica con la 'utilidad total' del acto o decisión, es decir su efecto benéfico. Sus teorías intentan expresar las condiciones necesarias y suficientes para que un acto sea considerado ético. Ello exime al 'agente' de calcular las diferentes utilidades derivadas de su acto, entre otras razones porque muy probablemente cometerán serios errores de cálculo que los llevarían a realizar actos que acotarían la utilidad. En cambio el agente debe seguir sus intuiciones éticas, ya que ellas lo conducirán a realizar actos o a tomar decisiones que maximicen la utilidad, al menos en circunstancias parecidas.

Los opositores a esta posición, de forma muy esquemática, han argumentado lo siguiente:

a) Si la utilidad total es el criterio de la corrección ética, entonces parecería que nadie podría establecer

39 El presente apartado sigue las líneas generales de Sinnott-Armstrong, Walter, "Consequentialism", (Winter 2015 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2015/entries/consequentialism/>.

lo qué es ético lo que desembocaría en un escepticismo general. Los consecuencialistas afirman que hay poderosas razones para creer que ciertos actos reducen la utilidad (terrorismo por ejemplo), aun en el caso de que no se haya evaluado cada consecuencia de un acto como ese, pero reconocen que existen severos límites al conocimiento de lo que puede ser éticamente correcto.

b) Hay que evaluar las consecuencias probables, previsibles o intencionadas en lugar de las reales. Las teorías que se enfocan en las consecuencias reales u objetivamente probables con frecuencia se describen como consecuencialismo objetivo, mientras que las que se centran en las consecuencias intencionales o previstas se agrupan bajo la denominación de consecuencialismo subjetivo.

Mediante el uso de la noción legal de causa próxima podrían acercarse ambas posiciones. Si los consecuencialistas definen consecuencias en términos de lo que es causado, entonces la noción de causalidad que se use para definir las consecuencias afecta directamente la clase y cantidad de eventos futuros que se asuman como consecuencias.

Cuando los actos voluntarios y las coincidencias intervienen en cierta cadena causal, entonces los resultados no son vistos como causados por los actos más allá de las condiciones necesarias que forman parte de la cadena causal. Ahora, si se asume que un acto debe ser una causa próxima de una consecuencia, un consecuencialistas argumenta que la corrección ética del acto está determinada únicamente por tal consecuencia próxima. Esta posición, que podría llamarse consecuencialismo próximo, hace más fácil para los agentes y para los observadores justificar los juicios éticos de los actos porque obvia la necesidad de predecir consecuencias no próximas en el tiempo o en la geografía.

Por otra parte, algunos consecuencialistas argumentan que un acto es éticamente incorrecto sí y sólo sí las consecuencias del acto incluyen un valor total menor desde la perspectiva del agente. Un movimiento clave aquí es adoptar la perspectiva del agente al juzgar el acto realizado, con ello se pretende capturar las intuiciones éticas de sentido común. Se aplicarán estas nociones más adelante.

Habiendo dicho eso, reflexionemos. Un ciberataque implica daño. El ciberdaño conlleva degradación del funcionamiento de un sistema (una persona, una máquina, un programa o una economía) o un artefacto (vehículo de conducción autónoma, marcapasos cardiaco inserto en una persona, por ejemplo) "causado intencionalmente por un agente, vía una red informática…"[40] para "crear efectos emergentes sobre sistemas interconectados de naturaleza física, social o de comportamiento"[41]

Para un país como el nuestro con el nivel de ciberataques registrados, es imperativo resguardar la integridad de sistemas y artefactos que benefician a los individuos mexicanos por medios pasivos, pero también es legítimo complementar nuestra ciberdefensa con medios activos, porque la promoción de la seguridad nacional implica la salvaguarda de la población, el territorio y el ejercicio de la soberanía en cualquier circunstancia.

6. Dilemas éticos del ciberconflicto

El problema de la atribución

Por la propia naturaleza del ciberespacio y de los ciberataques, la identificación de los perpetradores es una tarea compleja ya que con frecuencia, únicamente se cuenta con evidencia circunstancial. Dos incógnitas con repercusiones éticas plantea un ciberataque: a) atribuir el ciberdaño causado, y b) evaluar las consecuencias de responderlo activamente.

Sin duda, para justificar éticamente el adoptar una respuesta (R) en contra de una parte (P) se requiere determinar con alto grado de probabilidad que (P) es responsable de un intento real (H) del daño (D) y que éste implica violación a la soberanía y que causó intencionalmente degradación tangible a algún recurso nacional, sea de propiedad pública o privada, donde el monto de la justificación que es éticamente requerida depende en parte de la naturaleza tanto de R como de H, entre otros factores, como proporcionalidad, inmediatez

40 Randall R. Dipert, Op. cit., 397.
41 David Ormrod et al., Op. cit., p. 282.

y acotamiento de R exclusivamente a P [42]. Responder activamente, más concretamente, coordinar un contra ataque en el ciberespacio, implica iniciar un ciberconflicto[43] con todo lo que ello implica en el plano técnico, político, jurídico y ético.

Dipert opina que "Parece haber muy pocos casos históricos en los cuales un Estado haya sido atacado pero tenga muy poca información respecto de quién lo atacó". Las fuentes son fácilmente falsificables como "protocolos de internet (IP) o de los poco confiables de proveedores de internet (ISP)" [44]

Además, hay muchas técnicas informáticas y herramientas para ocultar la identidad propia en el ciberespacio "distribuyendo el ataque a través de múltiples sistemas o agentes, o disfrazando al responsable de algún H" [45] lo que tiene el potencial de involucrar a personas, sistemas e información inocente en un ataque. Parece poco probable que la definición de la identidad del perpetrador pueda lograrse por medios estrictamente técnicos.

Una solución ética y posible vendrá por lo que se ha llamado "métodos de atribución" que denota al conjunto de todas las "formas de inteligencia (electrónica y humana), junto con la información electrónica e información sobre las capacidades y los medios de producción del *malware*, y sobre la intención hostil [H]. Por tanto es mucho más probable, incluso si sigue siendo más incierto de lo que nos gustaría, identificar positivamente al agente hostil"[46] Pero existen tres dimensiones que hacen de esta tarea un reto formidable: a) distinción, b) la extensión, y c) tiempo.

a) Distinción: Sin lugar a duda hay Estados que utilizan los ciberataques como una herramienta de proyección del poder nacional, con lo cual una defensa activa es más fácil de justificar[47].

42 Cfr. David Danks Y Joseph H. Danks, Op. cit., p. 20.
43 David Ormrod et al., Op. cit., p. 289.
44 Randall R. Dipert, "Other-than..., p. 38.
45 David Danks Y Joseph H. Danks, Op. cit., p. 20.
46 Randall R. Dipert, "Other-than..., p. 38.
47 Una nación ciberhostil es "aquella que ha exhibido un patrón de ciber ataques o ciber espionaje extenso" Randall R. Dipert, "Other-than..., p. 48. Idealmente podría separarse estas dos formas de hostilidad.

Pero también muchos civiles con conocimientos especializados están motivados o patrocinados para atacar con ciberarmas. ¿Su condición de civiles los exime de responsabilidad? Éste es un asunto de complejo encuadre legal, si se atienden a las reglas ordinarias de la jurisdicción, al hecho de que no hubo intrusión al territorio o al espacio aéreo nacionales por personas (soldados) u objetos (aviones, tanques) y al hecho de que no existe consenso sobre lo que podría significar un "estado de ciberguerra".

Pero existen criterios que con autoridad pueden guiar la reflexión en este punto. Por ejemplo, interferir electrónicamente una red militar de computadoras o trasmitir inteligencia táctica de un blanco útil para un ataque específico, entre otros muchos ejemplos, implica para el Comité Internacional de la Cruz Roja que los civiles que así actúan "asumen una función de combate continua, en oposición a únicamente participar en hostilidades de forma espontánea, esporádica y desorganizada"[48]

b) Extensión: Por definición, el ciberespacio se estructura en un conjunto de redes donde los nodos son computadores de diferente capacidad, de propiedad pública o privada, y ubicadas prácticamente en cualquier punto del planeta. Como parte de las maniobras para ocultar su identidad los perpetradores usan esas redes para "distribuir el ataque". Un Estado que se defienda activamente de ese ataque podría causar daño intencional a propiedad pública o privada en puntos de la red geográficamente lejanos y de personas u organizaciones inocentes.

En un ciberataque, los recursos de una tercera nación frecuentemente están involucrados, sin ser atacante o atacado, ya que son los puntos de 'articulación' de ataque. "Empero, un análisis minucioso de las circunstancias de esos ciberrecursos de la tercera nación probablemente muestren que esas naciones han sido negligentes

48 Committee of the Red Cross, "Direct Participation in Hostilities: Questions and Answers", consultado el 10 de Agosto de 2018, disponible en: http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm

en 'supervisar' sus ISP's [proveedores de servicio de internet] y sus sistemas de usuarios, especialmente cuando esos medios de ciberataque son bien conocidos, como lo son ahora; de forma que ahora son usados para atacar a una tercera nación."[49]

Un Estado está obligado a proteger a sus ciudadanos, pero también a los ciudadanos de otras naciones, de las amenazas que se originan en su territorio. Hay quien opina que si no pueden hacerlo por falta de pericia o recursos deben acudir a la cooperación técnica internacional, pero si la rechaza "…pierde su derecho a la no intervención…"[50]

Pero esto ya ocurre a las espaldas de los gobiernos. La tecnología opera precisamente sobre la seguridad que otorga contar con datos distribuidos y consolidados alrededor del mundo.

c) Tiempo: Los ciberconflictos (ataque–defensa–contraataque) se resuelven "en segundos o incluso más rápido."[51] En todo caso, más allá de la reacción humana, lo que sugiere el uso combinado de "respuestas automatizadas" y de otra naturaleza, como generación de inteligencia mediante fuentes humanas, por ejemplo.

El punto es que el uso responsable y ético de respuestas automatizadas debería sustentarse en "políticas de la forma 'Si el evento E sucede en el contexto C, entonces ejecuta la respuesta R' (donde E, C y R pueden ser, todas, altamente complejas), donde R se ejecuta cada vez que los gatillos –combinaciones específicas de Es y Cs– ocurren son la necesidad, o quizás incluso la posibilidad, de ninguna intervención humana"[52]

Caracterizar el dilema ético conformado por las circunstancias anteriores clarificará las opciones a mano para México. Un fraseo posible es el siguiente:

Daño 1: La ciberdefensa integrada por medidas pasivas practicada por México hasta ahora lo coloca como el tercer país con mayor incidencia de

49 Randall R. Dipert, "Other-than..., p. 39.
50 Edward T. Barrett, Op. cit., p. 9.
51 David Danks Y Joseph H. Danks, Op. cit., p. 18.
52 David Danks Y Joseph H. Danks, Op. cit., p. 18.

ciberataques a nivel mundial lo que impacta negativamente a las personas, los negocios, y la infraestructura nacionales.

Daño 2: Una ciberdefensa integrada por medidas tanto pasivas como activas puede provocar "daños colaterales" domésticos y en el extranjero a personas o empresas inocentes, pero puede revertir la tendencia a la alza de la incidencia de cibertaques en México.

El problema de las consecuencias

Ante una ciberdefensa con medidas activas deben evaluarse las "reacciones en cadena". Al implementar tales medidas debe asumirse que el perpetrador opera con sus propias medidas de protección a su sistema de cómputo en anticipación a las medidas activas más obvias en inmediatas.

> "Si sus medidas son todas puramente defensivas, entonces el reto de la reacción en cadena no parecerá ser una barrera sustancial, ya que las acciones 'internas' del adversario no pareciera que fueran a desatar una respuesta ulterior para los defensores. Por supuesto, el mismo recurso que permite a los adversarios proteger sus propios sistemas también hace muy probable que algunas de esas contra respuestas automatizadas sean de naturaleza ofensiva. Los defensores incluso podrían tener conocimiento positivo… de que el adversario tiene instaladas ciber contra respuestas, y por tanto los defensores raramente sabrán algo más que 'es altamente posible una reacción en cadena'"[53]

Conviene complementar este cálculo de orden tecnológico con ponderaciones económicas, sociales y políticas. Pero implementar medidas activas automáticas siempre acarrea el peligro de caer en el "sesgo de auto proyección futura". Este consiste en que la decisión de establecer un sistema de respuestas automatizadas debe tomarse con base en predicciones condicionales, del tipo 'únicamente si se llega al hito de daño A se activan las contra medidas de clase A' "lo que demanda predecir las propias preferencias,

53 Ibid., pp. 25 y 26.

creencias y deseos futuros"[54] Ello añade una complejidad seria en un entorno en donde el orden mundial está cambiando de ejes[55] y donde los 'daños colaterales' pueden ser tan cercanos como el Hospital más próximo si es que computadoras ubicadas ahí están siendo parte de un ciberataque, sin que sus legítimos usuarios lo sepan.

El dilema ético que plantea el cálculo podría definirse de la siguiente manera:

Daño 1: La ciberdefensa integrada por medidas pasivas que practica México raramente provoca reacciones en cadena con lo cual, se evitan daños colaterales y si se provocasen, éstos se contendrían en las fronteras nacionales.
Daño 2: Una ciberdefensa integrada por medidas tanto pasivas como activas muy probablemente provoque reacciones en cadena y "daños colaterales" domésticos y en el extranjero.

7. Opciones éticas ante un ciberconflicto

Entonces ¿qué opción acota más el daño?, ¿la acumulación de ciberataques, que individualmente podrían no ser significativamente lesivos, motivan una medida activa de defensa?, si el daño causado a las activos nacionales no es físico como en la mayoría de los ciberataques actuales ¿la pérdida temporal de la funcionalidad de computadoras o sistemas, motiva una respuesta activa?, la autodefensa activa y anticipatoria ¿podría ser invocada en casos de espionaje o bombas lógicas cuando se calcula en desastrosos los daños potenciales? Las respuestas a estas preguntas son complejas. Empero existen opciones que pueden integrarse en un esquema de atención activo.

Primera. Cooperación internacional[56] en sus dos vertientes, preventiva para desarrollar infraestructura y

54 Ibid., p. 23.
55 Ya se vislumbra un orden asiático "Con la evolución de la tecnología moderna, las mayores potencias de Asia se han armado con arsenales militares muchísimo más destructivos que los que poseía el Estado europeo decimonónico más poderoso, con los consiguientes riesgos de error de cálculo" Henry Kissinger, Orden Mundial, 1ª. Reimp. Debate, 2017, p. 217.
56 Cfr. Charles J. Dunlap Jr., Op. cit., p. 27.

capacidades de ciberdefensa pasiva y activa para auxiliar diligentemente en la contención de un ataque en curso, de sus consecuencias, y en la ubicación geográfica de los nodos de las redes utilizadas para tal fin. Debe reconocerse que no están dadas las condiciones materiales para que la cooperación se cristalice en un acuerdo de control o prohibición del uso de ciberarmas, partiendo del hecho de que "Cualquier computadora es potencialmente una ciberarma y cualquiera con un conocimiento avanzado de sistemas de información es un potencial cibercombatiente."[57] Esta clase de entendimientos podrían fijar el grado de daño colateral que resulta tolerable en la eventualidad de que una de las partes se vea obligada a responder con un contrataque simple o automatizado, así como la naturaleza y extensión de las compensaciones que podrían exigirse para reparar el daño colateral.

Segunda. Ciberdefensa pasiva en los ámbitos públicos y privados guiados por una política pública que sea actualizada de forma frecuente. Ello se expresaría en forma de una mayor eficiencia en "la disuasión basada en negación en futuros intentos podría ser la única respuesta legítima"[58] Impulsar esa política con todos los instrumentos gubernamentales, desde la persuasión (comunicación social) hasta la coerción (supervisión y multa, pérdida de la concesión, etc.)

Tercera. Inteligencia especializada generada de forma autónoma o dentro de un esquema de cooperación bilateral, caso por caso, con la finalidad de entender la lógica y motivación del perpetrador, sus capacidades reales, su grado de cuidado en la preparación del ciberataque, de intentar reconstruir la red utilizada y ubicar físicamente el origen del ataque pasado como preparación de ataques futuros y en última instancia, su identidad.[59] Un buen lugar para empezar son los centros de desarrollo de *software* ya que,

> "Los conflictos futuros muy probablemente dependan fuertemente del para obtener una ventaja en rapidez

57 Randall R. Dipert, The Ethics..., p. 385.
58 Edward T. Barrett, Warfare in a New Domain: The Ethics of Military Cyber-Operations, Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 8.
59 Cfr. Ibid.

> y capacidad de ingestar grandes cantidades de datos para reducir el umbral de detección e identificar vulnerabilidades del adversario"[60]

Cuarta. Tecnología de autenticación avanzada cuyas mejoras incluyan biometrías y encripción para construir redes más confiables. Así lo reconoció el Grupo de los 20 (G20) en la declaración "Forjar un Mundo Interconectado" producto de su reunión sostenida en Hamburgo, Alemania, entre el 7 y el 8 de julio de 2017. Los veinte mandatarios argumentaron:

> "Confiar en las tecnologías digitales requiere una efectiva protección del consumidor, los derechos de propiedad intelectual, la transparencia, y la seguridad en el uso de TIC's. Apoyamos el libre flujo de información al tiempo de respetar los marcos legales atinentes a la privacidad, la protección de datos y los derechos de propiedad intelectual… Estamos comprometidos en ayudar a otorgar seguridad al entorno de las TIC's cuyos beneficios gozan todos los sectores y reafirmamos la importancia de atender colectivamente los temas del uso seguro de TIC's." [61]

Estas declaraciones políticas deberán respaldarse con presupuestos y entendimientos bilaterales. Mientras tanto, el *US National Intelligence Council* pronostica

> "requerirá establecer límites y estándares claros sobre la propiedad de datos, la privacidad y protección de datos, flujos transfronterizos de datos y ciberseguridad que podrían convertirse en puntos importantes de conflictos de políticas públicas domésticas e internacionales"[62]

La fuerza de los hechos y la intensidad de los ciberataques terminarán por mover la voluntad de las élites políticas y económicas, pero quizá no en la arena multilateral sino bilateral. Es muy alta la posibilidad de que los sistemas operativos más usados del mundo contengan "puertas

60 David Ormrod et al., Op. cit., p. 283.
61 Consultado el 29 de Agosto de 2018, disponible en http://www.consilium.europa.eu/media/23955/g20-hamburg-leaders_-communiqué.pdf
62 Christopher Castelli, Op. cit.

traseras" útiles para que el gobierno de EEUU o las mismas empresas desarrolladoras tengan acceso a que cualquier aplicación corra dicho sistema operativo. Ello motivó que Microsoft y el gobierno de la República Popular de China firmaran en 2003 un acuerdo que garantiza a éste último acceso al código fuente de Windows. Ello ya había sucedido con la OTAN, de Rusia, y del Reino Unido. Linux, con su sistema operativo de 'fuente abierta' quiere que miles de programadores alrededor del mundo aprovechen su acceso al código fuente y sugieran mejoras para acotar las vulnerabilidades que detecten. La motivación de Microsoft parecería más de orden político-comercial ya que,

> "En programas tan grandes como esos, es sin embargo intrínsecamente difícil entender el propósito o la debilidad explotable de cada línea o sección de código"[63]

China ya solicitó a las compañías que operan en su territorio "que mantengan los datos y aplicaciones de software dentro de las fronteras geográficas donde opera el negocio" para mantener control sobre los flujos transfronterizos de datos. Ello probablemente reducirá la eficiencia de las redes y tendrá algún efecto en la economía global. "La balcanización del internet cambiará la forma en que las compañías hacen negocios."[64] Esta cuasi regulación ad hoc tendrá también un impacto en contexto estratégico ya que podría constituirse internet para poderosos, para potencias emergentes y para pobres, lo que modificará la incidencia de ciberataques, registrada hasta ahora.

Quinta. Defensa activa dentro de un marco ético desde un abordaje consecuencialista, considerando al menos las tres dimensiones mencionadas líneas arriba: distinción, extensión y tiempo. Para lograr este último punto es necesario planeación de las respuestas, que en esencia son ciberataques automatizados.[65]

63 Randall R. Dipert, The Ethics..., p. 387.
64 Christopher Castelli, Op. cit.
65 David Danks Y Joseph H. Danks, Op.cit., p. 19.

El argumento básico para justificar éticamente una medida activa[66] de ciberdefensa es que el perpetrador ataque algún elemento de la infraestructura crítica nacional, precisamente por la extensión del daño que implicaría para esa sociedad la merma, inhabilitación o destrucción de algún componente de esa infraestructura. Pero ello implica otro dilema ético. Desafortunadamente ello implica que necesariamente,

> "Quedará una gran mayoría de sistemas y computadoras sin proteger, debido al costo. Y a través de estas computadoras y sistemas de información menos protegidos, como los orientados a finanzas, secretarías de Estado, y operaciones de contratación, probablemente podría fluir suficiente información para permitir a un enemigo sofisticado ensamblar las piezas e inferir información más sensible"[67]

Otro ingrediente de este cálculo estratégico es la "probabilidad de éxito" lo cual se facilita si se cuenta con inteligencia de algún tipo, sobre los métodos de ataque o los perpetradores frecuentes, aun si su identidad verdadera se ignora. Todos caen en patrones que a la larga dejan una 'firma' y terminan por ser predecibles.

Con todo ello se deberá imaginar y definir diferentes escenarios de ciberataque, en un ejercicio de prospectiva a nivel profesional y sofisticado. En cada uno de ellos se deberán fijar diferentes hitos de daño de manera que se programe la liberación de una clase de respuestas automáticas específicas cada vez que se llegue a un hito de daño o merma. Ello mantendrá proporcionalidad entre ataque y respuesta acotar el daño colateral causado e, idealmente, anunciarlo a otras naciones con las que se mantengan relaciones de cooperación bilateral en este campo. Por cierto, este último párrafo contiene los elementos esenciales de la misión de un Cibercomando, como el que reclama México.

66 Es decir, 'acciones deliberadas para alterar, desordenar, engañar, degradar o destruir sistemas o redes de cómputo o la información y/o programas residentes en o que están siendo trasmitidos en esos sistemas o redes' David Danks Y Joseph H. Danks, Op. cit., p. 25

67 Randall R. Dipert, "Other-than..., p. 45.

Conclusiones

Habiendo argumentado lo anterior, se arriba a los siguientes puntos:

a) Está éticamente justificado avanzar hacia una ciberdefensa integrada por medidas pasivas y activas.
b) Hacer de la ciberdefensa activa la misión institucional del Centro de Operaciones del Ciberespacio ya previsto. Apoyarlo con recursos humanos, financieros y materiales suficientes para hacerlo plenamente operativo en un lustro o menos.
c) Asumir como sociedad y como Estado que la ciberdefensa activa implica el desarrollo y uso de ciberarmas y que implica reinterpretar los alcances de los principios de política exterior consagrados en la fracción X del artículo 89 de la Constitución Política de los Estados Unidos Mexicanos.
d) Los protocolos de uso de las ciberarmas deben considerar al menos, los siguientes elementos inspirados en la ética consecuencialista:
   - La medida activa es una opción únicamente si se ataca algún componente de la infraestructura crítica nacional,
   - Para ser efectiva la medida activa puede ser automática, pero su uso será reactivo, nunca proactivo,
   - La medida activa automática es una opción siempre que su uso cause un 'daño colateral' menor al que provocaría el ciberataque,
   - El Estado mexicano debe asumir que toda medida activa provocará 'daño colateral' doméstico o en el extranjero que debe compensarse,
   - El uso de la medida activa debe ser graduado respecto de hitos de daño, definidos como parte integral de escenarios de riesgo concebidos con antelación,
e) La ciberdefensa que practique Mexico debe ser pública en sus líneas generales y debe poner énfasis en las medidas pasivas ya en uso y otras como:
   - Explorar esquemas de cooperación bilateral con países aliados,
   - Generar inteligencia especializada,
   - Invertir en tecnología de autenticación avanzada propia, lo que tendría un impacto favorable

al incluir a la sociedad civil en este esfuerzo nacional.

BIBLIOGRAFÍA

Adda, Jacques, *La Globalización de la Economía*, Editorial Sequitur, Madrid, 1999.

Bailey, Christopher E., "The Intelligence Comunity ethos: a closely regulated profession", International Journal of Intelligence Ethics, v. 3, n. 2, Autumn–Winter, 2012, p. 54. Disponible en: http://journals.fcla.edu/ijie/article/view/83453.

Barrett, Edward T., "Warfare in a New Domain: The Ethics of Military Cyber-Operations", Journal of Military Ethics, Vol. 12, No. 1, 2013.

Benítez Manaut, Raúl y Georgina Sánchez, "Avances y Límites de la participación de México en la Seguridad Hemisférica en el Siglo XXI" en *Cooperación y conflicto en las Américas. Seguridad Hemisférica: Un largo y sinuoso camino*; María Cristina Rosas (coordinadora); UNAM – Centro de Estudios de Defensa Hemisférica; México; 2003.

Castelli, Christopher, Revitalizing privacy and trust in a data-driven world, Key findings from GSISS 2018 PWC, consultado el 21 de Agosto de 2018, disponible en https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

David Danks Y Joseph H. Danks, "The Moral Permissibility of Automated Responses During Cyberwar", Journal of Military Ethics, Vol. 12, No. 1, 2013.

Dipert, Randall R. "Other-than-Internet (OIT) Cyberwarefare: Challenges for Ethics, Law, and Policy", Journal of Military Ethics, Vol. 12, No. 1, 2013.

_____, "The Ethics of Cyberwarfare", Journal of Military Ethics, Vol. 9, No. 4, 2010, p. 390. Se refiere a M. Walzer, Just and Unjust War, 4th ed., Basic Books, New York, 2006.

Dunlap Jr., Charles J., "Some Reflections on the Intersection of Law and Ethics in Cyber War", Air & Space Power Journal, January-February 2013.

Espinosa, Edgar Iván, "Hacia una estrategia nacional de ciberseguridad en México", Revista de Administración

Pública No. 136, Volumen L, Nº 1, (enero-abril 2015), INAP, México.
Galindo Ceballos, Enrique Francisco, "La seguridad cibernética en el nuevo entorno operativo", Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, p. 186
Kay, Sean, "Globalization, Power, and Security", Security Dialogue vol. 35, no. 1. march 2004, p. 11.
Kissinger, Henry, *Orden Mundial*, 1ª. Reimp. Debate, 2017, p. 217.
Leyva, Jeanette, "Bancos no acostumbran denunciar ciber delitos: PGR", El Financiero, 22 de agosto de 2018, p. 11.
Llorens. María Pilar, Los desafíos del uso de la fuerza en el ciberespacio, Anuario Mexicano de Derecho Internacional, vol. XVII, enero-diciembre, UNAM, 2017.
Noah, Timothy, Birth of a Washington Word, When warfare gets "kinetic", Slate, Noviembre de 2002, consultado el 5 de Agosto de 2018, disponible en:
http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html
Ormrod, David y Benjamin Turnbull, "The Cyber conceptual framework for developing a military doctrine", Defence Studies, 2016 Vol. 16, No. 3, Routledg.
Ortega, Omar, "México, la tercera nación con más ciberataques en el mundo", El Financiero, 30 de julio de 2018, p. 42. Cita al Reporte Semestral de Ciberseguridad de SonicWall. Disponible en: http://www.elfinanciero.com.mx/tech/mexico-la-tercer-nacion-con-mas-ciberataques-en-el-mundo
Pisanty, Alejandro, "Algunos rasgos del futuro de las agendas digitales nacionales: el caso de México", Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México.
Sinnott-Armstrong, Walter, "Consequentialism", T*he Stanford Encyclopedia of Philosophy* (Winter 2015 Edition), Edward N. Zalta (ed.), URL:
<https://plato.stanford.edu/archives/win2015/entries/consequentialism/>.
Thomas Rid y Peter McBurney, Cyber-Weapons, The RUSI Journal, Febrero de 2012, pp. 7 y 8, consultado el 10 de agosto, disponible en https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354

Documentos oficiales

Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

Código de Ética de los servidores públicos del Gobierno Federal, las Reglas de Integridad para el ejercicio de la función pública, DOF del 20 de agosto de 2015, consultado el 10 de agosto de 2018, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5404568&fecha=20/08/2015

Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, en su versión publicada en el DOF, 2 de febrero de 2016.

Committee of the Red Cross, "Direct Participation in Hostilities: Questions and Answers", consultado el 10 de Agosto de 2018, disponible en: http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm

Revista de Administración Pública

INAP

Inteligencia y ciberseguridad nacional

María José Rodríguez Rodríguez

Resumen: El objetivo de este artículo es documentar el papel sustantivo de la inteligencia para la seguridad nacional en la toma de decisiones estratégicas para la ciberseguridad nacional. Para ello se revisan los antecedentes del proceso en que la inteligencia se constituyó en un recurso de Estado, para después exlorar los aspectos del ciberespacio que plantean desafíos a la ciberseguridad nacional. El artículo continúa con un repaso de las características generales de los enfoques estratégicos a nivel europeo y de los Estados Unidos para enfrentar las amenazas a la ciberseguridad, poniendo énfasis en la relevancia que se otorga en cada caso a las tareas de inteligencia. Después de explorar el panorama general de la ciberseguridad en México, el rubro de conclusiones propone elementos para la discusión orientada a mejorar las condiciones de ciberseguridad nacional y sacar el mayor provecho de la inteligencia en esta empresa vital para el Estado mexicano.

Palabras clave: Inteligencia para la seguridad nacional, servicios de inteligencia, ciberespacio, estrategia de ciberseguridad, ciberamenaza

Intelligence and national cybersecurity

Abstract: The objective of this article is to document the substantive role of intelligence for national security in

strategic decision making for national cybersecurity. To do this, the background of the process in which intelligence was constituted as a State resource is reviewed, and then the aspects of cyberspace that pose challenges to national cybersecurity are examined. The article continues with a review of the general characteristics of the strategic approaches at European level and of the United States to face threats to cybersecurity, emphasizing the relevance given in each case to intelligence tasks. After exploring the general panorama of cybersecurity in Mexico, the conclusions section proposes elements for the discussion aimed at improving national cybersecurity conditions and making the most of intelligence in this company vital to the Mexican State.

Keywords: intelligence for national security; intelligence services; cyberspace; cybersecurity strategies; cyberthreat

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 31 de enero de 2019

Revista de Administración Pública

INAP

Inteligencia y ciberseguridad nacional

María José Rodríguez Rodríguez*

Introducción

Todo organismo por definición tiene un impulso vital de existencia cuyo ambiente favorece y desafía. El entorno de cada entidad vital y de todas en conjunto es un tejido denso de interacciones que impacta en sus expectativas de sobrevivencia y desarrollo. Conocer las características y potencialidades del entorno es un recurso clave para disminuir los riesgos y aumentar las posibilidades vitales; esta actividad se relaciona con el ejercicio de la inteligencia.[1]

Naturalmente esto aplica para el ser humano y las estructuras sociales creadas como expresión de su vida en comunidad –familia, clubes, partidos políticos, empresas, gobiernos– hasta llegar a la forma más compleja de organización: el Estado. Más que la llana sobrevivencia, cada una tiene objetivos e intereses conforme a su razón de ser, en los que concentran su atención y recursos para desarrollar capacidades para tomar decisiones en el presente y en el futuro.

* Estudios de Doctorado Relaciones Internacionales e Integración Europea. Universidad Autónoma de Barcelona, España. Master Universitario en Seguridad y Defensa Universidad Complutense de Madrid, España. Licenciatura en Ciencias Políticas y Administración Pública. UNAM, México. Experiencia profesional y académica en el campo de la Inteligencia para la Seguridad Nacional, de más de 25 años. Consultora y Profesora Experta en Análisis de información e inteligencia

1 El símil entre biología e inteligencia lo retomo del historiador David Kahn, quien destacó que el conocimiento del entorno para enfrentar sus amenazas es un impulso biológico básico, y que en ese reflejo está la base de la necesidad de inteligencia. David Kahn, "An Historical Theory of Intelligence", *Intelligence and National Security*, vol. 16, no. 3, Autumn, 2001, p. 79 [traducción propia]

El cierre del siglo XX fue testigo del surgimiento de un nuevo entorno de creación humana: el ciberespacio. Su profusa red de procesos y sistemas de flujo de información, interconectados e interdependientes, ha tendido una estructura puente entre el plano puramente digital y el ambiente físico. El ciberespacio ha ampliado y diversificado oportunidades de desarrollo en todos las vertientes de la actividad humana, y al mismo tiempo generado desafíos al funcionamiento y viabilidad de los Estados en un sentido amplio, grupos e individuos.

Sucesivos ataques registrados en distintas partes del mundo –contra instalaciones estratégicas, sistemas bancarios y financieros, bases de datos oficiales y empresariales, así como operaciones de influencia de la opinión pública– demuestran que el ciberespacio es un terreno activo de operaciones de inteligencia, que buscan ventajas para los intereses políticos y económicos de sus respectivos Estados, a costa de las vulnerabilidades de otros.

Este artículo tiene como objetivo destacar el papel sustantivo de la inteligencia para la seguridad nacional en la toma de decisiones estratégicas de los Estados relativas a su política de ciberseguridad nacional. El planteamiento tendrá como referentes los enfoques académicos actuales sobre Inteligencia, y la visión estratégica de la Unión Europea y los Estados Unidos en la materia. En última instancia lo que se busca es incentivar la discusión respecto al modelo óptimo y eficaz que debe construirse en México para enfrentar la ciberseguridad, con el componente de inteligencia/contrainteligencia bien integrado.

1. Inteligencia como recurso estratégico del Estado

La inteligencia como una práctica se remonta al pasado más lejano de la historia humana.[2] Básicamente, hasta

2 El interés por la historia de la inteligencia ha ido en aumento por parte de académicos civiles y militares alrededor del mundo, asi como para los interesados en desarrollar una historia política internacional, como para los especialistas en épocas, paises y culturas específicas. En todos los casos hay un acuerdo de que las referencias más antiguas sobre la práctica de la inteligencia es un fragmento en la *Biblia* (Libro Números, 13), el *Arte de la Guerra*, de Sun Tzu (cap. 13, "Uso de los Espías") y el indú *Arthasastra,* de Kautilya (100 a.C.). En 2018 Cristopher Andrew publicó un libro único en su tipo en el que trata de integrar toda la evidencia disponible sobre la historia de la inteligencia tanto en Oriente como en Occidente. Cristopher Andrew, *The Secret World. A History of Intelligence,* Yale: Yale University Press, 2018, 960 págs.

casi la mitad del siglo XX, consistía en personas que de forma encubierta o sigilosa recolectaban información valiosa sobre las motivaciones, planes y capacidades de un adversario interno o externo, para uso directo de los objetivos de emperadores, reyes, reinas, sultanes, jefes de la corte, jefes militares, obispos, entre otros. Todos ellos especialmente hábiles para obtener información secreta que permitiera a su cliente tomar decisiones anticipadas para ganar una guerra o preservar y ampliar su poder. Pero estas actividades carecían de procesos y métodos apoyados por una organización, los agentes estaban guiados por la intución y la experiencia propia.[3]

Con todo, las llamadas *fuentes humanas* hasta el día de hoy son el recurso central de recolección de inteligencia. Conforme avanzaría la historia surgirían otras fuentes que ampliarían el abanico de opciones de acceso a información valiosa, y que en su momento le darían mayor realce a la inteligencia para ser tomada en cuenta de forma estructural por gobiernos y Estados.[4]

La práctica de inteligencia tuvo nuevos alcances en el marco de la progresiva complejización y extensión geográfica de los conflictos militares y del impresionante avance tec-

3 Sun Tzu advirtió que el perfil del soldado promedio no era el adecuado para recolectar información, sino que se requería de otra clase de espacialistas que, ya por entrenamiento o capacidad innata, pudieran identificar qué información era significativa y fueran los suficientemente astutos o tramposos para obtenerla. Clauser añade: agentes y espias han sido siempre parte de cualquier sistema de inteligencia encubierto y probablemente continuarán siéndolo. Jerome Clauser, "The evolution and Definition of Strategic Intelligence", *An introduction to intelligence research and analysis*. Maryland: Scarecrow Professional Intelligence Education Series, No.3, Scarecrow Press Inc., 2008, p.1

4 Las fuentes humanas se conocen también por su acrónimo en inglés HUMINT, que viene de *human intelligence*. Se define como: "Tipo de inteligencia que se elabora a partir de la información recogida o suministrada directamente por personas... La información suministrada por fuentes humanas es muy útil porque puede proporcionar información imposible de adquirir por otros medios. Una fuente humana situada en el lugar y el momento adecuados puede dar a conocer los procesos de deliberación y las intenciones reales de un determinado adversario. También puede proporcionar las claves necesarias para interpretar los datos conseguidos mediante medios tecnológicos. Miguel A. Esteban, *Glosario de Inteligencia*. Madrid: Ministerio de Defensa, 2007, 87-88 p.p.

nológico. Con el inicio del siglo XX arrancó su reposicionamiento, en medio de Ia I Guerra Mundial (I-GM)[5] y con la invención de la comunicación por radio.[6] La radio trajo por primera vez la posibilidad de transmitir comunicaciones instantáneas en plena guerra: instrucciones de mando, de defensa y ataque, alertas sobre los movimientos del enemigo, la situación del campo de batalla, capacidades humanas y materiales, informes de daños… Un incesante flujo de información vital que fluía a través de los aires con la misma rapidez que se generaba. La posibilidad de intervenir estas comunicaciones de forma instantánea amplió los márgenes para actuar con anticipación. Con ello, la radio abrió paso a una nueva fuente de inteligencia conocida como inteligencia de intercepciones o inteligencia de señales –SIGINT[7]– la primera de tipo técnico.[8]

Países como Alemania, Estados Unidos, Italia y Reino Unido apreciaron el potencial de consolidar capacidades de recolección SIGINT, apoyada en el surgimiento del *criptoanálisis* para descifrar los mensajes del adversario

5 La I-GM transcurrió del 28 de julio de 1914 al 11 de noviembre de 1918, e involucró alrededor de 30 países de todos los continentes, menos Oceanía.

6 La revolución que provocó este invento abrió el camino a las comunicaciones inalámbricas. Se atribuye a Guillermo Marconi la invención de la radio en 1901, quien conectó Canadá (Terranova) con Inglaterra (Poldhu, Cornualles) mediante una señal radiotelegráfica, aunque actualmente se ha reivindicado al serbio Nikola Tesla como su inventor.

7 En concreto el acrónimo SIGINT es hoy en día un: "Tipo específico de la inteligencia técnica que se elabora a partir de la obtención y el procesamiento de datos provenientes de la detección, intercepción y descifrado de señales y transmisiones de cualquier clase. Es un término genérico que se emplea para designar el uso conjunto de datos provenientes de la inteligencia electrónica (ELINT), de la inteligencia de telecomunicaciones (COMINT) y de la inteligencia de mediciones (MASINT)… La inteligencia de señales es también la base para la guerra electrónica: el conjunto de acciones militares destinadas a la búsqueda, intercepción, identificación, perturbación y eliminacion de la emisión de radiaciones electromagnéticas por el adversario." Miguel A. Esteban, *op. cit.,* p. 89

8 TECHINT vine del inglés *technical intelligence*. "Tipo de inteligencia que se elabora a partir de la obtención y el procesamiento de información mediante el uso de medios técnicos. Es un término genérico que se emplea para designar el conjunto de datos provenientes de la inteligencia de señales (SIGINT) y la inteligencia de imágenes (IMINT)." *Ibid*., p. 93

obtenidos por SIGINT.[9] A contramano, empezaron a desplegar capacidades de *encripción* y *codificación,* como una medida de contrainteligencia[10] para proteger sus comunicaciones de la intercepción enemiga.

Un caso emblemático es el TELEGRAMA ZIMMERMANN (1917)[11] que para algunos historiadores de inteligencia es el "éxito más importante en la historia de inteligencia",[12] como ejemplo del poder y oportunidad que implica controlar el flujo de comunicaciones del adversario, pudiendo incluso cambiar el rumbo de la Historia. Brevemente, en plena I-GM la inteligencia naval británica interceptó y descifró un telegrama en que Alemania proponía a México aliarse en contra de Estados Unidos. Entonces la ferocidad de la guerra hacía estragos en el bando aliado sin verse claro el ingreso de Estados Unidos. El telegrama con la amenaza alemana matizó la oposición de la opinión pública a la entrada a la I-GM.

9 Kahn señala: "Gran Bretaña, Alemania, Italia y los Estados Unidos, ninguno de los cuales antes de la guerra, había tenido agencias `codebreaking' [para descifrar códigos y mensajes encriptados de los países adversarios] las establecieron después de ésta. Alemania, el Estado más conservador, cuyo cuerpo de generales había subordinado durante mucho tiempo la inteligencia a la planificación, creó por primera vez en su historia una agencia militar permanente en tiempo de paz para evaluar toda la información. La inteligencia se había convertido en un importante instrumento de guerra." Kahn, 2001 *op.cit.,* p. 82 [traducción propia]

10 "Actividades dirigidas a anular el conocimiento que los servicios de inteligencia extranjeros tratan de adquirir sobre aspectos escenciales del estado en los ámbitos político, económico o de serguridad. Por su enorme relevancia, es frecuente que los servicios dispongan de un órgano dentro de su estructura dedicado exclusivamente a contrainteligencia." Miguel A. Esteban, *op.cit*, p. 64

11 El libro de la historiadora Barbara Tuchman sobre el *telegrama Zimmermann* es una obra de referencia fundamental, poco conocida en México, para comprender los escenarios que convergieron en el entramado de este fascinante caso, que muestra también el valor geoestratégico de México para los intereses en juego de los actores en la I-GM. En 1917 la inteligencia naval inglesa interceptó y descifró un telegrama enviado por el Ministro de Asuntos Exteriores de Alemania, Arthur Zimmermann en que proponía a México (expresamente a su entonces presidente Venustiano Carranza) ir a la guerra contra Estados Unidos. A cambio los alemanes prometían reintegrar a México "el territorio perdido" de Texas, Nuevo México y Arizona. Para los estrategas germanos este escenario sustraería la atención de EEUU del conflicto militar en Europa y retrasaría aún más su entrada a esa guerra. Sin embargo, la operación inglesa dinamitó el plan alemán, que lo filtró al gobierno norteamericano y éste a la opinión pública. Estados Unidos entró a la IGM el 6 de abril de 1917. Barbara Tuchman, *El Telegrama Zimmermann. El documento secreto que cambió la Primera Guerra Mundial*. Barcelona: Edit. RBA. 2010, 333 págs.

12 *Idem.*

Después de un inestable período de entreguerras,[13] las capacidades desarrolladas en HUMINT y SIGINT siguieron demostrando ser decisivas en tiempos de guerra, ahora con la II Guerra Mundial (II-GM).[14] En ese escenario también se comprobó que una inteligencia deficiente y mal integrada tenía efectos catastróficos para un Estado, al ser incapaz de evaluar su entorno y anticipar riesgos estratégicos. El caso emblemático fue el BOMBARDEO JAPONÉS A PEARL HARBOR, EEUU (6 de diciembre de 1944) que causó la destrucción de la flota norteamericana en el Pacífico y precipitó la entrada de Estados Unidos a la II-GM. Este evento es un caso clásico de estudio como el primer *error de inteligencia*[15] del siglo XX, por la incapacidad de evaluar la amenaza japonesa y anticipar su ataque. Aunque al final el triunfo fue nuevamente del bando aliado, para los Estados quedó el desafío de contar con capacidades más allá de espías y cables, se necesitaba obtener algo más que los datos provenientes de la información recolectada para dilucidar una realidad cada vez más compleja.

El hito clave para la inteligencia lo marcó la Guerra Fría (1946-1989), el conflicto por diferencias ideológicas e interéses geopolíticos que enfrentó a Estados Unidos con la entonces Unión de Repúblicas Socialistas Soviéticas (URSS). Para comprender las amenazas, riesgos y oportunidades de este escenario de confrontación global, ya no sólo de tipo militar, hacía falta la interpretación del significado de los datos recolectados y su análisis por es-

13 El periodo de entreguerras fue del 11 de noviembre de 1918 al 1º de septiembre de 1939, fecha en la que inició la II-GM, que a su vez concluyó el 2 de septiembre de 1945.

14 De esta época datan los casos de éxito de la célebre máquina inglesa ENIGMA que rompió los códigos de encripción alemana con fama de indestructibles, frenando a la armada germana en el Atlàntico, y a la Wehrmacht en Francia (1944). Otros éxitos "Por ejemplo, el agrietamiento de la máquina *púrpura* japonesa permitió a los aliados leer los despachos del embajador japonés en Alemania, lo que el Jefe de Estado Mayor del Ejército de Estados Unidos, George C. Marshall, llamó *nuestra principal base de información sobre las intenciones de Hitler en Europa*. La batalla de Midway, que dio vuelta a la marea de la guerra en el Pacífico, fue posible por la inteligencia de 'codebreaking'." David Kahn, *op.cit.,* p. 83 [traducción propia]

15 Roberta Wohlstetter escribió un libro clásico sobre este caso, en el que señaló como causas de este error de inteligencia de Estados Unidos al: 1) sesgo de la evaluación de la amenaza japonesa; 2) la falta de análisis de la información recolectada, y 3) rivalidades entre las burocracias de las instituciones de seguridad. Roberta Wohlstetter, *Pearl Harbor. Warning and Decision*, Stanford: University Press, 1963, 428 págs.

pecialistas de distintas disciplinas, para integrar un producto relevante, oportuno y a la medida para la toma de decisiones de corto, mediano y largo plazos. Eso implicaba capacidades para dilucidar crisis presentes y proyectar escenarios futuros mediante la interpretación y análisis de la información, en apoyo al diseño de políticas de seguridad; con ello surgía la *inteligencia estratégica*[16] como misión de los servicios de inteligencia, bajo control Ejecutivo. Asi la Guerra Fría fue el escenario en que la inteligencia se convirtió en recurso institucional del Estado.

Adicionalmente, las características de este período determinaron la entonces naciente concepción de seguridad nacional, que Arnold Wolfers enunció como la ausencia de amenazas a los valores nacionales y la ausencia de temor de que estos sean atacados.[17] Esta concepción colocó al Estado como el objetivo central de la seguridad nacional, y asignó a los servicios de inteligencia de reciente creación la misión de generar inteligencia para la seguridad nacional:[18]

> "...conjunto de instancias de gobierno que llevan a cabo actividades secretas, incluyendo acciones

16 Para el autor clásico Sherman Kent, el padre del análisis de inteligencia, la inteligencia estratégica tiene como objetivo ayudar a proteger y a avanzar los intereses vitales del Estado. Requiere del conocimiento que evalúe las capacidades e intenciones de otros Estados, tanto en tiempos de guerra como en tiempos de paz. Además de la información obtenida de fuentes de inteligencia, para Sherman Kent no hay sustituto para el trabajo intelectual y el sentido crítico aplicados al análisis de inteligencia. Sherman Kent, *Strategic Intelligence for American Policy* (preface) Princeton: Princeton University Press, 1966, 2nd print., VII-XXIV p.p.

17 Arlond Wolfers, "National Security as an Ambiguous Symbol", *PressDiscord and Collaboration. Essays on Internacional Politics.* Baltimore: John Hopkins University, 1962, 149-154 p.p. [traducción propia]

18 Mark Lowenthal enlista sobre los objetivos básicos de un servicio de inteligencia: a) evitar una sorpresa estratégica que ponga en riesgo la existencia del Estado, por eso tan importantes sus capacidades de alerta y anticipación; b) proporcionar experiencia de largo plazo a los gobernantes, por parte de funcionarios altamente especializados en asuntos de seguridad nacional; c) apoyar al diseño y ejecución de políticas de seguridad nacional; y d) garantizar la secrecía de la información, métodos, fuentes de trabajo, requerimientos que atienden y de las prioridades de los tomadores de decisiones. La creación de los servicios de inteligencia requirió de reformas político-adminsitrativas por parte de los gobiernos para crear organizaciones especificas de naturaleza civil y/o militar, para el apoyo de los niveles ejecutivos. Mark Lowenthal, *Intelligence. From Secrets to Policy.* Los Angeles: SAGE/CQ Press, 2012, 5th edit., 2-4 p.p. [traducción propia]

> encubiertas, contrainteligencia y, principalmente, de recolección y análisis de información con el objetivo de esclarecer las deliberaciones de los responsables de la política, mediante el conocimiento oportuno y preciso de potenciales amenazas y oportunidades."[19]

Con ello, el arco presentado hasta aquí muestra que la consolidación de la inteligencia como un recurso de Estado alcanzó un momento clave con el surgimiento de organismos profesionales (de naturaleza militar, civil y policial) dedicados exclusivamente a la generación de inteligencia para la seguridad nacional –mediante su proceso de planeación, recolección, procesamiento y análisis, difusión y retroalimentación–, conocido como *ciclo de inteligencia.*[20]

2. Naturaleza del ciberespacio

El ciberespacio interesa al poder público y a todos los sectores de la sociedad en su conjunto por las ventajas que ha traido consigo. A nivel estatal este entorno y sus herramientas han sido positivas para: el diseño y ejecución de políticas nacionales, la eficiencia de sus procesos administrativos y de prestación de servicios a la ciudadanía, y la operación de las instituciones y su integración en sistemas nacionales (v. por ejemplo, procuración de justicia y seguridad nacional), entre otros. De igual forma los sectores industrial, privado y financiero han sido beneficiados con procesos automatizados de producción, distribución y oferta, asi como las corrientes de innovación y los fujos de inversión. Por su parte, la democratización del acceso a las tecnologías de información y sus dispositivos, ha empoderado a personas y sociedades por posibilitar su acceso al conocimiento especilizado, y a canales digitales de expresión, intercambio y organización.

19 Loch Johnson, *National security intelligence. Secrets operations in the Defense of Democracies,* Cambridge: Polity, 2017, 2nd Edit., p. 16 [traducción propia]

20 Para profundizar en el proceso de generación de inteligencia y sus nuevos enfoques se recomienda: Phythian, Mark (ed.), *Understanding the Intelligence Cycle.* London: Routledge, 2013, 184 pags.

De manera general el ciberespacio es un entorno de actividad humana y tecnológica alrededor de la información, cuyo surgimiento implicó una revolución que aún no concluye.[21] Para Machin y Gazapo (2016) el ciberespacio es un dominio de comunicación "…un conjunto de dispositivos conectados por redes en las que se almacena y se utiliza la información electrónica así como el espacio donde diversos actos comunicativos tienen lugar."[22]

El internet es la red que articula al ciberespacio que crece sin parar, primero por el proceso global de digitalización de la información,[23] seguido de la expansión y penetración de las tecnologías de información en los servicios de la vida diaria: alimentación, energía y combustibles, comunicación, transporte, educación, trabajo, economía, finanzas y seguridad, entre otros.

El ciberespacio se encuentra en expansión: en 2012 se registró un 34.3% de población mundial conectada a internet, que en 2018 creció a 55.1% de usuarios (equivalente a poco más de cuatro mil millones), según el corte de Internet World Stats (2018) Ver cuadro 1.

21 La irrupción de la Revolución de la Información que desconcentró los puntos de emisión y difusión de la información –hasta ahora en manos de gobiernos y sus agencias, y de los medios de comunicación tradicional–, y democratizó el acceso a dispositivos digitales (desde computadoras hasta smartphones) y al propio internet –recuérdese que la red fue una invención de la defensa norteamericana– que sólo se liberó en la pasada década de los noventa cuando se abrió a las universidades y centros de investigación.

22 Nieva Machin. y Manuel Gazapo. "La seguridad como factor crítico en la seguridad europea*", Revista UNISCI / UNISCI Journal,* No 42 (Octubre/October 2016) p. 49

23 "Esta explosión de datos es relativamente nueva. Recientemente, en el año 2000, sólo una cuarta parte del universo de información almacenada estaba en digital. El resto fue preservado en papel, películas y otros medios analógicos. Pero debido a la veloz expansión de la cantidad de datos digitales, que se duplican alrededor de cada tres años, esa situación se revirtió en un abrir y cerrar de ojos. En la actualidad, se estima que menos del 2% de toda la información almacenada es *no-digital*." **Kenneth Cukier* y Viktor Mayer-Schoenberge "**El auge de los grandes volúmenes de datos. Cómo está cambiando nuestra forma de ver el mundo", en *Foreign Affairs Latinoamérica***, v. 13, n. 3, julio – septiembre, 2013, 132 – 143 p.p.**

Cuadro 1
"Estadística de uso mundial de internet y población"
Actualizada al 30 de junio, 2018

ESTADÍSTICAS DE POBLACION Y USO DE INTERNET A NIVEL MUNDIAL ACTUALIZADO AL 30 DE JUNIO DEL 2018						
Regiones del mundo	Población (2018)	**% Población Mundial**	**Usuarios de Internet 30 junio 2018**	Nivel de penetración (% población)	Crecimiento 2000-2018	% Usuarios de Internet
África	1,287,914,329	16.9%	**464,923,169**	36.1%	10,199 %	11.0 %
Asia	4,207,588,157	55.1%	**2,062,197,366**	49.0%	1,704 %	49.0 %
Europea	827,650,849	10.8%	**705,064,923**	85.2%	570 %	16.8 %
Latinoamérica/ Caribe	652,047,996	8.5 %	**438,248.446**	67.2 %	2,325 %	10.4
Oriente Medio	254,438,981	3.3 %	**164,037,259**	64.5 %	4,894 %	3.9 %
Norte América	363,844,662	4.8 %	**345,660,847**	95.0 %	219 %	8.2 %
Oceanía/ Australia	41,273,454	0.6%	**28,439,277**	68.9 %	273 %	0.7 %
TOTAL MUNDIAL	**7,634,758,428**	**100.0 %**	**4,208,571,287**	**55.1 %**	**1,066%**	**100 %**

Fuente: Internet World Stats, en www.internetworldstats.com/stats.htm

Ahora bien, para evaluar el impacto de la dinámica del ciberespacio cabe considerar que la **dimensión digital no está separada de la dimensión física**. Hoy en día ambas forman un tejido cada vez más laberíntico de interacciones y procesos de distinta naturaleza, como lo señala Derek Reveron:

> "el entorno cibernético... Incluye hardware físico, como redes y máquinas; información, como datos y medios de comunicación; procesos cognitivos, como las operaciones mentales que la gente utiliza para comprender sus experiencias; y lo virtual, en el que la gente se conecta socialmente. Cuando al ciberespacio se agrega lo que pensamos sirve como una quinta dimensión en que la gente puede existir mediante una personalidad alternativa en blogs, sitios de redes sociales y juegos de realidad virtual."[24]

24 Derek S. Reveron (edit.), *Cyberspace and national security. Threats, opportunities and power in a virtual world*, Washington DC: Georgetown University Press, 2012, (Edición Kindle, posición 159-161) [traducción propia].

Para ilustrar el dinamismo en internet Jarmon y Yannakogeorgos lo plasman como una ciudad compuesta por: [25]

> "una plaza principal (donde la gente participa en política y se expresa), una calle principal (donde la gente compra), unos callejones oscuros (donde ocurren crímenes), unos corredores secretos (donde los espías están trabajando en espionaje económico y militar), y un campo de batalla."

A esta ciudad podríamos agregarle un aula de clases y un laboratorio de experimentación, donde la gente de todas partes del mundo está generando ideas innovadoras, entrando en contacto e interactuando las llamadas sociedades del conocimiento.[26] Esta gran ciudad digital con sus claroscuros, avanza hacia la integración de una superestructura digital, que cabe iluminar con el recurso de la inteligencia para potenciar sus oportunidades y contener sus riesgos.

Como dimensiones vinculadas, la dinámica digital es reflejo de la superficie física. De tal forma que los actores de poder y sus objetivos de influencia en una y otra son los mismos: Estados y "actores-no estatales"[27] con comportamientos hostiles. Es por eso que se requieren recursos de ciberinteligencia para comprender las tendencia y patrones de actuación en el ámbito digital, a fin de evaluar su nivel de riesgo para un Estado, y actuar anticipadamente para neutralizar o disminuir el daño de su acción disruptiva.

25 Jack Jarmon y Pano Yannakogeorgos, *The Cyberthreat and Globalization. The Impact on US National and International Security.* Lamham: The Rowman & Littlefield Publishing Group, (Kindle Edition)., p. 11 [traducción propia].

26 Las sociedades del conocimiento son aquellas que se benefician de las tecnologías de información y del internet para abrir nuevas opciones de conocimiento, desde una dimensión social, ética y política propias. UNESCO, *Informe Mundial: Hacia las sociedades del conocimiento.* https://unesdoc.unesco.org/ark:/48223/pf0000141908/PDF/141908spa.pdf.multi

27 "Los actores no estatales son organizaciones y personas que no están afiliadas al gobierno, ni están bajo su dirección, ni son financiadas por él, incluyendo empresas, instituciones financieras privadas y ONG, así como grupos paramilitares y de resistencia armada." *Red-DESC - Red Internacional para los Derechos Económicos, Sociales y Culturales.* https://www.escr-net.org/es/recursos/actores-no-estatales [25-01-2019]

3. El Ciberespacio como entorno de conflicto: la ciberseguridad

La otra cara de la moneda del ciberespacio es la dependencia crecientemente global en torno a las tecnologías de información y sus procesos, y el alcance de las amenazas que se ciernen sobre éstos. De esto se trata la ciberseguridad, **de los planes y acciones dirigidos a proteger las oportunidades y reducir los riesgos en el entorno cibernético**. En este sentido, es ilustrativa la siguiente precisión:

> "Otro enfoque que debemos dar a la definición del ciberespacio es la comprensión de la naturaleza del mismo y su propósito, siendo este último el procesamiento, manipulación y la explotación de la información, la facilitación y el aumento de la comunicación entre los individuos y la interacción entre personas y la información. De ahí se desprende la idea de que tanto la información como las personas son elementos fundamentales en la composición del ciberespacio, por tanto, individuos e información son susceptibles de sufrir amenazas o presentar vulnerabilidades."[28]

El trazo del binomio individuos–información de estos autores destaca la interdependencia alcanzada entre estos dos extremos, ya que un ciberataque a los datos implica un ataque desde distintos flancos a las personas y a las distintas estructuras y procesos en que participan –políticos, sociales y económicos– y sus sistemas político-electoral, financiero, de seguridad y defensa, industrial, entre otros.

Los actores potenciales de riesgo en el ciberespacio son Estados y servicios de inteligencia, empresas, organizaciones criminales nacionales o transnacionales, grupos terroristas. Pero también el ciberespacio ha gestado sus propios actores, que persiguen su propias causas u objetivos al margen, estos son los hackers y hacktivistas que entran en la categoría de actores-no estatales, con

28 MACHIN, N. y GAZAPO, M. *La seguridad como factor crítico en la seguridad europea,* Revista UNISCI / UNISCI Journal, No 42 (Octubre/October 2016) p. 49

capacidad de disrupción por su manejo especializado de lo cibernético. Las herramentas de ataque de todos ellos: códigos maliciosos o *malware*, virus, gusanos y troyanos, bots y bombas lógicas, entre otros.[29]

El ciberespacio es un ámbito de seguridad nacional porque en éste existe la gran mayoría de la información pública y privada, y se alojan sistemas y procesos, que de ser violados por una irrupción hostil no autorizada puede comprometer la viabilidad y funcionamiento de un Estado. Los blancos críticos son:

a) Defensa del Estado. Por un ciberataque dirigido a bloquear accesos o a penetrar, alterar sus instalaciones, o incluso inhabilitar los sistemas de información y comunicación militar. Dichas hostilidades pueden provocar desde un escalamiento del conflicto hasta una declaración de guerra, o ser un recurso para una guerra en curso; en las dos guerras contra de Chechenia (1994-1996, y 1999-2009) los rusos lograron sabotear las redes de comunicación del Ejército Checheno, al tiempo que emprendían una ofensiva militar.

b) Intereses nacionales. Operaciones de ciberespionaje contra la información y comunicaciones de líderes políticos o diplomáticos para hacer ineficaces sus planes y objetivos de política exterior, incluidas negociaciones económicas y políticas; las filtraciones de Edward Snowden (2003) develaron la intercepción masiva de comunicaciones que realiza la Agencia de Seguridad Nacional norteamericana en todo el mundo, que incluye a jefes de Estado y otras autoridades ejecutivas. En el ámbito de los intereses económicos, han cobrado auge las operaciones de *inteligencia económica* que utilizan el ciberespacio para el robo de propiedad intelectual del ámbito industrial y económico de los adversarios, y tra-

29 El término *hacker* se asocia a un programador con habilidades especiales para romper *firewalls* y apropiarse de información secreta o alterar procesos y sistemas informáticos. El término *hacktivista*, refiere a los *hackers* que tienen una causa o mensaje detrás de sus acciones en el ciberespacio. "Hacktivistas la amenaza del ciberespacio" en *El Mundo*.
Disponible en: https://www.elmundo.es/papel/historias/2017/08/22/599ac51e468aeba4728b4570.html [12-01-2019]

ducirlo en ventajas competitivas en los mercados; las denuncias de Estados Unidos contra China por espionaje económico son reiteradas.

c) **Soberanía y autodeterminación**. Mediante campañas de desinformación y propaganda desde el ciberespacio que siembren en la opinión pública incertidumbre sobre la legitimidad de las instituciones, e incluso influyan en favor/en contra de candidatos en procesos electorales –véase la operación rusa en las elecciones presidenciales de 2016, denunciada por la inteligencia norteamericana.[30]

d) **Funcionalidad y estabilidad.** Ciberataques dirigidos contra la infraestructura crítica nacional[31] y el sistema bancario y financiero que interrumpan, alteren o dejen inoperable a las plataformas y sistemas que provén servicios básicos y bancarios, son capaces de generar inestabilidad interna que disminuya los márgenes de gobernabilidad.

El horizonte de impacto de estos blancos no sólo ilustran la dimensión de seguridad nacional que tiene el ciberespacio, sino también su alcance para la seguridad regional e internacional.[32] En el peor de los escenarios, las consecuencias de un ciberataque pueden derivar en una guerra o una inestabilidad interna crítica que se desborde más allá de las fronteras: el caso de Estonia (2007) es

30 Este tema se abordará a profundidad más adelante, el escándalo por la cibercampaña rusa que buscó incidir en el resultado de las elecciones presidenciales en EEUU de 2016, sesgando a la opinión pública y redes sociales en favor de la candidatura republicana de Donald Trump en menos cabo de la demócrata y entonces Secretaria de Estado Hilary Clinton.

31 El carácter estratégico de las plantas de electricidad es poque vertebran a buena parte del funcionamiento cotidiano de un país –provisión de agua, alimentación, comunicación, energía y transporte, salud, entre otras. Su vulnerabilidad radica en que el acceso a su red digital de control es precisamente a través de dispositivos eléctricos.

32 Un ejemplo de cómo la ciberseguridad cobra interés internacional es la agenda del Foro Económico Mundial (2018) que entre su lista de principales riesgos mundiales incluyó a estas amenazas a la ciberseguridad : (i) guerra cibernética [o ciberguerra], (ii) ataque a infraestructura crítica, (iii) delito cibernético, (iv) riesgo sistémico y resiliencia, y (v) normas de colaboración. Estas cinco vertientes de impacto del tema de ciberseguridad se complementan en la agenda del Foro con las de: (vi) privacidad, (vii) tecnología y normas, y (viii) seguridad de las cosas. Ver diagrama resumen de interacción entre vectores de atención relacionados con ciberseguridad.
Disponible en: https://toplink.weforum.org/knowledge/insight/a1Gb00000015LbsEAE/explore/summary [última consulta 21-10-18]

considerado el ataque cibernético más letal contra un Estado, habiendo paralizado su funcionamiento y provisión de servicios financieros, y utilizado como referente en el debate internacional respecto a la ciberseguridad.[33]

El ciberespacio es un nuevo plano de expresión de poder o de *ciberpoder,* como lo llama María de Lourdes Puente, en el que convergen actores estatales y no-estatales, que buscan cumplir sus objetivos mediante la persuasión y/o coacción, lo que genera tensiones. Los Estados siguen siendo actores de primer orden y para ello tienen la opción de utilizar sus recursos de inteligencia:

> "**El ciberespacio es también una arena destacada para las operaciones de inteligencia, la guerra y la lucha militar**. Es asi que las naciones necesitan defender a su gobierno y a su sector privado de toda intrusión, pero también utilizar al ciberespacio para dirigir operaciones militares o de inteligencia en contra de adversarios presentes o futuros." [34]

Los tres tipos de operaciónes de los servicios de inteligencia tendrían como objetivos en el ciberespacio los siguiente:[35]

a) **Operaciones de recolección y análisis de información**. Para evaluar y alertar a los usuarios de oportunidades y amenazas en el ciberespacio, y apoyar a la toma de decisiones para obtener ventajas y ampliar la ciberseguridad frente a adversarios;
b) **Operaciones de contra-inteligencia**. Dirigidas a recolectar datos y operar medidas de seguridad para proteger sus sistemas de información y proceso, y también para romper las barreras defensivas digitales de adversarios; y

33 El caso de Estonia generó una gran preocupación entre los Estados miembros de la Organización del Tratado del Atlántico Norte (OTAN), lo que generó un proceso de discusión que derivó en la creación del Centro de Excelencia – Cooperación de Ciberdefensa de la OTAN. Este organismo invitó a un grupo de expertos que integraron lo que se conoce como el *Manual de Tallin de Derecho Internacional Aplicable a la Ciberguerra* (2013).
Una versión gratuita del documento está disponible en http://csef.ru/media/articles/3990/3990.pdf [10-01-19]

34 Mark Lowenthal, *op.cit.*, p. 274 [traducción propia]

35 Loch Johnson, *op. cit.,* p. 10 [traducción propia]

c) Operaciones encubiertas.[36] Su propósito es provocar o alterar el curso de los eventos, o modificar la percepción sobre los mismos; véase propaganda, operaciones políticas y económicas, o incluso tentativas ofensivas.

Dada su naturaleza el ciberespacio es un entorno propicio para las ciber-operaciones por que favorece el anonimato y opacidad, a lo que contribuye el incipiente desarrollo de normas y sanciones jurídicas, tanto para la protección efectiva de los datos como para la atribución de ciberdelitos y ciberataques.

Lo visto hasta aquí proporciona elementos para poder encuadrar y explicar la forma en que organizaciones supranacionales como la Unión Europea, además de los Estados Unidos (EEUU) y México, vienen construyendo su visión estratégica de ciberseguridad. Y de manera señalada, la forma en que la inteligencia está siendo considerada como un recurso de Estado.

4. Enfoques estratégicos de ciberseguridad y ciberinteligencia

A. Unión Europea – Consejo Europeo

La elaboración europea de su concepto estratégico de ciberseguridad es reciente, y está a cargo de la Comisión Europea y del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. En 2013 se emitió la *Estrategia de Ciberseguridad. Un cibespacio libre, abierto*

36 La contrainteligencia junto con las operaciones encubiertas conforma una zona opaca en la que los gobiernos y los propios servicios tienen un mayor margen para decidir y operar fuera de la mirada pública, pudiendo transgredir el Derecho Internacional e incluso los derechos de sus sociedades y ciudadanos, en buena medida los regímenes de control jurídico y de rendición de cuentas de los servicios de inteligencia se han construido a partir de escándalos relacionados con este tipo de operaciones cuando han salido a la luz, con diferencias de país a país y según su madurez democrática.

y seguro,[37] que delimitó cuatro campos de acción conjunta para la construcción de capacidades de ciberseguridad de los Estados miembros: 1) ciberresiliencia[38], en cooperación con sector privado; 2) ciberdefensa; 3) recursos industriales y tecnológicos, que amplíen la autonomía europea, y 4) ciberespacio internacional, para impulso de políticas internacionales coherentes con los valores europeos, con inspiración democrática.

De entre estos cuatro cabe destacar el componente de la ciberresiliencia, como una tendencia preventiva de trabajo sobre vulnerabilidades de ciberseguridad a nivel internacional, como se verá en los apartados siguientes. En general, la ciberresiliencia se refiere a la prevención, manejo y recuperación de los sistemas vulnerados, en medio de situaciones de crisis provocada por un ciberataque.

Ahora bien, la estrategia europea consideró al cibercrimen como la primera amenaza del ciberespacio, lo que determinó el destino de mayores capacidades y recursos al ámbito policial, incluidos los de inteligencia. En este contexto, se creó el *Centro Europeo de Cibercrimen (EC·3),* bajo control de EUROPOL.[39] Su división de Operaciones concentra las capacidades de *ciberinteligencia* para atender crímenes de alta tecnología, explotación sexual infantil via online y fraude de pagos, principalmente. La División Estratégica del EC-3 tiene un área de análisis estratégico que diagnostica y evalúa las tendencias globales del cibercrimen y proyecta escenarios futuros.

37 Además de ciberresiliencia para el cibercrimen, la Estrategia postula otros tres campos de acción en materia de ciberseguridad: European Commission & High Representative Of The European Union For Foreign Affairs And Security Policy *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Bruselas, 7-03-13, 4-5 p.p.
Disponible en: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [última consulta: 21-10-18] [traducción propia]

38 El sistema de ciberresiliencia enfatiza en estructuras de enlace y reacción a nivel regional que aseguren el *intercambio de información* y la cooperación entre países miembros y otros socios. Las bases del sistema de cooperación en ciberseguridad son EUROPOL, la Agencia Europea para la Seguridad de Redes y de Información (ENISA) –encargada de los ejercicios anuales de cibercrisis-, el Equipo de Respuesta a Emergencia Informaticas de la UE para instituciones, organismos y agencias de UE (CERT-UE) y el Centro de Análisis de Inteligencia de la UE (INTCEN). *Ibid*., p. 5

39 Información sobre el EC-3 está disponible en: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Más adelante, la perspectiva sobre el ciberespacio se encuadró en el concepto paraguas de *amenazas híbridas*[40], que ha sido desarrollado en respuesta a la complejidad creciente en materia de seguridad: "Las amenazas híbridas constituyen un asunto de defensa y seguridad nacional y de mantenimiento del orden público."[41] Destaca que para el tratamiento de estas redes de fenómenos interconectados se recurriera al apoyo de las capacidades de inteligencia, colocando una *célula de fusión contra las amenazas híbridas* en el Centro de Análisis de Inteligencia (INTCEN) de la Unión Europea. "Tenemos que alimentar y coordinar la inteligencia obtenida de las bases de datos europeas y poner las TIC, entre ellas los análisis de macrodatos, al servicio de una sensibilización situacional más profunda."[42] Esto es, diagnosticar mediante procesos de inteligencia la multiplicidad de entornos, para enfrentar los desafíos de manera efectiva, entre ellos los de la ciberseguridad.

Entre las iniciativas nacionales relacionadas con inteligencia y ciberseguridad, vale la pena destacar la existencia en España desde 2013 del Consejo Nacional de Ciberseguridad, organismo con apoyo del Consejo de

40 En 2017 se creó un *Centro de Excelencia – Para la lucha contra las amenazas híbridas*», a cargo del gobierno de Finlandia y con con apoyo de la UE y de la OTAN. "Las amenazas híbridas se entienden como una mezcla de actividades hostiles que combinan métodos convencionales y también no convencionales, donde estas actividades pueden ser coordinadas por actores estatales o no estatales, manteniéndose por supuesto por debajo del umbral de una guerra que ha sido declarada oficialmente. El objetivo de una amenaza híbrida está enfocado no sólo en causar un daño directo a la población, o aprovechar las vulnerabilidades, también a desestabilizar las sociedades completas y crear grandes incertidumbres que dificultan la toma de decisiones por los líderes de Estado." Instituto Internacional de Estudios en Seguridad Global (INISEG), "¿Qué son y cómo nos afectan las amenazas híbridas?", 6-08-18.
Disponible en: http://www.iniseg.es/blog/seguridad/que-son-y-como-nos-afectan-las-amenazas-hibridas/# [última consulta 25-10-2018]

41 Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (2016), *Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea,* Bruselas, 6-04-2016. P.2 Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018&from=EN [última consulta 25-10-2018] [traducción propia]

42 Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (2016), *Estrategia global para la política exterior y de seguridad de la Unión Europea. Una visión común, una actuación conjunta: una Europa más fuerte* p. 40.
Disponible en inglés: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf [traducción propia]

Seguridad Nacional (CSN) español. La presidencia la ostenta el titular del Centro Nacional de Inteligencia (CNI), para ser un enlace de coordinación y cooperaciones entre sectores público-privado en apoyo a la toma de decisiones en la materia por parte del propio CSN.[43]

B. Estados Unidos (EEUU)

Hasta la década anterior, la ciberseguridad no figuraba de forma relevante en las prioridades de seguridad nacional del gobierno norteamericano, donde el terrorismo ocupaba una posición destacada desde los ataques del 11-S (2001). Sin embargo, esta situación ha ido cambiando, pues como se argumentó al principio de este artículo, las ventajas del desarrollo tecnológico van aparejadas de vulnerabilidades, especialmente una vez que se extiende el uso de dichas tecnologías en los sistemas y operaciones de seguridad. De esta forma, los EEUU como país de vanguardia en tecnologías de información es uno de los Estados que marca la pauta en los frentes de ciberseguridad, situación a la que contribuye, sin duda, su política de poder en el contexto internacional.

A finales de 2016, la *Estrategia de Seguridad Nacional 2017* de este país estableció: [44]

> "Hoy actores como Rusia están utilizando herramientas de información en su intento de socavar la

43 Su misión es "reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, asi como entre los sectores público y privados, que facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de las iniciativas tanto en el ámbito nacional como en el internacional." Sobre el Consejo Nacional de Ciberseguridad: http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad El Estado español emitió en 2013 se Estrategia de Ciberseguridad Nacional en la que señala la importancia del recurso de inteligencia relacionado para el ámbito de la ciberdefensa y la lucha contra el terrorismo.
Disponible en: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional [última consulta 13-01-2019]

44 President of United States, *National Security Strategy of the United States of America-2017,* p. 14. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [última consulta 30-10-2018] [traducción propia]

> legitimidad de democracias. Los objetivos de estos adversarios son los medios, los procesos políticos, las redes financieras y los datos personales. El público norteamericano y los sectores público y privado deben reconocer esto y trabajar juntos para defender nuestra forma de vida. No se puede permitir que ninguna amenaza externa haga temblar nuestro compromiso compartido entorno a nuestros valores, socave nuestro sistema de gobierno o divida a nuestra Nacion."

El señalamiento norteamericano respecto a Rusia elevó el papel hostil de los Estados dentro de los ciberconflictos y sumó como objetivo de ciberseguridad a la estabilidad de los propios sistemas democráticos, junto con: infreastructura crítica, empresas privadas, redes federales y comunicaciones.

La Estrategia norteamericana dedica un apartado a la responsabilidad de la Comunidad de Inteligencia de EEUU de "generar inteligencia estratégica para anticipar los cambios geoestratégicos, asi como producir inteligencia de corto plazo para responder a los acciones de provocación de los adversarios."[45] Una base de este trabajo es la identificación y priorización de riesgos –una acción prioritaria que marca la Estrategia–[46] como el caso del análisis de las operaciones rusas en las elecciones presidenciales del 2016 –elaborado y desclasificado por la Oficina del Director de Inteligencia Nacional (ODNI, siglas en inglés), en 2017. Ver Cuadro 2.

45 En materia de inteligencia estableció tres líneas de acción prioritaria: 1) desarrollo de inteligencia económica, análisis sistemático de intereses y prioridades económicas de los adversarios, para anticipar y neutralizar las operaciones de espionaje económico; 2) explotación de información, especialmente de fuentes abiertas, como insumo para contrarrestar capacidades de Estados y actores no estatales para atacar a ciudadanos, y "degradar a las instituciones democráticas norteamericanas", y 3) fusión de información y análisis, mediante la integración de datos provenientes de los ámbitos diplomáticos, información militar y económica para "competir más eficazmente en la etapa geopolítica." *Íbid.,* p. 32 [traducción propia]

46 *Íbid.,* p. 13. [traducción propia]

Cuadro 2
Análisis de las Intenciones y acciones rusas en las recientes elecciones en Estados Unidos

Juicios clave

- … El presidente ruso Vladimir Putin ordenó una campaña de influencia en 2016 dirigida hacia las elecciones presidenciales de Estados Unidos.
- "Los objetivos rusos fueron socavar la credibilidad pública en el proceso democrático estadounidense, denigrar a la Secretaria [Hillary] Clinton y dañar su elegibilidad y potencial presidencia."
- "… Putin y el gobierno ruso desarrolló una clara preferencia por el triunfo del Presidente electo Trump."

Conclusiones sobre la operación rusa

- "La campaña de influencia de Moscú siguió una estrategia de mensajes que combinó operaciones de inteligencia encubierta –como la actividad cibernética– con esfuerzos abiertos por parte de agencias gubernamentales rusas, medios de comunicación financiados por el Estado, intermediarios terceros, y pagos a los usuarios de "trolls" en redes sociales."
- Los servicios de inteligencia rusos dirigieron operaciones cibernéticas contra objetivos relacionados con las elecciones, incluyendo objetivos vinculados con los dos principales partidos políticos de Estados Unidos.
- Inteligencia rusa obtuvo y mantuvo acceso a múltiples factores de juntas electorales estatales o locales de Estados Unidos.

Prospectiva:

- "estimamos que Moscú aplicará las lecciones aprendidas en la campaña dirigida por Putin a la elección presidencial de Estados Unidos, para influir en el futuro en todo el mundo, incluso contra los aliados estadounidenses y sus procesos electorales."

NOTA: Traducción y selección propia de los elementos que se consideran más destacados.
Fuente: DNI-Intelligence Community Assessment (ICA), Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-OID. Disponible el texto completo en: https://www.dni.gov/files/documents/ICA_2017_01.pdf [última consulta 22-01-2019]

La nota desclasificada del ODNI permite entrever el formato y estructura de este tipo de evaluaciones de inteligencia, al tiempo que sus conclusiones sustentan la visión norteamericana de que la disputa por el poder y la influencia en entre Estados, es una amenaza a la ciberseguridad, desde el 2015 opera el Centro de Integración de Inteligencia sobre Ciberamenazas (CTIIC, siglas en inglés), y es parte del ODNI. [47]

Llama la atención que el trabajo de disfusión del DNI contribuye a generar una cultura pública de ciberseguridad. En su *Evaluación de Amenazas Mundiales 2018* alerta de la importancia del trabajo internacional en materia de legislación específica para el ciberespacio, como una forma efectiva de disuadir y, en dado caso, sancionar a los responsable de acciones hostiles.[48] Su análisis alerta que el riesgo de un conflicto entre Estados es similar al nivel que tuvo la Guerra Fría. Al respecto resalta que los actores de mayor riesgo para EEUU, además de Rusia, son: China, a la que atribuye operaciones de *ciberespionaje económico* y acciones para fortalecer sus capacidades de ciberataque, como parte de su estrategia de seguridad nacional;[49] Irán al que responsabiliza de actividades de espionaje para penetrar las redes de EEUU y países aliados, y Corea del Norte por ciberoperaciones de recolecciópn de inteligencia o lanzar ciberataques contra *EEUU y Corea del Sur.*

Por último, el documento apunta a que los terroristas están haciendo operaciones de recolección e inteligencia en apoyo

47 Se creó en 2015 con el objetivo es generar análisis coordinado de la Comunidad de Inteligencia sobre ciberamenazas externas a los intereses nacionales de EEUU, asegurar el intercambio de información entre la cibercomunidad a nivel federal, y apoyar a los operativos, analistas, y tomadores de decisiones, con inteligencia oportuna sobre ciberamenazas y actores de amenaza significativos. https://www.dni.gov/index.php/ctiic-home [traducción propia]

48 DNI, *Worldwide Threat Assessment 2018 (statement for the record),* Febrero 13, 2018, 4-6 p.p. Disponible en: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf [última consulta 30-10-2018] [traducción propia]

49 Se tiene la perspectiva que China ve en sus capacidades de ciberataque un como soporte para sus prioridades de seguridad nacional, para lo que estableció en 2015, la Fuerza de Apoyo Estratégico, controlada desde el poder militar. El analisis atribuye a los norcoreanos el *virus ransome Wanna Cry*, que sembró incertidumbre mundial en 2017 al pedir dinero a cambio de la informacion "detenida" de las computadoras. Íbid. P. 6

a sus planes, mientras que establece que la delincuencia transnacional –en esto coincide con la valoración europea– utiliza el ciberespacio para sus objetivos tradicionales de perpetrar robo y extorsión:[50]

> "...la línea entre actividad criminal y las acciones de Estado-naciones se verá cada vez más borrosa, ya que los Estados están viendo a las herramientas cibercriminales como un medio relativamente barato y opaco para favorecer sus operaciones."

Finalmente, el enfoque norteamericano del binomio de inteligencia/ciberseguridad dio un nuevo paso que se plasmó en la estrategia de inteligencia norteamericana, dada a conocer a principios de 2019, al crear el concepto de *inteligencia de ciberamenazas,* como un objetivo a desarrollar con el apoyo de las tres inteligencias básicas: estratégica, anticipatoria y de operaciones.

> "La inteligencia de ciberamenazas es la recopilación, procesamiento, análisis y difusión de información de todas las fuentes de inteligencia sobre los programas cibernéticos de los actores extranjeros, sus intenciones, capacidades, investigación y desarrollo, tácticas, objetivos, actividades e indicadores operacionales, y su impacto o potenciales efectos sobre los intereses de seguridad nacional de los EEUU."[51]

C. México

Mediciones realizadas en 2017 reportaron que en ese año el 67% de la población mexicana mayor de seis años estaba conectada a internet –equivalente a 79.1 millones de usuarios–, lo que supuso un crecimiento de 12% con

50 Se tiene probada la amplia gama de actividades en internet por grupos terroristas para: organización, propaganda, recolección de fondos, instigar a la acción de sus seguidores y coordinar operaciones. *Idem*

51 DNI, *National Intelligence Strategy of the United States of America-2019,* p. 10. Disponible en: https://assets.documentcloud.org/documents/5691925/National-Intelligence-Strategy-2019.pdf [25-01-2019] [traducción propia]

respecto a 2016. Siete de cada diez mexicanos se conectan a través de un dispositivo *Smartphone.*[52]

El fraude cometido contra el Sistema de Pagos Electrónicos Interbancarios (SPEI) por alrededor de 800 millones de pesos (mayo, 2018) puso en evidencia la fragilidad del sistema financiero en materia de ciberseguridad, además de la falta de mecanismos de intervención integral a nivel Estado, incluyendo recursos jurídicos.[53] De acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), en el segundo trimestre de 2018 los fraudes cibernéticos crecieron un 31% respecto al mismo periodo de 2017. Del total de delitos de fraude, el 59% se realiza en la red (equivalentes a más de 2 millones de operaciones ilícitas) frente al 41% de tipo tradicional.[54]

A pesar de este dinamismo digital en ascenso, en el Índice Global de Ciberseguridad (2017) de la Agencia Especializada de las Naciones Unidas para las Tecnologías de Información y Comunicaciones (UIT), México ocupó la posición 28, entre un total de 134 Estados que respondieron a la encuesta. Estando ubicado en la región mejor posicionada del Continente, es patente la gran brecha de ciberseguridad frente a sus vecinos –veintiseis lugares por debajo de Estados Undos (2º) y dieciseis de Canadá (9º)– este desequilibrio potencialmente lo hace un blanco atractivo para ataques hostiles.[55]

52 La tendencia marca que los sectores que seguirán creciendo más son los de escasos recursos y los mayores de 45 años. Asociación de Internet.MX, *14o Estudio sobre los hábitos de los usuarios de Internet en México-2018.* Disponible en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid= [10-01-19]

53 "Esto es lo que sabemos del caso SPEI y su impacto en los bancos mexicanos", *Expansión*, mayo 14, 2018. Disponible: https://expansion.mx/economia/2018/05/14/esto-es-lo-que-sabemos-del-caso-spei-y-su-impacto-en-los-bancos-mexicanos [10-12-2018]

54 Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) https://www.condusef.gob.mx/gbmx/?p=estadisticas [última consulta 24-01-19]

55 Para la UIT es responsabilidad de todos los Estados avanzar en niveles óptimos de ciberseguridad para un ecosistema digital armónico que potencie las posibilidades de desarrollo. UIT, *Global Cybersecurity 2017*, p. 28. Disponible en: https://www.itu.int/pub/D-STR-GCI.01-2017 [última consulta 01-11-2018]

Como elementos básicos de ciberseguridad cabe hacer una anotación general, para posteriormente identificar los elementos de base que dieron lugar a su estrategia:[56]

a) Legal. En México existen normas relativas a la penalización del "acceso ilícito a sistemas y equipos informáticos", a la protección y privacidad de datos, y para las transacciones electrónicas,[57] que sin embargo no constituyen un paquete integrado y actualizado de normas relacionadas exprofesamente con la ciberseguridad.

b) Técnico. Instancias con capacidades para actuar directamente en materia de ciberseguridad, como es el caso del Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal.[58]

c) Organizacional. Los avances en materia de coordinación política y estratégica son incipientes, figurando el antecedente de la Subcomisión de Ciberseguridad, la cual quedó como responsable de integrar lo que sería la estrategia de ciberseguridad.[59]

56 La encuesta UIT–2017 utilizó estos campos de medición de avances en ciberseguridad, además el de **construcción de capacidades**, programas de investigación y desarrollo, formación y entrenamiento; profesionales certificados y agencias del sector público dedicadas a la contrucción de capacidades, y **cooperación**, alianzas, marcos de coorperación y redes de intercambio de información. En ambos México no tuvo una evaluación mínima. *Idem*.

57 Cámara de Diputados, *Codigo Penal Federal*, Artículo 211 Bis. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_051118.pdf [consulta 01-11-2018] Cámara de Diputados (2015) *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* 5 de julio, 2015. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf Cámara de Diputados (2018), *Código de Comercio*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_311218.pdf

58 El CERT-MX se encarga de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país.
https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es También existe un CERT–UNAM.

59 La Subcomisión de Ciberseguridad la preside la División Científica de la Policía Federal, tuvo como objetivos principales: (i) Articular los esfuerzos del Ejecutivo Federal y generar los criterios generales para que todas las dependencias y entidades de la Administración Pública Federal contribuyan a la generación de la ENCS y den seguimiento a la misma mediante acciones generales y específicas a desarrollar en el resto de la administración; (ii) Promover la participación y colaboración de la sociedad civil, sector privado, academia, comunidad técnica y organismos internacionales en materia de Ciberseguridad; establecer el Plan de Implementación de la ENCS, y (iii) Proponer el fortalecimiento institucional del ente responsable de dar seguimiento a la ENCS.

Las definiciones iniciales que darían lugar a la generación de una estrategia de ciberseguridad nacional datan de 2013 al calificar al ciberespacio como la "cuarta dimensión de la operaciones de seguridad" y prescribir que esa condición debía ser considerada en las futuras legislaciones de inteligencia civil, militar y naval, pendientes de concretar (*Plan Nacional de Desarrollo 2013–2018*)[60]. Posteriormente, el derivado programa sectorial de seguridad nacional incluyó en la lista de amanazas a la seguridad nacional de ese sexenio a la ciberseguridad en un tercer lugar, sólo por debajo de desastres, pandemias y delincuencia organizada transnacional. El documento marcó como objetivos centrales de esta amenaza a: "infraestructura crítica,[61] intereses económicos, redes de información y capacidades de defensa", señalando como actores de riesgo a gobiernos, grupos criminales y organizaciones terroristas.[62]

Lo anterior fue el marco para la presentación cuatro años depués (2017) de la *Estrategia Nacional de Ciberseguridad,* que se planteó el objetivo del aprovechamiento responsable de las TIC,[63] desde todos los ámbitos de actividad colectiva, pública y privada. Entre cuyos objetivos estratégicos destaca el de *seguridad pública*, relacionado con la prevención e investigación de cibercrimen; y el de *seguridad nacional,* que dicta:

> "Desarrollar capaciades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la

60 Gobierno de la República, México (2013) *Plan Nacional de Desarrollo 2013 – 2018,* p. 107 Disponible en: http://pnd.gob.mx/ [última consulta 1-11-2018]

61 Infraestructura crítica de información "Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia" SEGOB (2016), *ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias.* Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016 [10-01-2019]

62 Gobierno de la República, *Programa para la Seguridada Nacional 2014-2018.* Disponible en: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf [última consulta 1-11-2018]

63 Gobierno de la República, México (2017), *Estrategia Nacional de Ciberseguridad*. P. 4
Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [última consulta 25-01-2019]

> independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales."[64]

Esta Estrategia omite dar un papel explícito a la inteligencia en favor de la ciberseguridad, no obstante, como se ha visto a lo largo de este artículo la prevención de riesgos estratégicos, a los que se refiere la cita anterior, es una necesidad para lo que se requiere de tareas de inteligencia. Sin embargo, la riqueza de esta estrategia radica en que el documento fue producto de un periodo de consultas entre sectores, incluyendo el académico, que merece continuarse.

Conclusiones

El ciberespacio es un ámbito de conflicto de poder asimétrico, donde el conocimiento informático especializado es un arma de daño potencial que puede ser esgrimida por un Estado o un actor no estatal, siempre y cuando tenga la motivación para utilizarla. Los Estados deben ejercer su liderazgo en las políticas de ciberseguridad nacional, formando alianzas de interés con los demás sectores del país, y derivándolas a nivel regional e internacional. El mundo no ha estado tan hipervinculado en otra estapa de la historia humana, de ahí que la ciberseguridad debe ser una empresa común y comprometida.

Para una discusión sobre la inteligencia y la ciberseguridad nacional en México se proponen los siguientes elementos:

1. La Estrategia Nacional de Ciberseguridad 2017 puede usarse como base para profundizar en un enfoque estratégico mejor integrado y operable a largo plazo, que considere el papel de la inteligencia para la seguridad nacional, el intercambio de información con instancias homólogas, junto con la vertiente de la contrainteligencia, recuérdese que México ha sido un objetivo de inteligencia, incluyendo las operaciones de recolección masiva

64 Los otros objetivos estratégicos son: 1) sociedad y derechos; 2) Economía e innovación; y 3) Instituciones públicas. El objetivo de seguridad nacional se articula con los ejes transversales de: 1) cultura de ciberseguridad, 2) desarrollo de capacidades, 3) coordinación y colaboración, 4) infraestructuras críticas para la gestión de riesgos y el incremento de la resiliencia nacional, y 5) medición y seguimiento. *Ibid.*, 18-23 p.p.

de datos de la Agencia para la Seguridad Nacional (NSA en inglés) en negociaciones de tratados comerciales como en procesos políticos, por ejemplo el espionaje a Enrique Peña Nieto como candidato pesidencial en 2012, develado por las filtraciones de Edward Snowden.

2. La integración y ejecución de un enfoque estratégico de ciberseguridad requiere sistemáticamente de análisis de inteligencia sobre: el impacto internacional, regional y nacional de las tensiones de tipo geopolítico entre Estados; los patrones y objetivos de las operaciones de los servicios de inteligencia y escenarios futuros; las mejores prácticas en materia de política de ciberinteligencia; la tendencia del cibercrimen y los actores que están valiéndose de dichas prácticas.
3. Si bien las campañas de desinformación para manipular la percepción pública fue una táctica intensa en la Guerra Fría, la viralidad del internet las hace un recurso para actores disruptivos externos e internos, que propicia: la falta de una cultura de seguridad de la información, el nivel de conexión e interacción de la sociedad mexicana en las redes sociales digitales, la natural intensidad del debate político de las democracias, entre otros.
4. Toda estrategia debe definir distintos campos de operación con sus instancias responsables y recursos específicos**,** que al final permitan una mirada integral y completa de la ciberseguridad. Concentrar las amenazas prioritarias únicamente al cibercrimen, reduce la perspectiva y la capacidad de anticipación ante amenazas de otra naturaleza.
5. Considerar un proceso de fusión de inteligencia de ciberseguridad, con unidades descentralizadas de recolección para favorecer la participación de los demás sectores y el Estado, desde sus puntos de actividad. Ello implicaría un inversión en formación para uso de métodos estandarizados de evaluación y procesamiento de información, para garantizar el aprovechamento adecuado de los datos y los resultados de la sinergia entre redes de trabajo.
6. Creación de una instancia nacional de ciberseguridad autónoma, a la manera de un centro nacional de ciberseguridad, que coordinaría entre otras co-

sas la fusión de ciberinteligencia. Se propone una estructura público-privada de coordinación y seguimiento que integre las capacidades humanas, tecnológicas y de infraestructura relacionados al ámbito digital, que tenga un enlace con el Consejo de Seguridad Nacional.

7. Promoción de una cultura nacional de ciberseguridad. Integración y difusión de una agenda nacional de ciberseguridad, que afiance el consenso y el compromiso de todos los sectores público y privado con el principio de la corresponsabilidad en ciberseguridad. La idea es generar confianza en torno a un objetivo común que favorezca la armonización de iniciativas generadas desde los distintos ámbitos y el intercambio de información.
8. Participación en foros regionales e internacionales para la construcción de un régimen de ciberseguridad internacional y un desarrollo más específico del Derecho Internacional.

BIBLIOGRAFIA

Andrew, Cristopher, *The Secret World. A History of Intelligence*, Yale: Yale University Press, 2018, 960 págs.

Esteban, Miguel, *Glosario de Inteligencia*. Madrid: Ministerio de Defensa, 2007, 117 págs.

Evans, Graham, *The Penguin Dictionary of International Relations*. London: Penguin Books, 1998, 623 pags.

Gill y Phythian, *Intelligence in an Insecure* World. Cambridge: Polity, 2018, 3rd edit., 238 págs.

Jarmon, Jack, y Yannakogeorgos, Pano, *The Cyberthreat and Globalization. The Impact on US National and International Security*. Lamham: The Rowman & Littlefield Publishing Group, (Kindle Edition), 2018, 272 págs.

Johnson, Loch, *National Security Intelligence. Secrets operations in the Defense of Democracies*. Cambridge: Polity, 2017, 2nd edit., p. 16

Kent, Sherman, *Strategic Intelligence for American Policy* (Princeton: Princeton University Press, 1966, 2nd print., 226 págs.

Lowenthal, Mark, *Intelligence. From Secrets to Policy*. Los Angeles: SAGE/CQ Press, 2012, 5th edit., 417 p.p

Phythian, Mark (ed.), *Understanding the Intelligence Cycle.* London: Routledge, 2013, 184 pags.
Reveron, Derek (edit.), *Cyberspace and national security. Threats, opportunities and power in a virtual world*. Washington DC: Georgetown University Press, 2012, 258 págs.
Sanger, David, *The Perfect Weapon. War, sabotage, and Fear, in the Cyber Age.* Victoria: Scribe, 2018, 384 pags.
Sun-Tzu, *The Art of Warfare*. New York: Random House Publishing Group, 1993, 321 págs
Tuchman, Barbara, *El Telegrama Zimmermann. El documento secreto que cambió la Primera Guerra Mundial*. Barcelona: Edit. RBA. 2010, 333 págs.
Wohlstetter, Roberta, *Pearl Harbor. Warning and Decision*. Stanford: University Press, 1963, 428 págs.

HEMEROGRAFÍA

Alta Representante de la Unión Para Asuntos Exteriores y Política de Seguridad (2016), *Estrategia global para la política exterior y de seguridad de la Unión Europea. Una visión común, una actuación conjunta: una Europa más fuerte,* 60 pags. Disponible en inglés: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
Cámara de Diputados, *Codigo Penal Federal*, Artículo 211Bis. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_051118.pdf
Cámara de Diputados, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
Cámara de Diputados, *Código de Comercio*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_311218.pdf
Clauser, Jerome, "The evolution and Definition of Strategic Intelligence, *An introduction to intelligence research and analysis*. Maryland: Scarecrow Professional Intelligence Education Series, No.3, Scarecrow Press Inc., 2008, p.1
Comisión Europea y Alta Representante de la Unión Para Asuntos Exteriores y Política de Seguridad, *Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea,* Bruselas, 6-04-2016. 20 pags. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

DNI, *National Intelligence Strategy of the United States of America-2019,* p. 10. Disponible en: https://assets.documentcloud.org/documents/5691925/National-Intelligence-Strategy-2019.pdf

DNI, *Worldwide Threat Assessment 2018 (statement for the record),* Febrero 13, 2018, 28 pags. Disponible en: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf [

European Commission & High Representative Of The European Union For Foreign Affairs And Security Policy *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Bruselas, (2013), 20 pags. Disponible en: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Foro Económico Mundial, *Agenda 2018*, https://toplink.weforum.org/knowledge/insight/a1Gb00000015LbsEAE/explore/summary

Gobierno de la República, México (2017), *Estrategia Nacional de Ciberseguridad*. 30 págs. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de la República, México, *Plan Nacional de Desarrollo 2013 – 2018.* Disponible en: http://pnd.gob.mx/

Gobierno de la República, *Programa para la Seguridad Nacional 2014-2018.* Disponible en: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

ICA 2017-OID, Intelligence Community Assessment (ICA): *Assessing Russian Activities and Intentions in Recent US Elections*, Texto completo original en inglés: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Kenneth Cukier y Viktor Mayer-Schoenberge, "El auge de los grandes volúmenes de datos. Cómo está cambiando nuestra forma de ver el mundo", en *Foreign Affairs Latinoamérica***, v. 13, n. 3, julio – septiembre, 2013, 132 – 143 pags.**

Machin, N. y Gazapo, Manuel. "La seguridad como factor crítico en la seguridad europea*", Revista UNISCI / UNISCI Journal,* No 42, Octubre/October 2016, 68 págs.

President of United States, *National Security Strategy of the United States of America-2017,* 68 pags. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

UIT, *Global Cybersecurity 2017*, p. 28. Disponible en: https://www.itu.int/pub/D-STR-GCI.01-2017 [última consulta 01-11-18]

Wolfers, Arnold, "National Security as an Ambiguous Symbol", *Discord and Collaboration. Essays on International Politics*. Baltimore: John Hopkins University, 1962, 149-154 p.p.

Revista de Administración Pública

INAP

La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio

Anahiby Becerril Gil

Resumen: Las amenazas y riesgos en el ciberespacio se desarrollan en un espacio común global. En los últimos años hemos sido testigos de cómo las acciones negativas o el uso malicioso del ciberespacio han aumentado en su impacto, sofisticación y alcance y en un futuro no muy lejano podrían traer consecuencias humanitarias devastadoras. Ante este panorama la pregunta ya no es el por qué preocuparnos por el ciberespacio y la ciberseguridad, sino ¿cómo enfrentar los riesgos y retos que trae consigo el uso malicioso del ciberespacio a nuestra seguridad nacional? Los bits y las leyes deben trabajar juntos. Con este artículo se tiene el objetivo de llamar la atención y poner en la mesa la necesidad de desarrollar una Estrategia de Ciberseguridad para la Seguridad Nacional que considere las amenazas y retos que el ciberespacio y el empleo malicioso de las TIC traen consigo.

Palabras Clave: ciberespacio, ciberseguridad, ciberguerra, ciberataque, ciberarmas

Cybersecurity in National Security: threats and challenges in cyberspace

Abstract: Threats and risks in cyberspace develop in a global common space. In recent years we have witnessed

how negative actions or malicious use of cyberspace have increased in their impact, sophistication and scope and in the not too distant future could bring devastating humanitarian consequences. Against this background, the question is no longer the reason to worry about cyberspace and cybersecurity, but how to face the risks and challenges that the malicious use of cyberspace brings to our national security? Bits and laws must work together. This article aims to draw attention and put on the table the need to develop a Cybersecurity Strategy for National Security that considers the threats and challenges that cyberspace and the malicious use of ICTs bring.

Keywords: cyberspace, cybersecurity, cyberwar, cyber-attack, cyber weapons

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 5 de febrero de 2019

Revista de Administración Pública

INAP

La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio

Anahiby Becerril Gil*

La compleja realidad del ciberespacio

Las amenazas y riesgos en el ciberespacio se desarrollan en un espacio común global[1]. Las redes están tan interconectadas[2] que puede ser difícil limitar los efectos de un ataque contra una parte del sistema sin dañar otras o interrumpirlo del todo. Nuestros activos de información fluyen por igual en el ciberespacio. El intercambio y la salvaguardia de éstos hoy en día resultan críticos para proteger los intereses públicos y privados en el área de la seguridad, el desarrollo, la protección de los derechos humanos y la economía.

* Licenciada en Derecho por la Universidad de las Américas, Puebla (UDLAP). Doctora en Derecho y Globalización. Especialista en Gobernanza, Derechos Humanos y Cultura de Paz (UCLM, España). Investigadora en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, INFOTEC. Miembro del Sistema Nacional de Investigadores (SNI de CONACYT). Miembro de *Internet Society* (ISOC) y de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI).

1 Otros son: el espacio marítimo, aéreo y ultraterrestre.

2 Situación que ha sido materia de preocupación en el seno de la Asamblea General de la ONU donde se ha reconocido "que esa creciente interdependencia tecnológica se basa en una red completa de componentes de las infraestructuras de información esenciales"; *Cfr.* Preámbulo Resolución A/RES/58/199 de fecha 30 de enero 2004, disponible en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (Consultado el 28 de enero de 2019).

Si consideramos la cada vez mayor dependencia tecnológica a través de la cual las sociedades, individuos, empresas y países desarrollamos gran parte de nuestras actividades diarias, desde hace tiempo deberíamos ya habernos preguntado sobre nuestra seguridad personal, la pública y la seguridad nacional en el ciberespacio.

En gran medida, la tecnología ha premiado la interconectividad en detrimento de la seguridad[3]. En los últimos años hemos sido testigos de cómo las acciones negativas o el uso malicioso del ciberespacio han aumentado. Lo anterior consecuencia de la accesibilidad a las herramientas, así como mejoras en las metodologías y capacidades técnicas de ataque[4], lo que permite la sofisticación de los actores empeñados en causar estragos o interrupciones. Sus efectos también se han incrementado y en un futuro no muy lejano podrían traer consecuencias humanitarias devastadoras[5].

En mayo del año 2017, el *ransomware WannaCry* impactó a 150 países y cientos de miles de sistemas, paralizando la atención médica, las instalaciones de producción y las telecomunicaciones. En el año 2018 se expusieron nuevas debilidades del hardware y se sumaron violaciones masivas

3 Presidencia de Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, p. 34, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

4 "*… the attack tools and methodologies are becoming widely available and the technical capability and sophistication of users bent on causing havoc or disruption is improving*" (Traducción libre); *Cfr. United States National Strategy to Secure Cyberspace*, 2003, p. 6, disponible en: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Consultado el 28 de enero de 2019)

5 El Comité Internacional de la Cruz Roja ya ha alertado sobre el uso de operaciones cibernéticas en conflictos armados y las consecuencias humanitarias devastadoras que pueden traer consigo; *Cfr.* Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space," Interview on 16 Aug. 2011, *ICRC Resource Centre*, disponible en: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (Consultado el 28 de enero de 2019)

de datos: en India, Aadhaar[6], considerado el sistema de identificación biométrica más grande del mundo, sufrió violaciones que comprometieron los datos de los 1.100 millones de ciudadanos registrados; en septiembre, Facebook notificó a sus usuarios la violación masiva de datos más grande que ha sufrido, la cual afectaría a más de 50 millones de personas[7]. Y este año 2019 lo iniciamos con el "peor ataque de piratería informática"[8] que ha sufrido Alemania; documentos y mensajes personales, números telefónicos móviles, información de tarjetas de crédito, direcciones, correos (entre otros), se encuentran dentro de esta *große Datenleck*[9], algunas de las víctimas son la Canciller Alemana, el Presidente Alemán Frank-Walter Steinmeier, así como partidos políticos, periodistas y artistas entre otros[10].

La *European Union Agency For Network and Information Security*[11] (en adelante ENISA) reconoció como las

6 Aadhaar es la base de datos gestionada por la *Unique Identification Authority* (UIDAI) de la India. Proporciona un número aleatorio de 12 dígitos emitido por la UIDAI a los residentes de la India después de cumplir con el proceso de verificación establecido por la misma. Además de contener datos personales y demográficos contiene también información biométrica (diez huellas digitales, escáner del iris de ambos ojos y una fotografía facial). De conformidad con el Gobierno: "*La plataforma de identidad Aadhaar es uno de los pilares clave de la "India digital", en donde cada residente del país cuenta con una identidad única. El programa Aadhaar ya ha alcanzado varios hitos y es, con diferencia, el sistema de identificación biométrico más grande del mundo*"; *Cfr.* Unique Identification Authority of India, "*What is Aadhaar?*", Government of India, disponible en: https://uidai.gov.in/what-is-aadhaar.html (Consultado el 28 de enero de 2019)

7 De conformidad con Facebook, la violación habría sucedido en la tarde del 25 de septiembre. Los atacantes explotaron una función en el código de Facebook para obtener acceso a las cuentas de usuario y posiblemente tomar control de ellas; *Cfr.* Isaac Mike and Frenkel,Sheera, "Facebook Security Breach Exposes ccounts of 50 Millon Users", *The New York Times*, 28 de septiembre 2018, disponible en: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (Consultado el 28 de enero de 2019)

8 Enrique Müller, "Alemania Sufre el mayor "hackeo" de su historia con la filtración de datos personales de centenares de políticos", *El País Internacional*, 04 de enero de 2019, disponible en: https://elpais.com/internacional/2019/01/04/actualidad/1546595085_679572.html (Consulado el 20 de enero 2019)

9 Gran fuga de datos.

10 Markus Reuter, "Alles außer AfD: Was wir über das große Datenleck wissen", *Netzpolitik.com*, 04 de enero 2019, disponible en: https://netzpolitik.org/2019/alles-ausser-afd-was-wir-ueber-das-grosse-datenleck-wissen/ (Consultado el 20 de enero de 2019)

11 Agencia Europea de Seguridad de las Redes y de la Información

principales tendencias dentro en panorama de amenazas cibernéticas del 2018[12] las siguientes:

Figura I
Visión general y comparación del panorama actual de amenazas 2018 con el de 2017, ENISA[13]

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

12 En el documento "Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe", ENISA, hace referencia a las "existential threats", entendidas como las amenazas, que en caso de llegar a ocurrir "tienen el potencial de destruir la parte directamente afectada de la sociedad, la industria o las empresas" (*Those threats that if enacted have potential to destroy the directly impacted part of society, industry and business*); *Cfr.* European Union Agency for Network and Information Security ENISA, *Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe*, European Union Agency For Network and Information Security, 2018, disponible en: https://www.enisa.europa.eu (Consultado el 24 de enero 2019)

13 European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

De este panorama destacan los mensajes de correo electrónico y el denominado *phishing* como en el principal vector de infección de *malware*. Además se presenta un incremento en DDos *(Denial of service)*, *botnets*, fugas de información y violaciones de datos. Y se suma una nueva amenaza, que ejemplifica el *cybercrime-as-a-service* (CaaS): el *cryptohacking*[14]. ENISA estimó que durante la primera mitad de 2018 los *cyptominers* habían monetizado para sus usuarios más de 2.5 mil millones de dólares americanos.

Las predicciones para este año 2019 no son muy alentadoras. El Foro Económico Mundial (en adelante FEM), recientemente publicó su informe "*The Global Risks Report 2019"*[15], en donde sitúa al robo o fraude de datos y a los ciberataques dentro de los primeros 5[16] lugares en su "Encuesta de Percepción de Riesgos Globales" (*Global Risks Perception Survey*, GRPS), consolidando su posición junto con los riesgos medioambientales en el cuadrante de alto impacto y probabilidad del panorama de riesgos globales[17]. Para el caso de los ciberataques, tuvo un aumento de 82%, a nivel global. Dentro del informe el FEM también reconoció que el año pasado proporcionó evidencia adicional de los riesgos que los ciberataques plantean para la infraestructura crítica de los países.

Los ciberataques amenazan al mundo y nuestra seguridad. Es por lo que la ciberseguridad se ha vuelto una preocupa-

14 De conformidad con ENSIA, el *cryptohacking* o *cryptomining* es un ejemplo del funcionamiento del cibercrimen como servicio (*Cybercrime-as-a Service)*, conpetualizando así a los programas que emplean el poder del procesamiento de dispositivos de la víctima para extraer criptomonedas sin consentimiento, para más tarde obtener dinero en el mundo real, monetizado después de intercambios y transacciones legales. Este poder se utiliza para resolver rompecabezas criptográficos que se registran en la cadena de bloques; *Cfr.* European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

15 Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 5, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

16 En primer lugar se encuentran los acontecimientos climáticos extremos, seguido de el fracaso de la mitigación y adaptación al cambio climático y en tercero los desastres naturales.

17 Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 16, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

ción para la comunidad internacional. La Organización de Naciones Unidas (en adelante ONU) ha emitido diversas recomendaciones en donde enfatiza que "la difusión y el uso de las tecnologías y los medios de la información afectan los intereses de toda la comunidad internacional"[18], reconociendo que las tecnologías "también pueden ser empleadas con finalidades distintas de los objetivos de mantener la estabilidad internacional y la seguridad"[19].

A lo anterior debemos sumar una falta de ciberconfianza (*cybertrust*) global en el uso y desarrollo de capacidades y habilidades que los diversos *stakeholders* desarrollan dentro del ciberespacio.

Ante este panorama la pregunta ya no es el por qué preocuparnos por el ciberespacio y la ciberseguridad, sino ¿cómo enfrentar los riesgos y retos que trae consigo el uso malicioso del ciberespacio a nuestra seguridad nacional? Asegurar la ciberseguridad del Estado es uno de los desafíos clave de nuestro tiempo. Y debe ser una prioridad, tanto en el Plan Nacional de Desarrollo, como en la política exterior de nuestro país, así como en el seguimiento a la Estrategia Nacional de Ciberseguridad bajo sus tres principios: respeto de los Derechos Humanos, gestión de riesgos y un enfoque multidisciplinario y *multistakeholder.*

En este artículo no hablaremos del cibercrimen u operaciones en contra de la confidencialidad, disponibilidad e integridad de la información y los sistemas, amenazas que son principalmente tratadas bajo las leyes nacionales penales, tampoco nos referiremos al ciberterrorismo. Haremos mención de los diversos riesgos y retos que se presentan

18 "*... the dissemination and use of information technologies and means affect the interests of the entire international community*"; *Cfr.* Asamblea General de Naciones Unidas, Preámbulos de las Resoluciones A/RES/55/28 de 20 de Noviembre del año 2000; A/RES/56/19 de 29 de noviembre de 2001; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8 de diciembre de 2005; A/RES/61/54 de 6 de Diciembre de 2006; A/RES/62/17 de 05 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

19 Preámbulos de las Resoluciones A/RES/58/32 de 08 de diciembre de 2003; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8 de diciembre de 2005; A/RES/61/54 de 6 de diciembre de 2006; A/RES/62/17 de 5 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

en la ciberseguridad en materia de seguridad nacional (en adelante SN).

Esta contribución tiene como objetivo el hacer un llamado y poner en la mesa la necesidad de desarrollar una Estrategia de Ciberseguridad para la Seguridad Nacional que considere las amenazas y retos que el ciberespacio y el empleo malicioso de las TIC traen consigo.

2. El entorno "ciber-": consenso sobre el no consenso

Uno de los primeros retos a los que nos enfrentamos al entender este nuevo espacio, es la falta de un término único para los conceptos "ciberespacio", "ciberseguridad", ciberamenazas". Casi todas las palabras que emplean "ciber-", traen consigo falta de uniformidad.

Si bien en este artículo no pretendemos definir al ciberespacio y la ciberseguridad como conceptos unitarios, consideramos importante entender los efectos que tiene la falta de una terminología común para el ciberespacio, y cómo afecta esto a la búsqueda de la seguridad y estabilidad internacional.

2.1. El ciberespacio

Este espacio de realidades abstractas, ideas, información y sistemas lógicos, abarca cuestiones políticas, tecnológicas y sociales, fomentado por Internet es una creación humana que poco entendemos. Algunos países y organismos internacionales han reconocido a Internet como una herramienta para el ejercicio de los Derechos Humanos, en específico la libertad de expresión y acceso a la información[20], en otros este espacio constituye una amenaza. En

20 La Resolución A/HRC/20/L.132 del Consejo de Derechos Humanos de la Organización de Naciones Unidas: intitulada "Promoción, protección y disfrute de los derechos humanos en Internet", reconoció, en lenguaje de Derechos Humanos, una serie de derechos de acceso y empleo del Internet para todas las personas. En este sentido, en la Resolución se afirma que los DDHH de las personas deben ser reconocidos y garantizados en el mundo *offline*, así como en el *online*. Adicionalmente, se exhorta a los Estados para que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países; *Cfr.* Consejo de Derechos Humanos de Naciones Unidas, Resolución A/HRC/20/L.13, "Promoción, protección y disfrute de los derechos humanos en Internet", de 29 de junio el 2012, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf (Consultado el 20 de enero de 2019)

la visión China, por ejemplo, Internet tiene la capacidad de manipular la información, la verdad y el estado moral y psicológico de sus ciudadanos.[21]

El ciberespacio es definido por la *Estrategia Militar Nacional de Estados Unidos para Operaciones del Ciberespacio* como un "dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas"[22]. Por su parte la Unión Internacional de Telecomunicaciones (en adelante UIT) hace referencia al ciberentorno, para describir a "usuarios, redes, dispositivos, todo el *software*, procesos, información almacenada que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes"[23].

El ciberespacio es un mundo electrónico, un espacio común global en donde las personas se encuentran unidas para intercambiar ideas, servicios e incluso amistad[24]. Constituye un sistema nervioso, el cual controla a los países y la infraestructura crítica que los sostiene. Su funcionamiento saludable es esencial para la economía y la seguridad nacional[25]. Es un entono digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas, permitiendo el

21 Thimoty L. Thomas, "Information Security Thinking: A Comparation of U.S., Russian and China Concepts, Foreign Miltary Studies Office, julio, 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

22 "*domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and Exchange data via networked systems and associated physical infrastuctures*" (Traducción libre); *Cfr.* United States Department of Defense (DoD), *The National Military Strategy for Cyberspace Operatios*, diciembre 2006, p. ix, disponible en: https://www.hsdl.org/?view&did=35693 (Consultado el 20 de enero de 2019)

23 Unión Internacional de Telecomunicaciones, UIT-T X.1205, disponible en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es (Consultado el 20 de enero 2019)

24 Gobierno de Canadá, "Canada´s Cybersecurity Strategy. For a stronger and more prosperous Canada," 2010, disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx (Consultado el 27 de febrero 2019).

25 United States Government, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009, disponible en: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (Consultado el 27 de febrero 2019).

ejercicio de sus derechos y libertades, de la misma forma que lo hacen en el mundo físico[26]. La definición que se otorgue respecto al ciberespacio atiende en gran medida al uso que se le otorgue.

El ciberespacio como una función o dominio separado no forma parte de la concepción rusa. Para este país el concepto clave constituye la información, la cual puede ser almacenada en cualquier lugar y transmitida por cualquier medio. El Gobierno Ruso hace referencia a las "operaciones de red informática" (*computer network operations*, CNO), del "*information space*" (espacio de información)[27]. Este útlimo término es empleado para referirse a lo que el occidente conocemos como el ciberespacio. El término incluye el procesamiento informático y humano de la información (motivo por el cual la *information war* incluye el dominio cognitivo humano).[28]

Este entendimiento del espacio de información quedó plasmado en la propuesta para un "Código Internacional de Conducta para la Seguridad de la Información"[29], presentado por la Organización de Cooperación de Shanghai[30] a la Asamblea General de Naciones Unidas en el año 2011[31]. Además del proyecto propio elaborado por Rusia sobre una "Convención sobre Seguridad de la Información

26 Gobierno de México, "Estrategia Nacional de Ciberseguridad", México, 2017, disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado el 27 de febrero 2019).

27 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, pp. 7-8.

28 Thimoty L. Thomas, "Information Security Thinking: A Comparation of U.S., Russian and China Concepts", *Foreign Miltary Studies Office*, julio, 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

29 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

30 La también conocida SCO, por las siglas en inglés para *Shanghai Cooperation Organization* se encuentra conformada por los siguientes 8 países: Rusia, China, Kazajistán, Kirguistán, Tayikistán, Uzbekistán, India, Pakistán.

31 Asamblea General de Naciones Unidas, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*, 14 de septiembre 2011, disponible en: http://undocs.org/A/66/359 (Consultado el 18 de diciembre de 2019)

Internacional"[32]. El Código de Coducta propuesto contenía la definición del "espacio de información" (*information space*), como:

> "la esfera de actividad relacionada con la formación, creación, conversión, transferencia, uso y almacenamiento de información y que tiene un efecto en la conciencia individual y social, la infraestructura de información y la información en sí". [33]

Esta definición tiene algunas similitudes con la idea occidental del ciberespacio, además del enfoque sobre los efectos en la conciencia individual y social, como se había referido. Mientras que el concepto de "*information warfare*" (guerra de información) hace referencia a lo siguiente:

> "conflicto entre dos o más Estados en el espacio de información con el objetivo de infligir daños a los sistemas, procesos y recursos de información, así como a estructuras de importancia crítica y otras estructuras; socavando los sistemas políticos, económicos y sociales; llevar a cabo campañas psicológicas masivas contra la población de un Estado para desestabilizar a la sociedad y al gobierno; así como obligar a un Estado a tomar decisiones en interés de sus oponentes".[34]

En ambas definiciones de sostiene la idea de una esfera social dentro de los datos e información.

Lograr un consenso en el entendimiento de lo que se pretende proteger, representa uno de los principales problemas

32 Ministerio de Asuntos Exteriores de Rusia, *Convention on International Information Security*, 22 de septiembre 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (Consultado el 27 de enero de 2019).

33 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

34 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

en el consenso para la adopción de normas y principios para regular a este nuevo dominio.

2.2. La ciberseguridad

Debemos considerar que el ciberespacio constituye este cuarto dominio en donde se realiza gran parte de las actividades del gobierno, además de que a través de él se desarrolla el flujo de información, tanto crítica como estratégica de los países, instituciones y empresas. Dada su importancia, el ciberespacio debería situarse dentro de la Estrategia Global de Seguridad Nacional.

La ciberseguridad ayuda a identificar, evaluar y abordar las amenazas en el ciberespacio, para reducir ciber-riesgos y eliminar el impacto de los ciberataques, el cibercrimen, ciberterrorismo, ciberespionaje, en el sentido de fortalecer la confidencialidad, integridad y disponibilidad de datos, sistemas y otros elementos de la infraestructura de información y comunicación.

Por ejemplo, dentro de su Estrategia de Seguridad Nacional, España[35] reconoce que el ciberespacio está asociado a nuevas amenazas y que, al igual que espacios comunes como el espacio marítimo, el aéreo y ultraterrestre, resultado de sus características de fácil acceso y débil regulación, lo que permite que fácilmente puedan convertirse en escenario de confrontaciones.

Mientras que el gobierno ruso se refiere a la ciberseguridad como "seguridad de la información" (*information security*), para incluir también temas relacionados con el contenido en línea.[36]

35 Gobierno de España, "Estrategia de Seguridad Nacional. Un proyecto compartido de todos para todos", Presidencia del Gobierno, España, 2017, p. 65, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

36 Kleir Giles, Keir, "Russia's public stance on cyberspace issues", 2012, pp. 1-13, disponible en: https://www.researchgate.net/publication/261044707_Russia's_public_stance_on_cyberspace_issues (Consultado el 20 de enero 2019)

En nuestro país, la seguridad nacional[37] dentro del ciberespacio comprende el desarrollo de capacidades para "prevenir riesgos y amenazas en el ciberespacio que puedan afectar la independencia, integridad y soberanía nacional, afectando el desarrollo y los interesas nacionales"[38].

La ciberseguridad va a tratar de la seguridad de este ciberespacio. Podemos interpretar el término atendiendo a los conceptos otorgados por la comunidad técnica, y por los empleados por los documentos nacionales de ciberseguridad. Sin embargo, consideramos que la definición que la UIT[39] emitió en su Recomendación ITU-T X.1209 (12/2019), resulta adecuada al explicar el concepto, a saber:

> "3.2.5. ciberseguridad [b-ITU-T X.1205]: el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno*".*

37 La Seguridad Nacional (SN), de conformidad con el artículo 3 de la Ley en la materia, constituyen las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven entre otras a: *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; VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes*.

38 Gobierno de México, "Estrategia Nacional de Ciberseguridad", 2017, p. 18, disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado el 29 de enero de 2019)

39 El texto refiere: *"Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*"; *Cfr.* Union Internacional de Telecomunicaciones (UIT), Rec. ITU-T X.1209 (12/2019), Capabilities and their context scenarios for cybersecurity information sharing and exchange, ITU-T X-Series Recommendations, UIT, 2010, p. 1.

Identificando como los "activos" a los "dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, así como la totalidad de la información transmitida y/o almacenada en el ciberentorno. Reconociendo que la ciberseguridad garantiza se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Refiriendo a las propiedades de la ciberseguridad las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad.

La falta de una definición consensuada sobre lo que es el ciberespacio impacta sobre lo que, a través de la ciberseguridad, necesitamos proteger. Lo que también dificulta la aclaración de roles y atribuciones para los diferentes *stakeholders*.

3. El reconocimiento de las amenazas de ciberseguridad

Si bien las ciberamenazas pueden presentarse en la forma de ciberataques, también pueden ser el resultado de errores o incluso desastres naturales. En este apartado nos enfocaremos a los primeros, ejemplificando diversos modelos y métodos para causar daño asociados al ciberespacio.

3.1. Cyberarmas

Las armas son instrumentos de daño, las ciberarmas no son la excepción. Son patrones abstractos de *bits*[40]. Se conforman de "0" y "1", programados para causar daño, al igual que las armas tradicionales.

Para lograr su objetivo, utilizan primordialmente software[41]. Constituyen códigos de computadora que se em-

40 Neil, Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, p. 310. (307-326)

41 Neil Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, p. 309. (307-326)

plean o son diseñados para ser utilizados con el objetivo de amenazar o causar daño, lo que no les diferencia del armamento tradicional. Son instrumentos que se emplean, o están diseñados para ser utilizados, con el objetivo de amenazar o causar daños físicos, funcionales o mentales a estructuras, sistemas o seres vivos.[42]

Éstas pueden presentarse en la forma de programas modificados para controlar computadoras y otros dispositivos. Sus usos pueden ir desde evitar la respuesta o adecuado funcionamiento de un sistema de defensa de misiles, hasta borrar los programas de datos clave de un sistema informático para que no pueda realizar tareas, o bien podría bloquear el acceso a la red para que un sistema no pueda comunicarse con otros. Pueden incluso ocasionar un "apagón" masivo de sistemas críticos.

Constituyen armas especificas que pueden ser empleadas dentro de los ciberataques. Algunas son controladas por medios remotos a través de Internet empleando técnicas de "botnets" donde "la máquina del atacante envía ordenes a la máquina de la víctima" con fines de espionaje o sabotaje".[43] En los casos en que el objetivo no se encuentre en Internet, se pueden emplear mecanismos de tiempo o especificaciones de eventos desencadenantes para controlarlo[44].

Para Rowe, las características de las ciberarmas son las siguientes:

42 Thomas Rid & Peter McBurney, "Cyber-Weapons", *The RUSI Journal*, 157;1, 2012, 6-1, disponible en: https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354 (Consultado el 29 de enero de 2019)

43 Christopher Elisan, *Malware, Rootkits, and Botnets: A Beginner,s Guide*, McGraw Hill, 2013.

44 Randall Dipert, "Other-tahn-Internet (OTI) cyberwarfare: challenges for ethics, law and policy", *Journal of Military Ethics*, 12(1), abril, 2013, disponible en: https://www.researchgate.net/publication/263529399_Other-than-internet_oti_cyberwarfare_Challenges_for_ethics_law_and_policy (Consultado el 27 de enero de 2019)

Cuadro 1
Características de las ciberarmas[45]

Ciberarmas	No requieren proximidad física del atacante a la víctima, ya que los ataques se pueden realizar a través de Internet, o bien se pueden plantar bien en el avance del ataque (como "caballos de Troya") y se activan cuando el atacante ya no está.
	Son fáciles de ocultar, incluso más fáciles que las armas biológicas, ya que son solo patrones abstractos de bits. También pueden operar muy rápidamente y luego destruir toda evidencia de su presencia.
	Los ataques cibernéticos pueden ser muy difíciles de atribuir al actor atacante (estatal o no estatal) ... En una guerra cibernética pura, no acompañada por ataques tradicionales, es prácticamente imposible de justificar en el ciberespacio de acuerdo con los estándares de prueba exigidos por la ley de guerra.
	Las armas cibernéticas requieren fallas en su víctima o no funcionan en absoluto.
	Son considerablemente más variadas que las municiones convencionales. Las armas cibernéticas pueden sabotear las operaciones de los sistemas informáticos de muchas maneras diferentes, algunas bastante sutiles.
	Tienden a tener consecuencias inesperadas. Esto se debe a que los sistemas informáticos dependen de miles de millones de instrucciones de componentes que funcionan constantemente cada vez que se usan, y solo un error puede alterar la cadena de instrucciones de los agujeros, a menos que se tomen precauciones inusuales, como agregar funcionalidad redundante.

Finalmente, apunta el autor, las armas cibernéticas no tienen usos legítimos. Por lo tanto, encontrar ciberarmas es una evidencia *prima facie* de intención ofensiva.

45 Neil Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, pp. 310-311. (307-326)

Las ciberarmas pueden facilitar que individuos inocentes se conviertan en objetivos, consecuencia de la "ventaja" que le da el anonimato a través del control remoto que en algunos casos puede ejercer el atacante, como ha sucedido en los casos del empleo de drones para ataques militares.

Otro reto lo constituyen las tecnologías y servicios de doble uso, consideradas así por que pueden emplearse en el ámbito militar, empero se comercializan para la venta a civiles. En este contexto surge el *Arreglo Wassenaar*. Este constituye un régimen multilateral que establece controles sobre la transferencia de bienes y tecnologías de doble uso (militar y civil), Del cual México es parte desde el año 2012.

Sin embargo, el control de las ciberarmas planeta cuestiones como: conocer sí nos encontramos en el desarrollo de una carrera ciberarmamentista; en caso de que sea afirmativo lo anterior, debemos conocer cuál es el nivel de madurez y la etapa en que nos encontramos dentro de la carrera armamentista que emplea estas tecnologías; si es a través de un tratado internacional, la forma en que puede lograrse un acuerdo sobre el desarrollo, la imprevisibilidad, responsabilidad y atribución en el desarrollo de estas tecnologías. A estas interrogantes debemos sumar las cuestiones éticas en el uso de las ciberarmas. Además, falta realizar más estudios sobre los daños colaterales, psicológicos, además de humanos que pueden causar.

El analista estadounidense Coronel Timothy Thomas señala que hay varios elementos únicos en el enfoque de Rusia en la guerra de información, señalando que una "*information weapon"* o arma de información implica:

> "Un medio dirigido a activar (o bloquear) los procesos del sistema de información en los que el sujeto que usa las armas tiene interés. Un arma de información puede ser cualquier medio o sistema técnico, biológico o social que se utiliza para la producción, el procesamiento, la transmisión, la presentación o el bloqueo de datos y/o procesos que funcionan con los datos."[46]

46 Roland Heickerö, "Emerging Cyber Threats and Russian -views on Information. Warfare and Information Operatios", FOI, Swedish Defence Research Agency, 2010, pp. 13-15, disponible en: http://www.highseclabs.com/data/foir2970.pdf (Consultado el 29 de enero de 2019)

Para el autor el objetivo final del efecto de un arma de información es el conocimiento de un sistema de información específico y el empleo intencional de ese conocimiento para distorsionar el Modelo del mundo de la víctima.

Finalmente se debe considerar que estas armas de información, refería el exjefe adjunto del Estado Mayor Teniente General Aleksander Burutin en el año 2008, pueden ser empleadas de manera eficiente tanto en época de paz como durante la guerra[47].

3.2. Ciber ataques o ataques cibernéticos

> *Un conjunto de ataques maliciosos puede llegar a constituir un arma de destrucción masiva*[48].

Los ataques cibernéticos o ciberataques proporcionan al menos tres ventajas sobre otro tipo de armamento empleado en la guerra. Primero, pueden organizarse de forma relativamente más rápida y sistemática en todo el ciberespacio. Segundo, gracias a la hiperconectividad, ningún objetivo es demasiado remoto para un ataque cibernético. Tercero, los ataques cibernéticos tienen relativamente más opciones de herramientas, tiempo y objetivos de ataque para satisfacer sus objetivos y con costos limitados.[49]

Los ciberataques constituyen actos que se desarrollan en el ciberespacio y que podrían razonablemente causar daño[50]. Un ciberataque puede ser un acto de ciberespionaje, piratería o intento de obtener de forma ilícita contraseñas y preguntas de seguridad para obtener información secreta gubernamental o comercial. También puede constituir el

47 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 10.

48 BBC, "US launches cyber security plan," 29 mayo 2009, disponible en: http://news.bbc.co.uk/2/hi/americas/8073654.stm (Consultado el 20 de enero de 2019)

49 Chris Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia", *Pacetime Regime for State Activities in Cyberspace*, CCDCOE, pp. 598-602.

50 Michael Robinson & Kevin Jones & Helge Janicke, "Cyber warfare: Issues and challenges", *Computers & Security*, 2015, 49, pp. 70-94, disponible en: https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges (Consultado el 10 de enero de 2019)

bloqueo o desfiguración de un sitio web ya sea directamente o mediante una red de *bots*. Otro caso es el ataque contra la confidencialidad, disponibilidad o integridad de información crítica, o puede ser un acto genuino de guerra cibernética.

Lo que cuenta en el ciberataque, para ser considerado una amenaza de seguridad nacional, es el objetivo. Consideremos que algunas de las técnicas de software que pueden ser empleadas para la guerra cibernética, también lo son para llevar a cabo otro tipo de delitos comunes. Lo que difiere son los objetivos entre los cibercriminales. Si bien este tipo de armas implica la intromisión ilícita a sistemas informáticos, resulta distinto el robar la información personal para acceder a cuentas bancarias, enviar correos *spam* que con fines de sabotaje[51].

Por ello entendemos que, para el caso de seguridad nacional, un ciberataque debe estar encaminado a socavar las funciones de un sistema o red de computadoras con un propósito político o de seguridad nacional.

3.3. La ciberguerra (cyber warfare)

El 27 de abril del año 2007 Estonia fue atacada. Para ese año, el país había instituido un gobierno electrónico en el cual el 90% de los servicios bancarios, incluso sus elecciones parlamentarias, se desarrollaban a través de Internet. En cuestión de horas los portales de los principales bancos del país fueron colapsados. Todos los sitios web de los principales periódicos dejaron de funcionar. Las comunicaciones del Gobierno fueron bloqueadas. Docenas de objetivos estratégicos fueron atacados en todo el país. Aunque las consecuencias pueden ser medibles como efectos de guerra tradicional, un sistema de cómputo fue

51 Entendido como el daño, destrucción, perjuicio o entorpecimiento ilícito de vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal, órganos constitucionales autónomos o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios, de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa (artículo 140 Código Penal Federal)

responsable de todo[52]. Se contabilizaron al menos 128 ataques únicos *DDos*, dirigidos a los protocolos de Internet en Estonia durante este período[53]. Nunca se había atacado a un país entero en casi todos los frentes digitales a la vez.

Ciberguerra, *cyber warfare*, guerra cibernética, este término se emplea por diversos actores, cada uno con distintos significados. Aunque ha creado interés durante muchos años, carece de una definición generalmente aceptada. Incluso los analistas difieren en cuanto a si la etapa actual del conflicto cibernético puede considerarse como una guerra cibernética.

El concepto de guerra cibernética fue introducido por primera vez por John Arquilla y David Ronfelt en su artículo: "*CYBERWAR IS COMING!*"[54] (1993). En él, los autores describieron la guerra cibernética –distinta a la *netwar*[55]– como una forma de guerra que interrumpe, si no destruye, los sistemas de información y comunicaciones. También argumentaron que debido al cambio en la tecnología o la "revolución de la información[56]", la guerra cibernética se convertiría en un modo dominante de conflicto y guerra.

52 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *WIRED MAGAZINE*, agosto 21, 2007, disponible en https://www.wired.com/2007/08/ff-estonia/ (Consultado el 26 de enero de 2019)

53 Sean Kerner, *Estonia Under Russian Cyberattack?*, Security, mayo 18, 2007, disponible en: http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm (Consultado el 26 de enero de 2019)

54 John Arquilla y David Ronfeldt, "*CYBERWAR IS COMING!",* RAND, National Security Research División, 1993, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

55 Definida como los "conflictos de ideas de nivel social librados en parte a través de los modos de comunicación por Internet" (*societal-level ideational conflicts waged in part through internetted modes of communication*); *Cfr.* John Arquilla y David Ronfeldt, "*CYBERWAR IS COMING!*", RAND, National Security Research División, 1993, p. 27, https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 25 de enero de 2019)

56 Descrita por los autores como "el reflejo del avance de las tecnologías de información y comunicación computarizadas y las innovaciones relacionadas en la teoría de la organización y la gestión" ("*The information revolution reflects the advance of computerized information and communications technologies and related innovations in organization and management theory"*); *Cfr.* Arquilla, John y Ronfeldt, David, "*CYBERWAR IS COMING!", RAND*, National Security Research División, 1993, p. 25, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 25 de enero de 2019)

Desde el punto de vista del Derecho Internacional Humanitario, el Comité Internacional de la Cruz Roja, define el término –*cyber warfare*– como los "medios y métodos de guerra que consisten en operaciones cibernéticas que representan, o se llevan a cabo en el contexto de, un conflicto armado, en el sentido del Derecho Internacional Humanitario (DIH)"[57]. Es una operación contra una computadora o sistema informático, a través de un flujo de datos cuando se utiliza como medio y método de guerra en el contexto de un conflicto armado (a diferencia de las operaciones físicas y cinéticas o el uso del ciberespacio para la comunicación durante un conflicto armado)[58].

El Departamento de Defensa de Estados Unidos define a la guerra cibernética como "un conflicto armado llevado a cabo en su totalidad o en parte por medios cibernéticos".[59] Rusia, por su parte, emplea el término "*information war*" (IW) para referirse a "una batalla entre estados que involucran el uso exclusivo de armas de información en el ámbito de los modelos de información".[60] Dentro del contexto ruso no hay una diferencia importante entre los términos IW, lucha de información y batalla de información.[61]

Hay una distinción notable entre la psicología que sustenta el uso cibernético ruso y los métodos occidentales. Rusia ha dividido sus operaciones cibernéticas en dos: "información

57 *Cfr.* International Committee of the Red Cross, *Cyberwarfare and international humanitarian law: the ICRC's position*, ICRC, 2006, p. 1, disponible en: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (Consultado el 25 de enero de 2019)

58 Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space," entrevista de 16 agosto del año 2011, *ICRC Resource Centre,* disponible en: https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-inter- view-2011-08-16.htm (Consultado el 26 de enero de 2019)

59 "*Cyber Warfare (CW): An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. Includes cyber attack, cyber defense, and cyber enabling operations*" (Traducción libre); *Cfr.* Departamento de Defensa de Estados Unidos de América, *Cyberspace Operations Lexicon*, p. 8, disponible en: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (Consultado el 26 de enero de 2019)

60 Thimoty L. Thomas, *Comparing Us, Russian, and Chinese Information Operations Concepts*, Foreign Military Studies Office, 2004, p. 6, disponible en: http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

61 Ibíd.

técnica: ataques cibernéticos y DDoS e información-psicológica, que utiliza el ciberespacio para subvertir a otras sociedades".[62]

El concepto común resulta la información, la cual puede ser almacenada en cualquier lado y transmitida por cualquier medio, así como procesada de forma inmediata.

Existen autores que emplean el término "ciber conflicto" (*cyber conflict*). Para Valeriano y Maness ´éste implica:

> "*the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states*"[63]

Bajo esta tesitura, los autores consideran que la ciberguerra podría ser una escala mayor dentro del ciberconflicto que incluye la destrucción física y la muerte. Sin brindar una una definición clara de cuándo el conflicto cibernético se convierte en un escenario de guerra cibernética.

3.4. Conflictos híbridos

> *Una atribución de la guerra futura será la confrontación de la información ... la información se está convirtiendo en el mismo tipo de arma que los misiles, bombas, torpedos, etc.*[64]

El crecimiento en los conflictos y en las denominadas "acciones" o "guerras híbridas", han ido evolucionando

62 Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), *Russia: Implications for UK defence and security*, House of Commons, Reuno Unido, disponible en: https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10705.htm (Consultado el 29 de enero de 2019)

63 *El uso de tecnologías computacionales con fines malévolos y destructivos para impactar, cambiar o modificar las interacciones diplomáticas y militares entre los estados* (Traducción libre); *Cfr.* Brandon Valeriano & Bryan C. Maness, "Cyber War Versus Cyber Realities: Cyber Conflict in the International System", Oxford University Press, Oxford, 2015, pp. 3-4.

64 Slipchenko, *Future War (A Prognostic Analysis)*, January 1998, en Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

como amenazas en el ciberespacio con impactos en el mundo físico, que aún distan de conocerse a plenitud.

El potencial de conectividad que tiene Internet ha ayudado a la proliferación en el uso de armas de información masiva. O, mejor dicho, desinformación.

La creciente conectividad, el abaratamiento y accesibilidad de las tecnologías, ha generado un importante traslado de poder hacia actores no estatales. Las amenazas provienen de individuos y grupos que se encuentran emergiendo como actores relevantes, los cuales rápidamente ganan espacios e influencia, resultado de la "viralización" y la hiperconectividad que el ciberespacio nos provee.

Los conflictos que resultan de este tipo de acciones se caracterizan por no estar limitados a tiempo de guerra, ni siquiera se encuentran restringidos a una "fase inicial del conflicto", antes del inicio de hostilidades. Es una actividad continua independiente del estado de las relaciones que tenga el atacante con el Estado afectado.

Bajo el criterio ruso, nos encontramos en una "*informatsionnaya voyna*" (*information war*), donde la información, su intercepción, manipulación, distorsión y robo conforma el "conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y la comunidad internacional en todos los niveles".[65]

Los medios empleados en esta guerra de información pueden incluir: "desacreditar el liderazgo del adversario, intimidar al personal militar y a los civiles… falsificación de eventos, desinformación, entre otros"[66]. Todos ellos enfocados en el logro de fines políticos o diplomáticos, influyendo en el liderazgo y la opinión pública de Estados extranjeros, así como de organizaciones regionales e internacionales. La desinformación masiva, se perfila como

65 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 6, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

66 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 12, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

una amenaza para las sociedades. Debemos comenzar a analizar las consecuencias que pueden traer consigo la influencia en la percepción o decisión que tienen las personas al ser sometidas a campañas de desinformación masivas personificadas, gracias al *profiling* resultado de la información que dejan a través del uso de redes sociales o sus interacciones con otros.

Otra cuestión reside en las consecuencias que el "*affective computing*"[67] puede traer a la estabilidad de los individuos y las sociedades. Aún desconocemos cuales son los efectos que el perfilamiento de los usuarios con fines comerciales o las consecuencias ciertas de las implicaciones de Cambridge Analytica en las elecciones de Estados Unidos de América. Sin embargo, debemos considerar las amenazas que el empleo de algoritmos para conocer y manipular los sentimientos de las personas. Todos estos ingentes volúmenes de flujos de datos personales pueden ser generados por los nodos de IoT (Internet de las cosas, –*Internet of Things*– o por su acrónimo IoT), los cuales se transforman en la obtención de inteligencia, es decir, en información estratégica, útil, para la toma de decisiones y realización de acciones, o incluso, para el empleo de otros dispositivos y a partir de ahí, actuar sobre nosotros y nuestro entorno.

4. Los Retos

4.1. Algoritmos para la defensa y el ataque

El año pasado puso en relieve la importancia del uso de la Inteligencia Artificial (en adelante IA), el denominado *machine learning* (aprendizaje automático), y el Internet de las cosas IoT para la economía y los riesgos globales. Este trinomio aumenta los riesgos ya existentes y dan paso al surgimiento de otros.

La IA puede desempeñar un papel importante en la ciberseguridad, la inteligencia en la detección de ciberamenazas, en los análisis para detectar, contener y mitigar los

67 Entendida "cómo con el empleo de la Inteligencia artificial se puede reconocer, responder y manipular las emociones humanas"; *Cfr.* Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

advanced persistent threats (APTs), así como en la lucha y mitigación de actividades maliciosas en el ciberespacio. Un ejemplo de ello son las técnicas de inteligencia artificial empleadas para buscar de forma automática *malware* desconocido o vulnerabilidades de día cero (*zero-day*), en función de ciertas características y comportamientos.

La comprobación tradicional de vulnerabilidades de la red se basa en procesos que requieren mucha mano de obra y gran experiencia, sin embargo, son propensos a errores. El análisis y seguridad de las redes puede beneficiarse de los marcos automatizados basados en razonamiento para obtener una mejor conciencia cibernética del ciberespacio altamente dinámico. Comprender cómo se interconectan los dispositivos de red, cómo se procesa y cómo se almacena, resulta crucial para la conciencia cibernética que requieren las aplicaciones, como el monitoreo proactivo de la seguridad informática. La supervisión proactiva de la seguridad informática depende en gran medida de datos de red precisos, concisos y de calidad. Los sistemas inteligentes proporcionan mecanismos para reducir el impacto de los ataques cibernéticos y, siempre que sea posible, previenen los ataques y gestionan los riesgos de vulnerabilidad a través de la concienciación cibernética en tiempo real.[68]

Sin embargo, las técnicas y herramientas de IA también pueden y son explotadas con propósitos maliciosos. Imaginemos que con el empleo de la IA a la biotecnología se puedan crear patógenos, virus nuevas enfermedades que puedan ser empleados en contra de las personas. Otro ejemplo de ello es el empleo de técnicas de IA para identificar y explotar vulnerabilidades en sistemas y dispositivos. Distinto escenario constituye que un atacante (o grupo de atacantes) diseñe técnicas de IA para identificar y explotar vulnerabilidades en, vehículos autónomos o en drones, para facilitar ataques coordinados en lugares con grandes cantidades de personas o en horas pico. Además, a través de ataques coordinados, las técnicas de IA

68 Leslie F, Sikos, Dean Philp, Catherine Howard, Shaun Voigt, Markus Stumptner, y Wolfang Mayer, *Knowledge Representation of Network Semantics for Reasoning-Pwerd Cyber-situational Awareness*, en Leslie F. Sikos (editor), "AI in Cyberseucirty", Springer, Suiza, 2019, pp. 19-22 (19-46).

pueden explotar vulnerabilidades en infraestructuras de ciudades inteligentes (por ejemplo, sistemas de transporte inteligentes) para maximizar el impacto de dichos ataques, con el objetivo de causar pánico e inquietud en la sociedad. Por lo tanto, también existe la necesidad de defenderse contra los ataques ciberfísicos basados en la IA.

4.2. El cómputo cuántico

Dentro del flujo constante de información, el cifrado de las comunicaciones digitales ha cobrado una gran relevancia. Tal y como lo señaló el Relator Especial David Kaye, en el Informe A/HCR/29/32[69], en la actualidad el cifrado y anonimato son las principales vías de seguridad en línea que ofrecen a las personas un medio para proteger su privacidad, al permitirles elaborar y compartir ideas y opiniones, sin injerencia alguna. De esta forma reconoce las implicaciones sobre el uso del cifrado[70] y el anonimato como una forma de protección de la privacidad en la era digital.

69 David, Kaye, A/HRC/29/92 ,*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Organización de las Naciones Unidas, 2015, disponible en: *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx* (Consultado el 27 de enero de 2019).

70 El tema del cifrado tomó mayor relevancia en la conciencia pública derivado de la solicitud de FBI (*Federal Bureau of Investigation*) hacia la empresa Apple Inc., para colaborar en la investigación de los ataques terroristas que tuvieron verificativo en diciembre del año 2015 en San Bernardino, California. En esa ocasión el FBI solicitaba a la empresa la creación de una versión del sistema operativo de iPhone, que fuera capaz de evadir los sistemas de seguridad, lo que, bajo el argumento de la empresa, dicho *software* tendría el potencial para desbloquear cualquier dispositivo de esa clase y poner en riesgo la privacidad de sus usuarios. Para entender el contexto, la criptografía presupone la utilización de un método general de cifrado y una clave de cifrado. Mientras que el primero consiste en el sistema para encriptar el texto, la clave es una cadena que selecciona uno de los muchos cifrados disponibles. El cifrado se emplea comúnmente para la elaboración de firmas digitales, con la finalidad de identificar al emisor del mensaje y garantizar el contenido del mismo (como en el caso de la firma electrónica empleada por el Sistema de Administración Tributaria). El cifrado implica la codificación de datos para que sólo los destinatarios deseados puedan acceder a ellos. Derivado de la controversia suscitada entre la empresa Apple Inc., y el FBI y como un reconocimiento a la importancia de proteger la privacidad de los usuarios, aplicaciones como *WhatsApp* han creado un cifrado para proteger las conversaciones.

Mucha de la información que fluye a través del ciberespacio se encuentra cifrada, lo que aporta un elemento mayor de seguridad. Empero, "si alguna vez se construyen computadoras cuánticas a gran escala, podrán romper muchos de los sistemas de cifrado de clave pública que actualmente se encuentran en uso"[71]. Lo anterior comprometería la confidencialidad y la integridad de las comunicaciones digitales que se llevan a cabo a través de Internet y en otros lugares.

En el *Consumer Electronics Show* (CES) 2019, se presentó "IBM Q System One", considerado el primer sistema de computación cuántica de aproximación universal integrado del mundo, diseñado tanto para uso científico como comercial[72]. De esta forma IBM inicia la carrera en el mercado de ordenadores cuánticos con fines comerciales. Si consideramos que muchos de nuestros protocolos de comunicaciones más importantes se basan principalmente en tres funcionalidades criptográficas básicas: cifrado de clave pública, firmas digitales e intercambio de claves.[73] Con el surgimiento del cómputo cuántico comercial se acrecientan los riesgos y amenazas. Consideramos "segura" nuestra información, toda vez que se encuentra cifrada. Empero, el cifrado actual no representa ninguna barrera ante la computación cuántica.

La criptografía post-cuántica o criptografía resistente a la computación cuántica, tiene como objetivo el desarrollo de sistemas criptográficos que sean seguros contra computadoras. El robo de una base de datos que se encuentre cifrada, con la tecnología cuántica, podrá ser conocida. Por ello debemos empezar a trabajar en la investigación y desarrollo de soluciones de cifrado postcuántico que enfrenten los retos que trae aparejado.

71 National Institutoe of Standards and Technology, "Post-Quantum Cryptography", NIST, 2017, disponible en: https://csrc.nist.gov/projects/post-quantum-cryptography (Consultado el 29 de enero de 2019)

72 IBM, "IBM Unveils World's First Integrated Quantum Computing System for Commercial Use", 08 de enero 2019, disponible en: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use (Consultado el 22 de enero de 2019)

73 National Institute of Standards and Technology, "Report on Post-Quantum Cryptography", NISTIR 8105, 2016, p. 1.

Conclusiones

> *La ciberseguridad global implica una tremenda gama de problemas económicos, de privacidad y de seguridad nacional.* [74]

¿Entendemos las amenazas? No. A esto le sumamos una falta de unanimidad y claridad respecto a cómo afrontarlas. Igual que cualquier otra tecnología, el ciberespacio, empleado por las manos equivocadas representa un peligro importante para los individuos, las empresas, Estados y sociedades por igual. Empero lo anterior no significa que debamos desconectarnos y asilarnos de las bondades que esta tecnología y las TIC han traído consigo en pro de la humanidad.

Necesitamos emplear un enfoque holístico dentro de la ciberseguridad. Conocer cuáles son las amenazas que enfrenta el Estado y analizarlas. Conocer a los responsables de su planeación y financiación. Entender los riesgos e implementar una adecuada gestión de éstos. La falta de una visión completa de la problemática acrecienta los riesgos y tiene efectos al momento de decidir un curso de acción. toda vez que se carece de una visión de los impactos en el ámbito jurídico, estratégico, económico y político, a largo plazo, de cualquier decisión que se tome.

Otro reto que se presenta son las consideraciones éticas que trae consigo el uso de las ciberarmas y la guerra cibernética en general. Las ciberarmas son una nueva clase de armas, la guerra cibernética es una nueva clase de guerra. Al igual que sucede con la guerra tradicional, existen principios éticos que son seguidos por algunos actores, mientras que otros no tienen el mismo impulso de actuar éticamente. También resulta esencial identificar de manera concreta, las acciones que violen las pautas éticas acordadas en instrumentos internacionales. Esto nos permitirá resaltar el mal comportamiento en el ámbito internacional y responsabilizar a los perpetradores.

74 Martha Finnemore & Duncan B. Hollis, "Constructing Norms for Global Cybersecurity", The American Journal of International Law, Vol. 110, No. 3, 2016, pp. 425-479 (430)

No pueden trasladarse todas las experiencias y estrategias desarrolladas en el mundo físico al ciberespacio. La novedad y constante evolución de la tecnología plantea un serio un problema. Por ello la SN necesita actuar a la velocidad de las redes. El ciberespacio "no es un sistema de soporte aislado sino un ecosistema multidimensional que tiene que funcionar perpetuamente y de manera resistente, libre de amenazas o posibilidades de daño"[75]. Necesitamos crear un ecosistema cibernético resiliente. Podemos automatizar algunas herramientas en la implementación de la ciberseguridad, siempre que la toma de decisiones sea humana. Una ayuda pueden ser los sistemas de IA aplicados al rastreo y mitigación de riesgos. Lo anterior debe ir de la mano con la capacitación constante de la fuerza laboral de ciberseguridad, permitiéndoles adaptarse y responder a las amenazas conocidas y a las desconocidas, las cuales emplean técnicas y procedimientos tácticos aún no creados.

No necesitamos una militarización del ciberespacio. Necesitamos coordinación y colaboración, seguridad y resiliencia. Pero no restricciones arbitrarias ni violatorias de derechos humanos. Este espacio que llamamos ciberespacio es un lugar y herramienta en donde ejercemos nuestros derechos humanos, en especial la libertad de expresión, acceso a la información, pero donde principalmente peligran otros como la privacidad, la protección de nuestra información.

Para España, los esfuerzos por diseñar un sistema eficaz de gobernanza sobre las nuevas tecnologías son la clave para la Seguridad Nacional.[76] En nuestro caso también deberían serlo. La importancia de una Agenda Digital coherente. Coherente con las amenazas, riesgos, políticas y su implementación. Coherente con los *multistakeholders* que conforman el ecosistema del ciberespacio. Reforzados con sistemas fuertes de *accountability* para el gobierno y las empresas en materia de ciberseguridad, lo que podría ayudar a mitigar los riesgos.

75 Paul Cornish, "Cyber Warfare and Homeland Security", en Kostopolous, George, *Cyberspace and Cybersecurity*, Segunda Edición, CRC Press, Florida, p. 175.

76 Presidencia del Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, p. 35.

Necesitamos una política clara, conformada por un consenso compartido, formado por una discusión informada y creada por un cuerpo común de conocimiento. No se deben tomar decisiones a la ligera, ni a favor de un solo sector, de las cuales desconocemos sus impactos a mediano y largo plazo.

BIBLIOGRAFÍA

Arquilla, John & Ronfeldt, David, "CYBERWAR IS COMING!", *RAND*, National Security Research División, 1993, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 29 de enero de 2019)

Asamblea General de Naciones Unidas, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*, 14 de septiembre 2011, disponible en: http://undocs.org/A/66/359 (Consultado el 18 de diciembre de 2019)

BBC, "US launches cyber security plan," 29 mayo 2009, disponible en: http://news.bbc.co.uk/2/hi/americas/8073654.stm (Consultado el 20 de enero de 2019)

Consejo de Derechos Humanos de la Organización de Naciones Unidas, Resolución A/HRC/20/L.132 de 29 de junio 2012, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf (Consultado el 20 de enero de 2019)

Cornich, Paul "Cyber Warfare and Homeland Security", en Kostopolous, George, *Cyberspace and Cybersecurity*, Segunda Edición, CRC Press, Florida, 2017.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe", *WIRED MAGAZINE*, agosto 21, 2007, disponible en https://www.wired.com/2007/08/ff-estonia/ (Consultado el 26 de enero de 2019)

Departamento de Defensa de Estados Unidos de América, "Cyberspace Operations Lexicon", disponible en: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (Consultado el 26 de enero de 2019)

Departamento de Defensa de Estados Unidos de América, "The National Military Strategy for Cyberspace Operatios", diciembre 2006, disponible en: https://www.hsdl.org/?view&did=35693 (Consultado el 20 de enero de 2019)

Demchak, Chris, "Economic and Political Coercion and a Rising Cyber Westphalia", *Pacetime Regime for State Activities in Cyberspace*, CCDCOE NATO, 2013.

Dipert, Randall, "Other-tahn-Internet (OTI) cyberwarfare: challenges for ethics, law and policy", *Journal of Military Ethics*, 12(1), abril, 2013, disponible en: https://www.researchgate.net/publication/263529399_Other-than-internet_oti_cyberwarfare_Challenges_for_ethics_law_and_policy (Consultado el 27 de enero de 2019)

Droege, Cordula (ICRC Legal Adviser), "No legal vacuum in cyber space", entrevista 16 de agosto 2011, *ICRC Resource Centre,* disponible en: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (Consultado el 28 de enero de 2019)

Elisan, Christopher, "Malware, Rootkits, and Botnets: A Beginner,s Guide", McGraw Hill, 2013.

European Union Agency for Network and Information Security, "Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe", European Union Agency for Network and Information Security, 2018, disponible en: https://www.enisa.europa.eu (Consultado el 24 de enero 2019)

European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

Finnemore, Martha & Hollis, Duncan B., "Constructing Norms for Global Cybersecurity", *The American Journal of International Law,* Vol. 110, No. 3, 2016, pp. 425-479.

Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

Giles, Keir, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, disponible en:

https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

Gobierno de Canadá, "Canada´s Cybersecurity Strategy. For a stronger and more prosperous Canada", 2010, disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx (Consultado el 23 de enero de 2019)

Gobierno de Estados Unidos de América, "United States National Strategy to Secure Cyberspace", 2003, disponible en: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Consultado el 28 de enero de 2019)

Heickerö, Roland, "Emerging Cyber Threats and Russian -views on Information. Warfare and Information Operatios", FOI, Swedish Defence Research Agency, 2010, disponible en: http://www.highseclabs.com/data/foir2970.pdf (Consultado el 29 de enero de 2019)

IBM, "IBM Unveils World's First Integrated Quantum Computing System for Commercial Use", 08 de enero 2019, disponible en: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use (Consultado el 22 de enero de 2019)

International Committee of the Red Cross, *Cyberwarfare and international humanitarian law: the ICRC's position*, ICRC, 2006, disponible en: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (Consultado el 25 de enero de 2019)

Isaac, Mike & Frenkel, Sheera, "Facebook Security Breach Exposes ccounts of 50 Millon Users", *The New York Times*, 28 de septiembre 2018, disponible en: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (Consultado el 28 de enero de 2019)

Kerner, Sean, "Estonia Under Russian Cyberattack?", *Security*, mayo 18, 2007, disponible en: http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm (Consultado el 26 de enero de 2019)

Laity, Mark, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), *Russia: Implications for UK defence and security*, House of Commons, Reino Unido, disponible en: https://publications.parliament.uk/pa/cm201617/cmselect/

cmdfence/107/10705.htm (Consultado el 29 de enero de 2019)

Ministerio de Asuntos Exteriores de Rusia, "Convention on International Information Security", 22 de septiembre 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (Consultado el 27 de enero de 2019).

Müller, Enrique, "Alemania Sufre el mayor "hackeo" de su historia con la filtración. De datos personales de centenares de políticos", *El País Internacional*, 04 de enero de 2019, disponible en: https://elpais.com/internacional/2019/01/04/actualidad/1546595085_679572.html (Consulado el 20 de enero 2019)

National Institute of Standards and Technology, "Post-Quantum Cryptography", NIST, 2017, disponible en: https://csrc.nist.gov/projects/post-quantum-cryptography (Consultado el 29 de enero de 2019)

National Institute of Standards and Technology, "Report on Post-Quantum Cryptography", NISTIR 8105, 2016.

Presidencia de Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

Presidencia de Gobierno, "Estrategia de Seguridad Nacional. Un proyecto compartido de todos para todos", Presidencia del Gobierno, España, 2017, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

Rid, Thomas & McBurney, Peter, "Cyber-Weapons", *The RUSI Journal*, 157;1, 2012, disponible en: https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354 (Consultado el 29 de enero de 2019)

Reuter, Markus, "Alles außer AfD: Was wir über das große Datenleck wissen", *Netzpolitik.com*, 04 de enero 2019, disponible en: https://netzpolitik.org/2019/alles-ausser-afd-was-wir-ueber-das-grosse-datenleck-wissen/ (Consultado el 20 de enero de 2019)

Robinson, Michael & Jones, Kevin & Janicke, Helge "Cyber warfare: Issues and challenges", *Computers & Security*, 2015, 49, pp. 70-94, disponible en: https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges (Consultado el 10 de enero de 2019)

Rowe, Neil "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, pp. 307-326

Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

Thomas, Thimoty L., "Information Security Thinking: A Comparation of U.S., Russian and China Concepts", *Foreign Miltary Studies Office*, julio 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

Union Internacional de Telecomunicaciones (UIT), Rec. ITU-T X.1209 (12/2019), *Capabilities and their context scenarios for cybersecurity information sharing and exchange*, ITU-T X-Series Recommendations, UIT, 2010.

Unique Identification Authority of India, "*What is Aadhaar?*", Government of India, disponible en: https://uidai.gov.in/what-is-aadhaar.html (Consultado el 28 de enero de 2019)

Valeriano, Brandon & Maness, Bryan C., "Cyber War Versus Cyber Realities: Cyber Conflict in the International System", Oxford University Press, Oxford, 2015.

Resoluciones de la Asamblea General de Naciones Unidas
A/RES/55/28 de 20 de noviembre del año 2000
A/RES/56/19 de 29 de noviembre de 2001
A/RES/58/32 de 08 de diciembre de 2003
A/RES/58/199 de fecha 30 de enero 2004
A/RES/59/61 de 3 de diciembre de 2004
A/RES/60/45 de 8 de diciembre de 2005
A/RES/61/54 de 6 de diciembre de 2006
A/RES/62/17 de 05 de diciembre de 2007
A/RES/63/37 de 2 de diciembre de 2008

Revista de Administración Pública

INAP

Seguridad de la información en instituciones de educación superior de México

Rafael Espinosa García, Guillermo Morales Luna.

Resumen: Hacemos una investigación bibliográfica de la ciberseguridad en ambientes universitarios y centros de investigación gubernamentales de México. Planteamos la importancia de la seguridad informática en cuanto a la seguridad nacional y su normatividad actual. Las características principales de la seguridad de la información y la gobernanza de los datos y su valor agregado, en el ambiente propiamente universitario y científico para salvaguardarlos para la toma de decisiones de la entidad universitaria. Presentamos un caso de estudio para ilustrar la efectividad de las medidas que proponemos para resguardar los datos obtenidos en el laboratorio de investigación.

Palabras clave: Ciberseguridad, Gobernanza, Información, Acceso, Transparencia

Information security in Mexico's higher education institutions

Abstract: A bibliographical research is performed related to cybersecurity in academic and government scientific centers in Mexico. We analyze the relevance of information security with respect to national security and legal and technical standards. The main features of information

security and data governance are described in order to advice the academic and scientific authorities in decision making. A case of study is discussed with the purpose to illustrate the proposed measures to keep in protection the collected data in a scientific laboratory.

Keywords: Cybersecurity, Governance, Information, Access, Transparency

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 28 de enero de 2019

Revista de Administración Pública

INAP

Seguridad de la información en instituciones de educación superior de México

Rafael Espinosa García*
Guillermo Morales Luna**

1. Introducción

La seguridad informática a nivel nacional es de tanta importancia que ha de ser motivo de atención de la seguridad y la defensa nacional, y a nivel universitario es igualmente de gran relevancia. El conocimiento es poder, proclama el dicho popular, y las universidades y los centros de investigación son generadores de conocimiento. Tan sólo por este punto, la seguridad informática de los centros universitarios y de investigación es un tema de

* Licenciatura en Sistemas de Computación Administrativa por la UVM, Maestría en Ingeniería en Sistemas por la UVM. Perito Certificado en Cómputo Forense. Certificación CISCO CCNA. Iniciador del dominio cinvestav.mx, y administrador del mismo por 7 años. Intereses de investigación: Seguridad Informática, Protocolos de comunicación TCP/IP, Seguridad en Big Data y Programación de Sistemas IOT. Actualmente Auxiliar de Investigación en la Sección de Electrónica del Estado Sólido del Departamento de Ingeniería Eléctrica en Cinvestav-IPN.

** Investigador Titular en el Departamento de Computación del Cinvestav-IPN, Licenciatura en Física y Matemáticas por la ESFM-IPN, Maestro en Ciencias con especialidad en Matemáticas por el Cinvestav-IPN, y Doctor en Ciencias Matemáticas por el Instituto de Matemáticas de la Academia Polaca de Ciencias. Áreas de interés: Fundamentos Matemáticos de Computación, Lógica, Criptografía y Teoría de la Complejidad. Ha sido profesor en el IPN y en la B. Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y le fue concedida la ciudadanía polaca.

interés nacional. De manera global, nos referiremos a las instituciones de educación superior, a las universidades, y a los centros de investigación básica y de tecnología como centros académicos.

Dichos centros requieren manejar procesos administrativos (tanto de control de personal como de control escolar), educativos (en cuanto a cursos en línea, herramientas de auxilio a profesores, experimentos de laboratorio, accesos a bibliotecas digitales, o cualesquiera otros servicios digitales), de desarrollo tecnológico (tales como el diseño de dispositivos, vinculación universidad-empresa, resguardo de productos tecnológicos y biotecnológicos, realización de pruebas de calidad, calibración de equipos, certificación de componentes, etc.) y de investigación científica (control de experimentos, avances de investigaciones, publicación, diseminación, resguardo, seguimiento y validación de resultados, etc.) Todos estos procesos involucran el uso y la explotación de información sensible desde varios puntos de vista, tales como los de tipo social, institucional, organizativo y, también, comercial y económico. Pero ciertamente, los centros académicos han de esmerarse en el cuidado de su prestigio y de su buen nombre institucional.

Las vulnerabilidades de las que se pueda adolecer impactarían gravemente en los centros académicos. Pretendemos enfatizar en el presente texto la importancia que tiene la seguridad informática en los centros académicos a la luz de los más recientes recursos tecnológicos.

En una primera sección nos referimos al acceso a la red de redes en México y a los esfuerzos y estrategias gubernamentales en preservar la ciberseguridad a nivel nacional. Después nos referimos, de manera general y conceptual, a la seguridad informática. La tercera sección trata específicamente de la seguridad informática en centros académicos. Describimos los riesgos principales y bosquejamos una organización corporativa universitaria para afrontarlos, disminuirlos y acaso evitarlos y presentamos finalmente un caso de estudio concreto.

2. La carretera de la información a nivel nacional

2.1 Seguridad en la carretera de la información

México se clasifica como el segundo país de América Latina con más ataques cibernéticos. Hubo aproximadamente 10 millones de víctimas en 2014, y un incremento del 40% entre 2013 y 2014. Dado que el 57.4% de los 127 millones de habitantes en la República Mexicana son usuarios de Internet, cerrar las brechas en su entorno de seguridad cibernética es una tarea importante con implicaciones para una parte grande y creciente de su población. El gobierno, el sector privado y la sociedad civil deben mantenerse al día con la innovación constante en el sector de la tecnología de la información (TI), como usuarios y como posibles objetivos de ataques. México ocupa el segundo lugar después de Brasil entre los países que envían correos no deseados por medio de la red. Brasil, México y Colombia reciben o emiten el 75% del correo basura en Latinoamérica.[1]

En la Era del Conocimiento, el acceso a Internet se encuentra asociado de manera importante con el nivel de estudios. En particular, en México se ha encontrado que nueve de cada diez personas con nivel superior de estudios (licenciatura y posgrado), cuatro de cada cinco con nivel medio superior (preparatoria o equivalente), y poco menos de la mitad (48.7%) con nivel básico (primaria o secundaria) han incorporado en sus actividades diarias el uso de Internet.[2]

Actualmente las amenazas de ciberseguridad plantean un problema de riesgo creciente cada vez más común para colegios, universidades y centros de investigación, públicos

1 Parraguez K. L., The State of Cybersecurity un Mexico: An Overview, Wilson Center. Mexico Center, Woodrow Wilson Center. January 2017. Recuperado el 7 de julio de 2018. https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

2 INEGI, Estadísticas a propósito del día mundial del Internet (17 de mayo). 15 de mayo de 2017. Recuperado el 7 de julio de 2018. http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

y privados.[3] La continuidad del avance tecnológico y académico requiere la protección de la información personal e intelectual de investigadores, profesores, administradores y estudiantes. Además, en cualquier institución académica es imprescindible mantener un ancho de banda para cubrir sus necesidades de comunicación, procesamiento y almacenamiento, mientras se bloquean las amenazas e intromisiones que afecten el funcionamiento y el prestigio de la institución.[4]

2.2 Ciberseguridad y estrategia de seguridad nacional

A fines de 2012, el Presidente de la República, Enrique Peña Nieto, presentó el Plan de Desarrollo 2013-2018, en donde se establece la estrategia del Programa de Seguridad Nacional 2014-2018, y enfoca los intereses estratégicos y los objetivos nacionales de México.[5] Se creó el Comité Especializado de Seguridad de la Información, encargado de la redacción de la Estrategia Nacional para la Seguridad de la Información, basándose en una idea de seguridad multidimensional que abarque amenazas antiguas y nuevas, y se planteó que tal estrategia es un elemento importante en la preservación de la paz y la estabilidad no sólo del país, sino de todo el Continente Americano. En cuanto a las políticas específicas de ciberseguridad para proteger y promover los intereses nacionales, los principales compromisos que se detallan son: promover acciones para prevenir y combatir los ataques cibernéticos; fortalecer los mecanismos para prevenir incidentes en los sitios ejecutivos federales; defender el cumplimiento y el desarrollo de procedimientos para evaluar y fortalecer el

3 Dovey F. T., Clark C. and Lyn G. J., Elevating cybersecurity on the higher education leadership agenda: Increasing executive fluency and engagement in cyber risk. Deloitte Insights, February 2018. https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

4 Palo Alto Networks, Next Generation Security for Higher Education Institutions. 2017. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/higher-education-institutions-solution-brief

5 Gobierno de México, Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI. Publicado en el Diario Oficial de la Federación de México, el 30 de Abril de 2014. Recuperado el 4 de octubre de 2018. http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

desempeño de los equipos de respuesta ante incidentes de seguridad cibernética en los poderes federales; mejorar las capacidades de capital humano y la infraestructura tecnológica para abordar los incidentes de seguridad cibernética; establecer una cooperación internacional sobre seguridad cibernética y defensa cibernética, en particular con los países de América del Norte para prevenir y abordar los ataques a los sistemas informáticos del país.

Aunque en México el terrorismo no representa un riesgo alto, es necesario adoptar medidas preventivas para identificar vulnerabilidades y protegerse de amenazas y riesgos externos. El Gobierno de México estableció una serie de medidas y acciones en el Programa de Seguridad Nacional 2014-2018 para identificar posibles ataques contra la seguridad nacional. Expertos mexicanos mantienen colaboración estrecha y constante con más de 300 equipos de 69 países para prevenir y combatir estos delitos. México es miembro del Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST), una agrupación de 369 equipos en 78 países, y participa con cuatro agrupaciones.[6] La seguridad de la información en la red se ha vuelto cada vez más importante con la amenaza creciente en el ciberespacio. Sólo algunos ciberdelitos son punibles, ellos no siempre se encuentran explícitamente tipificados y el entorno legal está disperso en diversos ordenamientos de diversas índoles en los planos federal y local. El Gobierno Federal se ha centrado en fortalecer la seguridad cibernética y promover la legislación pertinente para garantizar la seguridad nacional y reducir el nivel de violencia. Reconoce los desafíos globales que conllevan problemas tecnológicos, energéticos, demográficos y ambientales, y describe las vulnerabilidades del Estado.

2.3 Regulación gubernamental de la información en México

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un organismo autónomo en México.[7] El organismo, antes

6 CERT-MX, Mnemo-CERT, Scitum-CSIR and UNAM-CERT FIRST (2016). https://www.first.org/members/map#mexico

7 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. http://inicio.ifai.org.mx/SitePages/ifai.aspx

conocido como Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), cambió de nombre en mayo de 2015 tras la aprobación de la Ley General de Transparencia y Acceso a la Información.

El organismo tiene la función, principalmente, de:

- Garantizar el derecho de acceso de las personas a la información pública gubernamental.
- Proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares.
- Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

A partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el 12 de junio de 2003, más de 240 dependencias y entidades del gobierno federal tienen la obligación de responder a solicitudes de información bajo la vigilancia del IFAI. El IFAI promovió la recepción de estas solicitudes a través de internet, mediante el sistema INFOMEX.[8]

Los centros académicos en nuestro país con base en sus Reglamentos de Transparencia y Acceso a la Información Pública establecen el catálogo de datos personales a proteger y su alcance, considerados en lo general como información confidencial. Estos reglamentos definen las reglas de cómo se identificarán y consultarán los documentos que se publicarán en la Plataforma de Transparencia y Obligaciones de cada entidad universitaria. Los reglamentos serán utilizados por las áreas universitarias para la elaboración de versiones públicas que deriven de solicitudes de información y aquéllas que sean necesarias para el cumplimiento de las obligaciones comunes de transparencia.

El año pasado el INAI publicó un estudio acerca de los alcances del derecho de acceso a la información, sin embargo, sólo se considera la rendición de cuentas y la

8 Plataforma Nacional de Transparencia. http://www.infomex.org.mx/gobiernofederal/home.action

transparencia en las entidades universitarias.[9] No hay una reglamentación en lo que respecta a los datos obtenidos en las investigaciones desarrolladas por los investigadores en los centros académicos.

El incremento en la adopción de procesos basados en Internet, el hecho de que la información fundamental se genera a partir de datos que se obtienen del consumidor, incrementan el riesgo en forma importante.

El establecimiento de una regulación gubernamental de la información, tanto en manos del gobierno como en la de particulares, es un avance importante en México, sin embargo, *el cumplimiento regulatorio no elimina el riesgo*.[10]

Es de suma importancia el desarrollo de estándares y procedimientos de seguridad adecuados a la realidad operativa de cada nivel escolar existente en el país, que permitan el aseguramiento de la información que se encuentra almacenada en los sistemas de cómputo y redes de los planteles del sector educativo nacional.

El desarrollo de una normatividad nacional de ciberseguridad orientada al sector educativo de México, podría ser encabezada por el INAI o establecer un organismo nacional dedicado al desarrollo, certificación y el establecimiento de estándares y procedimientos de innovación tecnológica en el área de seguridad de la información para el sector público o privado.

2.4 Agencia de Ciberseguridad Nacional

En 2017 se desarrolló un estudio por la CANIETI, la Asociación Mexicana de Tecnologías de la Información y la

9 Islas, J, Estudio sobre los alcances del derecho de acceso a la información en Universidades e Instituciones de Educación Superior públicas dotadas de autonomía, derivado de la Reforma Constitucional en materia de transparencia. INAI, Diciembre 2017. http://inicio.inai.org.mx/Estudios/AlcancesUniversidadesWeb.pdf

10 Kravchenko, S. and Riley, M., The American Fugitive From the JPMorgan Hack Turns Up in a Russian Cell. https://www.bloomberg.com/news/articles/2016-10-10/jpmorgan-hack-fugitive-said-to-seek-u-s-deal-from-russian-cell

Asociación de Internet MX, que mostró algunos hallazgos importantes.[11]

Dentro de los principales resultados y recomendaciones destacan:

- La necesidad de contar con una Agencia de Ciberseguridad Nacional que coordine la estrategia que se está definiendo y genere la ruta crítica de la gobernanza en Internet, y que además coadyuve a generar certeza y confianza en el nuevo ecosistema digital.
- La importancia de redefinir el marco jurídico para la ciberseguridad, armonizando las legislaciones federales y estatales, garantizando la protección a datos personales y estimulando la compartición de información. Un marco que dote a los cuerpos policiacos de herramientas adecuadas.
- Garantizar la protección de infraestructura crítica, sobre todo la ciberresiliencia bajo un enfoque de gestión de riesgo para que se tengan mecanismos y protocolos claros para la recuperación de los sistemas.
- El desarrollo de habilidades y competencias para el nuevo ecosistema digital, definiendo claramente las nuevas habilidades que serán necesarias ampliando, desarrollando y reclutando el mejor talento posible.

Por otra parte, de acuerdo al mismo estudio del sector privado, las brechas más importantes de las organizaciones mexicanas se encuentran: "en cuanto a clasificación de información, métricas de ciberseguridad, capacitación en continuidad de negocio o ciberresiliencia; así como pruebas de vulnerabilidades por terceros".

11 Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, Evaluación de la Ciberseguridad en México: brechas y recomendaciones en un mundo hiper-conectado, Octubre 2017. Recuperado el 26 de enero de 2019. https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html

3. Seguridad de la información

Las amenazas cibernéticas en México contra la seguridad en los sistemas de tecnologías de la información (TI), y en los datos incluyen los llamados *malware, spyware, keystroke loggers* (registradores de teclas), los accesos de *puertas traseras* a sistemas de TI, la suplantación de identidades y las estafas *dirigidas*, las cuales son diseñadas para robar partículas de identidad de usuarios, el mal uso intencional por usuarios con accesos legítimos, y los ataques de denegación de servicios. Quienes manejen los sistemas de TI y los datos contenidos en ellos deben protegerse de eventos fortuitos: desastres naturales, cortes de energía y recursos de TI perdidos o extraviados (p. ej., aspectos minúsculos como memorias USB perdidas que contengan datos confidenciales). También, se debe proteger a datos y a sistemas de acciones descuidadas realizadas por usuarios legítimos, como la eliminación accidental de datos importantes, la publicación accidental de datos confidenciales en un recurso público (una página *web*) o enviando información (digamos por correo electrónico) a personas indebidas.

La seguridad de la información se refiere a mecanismos que protegen datos. Con frecuencia, aquellos menos familiarizados con la seguridad de la información la consideran como meros procedimientos de control técnico en los sistemas de TI. Sin embargo, la seguridad de la información es más que eso y debe entenderse como el estudio y la práctica de protección de datos en todas sus formas (por ejemplo, almacenada en sistemas de TI o colocada en papel u otro medio físico). Los datos deben ser protegidos de cualquier tipo de amenazas, sean estas últimas perpetradas por personas externas o personas con acceso legítimo. La práctica de proteger datos incluye tres conceptos distintos de seguridad de la información, descritos a continuación.[12]

12 Lyn J. G., Understanding Information Security and Privacy in Postsecondary Education Data Systems. EDUCAUSE, May 2016. Recuperado el 22 de mayo de 2018.
http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy-executive_summary.pdf

Confidencialidad. Su propósito es proteger datos contra todas las formas de acceso no autorizado a lo largo de sus ciclos de vida (desde la creación de datos hasta la destrucción de ellos), impidiendo el acceso a individuos no afiliados a la organización que almacena datos (delincuentes, espías o *hackers*). También incluye el acceso de individuos dentro de una organización que exceden deliberadamente sus privilegios al acceder la información (por ejemplo, individuos que buscan los registros de celebridades u otras personas específicas cuando no tienen una razón profesionalmente legítima para hacerlo, o empleados desleales que usurpan funciones o alcances de superiores).[13] La confidencialidad es el concepto de seguridad de la información mayormente implicada cuando una organización sufre una violación de datos.

Integridad. Su propósito es garantizar que los datos dentro de los sistemas de TI sean correctos y completos al ser grabados o reproducidos en medios físicos. Los responsables de TI han de implantar controles dentro del sistema bajo su responsabilidad para garantizar que los usuarios ingresen y procesen los datos correctamente y que se identifiquen y resuelvan los elementos de datos conflictivos. Para la integridad se requiere que sólo usuarios autorizados puedan tener la capacidad de agregar, cambiar, mover o eliminar ciertos tipos de datos de los archivos. Cuando estos datos poseen integridad, se les considera precisos y se puede confiar en ellos para la toma de decisiones.

Disponibilidad. Esta propiedad garantiza que los datos estén al alcance de la mano cuando sea necesario y que los sistemas de TI funcionen confiablemente. Los llamados *stakeholders* pueden garantizar la disponibilidad de datos diseñando sistemas "redundantes" y robustos a ataques, asegurando que los usuarios hagan copias de seguridad de los datos regularmente.

Privacidad. Esta propiedad se refiere a conceptos que se aplican tanto a individuos como a la sociedad en general.

13 Gorman, A., and Sewell, A. (2015, July 12). Six people fired from Cedars-Sinai over patient privacy breaches. Los Angeles Times, July 12, 2013. http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713

Para los individuos, la privacidad entraña el derecho que tiene un individuo a controlar sus propios datos y para especificar cómo se recopilan, se usan y se comparten. La privacidad debería ser esencial en cualquier política de seguridad de la información. Es posible sin embargo imaginar una situación donde los datos son seguros pero no son privados. Los datos podrían almacenarse en un sistema de TI de una manera segura, pero si esos datos fueron recolectados sin el consentimiento de la persona propietaria u originaria, o sin la debida autoridad legal, entonces la privacidad de esos datos, en lo que se refiere a un individuo, puede estar comprometida. Por lo contrario, los datos pueden ser privados pero no seguros, por ejemplo, si los datos son recolectados con el consentimiento de una persona o de conformidad con una ley que permita la recopilación de datos, y éstos son almacenados en un sistema de TI que carece de la seguridad suficiente para protegerlos de quienes buscan robarlos, la seguridad de los datos está comprometida.

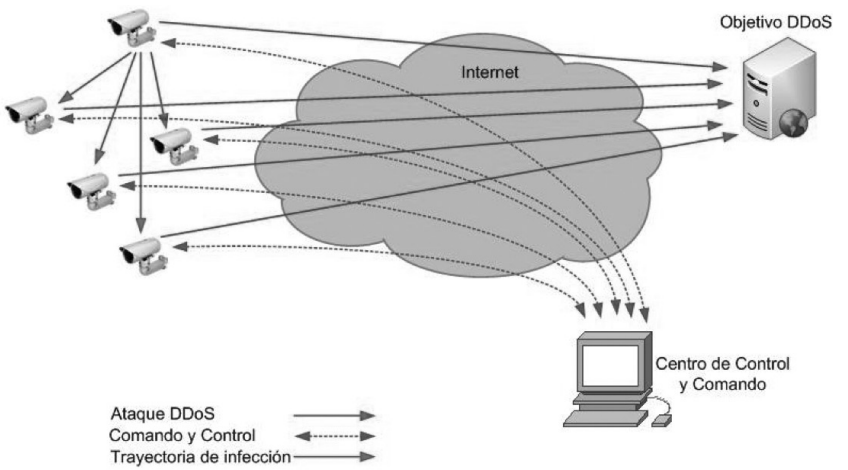
Los conceptos de seguridad de la información y privacidad deben considerarse en forma integral para proteger datos recopilados, almacenados, transmitidos y analizados dentro del ecosistema informático de cualquier institución de educación superior. Las medidas de privacidad y seguridad de la información deben ser utilizadas para proteger la confidencialidad, integridad y disponibilidad de cualquier información recolectada. En la actualidad existe una gran cantidad de dispositivos de IoT (*Internet of Things*) inseguros (*routers* domésticos, cámaras habilitadas para redes y grabadoras de vídeo digital), con un alto poder de cómputo, lo que los convierte en objetivos muy atractivos para los *hackers*, ya que los buscan para comprometerlos y usarlos en la construcción de *botnets* en gran escala, como se muestra en la figura 1. Un *botnet* (apócope de *bot network*, y éste a su vez de *web robot network*) es una red de máquinas infectadas llamados *bots* o *zombies* que forman una infraestructura de control y comando, la cual es utilizada para diversas actividades maliciosas tales como el lanzamiento de ataques distribuidos DDoS (*Distributed Denial of Service*).[14]

14 Bertino, E., and Islam, N., Botnet and Internet of Things Security. Computer, Vol. 50, Issue 2, Feb. 2017, pp. 76-79.

Entre los investigadores y estudiantes de nuestro país, es usual que para desarrollar sus actividades de investigación se apoyen en la tecnología BYOD (*Bring YOur Device*), lo que les permite una movilidad sin restricciones. Sin embargo, estos dispositivos incrementan la posibilidad de que puedan ser usados en ataques distribuidos en base a dispositivos de Internet de las Cosas (IoT), como son los ataques de negación de servicios (DDoS) o *malware*, o su combinación, si no se cumple con una política de seguridad institucional.[15]

De acuerdo a la investigación dirigida por *Markets and Markets*, hubo un crecimiento de 50% a finales del 2017 de los dispositivos móviles (laptops, teléfonos celulares y tabletas personales). Un estudio de Cisco Systems en 2017, concluyó que el 69% de las decisiones de tecnologías de la información favorecieron a BYOD.[16]

Figura 1
Plataforma distribuida para dispersión de malware o ransomware usando infraestructura de IOT para generación de ataques DDoS17



15 Aenugu, N.R., Butakov S., Zavarsky P., Aghili S. (2018) Security Perspective in Comparative Study of Platform-Based and Platform-Less BYOD Systems. In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017. Lecture Notes in Electrical Engineering, Vol. 450. Springer, Singapore.

16 Bouk, J., Top BYOD Trends for 2018. 14 november 2017, Cass Telecom Systems. https://www.casstelecom.com/blog/top-byod-trends-for-2018

17 Hinden, B., The Internet of Insecure Things. The Internet Protocol Journal, Volume 20, Number 1, March 2017.

3.1 Gobernanza de los datos

El término "gobernanza", en general, se refiere a la forma en que una organización asegura que las estrategias se establecen, se monitorean y se logran.[18] Como las Tecnologías de Información son torales en cada organización gubernamental o empresarial, por definición, el gobierno de TI se convierte en una parte integral de cualquier estrategia comercial, y cae bajo el gobierno corporativo.[19] Históricamente, los datos surgieron de sistemas transaccionales heredados dispares. Entonces, fueron vistos como un subproducto de la gestión del negocio, y tenían poco valor más allá de la transacción y la aplicación que los procesó, por lo tanto, los datos no se trataron como un activo valioso; esto continuó hasta principios de la década de los 90, cuando el valor de los datos comenzó a tomar otra tendencia más allá de las meras transacciones. Las decisiones y los procesos empresariales comenzaron a ser impulsados por los datos y sus correspondientes análisis. Una mayor inversión en la gestión de datos fue el enfoque adoptado al aumentar el volumen, la velocidad y la variedad de datos, como repositorios de datos complejos, almacenes de datos, *Enterprise Resource Planning* (ERP) y *Customer Relationship Management* (CRM).[20] Los enlaces de datos se volvieron muy complejos y compartidos entre sistemas múltiples, además de contar con la necesidad de proporcionar un solo punto de referencia para simplificar las funciones diarias, lo que se volvió crucial, dando origen a los datos maestros de gestión.[21]

18 Weber, K.; Otto, B.; Osterle, H. One Size Does Not Fit All—A Contingency Approach to Data Governance. ACM Journal of Data Information Quality, Vol. 1 Issue 1 June 2009 Article No. 4.

19 Salami, O.L.; Johl, S.K.; Ibrahim, M.Y. Holistic Approach to Corporate Governance: A Conceptual Framework. Global Business Management Research: An International Journal, vol. 6, No. 3, 2014.

20 Begg, C.; Caira, T. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation 2012, Vol. 15, pp 3–13.

21 Buffenoir, E.; Bourdon, I. Managing Extended Organizations and Data Governance. Advances in Intelligent Systems and Computing. 2013, Vol. 205, (pp 135–145), Springer, Berlin, Heildelberg.

Un primer esfuerzo para crear un marco de referencia de gobernanza de datos se publicó en 2007.[22], [23] Para lograr un gobierno de datos exitoso, las organizaciones requieren un marco estratégico que pueda ser fácil de implementar de acuerdo con las necesidades y los recursos de la información.[24], [25] Una buena información en el marco de la gobernanza también puede ayudar a las organizaciones a crear una misión clara, lograr transparencia, aumentar la confianza en el uso de los datos de la organización, establecer responsabilidades, mantener el alcance y el enfoque, así como definir éxitos medibles.[26] Para facilitar el gobierno de los datos, las organizaciones deben diseñar un modelo de gobierno de datos donde las responsabilidades de las funciones sirvan para identificar a las personas que tienen un nivel de responsabilidad para definir, producir y usar datos en la organización[27]. En líneas similares, se ha argumentado que las organizaciones deben obtener la responsabilidad de los datos del departamento de tecnologías de la información con la participación y el compromiso del personal de TI, la gestión empresarial y el patrocinio ejecutivo de alto nivel en la organización.[28] Los expertos en este campo hablan de que el caos no es tan obvio dentro de las organizaciones que no implementen la gobernanza de datos, pero los indicadores son elocuentes, y esas organizaciones conllevan datos sucios, redundantes e inconsistentes, incapacidad para integrarse, bajo rendimiento, escasa disponibilidad, poca responsabilidad, usuarios que están cada vez más insatisfechos con el

22 Wende, K., A Model for Data Governance - Organizing Accountabilities for Data Quality Management. In Proceedings of the 18th Australasian Conference on Information Systems; University of Southern Queensland: Toowoomba, Australia, 5-7 Dec 2007; pp. 417–425.

23 Poor, M. Applying Aspects of Data Governance from the Private Sector to Public Higher Education; University of Oregon: Eugene, OR, USA, July 2011.

24 Fu, X.; Wojak, A.; Neagu, D.; Ridley, M.; Kim, T. Data governance in predictive toxicology: A review. Journal of Cheminformatics. 2001, 3, 24.

25 Prasetyo, H.N.; Surendro, K., Designing a Data Governance Model Based on Soft System Methodology (SSM) in Organization. Journal of Theoretical and Applied Information Technology,10 August 2015, Vol. 78, pp. 46–52.

26 Panian, Z., Some Practical Experiences in Data Governance. World Academy of Science, Engineering and Technology, Vol. 62, 2010, pp. 939–946.

27 Seiner, R.S., Non-Invasive Data Governance. 1st ed.; Technics Publications: New York, NY, USA, 2014.

28 Russom, P., Data Governance Strategies: Helping Your Organization Comply, Transform, and Integrate; The Data Warehousing Institute: Los Angeles, CA, USA, 2008.
http://download.101com.com/pub/tdwi/Files/TDWI_BPR_DG_Q208.pdf

rendimiento de TI, y una sensación general de que las cosas están fuera de control.[29]

El cómputo en la nube es un desarrollo relativamente nuevo de la tecnología. El *National Institute of Standards and Technology* (NIST) de los Estados Unidos[30] definió al cómputo en la nube como "un modelo para permitir acceso a la red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios". El modelo de cómputo en la nube mejora la disponibilidad y se compone de cinco características esenciales, cuatro modelos de implementación y tres modelos de servicio.[31] Las características esenciales incluyen autoservicio bajo demanda, amplio acceso a la red, agrupación de recursos, elasticidad rápida y servicio medido.[32] Los modelos de implementación de la nube son el privado, el público, el híbrido y el comunitario.[33] Los modelos de prestación de servicios, son: Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como servicio (IaaS).[34] El cómputo en la nube ofrece beneficios potenciales para el público y organizaciones privadas al poner a

29 Kamioka, T.; Luo, X.; Tapanainen, T., An Empirical Investigation of Data Governance: The Role of Accountabilities. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, Summer 6-27-2016. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1028&context=pacis2016

30 Mell, P.; Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145; Gaithersburg, MD, USA, 2011.

31 Almarabeh, T.; Majdalawi, Y.K.; Mohammad, H., Cloud Computing of E-Government. Communications and Network, Scientific Research Publishing, 2016, 8, 1–8.

32 Kshetri, N., Cloud computing in developing economies. IEEE Computer 2010, No. 10, Vol. 43, pp. 47–55.

33 Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). Procedia Computer Science Vol. 110, 2017, pp. 378–385.

34 Bojanova, I.; Samba, A., Analysis of Cloud Computing Delivery Architecture Models. Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 453–458.

disposición los servicios de TI como un producto básico.[35],[36] En general, los beneficios del cómputo en la nube incluyen: eficiencia de costos, almacenamiento ilimitado, respaldo y recuperación, integración automática de software, fácil acceso a la información, implementación rápida, facilidad para ampliar servicios, y entrega de nuevos servicios;[37] incluye otros beneficios tales como utilización optimizada del servidor, ampliación dinámica y desarrollo del ciclo de vida minimizado de nuevas aplicaciones. Sin embargo, la nube aún no se ha adaptado como debiera a la informática debido a muchos factores, principalmente relacionados con el movimiento de la información administrado por un tercero, donde, además del consumidor y proveedor de la nube, hay otros actores: el auditor, el intermediario y el operador de la nube.[38] Por lo tanto, en la administración de los datos, la pérdida de control, seguridad y privacidad, calidad y seguridad, etc., son citados como preocupaciones reales al adoptar el modelo de cómputo en la nube.[39] El bloqueo de datos es otro riesgo potencial, donde los clientes de la nube pueden enfrentar dificultades para extraer sus datos.[40] Los consumidores de la nube pueden sufrir desafíos operacionales y regulatorios como el de la territorialidad a medida que las organizaciones transfieren sus datos a terceros para su almacenamiento y procesamiento.[41] Además, puede ser difícil para los

35 Forell, T.; Milojicic, D.; Talwar, V., Cloud Management: Challenges and Opportunities. Proceedings of the 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 16–20 May 2011; pp. 881–889.

36 Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science Vol.94, 2016, pp. 160–167.

37 Ko, R.K.L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S., TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.

38 Bumpus, W., US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft), NIST Special Publication 500-293, Gaithersburg, MD, USA, 2011.

39 Ramachandra, G.; Iftikhar, M.; Khan, F. A., A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science Vol. 110, 2017, pp. 465–472.

40 Opara-Martins, J. N., A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS Category) Migration; Bournemouth University: Poole, UK, 2017.

41 Jennings, B.; Stadler, R., Resource Management in Clouds: Survey and Research Challenges. Journal of Network and Systems Management, July 2015, Vol. 23, No. 3, pp. 567–619.

consumidores la verificación de mejores prácticas de manejo de datos del proveedor de la nube o cualquiera de los otros actores involucrados.[42], [43] El modelo de cómputo en la nube es una tecnología altamente emergente, de tal forma que la adopción de sus servicios requiere estrategias de gobernanza de datos aún más rigurosas y programas más complejos, pero necesarios.

El consenso general es que el gobierno de datos se refiere a la totalidad de la decisión de derechos y responsabilidades relacionados con la gestión de datos como activos en las organizaciones. Sin embargo, no proporciona la misma importancia para la gobernanza de datos dentro de la computación en el contexto tecnológico de la nube, por lo tanto, este déficit requiere una comprensión profunda de la gobernanza de datos y del cómputo en la nube. Esta tendencia, contribuye a los cambios en la estrategia de gobierno de datos en la organización, así como en la estructura y las regulaciones legales, las personas, la tecnología, los procesos, los roles, y responsabilidades Este es uno de los grandes desafíos que enfrentan las organizaciones hoy en día cuando ubican sus datos a entornos de cómputo en la nube, particularmente con respecto a cómo la tecnología de la nube afecta a la gobernanza de los datos. La observación general de los autores revela que el área de gobernanza de datos en general ha sido investigada poco y por lo general no se practica por las organizaciones, y mucho menos la nube informática, donde la investigación está en su infancia y aún lejos de alcanzar su madurez. En la figura 2, se muestran las interrelaciones entre los dominios de gobernanza de datos en la nube.

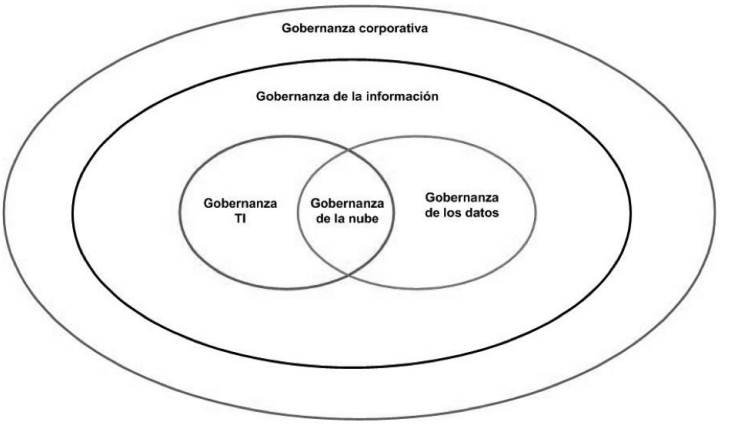
Pero la mayoría de los términos comúnmente utilizados, ya sean de gobierno, gestión o administración, describen

42 Rifaie, M.; Alhajj, R.; Ridley, M., Data Governance Strategy: A Key Issue in Building Enterprise Data Warehouse. Proceedings of the iiWAS '09, 11th International Conference on Information Integration and Web-Based Applications & Services, Kuala Lumpur, Malaysia, 14–16 December 2009; pp. 587–591.

43 Neela, K.L.; Kavitha, V., A Survey on Security Issues and Vulnerabilities on Cloud Computing. International Journal Computer Science & Engineering Technology, Vol 4, No. 7, 2013, pp. 855–860.

diferentes aspectos del mismo objetivo: utilizar datos para "gobernar" mejor la institución.[44]

Figura 2
Las interrelaciones entre los dominios de gobernanza en la nube[45]



En esencia, la gobernanza de datos implica implementar políticas y sistemas para garantizar que las personas tengan acceso a los datos que requieren para tomar decisiones sólidas y para llevar a la institución hacia el éxito. El gobierno de datos tiene esencialmente cuatro componentes básicos:

Propiedad de los datos. Al igual que en cualquier área de la vida, si no hay alguien explícitamente responsable de hacer que suceda algo, es probable que no lo haga. Las instituciones no pueden arriesgarse con los datos. La gobernanza implica asignar en la organización a las

44 Dvries, H., Data Governance. Ellucian, February, 15, 2018. Recuperado 25 de julio de 2018. https://www.ellucian.com/Insights/The-analytics-powered-campus/

45 Al-Ruithe, M., Benkhelifa, E. and Hameed, K., Data governance Taxonomy: Cloud versus Non-Cloud. Sustainability 2018, 10(1), 95. https://doi:10.3390/su10010095

personas adecuadas la responsabilidad de administrar, definir, interpretar y proteger los datos apropiados.

Acceso a los datos. Establecer reglas sobre la jerarquización de los datos, y luego implementar los sistemas para hacer cumplir esas reglas, es una de las metas angulares de la gobernanza. Sin reglas, se corre el riesgo de no cumplir con las regulaciones gubernamentales de privacidad; el personal no compartirá datos por temor a un uso incorrecto; y no estará disponible la información relevante que se necesita para desarrollar el trabajo.

Calidad de los datos. "Datos erróneos" es lo que las personas asocian más a menudo con la falta de gobierno. Esto se debe a que los datos no confiables, faltantes o inexactos tienen el impacto más visible en las operaciones diarias. La gobernanza implica la creación de procesos formales para la entrada cuidadosa de datos, así como la definición, codificación e interpretación de datos en forma consistente en la organización.

Seguridad de los datos. Obviamente hay un gran componente de TI para la seguridad de los datos, la forma en que los usuarios medios manejan los datos es muy importante. La gobernanza implica el establecimiento y la aplicación de reglas sobre cómo se pueden mostrar, compartir y eliminar los datos.

4. Seguridad en ambientes universitarios en México

4.1 Ciberdelincuentes buscan datos de los centros académicos

Las instituciones de educación superior son objetivos atractivos para los cibercriminales por las siguientes razones:

- Se maneja una amplia variedad de datos muy sensibles: las instituciones de educación superior poseen datos confidenciales sobre estudiantes, padres, ex-alumnos, profesores y personal. Los registros se retienen por lo común durante décadas. Por otro lado, los centros académicos, particularmente aquellos que involucran altos volúmenes de investigación, a menudo alojan datos

que pertenecen a una amplia gama de corporaciones y entidades gubernamentales; las instituciones vinculadas con hospitales locales y regionales, en general, almacenan datos médicos confidenciales.

- Se carece de una estructura centralizada: las instituciones tienden a albergar sus datos sensibles en diversas ubicaciones diferentes en lugar de uno centralizado. Los datos de los estudiantes se pueden guardar por separado en cada campus, dentro de una universidad o en diferentes ramas en un sistema universitario estatal. Los mismos datos se pueden guardar en una variedad de lugares, oficinas de exalumnos, administración central, o incluso a nivel departamental para programas de posgrado.
- Los datos sensibles relacionados con las subvenciones corporativas o gubernamentales pueden estar alojados en departamentos que reciben esas subvenciones o incluso en dispositivos individuales de profesores y estudiantes de posgrado que desempeñan funciones claves de investigación. Esta estructura descentralizada puede dar a los ciberdelincuentes diversas rutas para explotar vulnerabilidades en diferentes sistemas que alberguen datos confidenciales.
- Vulnerabilidades organizacionales: La naturaleza descentralizada del almacenamiento de datos en instituciones de educación superior se debe a menudo a cuestiones organizativas y estructurales. La responsabilidad de implementar las medidas de seguridad y determinar los procesos pueden recaer en diferentes instancias interesadas, en la amplia gama de departamentos universitarios. Las instituciones carecen por lo general de una estructura de mando vertical y eso hace que las nuevas medidas sean difíciles de implementar; por lo tanto, departamentos, profesores o estudiantes pueden tardar en adoptar las mejores prácticas necesarias para mejorar la seguridad.
- Uso generalizado de dispositivos personales: los administradores, el profesorado o la planta científica pueden desconocer en qué medida exponen a su institución a riesgos cibernéticos cuando

descargan en sus dispositivos datos confidenciales provenientes de personal menos protegido. Como resultado, incluso si una institución tiene medidas de seguridad sólidas, cualesquiera personas en la institución pueden, ya sea por descuido, de manera involuntaria, o por falta de conocimiento, exponer o propagar datos confidenciales.

En resumen, el gran volumen de datos potencialmente valiosos, almacenados en la mayoría de las instituciones de educación superior, tiende a convertirlas en objetivos altamente atractivos. Los ejemplos también ilustran que las vulnerabilidades de la seguridad cibernética son causadas por la combinación de elementos técnicos y humanos en un sistema. Los elementos técnicos pueden incluir vulnerabilidades de software que permitan el acceso no autorizado a través de programas particulares. Los usuarios legítimos pueden ser dirigidos por la ingeniería social que los alienta a tomar ciertas acciones o divulgar información que permitan a los atacantes acceder a los sistemas. El acceso remoto persistente también se puede lograr mediante el acceso físico no autorizado a redes, y por medios transportables o extraíbles como computadoras portátiles o dispositivos móviles.

El riesgo principal de las diferentes amenazas cibernéticas es la pérdida de la continuidad del trabajo de una institución, provocado por el robo de información o daño a las redes, es decir, imposibilitan a la universidad y a su comunidad hacer su trabajo. Las instituciones o los investigadores pueden perder acceso a datos esenciales, los datos pueden corromperse, la información puede ser robada, sin considerar los costos de impacto al proyecto o a la institución. Esto puede tener una serie de implicaciones, por ejemplo:

De prestigio. El robo de información y los problemas de integridad pueden dañar gravemente el prestigio de una universidad a los ojos de estudiantes, socios, empresas y gobiernos.
De tipo legal. El robo de información puede dejar en tal situación a las instituciones que infrinjan la legislación o los contratos vigentes y el riesgo de ser enjuiciados,

sancionados y el retiro de fondos de proyectos existentes y futuros.
De tipo económico. El robo de información puede directamente minar a la universidad o la capacidad del investigador para capitalizar el potencial de la propiedad intelectual o en la transferencia de conocimiento.
De tipo operacional. Puede haber daños inmediatos a las redes e infraestructura que dificulta las actividades de una institución y que da como resultado importantes costos de reparación.

Un enfoque institucional para la evaluación de riesgos tendrá que identificar y evaluar los activos de datos y sus riesgos. Un proceso de evaluación de riesgos debe tener en cuenta lo siguiente:

- ¿Qué información se considera crítica por la universidad?
- ¿Qué información puede ser de interés para fines delincuenciales, políticos o económicos?
- ¿Cómo y dónde se puede acceder la información en forma legítima e ilegítima?
- ¿Los controles y políticas que administran acceso y uso de datos son los adecuados?

Es esencial para este proceso de evaluación de riesgos estar integrado en la gobernanza de la información y la investigación para permitir decisiones de gestión de riesgos que permitan establecer un equilibrio apropiado entre:

- El riesgo de ciberseguridad, en donde se incluyen a la probabilidad, naturaleza e impacto potencial
- Prioridades de gestión de datos, incluidos acceso, usuarios y ciclo de vida de la publicación
- Los costos de implementación de controles, incluyendo los recursos y los costos indirectos

4.2 Equilibrio de seguridad cibernética con la apertura

La seguridad y la apertura se pueden abordar como dos temas en una misma administración de datos y proceso de evaluación de riesgos. La evaluación de riesgos efectiva deberá permitir que una universidad identifique el manejo

adecuado y seguro en todo el ciclo de vida de los diferentes tipos de información que son producidos y utilizados. El proceso debe incluir la evaluación de las prioridades de administración, riesgos de seguridad, controles de acceso apropiados y la forma de publicación e infraestructura de almacenamiento. Un enfoque integrado podría permitir a una institución abordar la seguridad cibernética y los datos abiertos, así como la transferencia de conocimiento, con confianza, en el conocimiento que los datos son apropiados para su reutilización por parte de terceros.

4.3 Implementación de seguridad cibernética en la gobernanza de la información

Las universidades deberían considerar quién en la institución 'tiene' o 'controla' los datos para establecer líneas claras de evaluación, rendición de cuentas y monitoreo entre la producción descentralizada y el uso de los datos de la institución que comparte los costos de las fallas de seguridad. Las instituciones universitarias deberán también realizar auditorías internas y externas de sus riesgos, prioridades de administración y sistemas. La identificación y la selección de controles de seguridad en ciertos tipos de datos sólo se pueden lograr con la participación activa de los controladores de datos. Estos grupos están en mejor posición para identificar activos, evaluar cuales tipos de controles serán los más apropiados e implementarlos en última instancia, así como para ser responsables de mantener la integridad de sistemas y datos. El equipo ejecutivo informa al rector, quién por lo general tiene acceso sin límite de los datos corporativos de la institución, aunque los datos también estarán en manos de las instancias académicas y tutores. En el caso de la investigación, los investigadores principales y decanos de las áreas de investigación pueden ser principalmente responsables de controlar los datos. Como resultado, es importante que desempeñen un papel central al decidir las vulnerabilidades de riesgo de una institución y la identificación y evaluación de activos de información.

La seguridad de la red académica es una responsabilidad de toda la institución. Los administradores de red pueden mantener el conocimiento actualizado de amenazas y

contramedidas a través del intercambio de información con compañeros y con agencias de gobierno. Sin embargo, son los usuarios quienes juegan roles cruciales para la seguridad de cualquier red y de la información. Los usuarios deben tener un papel central en la evaluación del riesgo que enfrenta la información, configuración de gestión y las prioridades de la seguridad, en última instancia, como usuarios, son responsables para la implementación de controles. Es esencial que los usuarios de la red, incluso aquellos usuarios que manejan activos más sensibles, sean conscientes de sus responsabilidades y actúen en consecuencia.

4.4 Gobernanza corporativa universitaria

Todas las instituciones de educación superior deben conocer sus responsabilidades con respecto a la protección de datos administrativos, personales y financieros y, por tanto, tener medidas apropiadas para garantizar que cumplan con la Ley de Protección de Datos del INAI. También deben tener diferentes estructuras para la administración de datos e investigación, y contar con los procedimientos apropiados de supervisión; es necesario que las instituciones y los investigadores desarrollen políticas y planes para la administración de datos, teniendo una supervisión corporativa adecuada. Estas características se presentan como desafíos a un gobierno corporativo para entender ambos problemas y los enfoques que se pueden emplear para ayudar a desarrollar la práctica de seguridad cibernética en la universidad. La figura 3 (página siguiente), muestra el proceso de administración de amenazas de seguridad cibernética en una universidad .

La seguridad cibernética corporativa universitaria efectiva debe tener en cuenta la estructura descentralizada de la administración de datos, considerando el riesgo de toda la institución que puede ser asociado con cualquier falla de gestión. La supervisión corporativa de los riesgos inevitablemente depende de la comunicación y la gestión por aquellos con responsabilidad para controlar los datos. Una función de supervisión puede ser integrada en procesos

de aprobación de investigación existentes; no obstante, estos pueden necesitar ser ajustados para tomar en cuenta los riesgos económicos potenciales, los requisitos éticos, legales y contractuales. Cuando se establece la política, el gobierno corporativo debe buscar respuestas claras a las siguientes preguntas:

- ¿Qué información tiene su universidad, que la ley, los donantes o socios consideren sensibles?
- ¿Quién posee o controla los datos dentro de la institución?
- ¿Cómo se deberían establecer las prioridades de administración para los datos?
- ¿Cuáles son los canales para monitorear y administrar los riesgos de seguridad?

Figura 3
Modelo de proceso para la gestión de amenazas de seguridad cibernética en instituciones de educación superior[46]

46 Universities UK, Cyber security and universities: managing the risk. 28 November 2013. Recuperado el 10 de septiembre de 2018. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

4.5 Recomendaciones para gobernanza corporativa

- Es importante valorar la implementación de un comité de gobernanza para mantener la supervisión institucional de la administración de datos y riesgos de la seguridad cibernética.
- Considere realizar una evaluación institucional de riesgos de ciberseguridad y gestión de prioridades de los datos de los activos existentes y nuevos.
- Asegurar de que existen canales claros de comunicación y reportes entre controladores de datos y la gobernanza de riesgos y la administración de prioridades.
- Valore la función de auditoría interna e independiente para evaluar el gobierno corporativo y la administración de la ciberseguridad incluidos más allá de las responsabilidades legales.

4.6 Administración de los datos de investigación

Medidas para mejorar la seguridad de los datos dentro de las áreas de investigación de las universidades, que deben trabajar con políticas de administración de datos en evolución y estructuras de apoyo. La política debe enfocarse a que los investigadores puedan administrar eficazmente los datos de investigación de forma tal que puedan ser presentados en repositorios de acceso abierto o tener controles de seguridad apropiados como la administración de prioridades de los datos que evolucionan.

Las universidades deben considerar auditorías de los datos para identificar los datos potencialmente sensibles y evaluar sus riesgos y prioridades de administración. Los objetivos para la auditoria deben hacerse explícitos a todos aquellos involucrados en la identificación y evaluación de riesgos, deben cubrir las consideraciones de seguridad tan amplias como sean posibles, las políticas de administración y prioridades de las mejores prácticas con el fin de apoyar a los investigadores en su trabajo. Los parámetros de cualquier auditoría deberían ser cuidadosamente definidos para asegurar que sólo se incluyen datos relevantes en el proceso. Debido a esto una auditoría puede considerar centrarse en la evaluación de una serie de conjuntos

de datos de investigación significativos y la naturaleza de las mejores prácticas de administración existentes, con una visión para informar una política y una práctica más integrales.

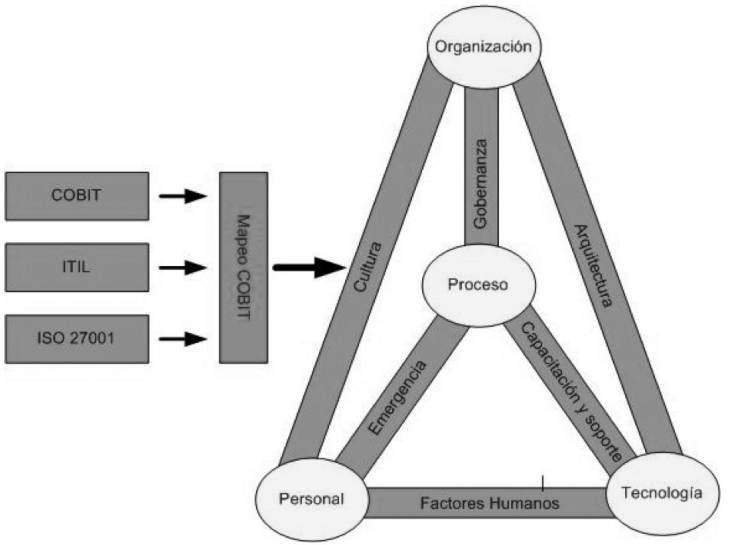
4.7 Recomendaciones para administrar la investigación

- Desarrollar una auditoría y evaluación de enfoque ligero bajo un marco de referencia para evaluar riesgos y administración de medidas a los datos existentes.
- Revisar los planes de manejo de datos como parte de una revisión ética e investigación en curso de procesos de gobierno, para evaluar el potencial de riesgos de seguridad y prioridades de gestión.
- Requerir que las consideraciones de seguridad sean incluidas en los planes de administración de los datos para todas las nuevas propuestas de investigación.

4.8 Modelo de madurez de seguridad de la información

El modelo de madurez de seguridad de la información (ISMM) está pensado como una herramienta para evaluar la capacidad de las organizaciones para cumplir los objetivos de seguridad: confidencialidad, integridad y disponibilidad a la vez que previene los ataques y logra la misión de la organización a pesar de los ataques e infracciones. El modelo define un proceso que administra, mide y controla todos los aspectos de la seguridad. Se basa en cuatro indicadores básicos para la evaluación comparativa y sirve como ayuda para comprender los requerimientos de seguridad de la universidad. Estos indicadores están orientados a la meta de alcanzar las necesidades de seguridad. Muchos de estos modelos son bastante detallados y cumplen los requisitos de seguridad con respecto a los requisitos tecnológicos, generalmente conduce a un programa de trabajo muy costoso para implementar la seguridad que se centra en la tecnología, pero no es orientado a los negocios. La figura 4 muestra la arquitectura del modelo de madurez de seguridad de la información.

Figura 4
Modelo de seguridad de la información[47]



Se han usado otros modelos, incluyendo la restricción del alcance para unidades administrativas individuales o dado su alcance en términos de los procesos de la administración universitaria. Un análisis del desarrollo del modelo de gobierno de TI se muestra en la Figura n para ilustrar los conceptos básicos de los enfoques teóricos.

Este modelo comienza con el modelo de Madurez COBIT 5 utilizando el proceso de control RACI (Responsable, Contable, Consultado e Informado). Una combinación del modelo de madurez de gobierno de TI, COBIT® 5, ISO 27001 e ITIL ® V3 alcanzando en el nivel de estándares y procesos dentro del marco de referencia más que a nivel de control objetivo. El proceso clave de ITIL ® V3 es para la gestión de cambios

47 Suwito M.H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. (2016) An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, Vol. 376. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-10-0557-2_69

y modelos de procesos de administración de liberación de aplicaciones mapeadas a ISO 27001 y luego presentado en un programa convencional de estructura de gestión EPM para la elaboración de informes y administración continua. Cada concepto de seguridad, construcción o tipo de dispositivo tiene una dimensión asociada con los cambios que se identifican en este modelo.

El objetivo de la seguridad de la información es proteger adecuadamente este activo y garantizar la continuidad de operación de la institución universitaria, reducir el daño a la universidad y mejorar el rendimiento de inversiones realizadas en la institución. Según lo definido por la norma ISO 27001, la seguridad se describe como preservación,[48] considerando los siguientes principios:

- Confidencialidad: Esto es para asegurar que la información es accesible solo para aquellos que están autorizados y tienen derecho a acceso
- Integridad: esto es para garantizar que la información sea precisa y ahora debe modificar y mantener de forma segura la exactitud e integridad de la información, así como los métodos de procesamiento
- Disponibilidad: esto es para asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

4.9 Combinación de estándares

A medida que un marco de referencia y diferentes estándares evolucionan, crean confusión, especialmente al usar uno de ellos. Al mirarlos más de cerca, es muy claro que se pueden alinear con éxito. Realizar el proceso de prestación de servicios informáticos sin definir realmente las medidas para monitorear el proceso, generará un mayor riesgo y sería menos eficiente. Este es uno de los argumentos para la combinación de COBIT® 5, ITIL ® V3 e ISO / IEC 27001. Por lo tanto, las mejores prácticas deben adaptarse a las necesidades de la universidad e integrarse entre sí con los procedimientos internos. COBIT® 5 se puede utilizar al

48 Daminda, P., ISO/IEC 27001, Information Security Management System, ISO 27001 Family, pp. 2-21 (2008). https://www.dnvgl.com/services/iso-iec-27001-information-security-management-system-3327

más alto nivel, proporcionando un marco de control general basado en el modelo de proceso de TI que debe adaptarse a cada organización en general. Prácticas y estándares específicos como ITIL ® V3 e ISO/IEC 27002 cubren áreas discretas que pueden ser mapeadas al marco de referencia de COBIT® 5, proporcionando una guía jerárquica de materiales de orientación.

Las instituciones de educación superior enfrentan retos que las hacen competir estratégicamente, como otras organizaciones sin fines de lucro. Para soportar este nuevo enfoque sus sistemas de información y estrategias comerciales deben estar totalmente alineados. El entorno actual de sistemas de información heterogéneos y aplicaciones implementadas en diversas instituciones puede comprometer tal objetivo. Para enfrentar estos retos han surgido las arquitecturas y modelos de referencia como instrumentos adecuados para auxiliar a los tomadores de decisiones de la universidad. Aunque muchos de estos modelos de software ya existen para diversas industrias, hasta ahora se ha hecho poco en la educación superior. Se han construido algunos desarrollos que pueden considerarse como un modelo de referencia de sistemas de información unificados específicamente para instituciones de educación superior.[49]

4.10 Caso de estudio

Se estableció la gobernanza de los datos en un centro de investigación, implementando una solución de seguridad en un laboratorio que es susceptible de ser visitado frecuentemente por *hackers* para intentar extraer información de su servidor principal de diseño. En algún momento, se tuvo un ataque de negación de servicios en una computadora personal de un integrante del laboratorio. Por lo anterior, se establecieron políticas de seguridad más radicales y se establecieron controles para la navegación *web*, así como perfiles de uso por usuario y por computadora.

49 Sánchez-Puchol F., Pastor-Collado J. A., Borrell B., Towards an Unified Information Systems Reference Model for Higher Education Institutions, Procedia Computer Science, Vol. 121, 2017, pp. 542-553. https://doi.org/10.1016/j.procs.2017.11.072.

La infraestructura de red de este laboratorio consta de un enrutador que administra los enlaces de red Ethernet de 1 Gb de ancho banda, un dispositivo de almacenamiento en red con 2 Tb de almacenamiento, una antena inalámbrica de 700 Mhz de ancho de banda, un servidor Blade Intel X64 de 1 Tb de almacenamiento y 8 Gb de RAM, dos impresoras en red y 12 estaciones personales Intel Windows X64. Se cuenta con las herramientas de diseño electrónico de tipo industrial, que permiten diseñar un circuito desde su modelado matemático hasta la generación de los archivos necesarios para su construcción en silicio. Desde cualquier computadora personal es posible acceder al servidor de diseño a través de un software de comunicación que permite tener el ambiente gráfico de las herramientas de diseño electrónico que se tienen en una estación de trabajo de alto desempeño.

Se implantó el software que establece la función de consola que vigila la red de prueba y realiza la función principal de administración del antivirus y del cortafuegos, además de parametrizar los perfiles de seguridad de cada grupo o usuario a vigilar de acuerdo a su jerarquía en la red. La consola interactúa con los sistemas operativos Windows, Mac OS y diversas versiones de Linux. Sin embargo, con el sistema Windows cualquier versión tiene mejor disponibilidad de funciones de monitoreo con respecto a los otros sistemas, inclusive es posible dar mantenimiento al registro y defragmentar el disco duro de cada computadora que tenga Windows, en forma remota. Las estaciones personales se monitorean a través de un agente que se instala en cada una de las computadoras y tiene acceso completo al equipo remoto. El dispositivo de almacenamiento en red tiene su propio sistema de seguridad. El uso de los recursos del laboratorio tiene que mantener la sencillez de siempre al utilizarlos.

La consola de monitoreo se apega a lo dispuesto por el ISO 27001, permite definir políticas de seguridad de acuerdo a los perfiles que se requieran. El posible detectar el polimorfismo de los archivos que se reciben en el correo electrónico, previene los ataques de negación de servicios; además, cada agente que reside en cada una de las computadoras tiene un detector de malware.

Se busca que se pueda generar una red de repositorios de almacenamiento en red que respalden en automático la información de cada computadora que esté conectada a la red, y que tengan políticas de seguridad que limiten el posible hurto de la información generada de las investigaciones en los distintos laboratorios de investigación de la institución.

Por el otro lado, se pretende integrar los dispositivos de almacenamiento masivo en red a través de protocolo LDAP, lo que permitirá unificar el acceso bajo una política de seguridad institucional; al igual que los dispositivos de IoT. Lo anterior es con el fin principal de que los dispositivos de almacenamiento masivo por edificio pueden garantizar que la información no sea robada o alterada, y en caso que se requiera compartir que sea bajo una política de seguridad.

La gobernanza de los datos que se implantó ha protegido los diseños tecnológicos y la propiedad intelectual de este laboratorio. Los usuarios se han apegado a las reglas implantadas para el uso de los recursos computacionales. Aun cuando se implantó una plataforma de bajo costo, los beneficios que se obtuvieron son de alto valor. Se evaluaron soluciones de mayor seguridad, pero por su alto costo y las restricciones del presupuesto no fue posible implantarlas.

Conclusiones

La seguridad informática es una componente esencial de la seguridad nacional. En el ambiente académico, la confidencialidad, la privacidad, la disponibilidad y la integridad de la información ha de preservarse y garantizarse, tanto la de tipo administrativo, como educativo, de desarrollo tecnológico y de investigación básica.

Los centros académicos por sus propias características de plena libertad y consciencia crítica han sido desde siempre blancos predilectos de ciberdelincuentes, los que han tenido éxitos de diverso tipo en sus ataques: ha habido ataques inocuos e infructuosos, algunos que significan incomodidades intrascendentes a la vida académica, pero ha habido también ataques exitosos, como el control de equipo, el robo de información, la suplantación de identidades ola tergiversación de resultados, con lo cual el prestigio institucional se ha visto fuertemente afectado.

Así pues, cada centro académico ha de poner especial atención en su política de seguridad informática. Hemos presentado esquemas convencionales de tipo organizativo que se han implantado en diversas universidades en el mundo, y que ciertamente nos atrevemos a recomendar para el medio universitario mexicano. La adopción de tales políticas la ilustramos con un caso de estudio propio de nuestro centro de investigación.

BIBLIOGRAFÍA

Aenugu, N.R., Butakov S., Zavarsky P., Aghili S. (2018) Security Perspective in Comparative Study of Platform-Based and Platform-Less BYOD Systems. In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017. Lecture Notes in Electrical Engineering, Vol. 450. Springer, Singapore.

Almarabeh, T.; Majdalawi, Y.K.; Mohammad, H., Cloud Computing of E-Government. Communications and Network, Scientific Research Publishing, 2016, 8, 1–8.

Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science Vol.94, 2016, pp. 160–167.

Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). Procedia Computer Science Vol. 110, 2017, pp. 378–385.

Al-Ruithe, M., Benkhelifa, E. and Hameed, K., Data governance Taxonomy: Cloud versus Non-Cloud. Sustainability 2018, 10(1), 95. https://doi:10.3390/su10010095

Begg, C.; Caira, T. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation 2012, Vol. 15, pp 3–13.

Bertino, E., and Islam, N., Botnet and Internet of Things Security. Computer, Vol. 50, Issue 2, Feb. 2017, pp. 76-79.

Bojanova, I.; Samba, A., Analysis of Cloud Computing Delivery Architecture Models. Proceedings of the 2011 IEEE Workshops of International Conference on Advanced In-

formation Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 453–458.
Bouk, J., Top BYOD Trends for 2018. 14 november 2017, Cass Telecom Systems. https://www.casstelecom.com/blog/top-byod-trends-for-2018
Buffenoir, E.; Bourdon, I. Managing Extended Organizations and Data Governance. Advances in Intelligent Systems and Computing. 2013, Vol. 205, (pp 135–145), Springer, Berlin, Heildelberg.
Bumpus, W., US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft), NIST Special Publication 500-293, Gaithersburg, MD, USA, 2011.
Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado, Octubre 2017. Recuperado el 26 de enero de 2019. https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html
CERT-MX, Mnemo-CERT, Scitum-CSIR and UNAM-CERT FIRST (2016). https://www.first.org/members/map#mexico
Daminda, P., ISO/IEC 27001, Information Security Management System, ISO 27001 Family, pp. 2-21 (2008). https://www.dnvgl.com/services/iso-iec-27001-information-security-management-system-3327
Dovey F. T., Clark C. and Lyn G. J., Elevating cybersecurity on the higher education leadership agenda: Increasing executive fluency and engagement in cyber risk. Deloitte Insights, February 2018. https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html
Dvries, H., Data Governance. Ellucian, February, 15, 2018. Recuperado 25 de julio de 2018. https://www.ellucian.com/Insights/The-analytics-powered-campus/
Forell, T.; Milojicic, D.; Talwar, V., Cloud Management: Challenges and Opportunities. Proceedings of the 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 16–20 May 2011; pp. 881–889.

Fu, X.; Wojak, A.; Neagu, D.; Ridley, M.; Kim, T. Data governance in predictive toxicology: A review. Journal of Cheminformatics. 2001, 3, 24.

Gobierno de México, Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI. Publicado en el Diario Oficial de la Federación de México, el 30 de Abril de 2014. Recuperado el 4 de octubre de 2018. http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

Gorman, A., and Sewell, A. (2015, July 12). Six people fired from Cedars-Sinai over patient privacy breaches. Los Angeles Times, July 12, 2013. http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713

Hinden, B., The Internet of Insecure Things. The Internet Protocol Journal, Volume 20, Number 1, March 2017.

Islas, J, Estudio Sobre Los Alcances del Derecho de Acceso a la Información en Universidades e Instituciones de Educación Superior Públicas Dotadas de Autonomía, Derivado de la Reforma Constitucional en Materia de Transparencia. INAI, Diciembre 2017. http://inicio.inai.org.mx/Estudios/AlcancesUniversidadesWeb.pdf

INEGI, Estadísticas a propósito del día mundial del Internet (17 de mayo). 15 de mayo de 2017. Recuperado el 7 de julio de 2018. http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. http://inicio.ifai.org.mx/SitePages/ifai.aspx

Jennings, B.; Stadler, R., Resource Management in Clouds: Survey and Research Challenges. Journal of Network and Systems Management, July 2015, Vol. 23, No. 3, pp. 567–619.

Kamioka, T.; Luo, X.; Tapanainen, T., An Empirical Investigation of Data Governance: The Role of Accountabilities. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, Summer 6-27-2016. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1028&context=pacis2016

Ko, R.K.L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S., TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.

Kravchenko, S. and Riley, M., The American Fugitive From the JPMorgan Hack Turns Up in a Russian Cell. https://www.bloomberg.com/news/articles/2016-10-10/jpmorgan-hack-fugitive-said-to-seek-u-s-deal-from-russian-cell

Kshetri, N., Cloud computing in developing economies. IEEE Computer 2010, No. 10, Vol. 43, pp. 47–55.

Lyn J. G., Understanding Information Security and Privacy in Postsecondary Education Data Systems. EDUCAUSE, May 2016. Recuperado el 22 de mayo de 2018. http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy-executive_summary.pdf

Mell, P.; Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145; Gaithersburg, MD, USA, 2011.

Neela, K.L.; Kavitha, V., A Survey on Security Issues and Vulnerabilities on Cloud Computing. International Journal Computer Science & Engineering Technology, Vol 4, No. 7, 2013, pp. 855–860.

Opara-Martins, J. N., A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS Category) Migration; Bournemouth University: Poole, UK, 2017.

Palo Alto Networks, Next Generation Security for Higher Education Institutions. 2017. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/higher-education-institutions-solution-brief

Panian, Z., Some Practical Experiences in Data Governance. World Academy of Science, Engineering and Technology, Vol. 62, 2010, pp. 939–946.

Parraguez K. L., The State of Cybersecurity un Mexico: An Overview, Wilson Center. Mexico Center, Woodrow Wilson Center. January 2017. Recuperado el 7 de julio de 2018. https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

Poor, M. Applying Aspects of Data Governance from the Private Sector to Public Higher Education; University of Oregon: Eugene, OR, USA, July 2011.

Prasetyo, H.N.; Surendro, K., Designing a Data Governance Model Based on Soft System Methodology (SSM) in Organization. Journal of Theoretical and Applied Information Technology,10 August 2015, Vol. 78, pp. 46–52.

Ramachandra, G.; Iftikhar, M.; Khan, F. A., A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science Vol. 110, 2017, pp. 465–472.

Rifaie, M.; Alhajj, R.; Ridley, M., Data Governance Strategy: A Key Issue in Building Enterprise Data Warehouse. Proceedings of the iiWAS '09, 11th International Conference on Information Integration and Web-Based Applications & Services, Kuala Lumpur, Malaysia, 14–16 December 2009; pp. 587–591.

Russom, P., Data Governance Strategies: Helping Your Organization Comply, Transform, and Integrate; The Data Warehousing Institute: Los Angeles, CA, USA, 2008. http://download.101com.com/pub/tdwi/Files/TDWI_BPR_DG_Q208.pdf

Salami, O.L.; Johl, S.K.; Ibrahim, M.Y. Holistic Approach to Corporate Governance: A Conceptual Framework. Global Bussiness Management Research: An International Journal, vol. 6, No. 3, 2014.

Sanchez-Puchol F., Pastor-Collado J. A., Borrell B., Towards an Unified Information Systems Reference Model for Higher Education Institutions, Procedia Computer Science, Vol. 121, 2017, pp. 542-553. https://doi.org/10.1016/j.procs.2017.11.072.

Seiner, R.S., Non-Invasive Data Governance. 1st ed.; Technics Publications: New York, NY, USA, 2014.

Suwito M.H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. (2016) An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, Vol. 376. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-10-0557-2_69

Universities UK, Cyber security and universities: managing the risk. 28 November 2013. Recuperado el 10 de septiembre de 2018. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

Weber, K.; Otto, B.; Osterle, H. One Size Does Not Fit All—A Contingency Approach to Data Governance. ACM Journal of Data Information Quality, Vol. 1 Issue 1 June 2009 Article No. 4.

Wende, K., A Model for Data Governance - Organizing Accountabilities for Data Quality Management. In Proceedings of the 18th Australasian Conference on Information Systems; University of Southern Queensland: Toowoomba, Australia, 5-7 Dec 2007; pp. 417–425.

Revista de Administración Pública

INAP

DNSChain y Namecoin: Una mirada a la revolución del DNS

Salvador Camacho Hernández

Resumen: Se analiza la implementación de una nueva infraestructura para soportar el Sistema de Nombres de Dominio (DNS) a través de una arquitectura basada en Blockchain y que se conoce como DNSChain o Namecoin, derivado del ciberataque ocurrido en 2016 en contra de Dyn. Asimismo, a manera de introducción se realiza una explicación sobre el funcionamiento del DNS, así como los tipos o clases de nombres de dominio que existen actualmente.

Palabras clave: Blockchain, DNSChain, Namecoin, Nombres de Dominio

DNSChain and Namecoin: A look at the DNS revolution

Abstract: The implementation of a new infrastructure to support the Domain Name System (DNS) is analyzed through a Blockchain-based architecture known as DNSChain or Namecoin, derived from the cyberattack that occurred in 2016 against Dyn. Also, as an introduction an explanation is made about the operation of the DNS, as well as the types or classes of domain names that currently exist.

Keywords: Blockchain, DNSChain, Namecoin, Domain Names

Fecha de recepción: 15 de enero de 2019
Fecha de aceptación: 28 de marzo de 2019

Revista de Administración Pública

INAP

DNSChain y Namecoin: Una mirada a la revolución del DNS

Salvador Camacho Hernández*

"Nada en el universo es capaz de resistirse al ardor convergente de un número bastante de inteligencias agrupadas y organizadas."
Pierre Teilhard de Chardin S.J.

1. Introducción

Internet es un fresno perenne: el árbol de la vida, o fresno del universo. Sus raíces y ramas mantienen unidos los diferentes mundos: ***Web comercial, Deep Web, Dark Web, Redes empresariales, Redes académicas, Redes gubernamentales, IoT*** (*Internet of Things*), ***Apps*** *(*Programas *Application)* y ***Cloud.*** De su ***DNS*** (*Sistema de Nombres de Dominio)* emana la fuente que llena el pozo del

* Licenciado en Derecho por la UNAM, Especialización en Propiedad Intelectual en esta misma Universidad. Está en proceso de titulación de la Maestría en Derecho de las Tecnologías de la Información y Comunicación. Forma parte del Grupo de Trabajo de ICANN que revisará las políticas relativas a conflictos de nombres de dominio y propiedad intelectual a nivel internacional.
Es Presidente de los Comités de Nombres de Dominio y Esports de la Academia Mexicana de Derecho Informático (AMDI) y miembro activo de la Asociación Mexicana para la Protección de la Propiedad Intelectual (AMPPI), del Capítulo México y del Observatorio de la Juventud de la Internet Society (ISOC), así como de la Red Académica de Videojuegos MX y de la Esports Bar Association de Estados Unidos de América (EBA). Asimismo, ha sido invitado a diversos foros de Gobernanza de Internet y Nombres de dominio en Estados Unidos, Asia, Europa y Latinoamérica.

conocimiento, custodiado por ***ICANN*** *(Internet Corporation for Assigned Names and Numbers).*

A los pies del árbol se encuentra el dios ***Akamai,*** que es el encargado de protegerlo de los ataques del dragón ***DDoS*** *(ataque de denegación de servicio)* y de una multitud de gusanos que tratan de corroer sus raíces y derrocar a los dioses a los que este representa.

Pero también cuenta con la ayuda de ***Google*** que lo cuida regándolo con las aguas del pozo de ***Big Data***. Un puente une ***Internet*** con la morada de los dioses, el ***TCP/IP*** *(Transmission Control Protocol/Internet Protocol*), el arco iris, todos los dioses cruzan por él para entrar en ***Conexión***.

Desde la noche de los tiempos, el ser humano ha necesitado de la mitología para intentar explicar su existencia y su conexión con la realidad. Incluso en la actualidad, época en la que aparentemente estamos más desconectados del mundo antiguo debido a los avances tecnológicos, encontramos que la mitología antigua sigue estando vigente como una manera de explicar los fenómenos.

A continuación, transcribiremos el fragmento de un antiguo mito nórdico, sobre el cual realizamos adecuaciones para crear una mitología de Internet en los primeros tres párrafos de esta lectura, donde únicamente sustituimos los nombres de los dioses y las representaciones sagradas escandinavas por los nombres de tecnologías actuales:

> ***"Yggdrasill*** *es un fresno perenne: el árbol de la vida, o fresno del universo. Sus raíces y ramas mantienen unidos los diferentes mundos:* ***Asgard, Midgard, Helheim, Niflheim, Muspellheim, Svartalfheim, Alfheim, Vanaheim y Jötunheim****. De su* ***raíz*** *emana la fuente que llena el pozo del conocimiento, custodiado por* ***Mímir****.*
>
> *A los pies del árbol se encuentra el dios* ***Heimdall*** *que es el encargado de protegerlo de los ataques del dragón* ***Níðhöggr*** *y de una multitud de gusanos que tratan de corroer sus raíces y derrocar a los dioses a los que éste representa.*

> *Pero también cuenta con la ayuda de las **nornas** que lo cuidan regándolo con las aguas del pozo de **Urd**. Un puente une el **Yggdrasill** con la morada de los dioses, el **Bifröst**, el arco iris, todos los dioses cruzan por él para entrar en el **Midgard**."* [1]

Ahora que hemos concluido nuestro experimento de mitología tecnológica, el presente documento realizará un breve pero conciso estudio y acercamiento a *Blockchain*, sobre el cual funciona Bitcoin, pero acotaremos la información a un uso de esta herramienta que tiene un par de años en desarrollo y que promete revolucionar el *Sistema de Nombres de Dominio (DNS)* como lo conocemos. Nos referimos a ***DNSChain* y *Namecoin*.**

2. Breve historia y funcionamiento del DNS

Hace casi cinco décadas que Internet fue inventado para revolucionar nuestra forma de comunicarnos y compartir información; empezando como un proyecto militar, desarrollándose hacia una investigación académica, evolucionando como una herramienta comercial y transformándose en una nueva forma de experimentar nuestra existencia humana.

Es en el año de 1983 cuando Paul V. Mockapetris propone la arquitectura del Sistema de Nombres de Dominio o *DNS*, por sus siglas en inglés, en los RFC[2] 882[3] y 883[4], y se le considera el padre de este sistema junto con Jonathan Bruce Postel. El DNS, de acuerdo al chileno Humberto Rolando Carrasco Blanc es "*un sistema mnemotécnico que permite la asignación y el uso de un nombre unívoco para*

1 GRANT, JOHN *Los vikingos, cultura y mitología*, Ed. TASCHEN BENEDIKT, Alemania, 2008.

2 Los RFC, del inglés "Request for Comments", son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general. El primero fue escrito por Stephen D. Crocker y fue quien acuñó el término.

3 http://tools.ietf.org/html/rfc882 Fecha de consulta: 31 de enero de 2019.

4 http://tools.ietf.org/html/rfc883 Fecha de consulta: 31 de enero de 2019.

cada computadora que se encuentre conectada a Internet"[5]. Debemos destacar que el DNS opera de forma jerárquica y es administrado por la *Internet Corporation for Assigned Names and Numbers*, *ICANN* por sus siglas en inglés, y es la entidad a nivel internacional que resguarda el *Root Zone.*

Cada equipo conectado a Internet tiene asignada una dirección IP, la cual es el número único identificador del dispositivo en la red. Para que el acceso a un sitio web sea más fácil y rápido se crearon los nombres de dominio, direcciones consistentes en caracteres alfanuméricos, bajo los cuales están las direcciones IP, por ejemplo, el nombre de dominio **google.com** está relacionado con la IP **216.58.194.110.**

La función principal del DNS es facilitar a los usuarios la navegación en Internet, como una especie de brújula o directorio digital, siendo de gran utilidad debido a que permite encontrar de manera ágil y dinámica el contenido. De tal forma que, en palabras del español Fernando Carbajo Cascón, "*el DNS constituye el sustento principal, la columna vertebral de la red de redes Internet"* [6].

3. Generalidades de los Nombres de Dominio

3.1 Definición

Al respecto existe una gran variedad de definiciones, debido a que es un tema que ha ido creciendo cada día de manera acelerada al tratarse de un elemento fundamental de Internet, por lo que el concepto que en un inicio se estableció se ha tomado como base para crear nuevas definiciones y conceptos que se encuentren más acordes a nuestra actualidad. A continuación, mencionaremos las definiciones más acuñadas y que dan más luz para

5 HUMBERTO ROLANDO, CARRASCO BLANC, *Consideraciones sobre el conflicto entre los nombres de dominio y los signos distintivos en Chile. Algunos casos prácticos*, Derecho Informático Volumen II, Ed. Juris, Chile, 2001. Artículo recuperado en archive.org y que puede ser consultado en el siguiente enlace: https://web.archive.org/web/20120119034802/http://www.dominiuris.com/congreso/congreso1/carrasco.htm Fecha de consulta: 31 de diciembre de 2018.

6 FERNANDO, CARBAJO CASCÓN, *Conflictos entre signos distintivos y nombres de dominio en Internet*, Segunda edición, Ed. Aranzadi, España, 2002.

entender que es un nombre de dominio desde el punto de vista funcional, pasando por el técnico y llegando al jurídico.

La Organización Mundial de la Propiedad Intelectual en su informe del Comité Permanente sobre el Derecho de Marcas, Dibujos, Modelos Industriales e indicaciones Geográficas, en su recomendación conjunta relativa a las disposiciones sobre protección de marcas notoriamente conocidas, de noviembre del año de 1999, definió al nombre de dominio de la siguiente manera: *"Una serie alfanumérica que corresponda a una dirección numérica en Internet".*[7]

El chileno Humberto Rolando Carrasco Blanc define al nombre de dominio como *"una expresión mnemotécnica, dirección alfa numérica utilizada en el sistema de nombres de dominio y que permite la comunicación entre los distintos computadores interconectados a Internet".*[8]

La definición que nos otorga el peruano Erick Américo Iriarte Ahon, quien lo define de la siguiente manera: *"Un nombre de dominio, es un identificador basado en caracteres alfanuméricos destinado a facilitar la recordación de una máquina conectada a la Red. Su naturaleza es un derecho de uso sui géneris, pudiendo configurarse como una posesión y eventualmente, estaríamos frente a un derecho de propiedad al nombre de dominio".*[9]

Asimismo, el chileno Andrés Echeverría Bunster define de una manera muy particular el nombre de dominio: "*El nombre de dominio sería una creación intelectual del*

7 Organización Mundial de la Propiedad Intelectual, Recomendación conjunta relativa a las disposiciones sobre protección de marcas notoriamente conocidas, 7 de octubre de 1999, http://www.wipo.int/edocs/mdocs/sct/es/sct_3/sct_3_8.pdf Fecha de consulta: 11 de enero de 2019.

8 HUMBERTO ROLANDO, CARRASCO BLANC, *Consideraciones sobre el conflicto entre los nombres de dominio y los signos distintivos en Chile. Algunos casos prácticos*, Derecho Informático Volumen II, Ed. Juris, Chile, 2001. Artículo recuperado en archive.org y que puede ser consultado en el siguiente enlace: https://web.archive.org/web/20120119034802/http://www.dominiuris.com/congreso/congreso1/carrasco.htm Fecha de consulta: 01 de febrero de 2019.

9 ERICK AMÉRICO, IRIARTE AHON, *Dándole Nombres al Internet. Sobre Nombres de Dominio.* Artículo recuperado en archive.org y que puede ser consultado en el siguiente enlace: https://web.archive.org/web/20060718214032/http://www.ieid.org/congreso/ponencias/Iriarte%20Ahon,%20Erick%201.pdf Fecha de consulta: 29 de enero de 2019.

titular sobre la cual éste tendría un derecho de propiedad intelectual".[10]

Aunque parezca que existe una fuerte similitud entre el nombre de dominio y la marca, debemos mencionar que no se puede considerar al nombre de dominio como una marca, debido a que el nombre de dominio no atiende a los dos principios básicos de una marca, tales como lo son la Territorialidad y la Especialidad, aunado a que se trata de un recurso crítico de Internet.

Asimismo, complementamos la idea anterior con el documento RFC 1591, emitido por IANA[11] en marzo del año de 1994, en el cual se define que los nombres de dominio no pueden ser considerados como marcas, estableciéndolo de la siguiente manera: *"El registro de un nombre de dominio no tiene el estatus de una marca. Le corresponde al solicitante asegurarse de no violar la marca de un tercero".*[12]

3.2 Clases de Dominios

Teniendo una noción clara de que es un nombre de dominio, procederemos a explicar y detallar las clases en las que se dividen los dominios.

Existen dos tipos distintos de niveles, los dominios de "primer nivel" o TLDs, el cual tiene cuatro variantes: gTLDs, ccTLDs, IDNs y nuevos gTLDs, y por otro lado tenemos a los dominios de "segundo nivel", los cuales se conforman por la denominación que distinguirá al nombre de dominio.

A manera de ejemplo utilizaremos el nombre de dominio **www.unam.mx**, el cual contiene tres niveles, leyendo de derecha a izquierda de la siguiente manera: primeramente tendremos el dominio de primer nivel, que en este caso es un dominio geográfico de país "**.mx**"; como dominio de nivel secundario tenemos el término "**unam.**" que es la parte

10 ANDRÉS, ECHEVERRÍA BUNSTER, *Uso de marcas y nombres de dominio*, en Derechos Intelectuales, Tomo 9, Colección Derechos Intelectuales, Ed. Astrea, Argentina, 2001.

11 Internet Assigned Numbers Authority.

12 JON, POSTEL, *RFC 1591: Estructura y Delegación del Sistema de Nombres de Dominio*, marzo de 1994, http://www.rfc-es.org/rfc/rfc1591-es.txt. Fecha de consulta: 15 de enero de 2019.

identificadora; como dominio de tercer nivel encontramos "**www.**", que indica el lugar de Internet en el cual se realiza la búsqueda.

3.2.1 Dominios de Primer Nivel (TLDs)

Los dominios de Primer Nivel o TLD[13], por sus siglas en inglés, son una parte básica de la estructura del nombre de dominio, ya que son indispensables para el funcionamiento del Sistema de Nombres de Dominio, mejor conocido como DNS.

Los TLDs iniciales fueron especificados por Jonathan Bruce Postel y J. Reynolds en el RFC 920[14], publicado en Octubre de 1984, en el cual se definieron los dos tipos principales de TLDs, los cuales serían conocidos tiempo después como Dominios de nivel superior o genéricos (gTLDs) y los Dominios de códigos de países o nacionales (ccTLDs).

En el año de 2009, en la junta anual de ICANN[15] realizada en Corea del Sur, se discutió y aprobó la introducción de los nombres de dominio internacionalizados (IDNs)[16], los cuales permiten el uso de alfabetos diferentes a los alfabetos "latinos" en el registro de nombres de dominio[17], con la finalidad de tener un Internet más inclusivo.

3.2.1.1. Dominios de nivel superior genéricos (gTLD)

Los llamados dominios de nivel superior genéricos (gTLD)[18] surgieron en la década de 1980 y se crearon con la finalidad de poder definir e indicar los usos que tendrían los dominios que se registraran con esta terminación y su regulación se encuentra a cargo de ICANN.

13 Top Level Domain.
14 JON, POSTEL, y J., REYNOLDS, *RFC 920: Domain Requirements*, https://tools.ietf.org/rfc/rfc920.txt, octubre de 1984. Fecha de consulta: 15 de enero de 2019.
15 Internet Corporation for Assigned Names and Numbers.
16 Internationalized Domain Names.
17 http://www.icann.org/en/resources/idn/fast-track/string-evaluation-completion Fecha de consulta: 18 de enero de 2019.
18 Generic Top-level Domains.

La definición que nos otorga ICANN sobre un gTLD es la siguiente: *"La mayoría de los TLDs con 3 o más caracteres se conocen como TLDs genéricos o "gTLDs". Pueden ser subdivididos en dos clases, los TLDs "patrocinados" (sTLDs) y los TLDs no patrocinados (uTLDs)".*[19] En el año de 1994 se listaron los siete gTLDs iniciales y sus usos previstos, los cuales son los siguientes: .COM, .ORG, .EDU, .GOV, .INT, .MIL y .NET.

En el mes de Julio del año 1999, ICANN a través de la DNSO[20] estableció un grupo de trabajo denominado como "Grupo C de trabajo", el cual fue el encargado de introducir nuevos gTLDs, pero de manera limitada, por lo que el 14 de Noviembre del año 2000, se aprobaron 7 nuevos gTLDs de entre 44 propuestas[21] y fueron implantados durante los años 2001 y 2002, y fueron los siguientes: .BIZ, .INFO, .NAME, .PRO, .AERO. COOP y .MUSEUM. Posteriormente en el año de 2006 se introdujeron los siguientes gTLDs: .ASIA, .CAT, .JOBS, .MOBI, .POST, .TEL, .TRAVEL y hasta el año de 2011 se aprobó el .XXX para sitios con contenido para entretenimiento de adultos.

3.2.1.2 Dominios de nivel superior de códigos de país (ccTLD)

Los dominios de nivel superior de códigos de país o geográficos (ccTLD)[22] son códigos de dos letras, tales como .UK, .MX o .ES, entre otros, y corresponden a un país, territorio económico u otra ubicación geográfica y se encuentran basados en la Tabla ISO 3166-1 alpha 2[23] creada por la Organización Internacional de Normalización (ISO). Surgen del interés que generó la colaboración internacional del proyecto de enlazar las redes y entre la

19 *Internet Corporation for Assigned Names and Numbers Glossary Letter G* https://www.icann.org/resources/pages/glossary-2014-02-03-en#g Fecha de consulta: 20 de marzo de 2019.

20 Domain Name Supporting Organisation u Organización de Apoyo a los Nombres de Dominio.

21 *ICANN Yokohama Meeting Topic: Introduction of New Top-Level Domains*, documento que puede ser consultado en el siguiente enlace: http://archive.icann.org/en/meetings/yokohama/new-tld-topic.htm Fecha de consulta: 18 de marzo de 2019.

22 Country Code Top-level Domain.

23 http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm Fecha de consulta 20 de marzo de 2019.

comunidad internacional se planteó la necesidad de crear TLDs que atendieran aspectos geográficos.

El primer ccTLD se creó en el año de 1985 y fue .UK, el cual se asoció con el Reino Unido, en América Latina el primer país en tener un ccTLD fue Argentina en el año de 1987 y nuestro país obtuvo .MX en el año de 1989. México también forma parte de los países fundadores de la ccNSO[24] que es la organización encargada de apoyar en materia de códigos geográficos a ICANN.

En la actualidad existen 293 ccTLDs. Se encuentran ligados a una entidad administradora, generalmente conocida como NIC[25], que es plenamente soberana pero que tiene una relación contractual con ICANN, y son las organizaciones encargadas de desarrollar políticas propias de delegación, las cuales tendrán que considerar el RFC 1591 y concordar con las establecidas por ICANN.

3.2.1.3 Dominios de nuevas extensiones (nuevos gTLDs)

En el año 2011 se generó un hito en la historia de Internet, debido a que se llevó a cabo una reunión de ICANN, que tuvo lugar del 19 al 24 de junio de ese año en Singapur, planteando uno de los mayores cambios en el Sistema de Nombres de Dominio. Se gestionó a través de ICANN, la creación de nuevas extensiones de nombres de dominio de nivel superior (gTLD). Estas extensiones, atienden a que el usuario se acostumbre a refinar los términos de su búsqueda, logrando una mayor especialización que los denominados Dominios Legado o de Primera Generación como .COM, .INFO, .NET, .ORG, entre otros.

Lo anterior, permitió que dichas extensiones puedan contener cualquier palabra en cualquier idioma, ya sea el nombre de una empresa, ciudad, persona; abriendo un mundo de nuevas posibilidades, lo cual podría cambiar en un futuro la forma de buscar información en Internet.

A finales del año 2012 ICANN publicó la lista con las solicitudes recibidas de nuevos gTLD que alcanzaron la cifra

24 Country Code Names Supporting Organization.
25 Network Information Center.

de 1,930, con un enfoque mayor en la especialización del mercado por sector específico: Negocios, entretenimiento, servicios, ciudades, etc. Algunos ejemplos de las extensiones que fueron aceptadas por ICANN tras cumplir los requisitos solicitados son los siguientes: .REST, .BAR, .TOP, .NIKE, .CLUB, .VEGAS, .NYC, .XYZ, .BLOG, .GURU, .PHOTO, .MOVIE, .DIGITAL; y alrededor de 1,200 que ya han sido delegadas.

En 1968 el escritor francés Jacques Bergier, redactó algunas predicciones sobre el futuro de las telecomunicaciones en su libro llamado "El Planeta de las Posibilidades Imposibles". En este sentido, podemos decir que el programa de nuevos gTLDs, se asemeja mucho al título de aquel libro, ya que cambiará la forma en la que conocemos, entendemos y utilizamos Internet, otorgándonos amplias posibilidades, las cuales serán limitadas únicamente por la imaginación. De igual manera, esta nueva era en los nombres de dominio también se asemeja al cambio radical que impuso la invención de la televisión a color.

Al respecto citaremos a Rod Beckstrom, expresidente y exdirector ejecutivo de ICANN quien declaró lo siguiente:

> "ICANN ha abierto el sistema de direcciones de Internet a las ilimitadas posibilidades de la imaginación humana. Esta decisión respeta los derechos de cualquier grupo para crear dominios de primer nivel en cualquier lengua y escritura. Esperamos que esto permita que el sistema de nombres de dominio sirva para mejorar a toda la humanidad".[26]

Actualmente, se encuentra en revisión por parte de ICANN la implementación de estas nuevas extensiones, con miras a abrir una segunda ronda de aplicaciones de solicitud de nuevos gTLDs en los próximos años.

26 *El regulador de nombres de Internet da luz verde al uso de cualquier palabra en los dominios,* Periódico El Mundo, Publicado el 20 de junio de 2011. Artículo que puede ser consultado en el siguiente enlace: http://www.elmundo.es/elmundo/2011/06/20/navegante/1308550917.html Fecha de consulta: 21 de febrero de 2019.

4. El Ciberataque a Dyn

La mañana del 21 de octubre de 2016, supuso un duro golpe para la infraestructura de Internet, ya que a través de un *DDoS*[27], utilizando dispositivos *IoT* infectados, se llevó a cabo un ataque a los servidores de la empresa *Dyn*, proveedora de servicios de DNS, dejando al mundo entero prácticamente sin Internet por unas cuantas horas, lo que generó millones de dólares en pérdidas y desesperación de los más asiduos por no poder conectarse.

Si bien este ataque no afectó toda la infraestructura de la red, el hecho de que *Dyn* fuera el blanco de esta agresión digital, representó que sus clientes fueran afectados, los cuales tienen la mayor parte de usuarios y tráfico por los servicios que otorgan. Entre la lista de afectados se encontraban empresas como AirBnb, Amazon, BBC, Etsy, GitHub, HostGator, Netflix, PayPal, PlayStation Network, Reddit, Shopify, Slack, Spotify, Twitter, Visa, Xbox Live, entre muchos otros.

El problema fue resuelto el mismo día por la tarde. Sin embargo, generó muchas dudas acerca de la estabilidad del DNS para operar ante situaciones similares o aún peores que implicaran una verdadera caída de todo el sistema.

5. ¿Qué son DNSChain y Namecoin?

La notoria vulnerabilidad del DNS demostrada con el ataque a los servidores de *Dyn*, logró posicionar de nueva cuenta en las discusiones a nivel internacional, el uso de un nuevo sistema o la evolución del mismo. Dicha situación, desde el año 2010, en diversos foros de Bitcoin se empezó a discutir la posibilidad de utilizar esta tecnología para crear una alternativa al DNS administrado por ICANN e incluso el mismo *Aaron Swartz* soñaba con implementarlo.

27 Un ataque de denegación de servicio, también llamado DDoS (por sus siglas en inglés), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
Fecha de consulta: 7 de febrero de 2019.

Blockchain, funciona como una base de datos distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado, contando con aspectos como almacenamiento de datos, transmisión de datos y confirmación de datos[28], lo que genera gran seguridad porque la cadena no permite añadir información que no cumpla con los estándares requeridos.

DNSChain opera bajo la tecnología proveída por Blockchain para crear un sistema que se caracterice por ser un DNS incensurable, inmodificable, seguro y resistente a ataques. La diferencia principal entre el DNS tradicional y *DNSChain,* se encuentra en que en este último la información está descentralizada, lo que teóricamente permite que se puedan evitar sucesos como el del 21 de octubre de 2016.

Namecoin es la aplicación funcional de la teoría detrás de *DNSChain.* Es la primera criptomoneda alterna a Bitcoin, que actúa como un DNS descentralizado funcional diferente al que administra ICANN, permitiendo que se puedan registrar nombres de dominio en Blockchain, siempre que cumplan con los estándares solicitados por la cadena. Su símbolo es el siguiente: N.

Sobre este nuevo DNS, se creó la extensión *top-level domain* .BIT, que sustituye el dominio legado .COM y que otorga una amplia libertad, ya que no se puede censurar. Recordemos que la creación de nuevas extensiones y aprobación de las mismas, corre a cargo de ICANN, situación que con .BIT no sucedió, lo que podría poner en duda la funcionalidad de dicha extensión. En este ámbito de nuevos DNS, también se encuentra **Blockstack**, con lo que se empieza a expandir Internet no sólo a nuevos nombres de dominio, sino a diferentes DNS.

6. Beneficios de la implantación de Namecoin

De acuerdo con quienes están detrás del uso y la aplicación de Blockchain como DNS y en el caso específico de Namecoin,

28 https://es.wikipedia.org/wiki/Cadena_de_bloques Fecha de consulta: 10 de febrero de 2019.

este sistema desafía el Triángulo de Zooko[29], ya que cumple con los tres rasgos deseables de dicho diagrama; además de que funciona bajo los mismos principios de Bitcoin: *Peer-to-peer*, tarifas bajas, global, seguro e ilimitado[30].

Además de lograr lo anterior, se proclaman valores añadidos como los siguientes[31]:

- Incensurable: La cadena de bloques no permite eliminar el contenido una vez que éste ha sido añadido a la cadena.
- Seguro: Al funcionar bajo los mismos principios que Bitcoin, es prácticamente imposible que puedan robar un nombre de dominio o atacar un sitio web.
- Privado: Al no generar tráfico en la red cuando se visita un sitio, terceros no pueden conocer la información que has consultado para deducir los siguientes sitios que visitarás.
- Rápido: La información del DNS se replica en un promedio de 40 minutos y ver sitios web toma menos de 3 milisegundos
- Gratuito: Al tratarse de un software *open source*, no tiene costo y es auditable por cualquiera, lo que resuelve los tiempos de resolución de incidencias.

Conclusiones

Sin duda alguna, las nuevas herramientas que hemos descrito y que buscan evolucionar el funcionamiento del DNS actual, están logrando que nuestra concepción del sistema cambie de forma sustancial. Hasta hace apenas algunos años, no se conocían las posibilidades de poder utilizar nombres de dominio con diferentes terminaciones a las tradicionales y vigentes por años, situación que ha cambiado, aunque sin tanto éxito inicial como fue previsto, pero que se espera que en algunos años puedan repuntar en registro y uso por parte de los consumidores tradicionales.

29 El Triángulo de Zooko define tres rasgos deseables en un identificador de protocolo de red como los siguientes: Significativo para humanos, Descentralizado y Seguro.
https://en.wikipedia.org/wiki/Zooko's_triangle Fecha de consulta: 11 de febrero de 2019.

30 https://youtu.be/NCxJ-k0A8xY Fecha de consulta: 12 de marzo de 2019.

31 https://bit.namecoin.org/ Fecha de consulta: 12 de marzo de 2019.

De igual manera, hace algunos años únicamente teníamos la capacidad de concebir un único DNS administrado por ICANN, ahora las posibilidades se abren para poder entender Internet no sólo como un símil del Universo, sino que nos lleva a la realidad donde múltiples universos coexisten. Asimismo, es interesante la manera de funcionar de Blockchain en la que imita a la naturaleza atómica o biológica, aceptando únicamente los bloques que cumplen con los estándares requeridos.

Además, consideramos que si bien se trata de un importante avance en el desarrollo del DNS para poder subsistir a ataques que busquen evitar que los usuarios accedan a la información que necesitan; también implica interesantes problemas legales desde el punto de vista de los nombres de dominio, como la imposibilidad de recuperar un nombre de dominio de una marca en la extensión .BIT ya que no se encuentra dentro del listado de dominios que se pueden rescatar legalmente a través de procedimientos como el UDRP que funciona para la mayoría de las extensiones de dominio.

Decidimos ahondar en el tema de Nombres de Dominio y del DNS, en la medida de que es un tema que muchas veces se ha dejado de lado en foros o eventos de ciberseguridad por considerarse algo "muy básico" y "sin mayor problema técnico". Sin embargo, debemos recalcar que gran parte de las medidas básicas de ciberseguridad, muchas veces recaen en las medidas más simples como lo es un buen control y manejo de los nombres de dominio, así como una educación digital básica al usuario respecto de las diversas vulnerabilidades que existen en Internet al teclear o buscar dominios.

Como bien se conoce, esta educación digital básica para el usuario promedio es fundamental para poder mitigar vulneraciones de cualquier tipo. Sin embargo, pocas son las organizaciones, tanto privadas como públicas, que se preocupan en capacitar a los usuarios, por lo que hasta en tanto eso no se corrija, la principal vulnerabilidad en materia de ciberseguridad seguirá sucediendo a través de la Capa 8.

La implementación de Blockchain para crear un nuevo DNS pudiera, para los más puristas, amenazar la misma

existencia de ICANN debido a que al no tener la necesidad de administrar el sistema, la permanencia de esta institución carecería de sentido. Esto ha generado diversas discusiones al interior de ICANN, mismas que el autor ha hecho públicas en los Foros Públicos de dicha organización, donde la respuesta siempre ha sido la misma: "En el momento que se tenga que migrar a una nueva tecnología, se hará".

Asimismo, consideramos que un DNS no elimina al otro, ya que en la medida en la que sean utilizados, pudieran coexistir en la misma esfera para distintos usos. Sin embargo, esto acarrea una posible fragmentación del DNS como lo conocemos, lo que sin duda implicaría una revolución, aun sin saber las consecuencias, en cómo utilizamos la herramienta que ha cambiado a la humanidad radicalmente: Internet.

Derivado de lo anteriormente expuesto, es importante mencionar que en la sociedad digital que vivimos actualmente, la ciberseguridad nacional compromete elementos importantes, tanto para la iniciativa privada como para la iniciativa pública, como lo son la protección de datos personales, la seguridad nacional, la economía y el cibercrimen. Cuando estos elementos fundamentales convergen, dan lugar a elementos aún más complejos como el ciberterrorismo, la privacidad de la ciudadanía, los modelos de negocio basados en los datos para generar una economía digital; y el crimen organizado digital y las economías del malware.

Es así como las organizaciones de la iniciativa privada y pública, que no participen en el desarrollo científico y tecnológico de herramientas para hacer evolucionar Internet, se quedarán rezagadas en las "épocas del oscurantismo digital". Mientras que aquellas que entiendan que la tecnología debe estar basada en un sustento científico para ser más sustentable y con mayor impacto, estarán a la vanguardia económica y con rumbo a la tan prometida utopía digital.

Finalmente, las economías digitales que desarrollen una mejor infraestructura, tanto técnica como educativa para fortalecer la ciberseguridad nacional, serán aquellas que no sólo controlen la narrativa de la evolución del ecosistema digital, sino que también serán aquellas que, en caso de

conflicto, se impondrán frente a sus pares con menores avances en esta materia. En una era donde la economía se nutre de información y datos, una de las frases más reconocidas del ilustre Francis Bacon, "la información es poder", toma una relevancia nunca concebida ya que vivimos en un mundo dominado por la información, donde ya no sólo es poder, sino que la información y la interpretación que se derive de la misma, será una ventana al futuro para controlar el poder.

BIBLIOGRAFÍA

LIBROS

AGUSTINOY GUILAYN, ALBERT, *Régimen jurídico de los nombres de dominio. Estudio práctico sobre sus principales aspectos técnicos legales,* Editorial Tirant lo Blanch, Valencia, 2002.

CARBAJO CASCÓN, FERNANDO, *Conflictos entre signos distintivos y nombres de dominio en Internet,* Segunda Edición, Editorial Aranzadi, España, 2002.

ECHEVERRÍA BUNSTER, ANDRÉS, *Uso de marcas y nombres de dominio*, en Derechos Intelectuales, Tomo 9, Colección Derechos Intelectuales, Editorial Astrea, Argentina, 2001.

GRANT, JOHN, *Los vikingos, cultura y mitología*, Ed. TASCHEN BENEDIKT, Alemania, 2008.

ITÉANU, OLIVIER y KAPLAN, DANIEL, *La Réforme des noms de domaines géneriques, Lami Droit de l'informatique*, num. 1343, 1997.

LINDSAY, DAVID, *International Domain Name Law ICANN and the UDRP,* Editorial Hart Publishing, Portland, 2007.

LLANEZA GONZÁLEZ, PALOMA, *Internet y comunicaciones digitales*, Editorial Bosch, España, 2000.

PAUWELS, LOUIS y BERGIER, JACQUES. *"El Retorno de los Brujos",* Ed. Plaza & Janes, Barcelona, 1962.

SANZ DE ACEDO HECQUET, ETIENNE, *Marcas renombradas y nombres de dominio en Internet: en torno a la ciberpiratería*, Editorial Civitas Ediciones, Madrid, 2001.

VIBES, FEDERICO PABLO, *El Nombre de Dominio de Internet,* Editorial La Ley, Buenos Aires, 2003.

ARTÍCULOS

AGUSTINOY GUILAYN, ALBERT*, ¿De qué hablamos cuando hablamos de nombres de dominio?*, Revista Aranzadi de Derecho y Nuevas Tecnologías, Enero, Vol. 7, Enero, 2005.

NAJARIAN, DAVID, *Internet domains and trademarks claims: First Amendment considerations*, IDEA Journal of Law and Technology, Franklin Pierce Law Center, Vol. 41, No. 1, 2001, p. 127.

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, *Informe de Comercio Electrónico y Propiedad Intelectual*, apartado 181, Informe emitido en mayo de 2000.

SANDOVAL LÓPEZ, RICARDO, *Marcas Comerciales y Nombres de Dominio,* Actualidad Jurídica Número 2, Chile, 2004, p.235.

RECURSOS ELECTRÓNICOS

CARRASCO BLANC, HUMBERTO ROLANDO, *Consideraciones sobre el conflicto entre los nombres de dominio y los signos distintivos en Chile. Algunos casos prácticos*, Derecho Informático Volumen II, Ed. Juris, Chile, 2001. https://web.archive.org/web/20120119034802/http://www.dominiuris.com/congreso/congreso1/carrasco.htm

ICANN Consumer Research Wave 2, https://www.icann.org/news/announcement-2-2016-06-23-en

Internet Corporation for Assigned Names and Numbers Glossary http://www.icann.org/en/about/learning/glossary

ICANN String evaluation completition http://www.icann.org/en/resources/idn/fast-track/string-evaluation-completion

ICANN Yokohama Meeting Topic: Introduction of New Top-Level Domains http://archive.icann.org/en/meetings/yokohama/new-tld-topic.htm

IRIARTE AHON, ERICK AMÉRICO, *Dándole Nombres al Internet. Sobre Nombres de Dominio.* Artículo recuperado en archive.org y que puede ser consultado en el siguiente enlace: https://web.archive.org/web/20060718214032/http://www.ieid.org/congreso/ponencias/Iriarte%20Ahon,%20Erick%201.pdf

ISO Country names and code elements http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm

KAUFMAN, IAN JAY, *El Sistema de Nombres de Dominio: Actuar Ahora o Lamentar Después,* junio 2005. http://www.alfa-redi.org/node/9859

Periódico El Mundo, *El regulador de nombres de Internet da luz verde al uso de cualquier palabra en los dominios,* http://www.elmundo.es/elmundo/2011/06/20/navegante/1308550917.html

POSTEL, JON, *RFC 1591: Estructura y Delegación del Sistema de Nombres de Dominio*, marzo de 1994, http://www.rfc-es.org/rfc/rfc1591-es.txt

POSTEL, JON y REYNOLDS J., *RFC 920: Domain Requirements,* https://tools.ietf.org/rfc/rfc920.txt

OTROS RECURSOS ELECTRÓNICOS

https://bit.namecoin.org/

https://bytecoin.org/blog/blockchain-technology-vs-centralized-icann/

https://cointelegraph.com/news/change-is-coming-how-the-blockchain-will-transform-the-domain-name-business

https://www.quora.com/Could-blockchain-replace-DNS

https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

https://en.wikipedia.org/wiki/.bit

https://es.wikipedia.org/wiki/Cadena_de_bloques

https://en.wikipedia.org/wiki/Namecoin

https://en.wikipedia.org/wiki/Zooko's_triangle

https://github.com/okTurtles/dnschain

https://namecoin.org/

http://simondlr.com/post/94988956673/an-intro-to-dnschain-low-trust-access-to

http://tools.ietf.org/html/rfc882

http://tools.ietf.org/html/rfc883

https://web.archive.org/web/20120119034802/http://www.dominiuris.com/congreso/congreso1/carrasco.htm

http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

https://youtu.be/NCxJ-k0A8xY

Revista de Administración Pública

INAP

Tecnología cuántica y Ciberseguridad

Salvador E. Venegas Andraca

Resumen: En la tecnología cuántica, campo del conocimiento en que se conjugan la física, la matemática, la ciencia computacional y la ingeniería, buscamos entender cómo la física cuántica (la física de lo tremendamente pequeño) se puede utilizar para incrementar dramáticamente nuestra capacidad de recolección, procesamiento, transmisión y almacenamiento de la información.

En este artículo se presenta una introducción sucinta a las nociones fundamentales de la tecnología cuántica así como algunos de los retos y oportunidades más importantes que esta tecnología tiene en el ámbito de la ciberseguridad.

Palabras clave: tecnología cuántica, distribución cuántica de llaves, ciberseguridad, sensores cuánticos, internet cuántico.

Quantum Technology and Cybersecurity

In quantum technology, the field of knowledge in which physics, mathematics, computational science and engineering are combined, we seek to understand how quantum physics (the physics of the tremendously small) can be used to dramatically increase our collection capacity, processing, transmission and storage of information.

This article presents a succinct introduction to the fundamental notions of quantum technology as well as some of the most important challenges and opportunities that this technology has in the field of cybersecurity.

Keywords: quantum technology, quantum distribution of keys, cybersecurity, quantum sensors, quantum internet.

Fecha de recepción: 11 de febrero de 2019
Fecha de aceptación: 1 de abril de 2019

Revista de Administración Pública

INAP

Tecnología cuántica y Ciberseguridad

Salvador E. Venegas Andraca*

I. Introducción

La viabilidad y el progreso de la especie humana están ligados a la ciencia y la tecnología. Más aún, los productos de alto valor agregado que resultan de la investigación científica y tecnológica son fuente de riqueza material para las sociedades que inviertan capital humano y económico en estos quehaceres.

Las actividades del mundo moderno tienen una herramienta de trabajo común: la ciencia y la ingeniería de la computación. Esto se debe, entre otros motivos, a que:

- El empleo de plataformas computacionales poderosas es esencial para el análisis de datos experimentales. Ejemplo: estudio del genoma humano y redes complejas como Internet o las redes de suministro eléctrico.
- La eficiencia y precisión requeridas actualmente en transacciones financieras sería imposible de lograr sin sistemas computacionales avanzados.

* Doctor en Física y Maestro en Ciencias por la Universidad de Oxford. Maestro en Administración (MBA) e Ingeniero en Sistemas Electrónicos por el Tecnológico de Monterrey. Es fundador del cómputo cuántico en México y profesor-investigador en esa institución, en la que dirige el Grupo de Procesamiento Cuántico de la Información. Por sus contribuciones científicas, Salvador es miembro de la Academia Mexicana de Ciencias, Senior Member de la ACM y Premio Rómulo Garza 2015, además de miembro del Sistema Nacional de Investigadores y socio titular de la Somedicyt.

- El diseño de algoritmos sofisticados y el empleo masivo de hardware en la simulación de procesos y fenómenos naturales es una actividad cotidiana en la investigación actual. Ejemplo: estudio y predicción de estructuras tridimensionales de proteínas.

En este ir y venir de datos a través de computadoras y redes digitales, cuya expresión más refinada es Internet, hay un requerimiento esencial: la seguridad de la información, esto es, la existencia de métodos que garanticen lo siguiente [1]:

a) Que los remitentes y receptores de la información sean legítimos.
b) La integridad de la información, esto es, que en cualquier proceso, la información generada, enviada y recibida sea la misma.
c) Que cualquier desviación del comportamiento esperado en los incisos anteriores sea detectada y reportada a la brevedad.

A lo largo de la era digital, se ha creado una plétora de métodos para cumplir con las expectativas mencionadas en seguridad de la información, métodos que se pueden agrupar en dos rubros: autenticación (verificación de identidades) y criptografía (ocultamiento y develación de información). Algunos de estos procedimientos son muy sólidos en sus fundamentos matemáticos pero son difíciles de implantar, en tanto que otros tienen sus cimientos en conjeturas matemáticas, mas la implantación es más ágil que en el caso anterior.

Es en este contexto que la noción de tecnología cuántica toma relevancia en el mundo de la seguridad informática. Comencemos con una definición:

La tecnología cuántica es el conjunto de productos y procesos que, con el propósito de recolectar, transmitir, procesar y almacenar información, emplea objetos físicos cuyo comportamiento es descrito por la mecánica cuántica. A su vez, la mecánica cuántica es la rama de la física que estudia y describe el comportamiento de objetos muy pequeños, de tamaño atómico y subatómico [2].

En la tecnología cuántica, campo del conocimiento en que se conjugan la física, la matemática, la ciencia computacional

y la ingeniería, buscamos entender cómo la física cuántica (la física de lo tremendamente pequeño) se puede utilizar para incrementar dramáticamente nuestra capacidad de procesamiento de información, esto es, de cómputo y de comunicación de datos. Ejemplos de tecnología cuántica son la criptografía cuántica, las computadoras cuánticas y los sensores cuánticos.

La tecnología cuántica ha producido importantes avances teóricos y experimentales en la que participan universidades y centros de investigación de prestigio mundial (por ejemplo, Oxford, Cambridge, MIT, Caltech y el Instituto Max Planck, por ejemplo) y gobiernos (Canadá, China, EE.UU., Japón, Reino Unido y Singapur, entre otros).

Además, la tecnología cuántica es ya un mercado emergente cuyo valor se estima en cientos de miles de millones de dólares estadounidenses en el futuro cercano [3,4]. Algunos resultados sobresalientes de esta disciplina son:

- El diseño de algoritmos cuánticos como el algoritmo de Shor [5], capaz de factorizar números enteros largos en tiempo razonable usando una computadora cuántica; el algoritmo de Grover [6], el cual encuentra elementos en conjuntos desordenados de forma más eficiente que cualquier algoritmo posible ejecutado en computadoras convencionales; finalmente, el algoritmo de Childs *et al*, el cual atraviesa una red con conexiones aleatorias en menos tiempo que cualquier algoritmo diseñado anteriormente [7].
- En el caso de la transición del laboratorio a la industria, uno de los resultados más maduros de la tecnología cuántica es la criptografía cuántica comercial. El corazón de esta tecnología es el uso de sistemas cuánticos para generar claves de encriptamiento de datos, claves que gozan de una robustez en su generación y secrecía sin paralelo en el mundo de la criptografía no cuántica. Los sistemas comerciales de criptografía cuántica existen desde 2003 e ID Quantique [8] es la compañía de referencia en este rubro.
- Computadoras cuánticas comerciales. IBM [9] y D-Wave [10] han fabricado computadoras cuánticas que están ya disponibles en el mercado. IBM tiene

> varios modelos de computadoras cuánticas de propósito general, el acceso a estos ordenadores es vía Internet y puede ser gratuito o por pago, dependiendo de la capacidad de procesamiento requerida. Las computadoras cuánticas de D-Wave están hechas para resolver problemas de optimización (esto es, problemas cuya solución requiere conocer el valor máximo o mínimo de uno o varios parámetros) y se puede tener acceso a ellas vía compra directa o a través de Internet.

Por su capacidad disruptiva en capacidades científicas y nuevos mercados tecnológicos, la tecnología cuántica es una área observada y estudiada por organizaciones de alcance continental como el BID [11] y la Unión Europea [12], además de los países ya mencionados y otros.

En este artículo se presenta una introducción-reflexión sobre el desarrollo, uso y aplicaciones de tecnología cuántica en el contexto de la ciberseguridad nacional.

2. Tecnología cuántica y su relación con la ciberseguridad

De acuerdo con la Unión Internacional de Telecomunicaciones, la ciberseguridad se define como *el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno* [13].

Como se declara en la sección anterior, la tecnología cuántica es el conjunto de productos y procesos que, con el propósito de recolectar, transmitir, procesar y almacenar información, emplea objetos físicos cuyo comportamiento es descrito por la mecánica cuántica. Los objetos cuánticos, al ser utilizados como recursos tecnológicos, proveen a la humanidad de nuevas e inesperadas capacidades computacionales y de comunicación de datos. Por ejemplo, pueden ser empleados para desarrollar algoritmos poderosos [14] o para teletransportar información [15].

Las propiedades de la tecnología cuántica representan, simultáneamente, un reto mayúsculo y una oportunidad

excepcional para la ciberseguridad global y, en particular, la de nuestro país. En las siguientes líneas damos cuenta de algunos de resultados y tendencias más importantes de la tecnología cuántica en el ámbito de la ciberseguridad.

2.1 Criptografía cuántica.

Breve introducción a la criptografía

La criptografía puede definirse como la rama de la ciencia y la ingeniería dedicada al diseño e implantación de métodos para tener comunicaciones seguras, bajo el supuesto de que hay un tercer involucrado (un espía) que está interesado en leer nuestros mensajes [1]. Más aún, el tercer involucrado está dispuesto a invertir tiempo, capital humano y recursos financieros en lograr su cometido. Es costumbre utilizar los nombres de Alice y Bob para referirnos al emisor y receptor de un mensaje, en tanto que Eve es el nombre empleado para referirnos al espía.

Existen dos tipos de métodos criptográficos: simétricos y asimétricos.

- Los métodos simétricos, también conocidos con el nombre de criptosistemas de llave privada, son algoritmos que emplean el mismo conjunto de símbolos para encriptar (ocultar) y desencriptar (develar) información. En los métodos de llave privada, Alice y Bob tienen el mismo conjunto de símbolos, conjunto que es conocido solamente por ellos y que emplearán para ocultar y develar mensajes.
- Los métodos asimétricos, también llamados criptosistemas de llave pública, son algoritmos que emplean dos llaves para ocultar y develar datos, una privada (conocida sólo por Alice y Bob) y otra pública (esta llave la conoce todo mundo).

Como ejemplo de un criptosistema de llave privada, suponga que Alice desea enviar a Bob el mensaje **EL CULPABLE TIENE LLAVES** y que acordaron, tiempo atrás, emplear la clave **BHGCAL** para construir una llave privada.

Los pasos que Alice y Bob convinieron seguir, para la transmisión de cualquier mensaje, es el siguiente (conocido como el método de Vigenère):

a) Los espacios del mensaje que se encriptará son eliminados.
b) La llave de encriptación se genera yuxtaponiendo la palabra clave.
c) Las letras del mensaje y la llave de encriptación se alinean en columnas.

El resultado de estos incisos, con el mensaje **EL CULPABLE TIENE LLAVES** y la palabra clave **BHGCAL**, es el siguiente:

Mensaje	E	L	C	U	L	P	A	B	L	E	T	I	E	N	E	L	L	A	V	E	S
Llave	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G

d) Ahora, las letras del texto a encriptar son sustituidas por las letras que resultan del siguiente procedimiento:

- Seleccione una letra del texto a encriptar y la letra correspondiente de la llave de encriptación.
- En la Fig. (1), localice la letra que está en el cruce del renglón que corresponde a la letra del texto y la columna que corresponde a la letra de la llave.
- Sustituya la letra del mensaje por la letra de la Fig. 1 encontrada conforme el inciso anterior.

En nuestro ejemplo, el resultado es:

Mensaje	E	L	C	U	L	P	A	B	L	E	T	I	E	N	E	L	L	A	V	E	S
Llave	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G
Mensaje encriptado	**F**	**R**	**I**	**W**	**L**	**A**	**B**	**I**	**Q**	**G**	**T**	**S**	**F**	**T**	**K**	**N**	**L**	**L**	**W**	**L**	**Y**

Los protocolos de llave privada pueden ser muy poderosos. Si las llaves cumplen con: i) ser en verdad privadas (esto es, que se puede garantizar que son de la exclusiva propiedad de Alice y Bob); ii) generada aleatoriamente; iii) de tamaño al menos igual al mensaje que se desea encriptar y iv) utilizada sólo una vez, entonces es posible construir protocolos de criptografía de llave privada invencibles, esto es, protocolos para los que es imposible que un espía pueda recuperar

el mensaje enviado a partir del mensaje encriptado [16]. Empero, las condiciones que las llaves privadas deben cumplir son extremadamente difíciles de cumplir, de ahí que se haya buscado esquemas de criptografía alternativos, como los de llave pública.

Figura 1
Tabla del método de Vigenère

		Llave																										
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Texto	**A**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	Ñ	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
	U	U	V	W	X	Y	Z	V	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Distribución cuántica de llaves:
una solución al problema de secrecía

En los métodos tradicionales de distribución de llaves privadas, la mayor dificultad a vencer es garantizar la secrecía de la llave, esto es, que la llave sea del conocimiento exclusivo de Alice y Bob. Las llaves distribuidas en medios impresos pueden ser fácilmente copiadas sin que Alice ni

Bob se enteren (esto fue, en buena medida, la ruina del código Enigma, protocolo de encriptación utilizado por el gobierno alemán durante la Segunda Guerra Mundial [17]). Lo mismo sucede con llaves distribuidas a través de medios eléctricos o electrónicos: telégrafo y télex antaño, hoy correos electrónicos, chats y cualquier tipo de mensajería digital, una llave que se distribuya por estos u otros medios es posible copiarla ***sin*** que los responsables/usuarios se percaten de esto.

Una pertinente acotación a lo anterior es que los medios digitales modernos encriptan los mensajes que se envían a través de sus plataformas. Whatsapp, por ejemplo, utiliza *end-to-end encryption*, un método criptográfico asimétrico que, con la tecnología disponible en la empresa, es difícil de vencer. Difícil mas no imposible pues *end-to-end encryption* adolece de los problemas que todo método asimétrico tiene, además de existir ya documentación técnica respecto de fallas en *end-to-end encryption* debidas a problemas de autenticación [18]. En consecuencia, la secrecía en la distribución de llaves privadas tampoco está garantizada por la tecnología contemporánea de mensajería electrónica.

En línea con estos esfuerzos, Charles Bennett y Giles Brassard publicaron en 1984 un método de generación de llaves privadas empleando sistemas cuánticos [19] conocido como el protocolo BB84. En esencia, el BB84 consiste en crear llaves privadas mediante la transmisión y medición de sistemas cuánticos. Ejemplos de estos sistemas cuánticos son los electrones y los fotones (los fotones son las partículas de las que se compone la luz). Una vez construida una llave privada a través del BB84, esta llave puede utilizarse en cualquier protocolo simétrico (AES o DES, por ejemplo [20]).

Las propiedades físicas de los sistemas cuánticos del BB84 permiten determinar, ***durante el proceso de construcción y distribución de una llave privada***, si hay un espía escuchando en el canal de comunicaciones cuánticas usado para dicho proceso. En caso de detectarse la presencia de un espía, el proceso de creación y distribución de la llave se interrumpe de inmediato, para después intentarlo nuevamente. Obsérvese que la detección de espías por parte del protocolo BB84 se hace mucho antes de que dicho agente intente tener acceso al mensaje encriptado.

En otras palabras, el mensaje a transmitir nunca se ve comprometido.

Con la llegada de la criptografía cuántica, la transmisión de datos tiene una nueva dimensión en seguridad pues la privacidad de la información está ahora vinculada a las propiedades físicas de los objetos con los que construimos llaves privadas.

Además del BB84, existen otros protocolos de distribución cuántica de llaves. Información técnica sobre estos protocolos y otras técnicas dedicadas al ocultamiento de información usando sistemas cuánticos (por ejemplo, tecnología cuántica y su relación con Blockchain y procesamiento de imágenes) puede encontrarse en [21, 22, 23, 24, 26, 27, 28, 29, 30].

2.2 Algoritmos cuánticos

Construir computadoras sin aprovechar las propiedades físicas de los materiales usados es como escribir un relato usando pocas palabras: la capacidad de contar el cuento está limitada no sólo por la imaginación, también lo está por la pobreza del lenguaje empleado en el relato. Ampliar el vocabulario empleado abona a la mejora del cuento; de la misma forma, enriquece sumar la física de los sistemas de procesamiento de datos a los modelos matemáticos computacionales.

La computación cuántica es una disciplina dedicada al desarrollo de computadoras y programas cuyo comportamiento se describe y predice empleando las leyes de la física cuántica. El objetivo es desarrollar *hardware* y *software* para resolver problemas de altísima complejidad y gran importancia en la ciencia y la industria.

Un algoritmo cuántico es un procedimiento que usa mecánica cuántica para solucionar un problema. La creación de algoritmos cuánticos es una tarea de alto nivel científico pues, además de resolver el problema para el que fue diseñado, un algoritmo cuántico debe tener ventajas adicionales sobre cualquier algoritmo clásico pensado para solucionar el mismo problema (por ejemplo, ser más rápido).

Entre los algoritmos cuánticos más famosos se encuentra el creado por Peter Shor en 1994 [5]. La contribución de este artículo consiste en presentar un algoritmo cuántico capaz de factorizar un número entero rápidamente. La importancia del algoritmo de Shor en el contexto de la ciberseguridad deriva de lo siguiente:

En la sección 3.1, comentamos que existen dos tipos de métodos de encriptación: simétricos y asimétricos. Los asimétricos utilizan una llave pública y otra privada para hacer los procesos de ocultamiento y develación de datos.

El protocolo RSA [32], una de las implantaciones más conocidas de criptosistemas asimétricos, debe su popularidad al balance de seguridad y practicidad que observa. El protocolo RSA es empleado por gobiernos en muchos tipos de transacciones digitales. También es empleado por prácticamente todas las empresas que venden productos y servicios a través de Internet.

La seguridad de RSA radica en una conjetura matemática: la dificultad de encontrar los factores primos de un número entero. Por ejemplo, 7 y 5 son los factores primos de 35 pues 7 y 5 son números primos y 35 = 7x5. En la misma lógica, los factores primos de 485 son 5 y 97 pues 485 = 5x97 y, además, 5 y 97 son números primos. Un último ejercicio, 5336921 =127 x 42023, debe permitirnos ver que el tiempo que hay que invertir en encontrar factores primos crece conforme también crece el número entero que deseamos factorizar.

La factorización en primos de un número entero está garantizada, siempre es posible hacerla [33]. La dificultad de encontrar los factores primos de un número entero radica en que, al día de hoy, no hay un solo algoritmo que, corriendo en computadoras convencionales, pueda hacer este proceso en poco tiempo. Por ejemplo, con los algoritmos y computadoras actuales, podemos tardarnos cientos de años en encontrar los factores primos de números de mil dígitos.

De lo anterior emana la importancia del algortimo de Shor: la seguridad del protocolo RSA, consistente en los largos tiempos requeridos para factorizar números enteros muy grandes, queda seriamente lastimada con la aparición

del algoritmo de Shor pues éste es capaz de encontrar, en minutos u horas, los factores primos que a otros algoritmos tomaría siglos.

2.3 Tecnologías emergentes y su relación con la tecnología cuántica

Aprendizaje computacional cuántico. El aprendizaje computacional (*Machine Learning*, en inglés) es una rama de la ciencia computacional que, con base en técnicas estadísticas, cálculo de correlaciones y reglas emanadas del conocimiento experto en diversos dominios, desarrolla algoritmos para: a) identificar y clasificar patrones desconocidos, y b) desarrollar estrategias, basadas en la experiencia, para resolver problemas complejos.

Los sistemas de aprendizaje computacional, en boga durante los últimos años, son útiles para identificar tendencias y comportamientos anómalos en redes complejas, los mercados financieros por ejemplo. El aprendizaje computacional, sumados a otras disciplinas como la visión computacional, son la base de sistemas avanzados de vigilancia, supervisión y seguimiento (*tracking*). Ejemplo concreto de uso de aprendizaje computacional en ciberseguridad es su empleo en predicción de actividades criminales [33,34].

Los orígenes del aprendizaje automático se remontan a 1950, con los trabajos de Turing, Minsky y otros científicos [35]. A pesar de los avances cruciales en esta disciplina, un inconveniente constante del aprendizaje computacional es que la ejecución de sus algoritmos tiende a requerir mucho poder de cómputo. Esto se debe a la cantidad de datos por procesar y a la complejidad de los modelos matemáticos empleados para describir problemas y situaciones de interés.

Con frecuencia, las técnicas de aprendizaje computacional requieren construir modelos en los que estamos interesados en conocer el valor máximo de una variable. Este tipo de problemas se llaman de **optimización**. Algunos ejemplos son: ¿cuál es la demanda máxima de energía eléctrica, segmentado por horas y municipios, que se espera que consuma la ciudad de México en los siguientes seis meses? o ¿cuál cara, de todas las que están en nuestra base de

imágenes, es la más parecida al rostro de una persona grabada en un aeropuerto?

Los algoritmos de optimización tienden a consumir mucho tiempo y recursos computacionales, razón por la que hay comunidades científicas dedicadas a diseñar mejores algoritmos de optimización. Estas comunidades incluyen a especialistas en computación cuántica, debido a que los ordenadores cuánticos son buenos candidatos para resolver problemas de optimización (por ejemplo, vea [36] para una introducción a la programación de computadoras *D-Wave*).

El aprendizaje computacional cuántico es, entonces, una disciplina dedicada a crear algoritmos cuánticos cuyo objetivo es identificar y clasificar patrones desconocidos así como desarrollar estrategias, basadas en la experiencia, para resolver problemas complejos. Las aplicaciones que de este campo emanan, en particular las relacionadas con vigilancia en Internet y a través de redes digitales, de importancia en el mundo de la ciberseguridad. Para aprender más sobre aprendizaje computacional cuántico recomendamos la lectura de [36,37,38].

Redes cuánticas e Internet cuántico. Entre los elementos del portafolios de la tecnología cuántica encontramos, además de computadoras y sistemas de distribución cuántica de llaves, sensores cuánticos.

Estudios teóricos y experimentales sobre la recolección de datos muestran que es posible construir sensores cuánticos cuya sensibilidad (capacidad de recolección de datos) es mayor que la tecnología desarrollada al día de hoy. Ejemplos de este tipo de sensores son los empleados en la construcción de radares cuánticos [40,41] y mediciones ultraprecisas del campo gravitacional de la tierra [42].

La información generada por ordenadores, sistemas de distribución cuántica de llaves y sensores cuánticos requiere de un medio de transmisión que preserve la naturaleza cuántica de la información que se enviará, de ahí la pertinencia de construir redes cuánticas. Internet cuántico, neologismo cuya definición está en evolución constante, en esencia es la idea de tener una red mundial (como Internet) que permita la transmisión de información

cuántica entre sensores, computadoras y otros dispositivos. El estudio de las redes cuánticas y la posible creación de Internet cuántico es de clara importancia en los programas de ciberseguridad de México.

3. Tecnología cuántica y ciberseguridad en el plano internacional

La tecnología cuántica ha despertado el interés de varias naciones por sus avances y potencial impacto en ciberseguridad, nuevas tecnologías y desarrollo económico. En ciberseguridad, el uso del algoritmo de Shor en computadoras cuánticas robustas representa un reto futuro de proporciones mayúsculas para las transacciones digitales que empleen RSA, en tanto que la distribución cuántica de llaves es un paradigma promisorio para la construcción y fortalecimiento de protocolos criptográficos. Respecto de nuevas tecnologías, el interés surge desde la creación de nuevos materiales para computadoras cuánticas hasta el desarrollo de algoritmos cuánticos para la solución de problemas de frontera. En todo lo anterior, la inversión que hagan gobiernos y empresas permitirá crear ramas emergentes de la industria y, con ello, nuevos empleos.

En los Estados Unidos de América existe una extensa red de organizaciones académicas, empresariales y gubernamentales dedicadas a la investigación en tecnología cuántica y sus implicaciones en ciberseguridad. Más aún, desde diciembre de 2018, con la promulgación del Acta de la Iniciativa Nacional Cuántica (*National Quantum Initiative Act*) [43], el gobierno federal de ese país coordina una agenda de investigación científica y desarrollo tecnológico centrada en la ciencia de la información cuántica (*quantum information science*).

La Iniciativa Nacional Cuántica tiene por objetivo principal "asegurar el liderazgo de los EE. UU. en la ciencia de la información cuántica" (página 4 de [43]). Entre los objetivos específicos de esta iniciativa, se encuentra "promover el desarrollo de estándares internacionales para la ciencia cuántica de la información y la seguridad tecnológica" y, en particular, "alcanzar metas económicas y de seguridad nacional" de los Estados Unidos de América (página 4 de [43]). Además, la Iniciativa Nacional Cuántica tiene un subcomité en el que participan El Instituto Nacional de

Estándares y Tecnología (*NIST*, por su siglas en inglés), la Dirección de Inteligencia Nacional, el Departamento de la Defensa y la NASA. El NIST tiene por encargo convocar a un consorcio de personas y empresas interesadas en el crecimieno de la industria de la tecnología cuántica, siendo la ciberseguridad uno de los aspectos a desarrollar (página 7 de [43]) .

Desde el inicio del siglo XXI, la Unión Europea tiene un programa de amplio alcance para el desarrollo de tecnología cuántica que incluye temas prioritarios para la ciberseguridad europea, entre los que destacan [12]:

- La construcción de computadoras cuánticas robustas. Estas máquinas tendrán los sistemas de control y corrección de errores necesarios para ejecutar el algoritmo de Shor, entre otros algoritmos cuánticos.
- Generación de números aleatorios. Estos números, que son insumo crucial para diversas ramas de la ciencia y tecnología, no pueden ser generados por computadoras digitales convencionales.
- Redes de comunicaciones cuánticas de alcance continental. Estas redes constituirán la primera versión del Internet Cuántico Europeo.
- La infraestructura necesaria para hacer distribución cuántica de llaves.

Algunos de estos temas convergen, con otras tecnologías, en uno de los objetivos centrales de la ciberseguridad europea: la creación de los mecanismos y herramientas que permitan dotar, a todo habitante europeo, de identidad digital. Dado que el anonimato es un factor toral en la comisión de delitos en el ciberespacio, la creación de identidades digitales permitirá reducir significativamente el campo de acción de cibercriminales en robo de identidad, por ejemplo. Otro objetivo que comparten EE UU, Europa y países asiáticos es el desarrollo de protocolos criptográficos post-quantum, esto es, métodos de ocultamiento y develamiento de datos capaces de resistir ataques cuánticos.

4. Tecnología cuántica y ciberseguridad en México

Si bien existen algunos estudios y marcos de referencia preliminares [44,45], la construcción de la estrategia digital

mexicana es un proceso en ciernes, hecho que nos pone en desventaja respecto de agrupaciones delincuenciales dedicadas a la extorsión y robo de información por medios digitales [45]. Empero, este estado de las cosas es también una oportunidad para construir una estrategia que incluya la opinión y participación de los sectores público, académico y privado, de hacer de la estrategia un productor de conocimiento así como un detonador de desarrollo y nuevos mercados.

Uno de esos nichos con amplias oportunidades para México es la tecnología cuántica para la ciberseguridad. En este sentido, cualquier estrategia de ciberseguridad debería comprender al menos los siguientes rubros:

- Distribución cuántica de llaves.
- Redes cuánticas.
- Algoritmos cuánticos.
- Criptografía post-cuántica.
- Generadores portátiles de números aleatorios.

México cuenta con científicos e infraestructura para avanzar en los aspectos teóricos, experimentales y de implantación de la tecnología cuántica. México cuenta con capital humano e instituciones como el grupo de ciberseguridad del Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), el laboratorio de fotónica cuántica del Centro de Investigaciones en Óptica (CIO), los Institutos de Física, Ciencias Nucleares y Matemáticas Aplicadas de la UNAM, el Centro de Investigación en Computación del IPN, CINVESTAV, el Instituto de Física de la Universidad Autónoma de San Luis Potosí y el Grupo de Procesamiento Cuántico de la Información del Tecnológico de Monterrey Campus Estado de México, entre otras organizaciones de educación superior y centros de investigación. Estas mismas instituciones serían clave en la formación del capital humano requerido para el diseño e implantación de estrategias basadas en tecnología cuántica.

En el ámbito empresarial, el ecosistema es generoso en tamaño y oportunidades. Desde desarrollos puntuales hechos por emprendedores hasta la participación de *clusters* de tecnologías de la información como los existentes en Guadalajara y Yucatán, la comunidad empresarial mexicana dedicada a la innovación tecnológica vería en

la tecnología cuántica para ciberseguridad un área de crecimiento y de protección para ella misma.

Finalmente, nuestra nación está en posibilidad de asumir el liderazgo regional en la creación de tecnología cuántica para ciberseguridad pues, en toda América Latina, solamente Brasil cuenta con capacidades similares a las nuestras en capital humano e infraestructura científico-tecnológica.

Conclusiones

La tecnología cuántica ha logrado atraer, por su desarrollo actual y prometedor potencial en la solución de problemas científicos y tecnológicos de frontera, la atención de matemáticos, físicos, científicos computacionales, ingenieros, economistas, mujeres y hombres de negocios, políticos y estudiantes, entre otros.

En tecnología cuántica, México está hoy en la encrucijada de ser agente activo en esta revolución científica y tecnológica, y así formar parte del muy selecto grupo de países que dominarán los mercados de esta tecnología, o bien quedarse en la orilla y convertirse en simple consumidor del conocimiento y aplicaciones que hoy se gestan. En particular, el desarrollo de tecnología cuántica y capital humano especializado en este rubro es de capital importancia para la ciberseguridad de nuestra nación.

BIBLIOGRAFÍA

[1] Andress, Jason. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Elsevier, MA, USA, 2014.
[2] Acín, A. et al, “The quantum technologies roadmap: a European community view”, New Journal of Physics, vol. (20), 2018, 080201.
[3] Russo, M., Thaker, A., and Adam, S. “The Coming Quantum Leap in Computing”. A Boston Consulting Group Report (2018). Recuperado el 27/marzo/2019 del sitio https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

[4] "The quantum age: technological opportunities". The UK Office for Science (2018). Recuperado el 27/marzo/2019 del sitio https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf
[5] Shor, P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Algorithms on a Quantum Computer", Proc. of the IEEE 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
[6] Grover, L.K., "A fast quantum mechanical algorithm for database search", Proceedings of the 28th annual ACM symposium on the Theory of Computing, 1996, pp. 212–219.
[7] Childs, A.M., Cleve, R., Deotto, E., Farhi, E., Gutmann, S., and Spielman, D. "Exponential algorithmic speedup by quantum walk", Proceedings of the 35th ACM Symposium on The Theory of Computation (STOC'03) ACM, 2003, pp. 59–68.
[8] https://www.idquantique.com/
[9] https://www.research.ibm.com/ibm-q
[10] https://www.dwavesys.com
[11] Allende López, Marcos y Da Silva, Marcelo Madeira. Tecnologías cuánticas. Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social. Reporte técnico (white paper), Banco Interamericano de Desarrollo, 2019. DOI:10.18235/0001613
[12] Riedel, M., Kovacs, M., Zoller, P., Mlynek J., and Calarco T., "Europe's Quantum Flagship initiative" Quantum Science and Technology, vol. (4), No. 2020501, 2019.
[13] Unión Internacional deTelecomunicaciones. Recomendación UIT-T X.1205, página 3, de la serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad (abril 2008). Recuperado el 28 de marzo de 2019 de https://www.itu.int/rec/T-REC-X.1205-200804-I/es UIT–T X.1205
[14] Orús, R., Mugel, S., and Lizaso, E., "Quantum computing for finance: Overview and prospects", Reviews in Physics, vol. (4), 2019, 100028.
[15] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein–

Podolsky–Rosen Channels. Phys. Rev. Lett. 70 (13), pp. 1895–1899 (1993). DOI:10.1103/PhysRevLett.70.1895
[16] G.S. Vernam. Secret signaling system. US Patent US1310719A (1918)
[17] A. Ray Miller. the cryptographyc mathematics of Enigma. Cryptologia vol(19) No. 1, pp. 65-80 (1995). DOI: 10.1080/0161-119591883773
[18] https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/
[19] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179 (1984).
[20] Richard A. Mollin. An Introduction to Cryptography (2nd Edition). CRC Press (2006).
[21] Abd-El-Atty B., Venegas-Andraca S.E., Abd El-Latif A.A. Quantum Information Protocols for Cryptography. In: Hassanien A., Elhoseny M., Kacprzyk J. (eds) Quantum Computing: An Environment for Intelligent Large Scale Real Application. Studies in Big Data, vol 3, pp. 3--23, Springer . (2018). DOI: 10.1007/978-3-319-63639-9_1
[22] S. Loepp and W.K. Wootters. Protecting Information: From Classical Error Correction to Quantum Cryptography. Cambridge University Press (2006)
[23] Ekert, A.K., "Quantum cryptography based on Bell's theorem". Physical Review Letters vol. 67(6), 00. 661--663, 1991.
[24] Bennett, C., "Quantum cryptography using any two nonorthoganol states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124.
[25] S.E. Venegas-Andraca and J.L. Ball. Processing Images in Entangled Quantum Systems. Quantum Information Processing, vol. 9(1), pp. 1-11 (2010). DOI:10.1007/s11128-009-0123-z
[26] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca. A survey of quantum image representations. Quantum Information Processing 15(1), pp. 1-35 (2016). ISSN: 0960-1295 (print), ISSN: 1469-8072 (online). https://doi.org/10.1007/s11128-015-1195-6
[27] A.A. Abd EL-Latif, B. Abd-El-Atty, and S.E. Venegas-Andraca. A novel image steganography technique based on quantum substitution boxes. Optics and

Laser Technology 116, pp. 92-102 (Aug 2019). https://doi.org/10.1016/j.optlastec.2019.03.005
[28] C. Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunkovic, Andre Souto. Quantum key distribution with quantum walks. Quantum Inf Process (2018) 17: 288. https://doi.org/10.1007/s11128-018-2055-y
[29] A.K. Fedorov, E.O. Kiktenko, and A.I. Lvovsky, "Quantum computers put blockchain security at risk", NAture vol. 465, pp. 465-467 (2018).
[30] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, "Quantum-secured blockchain", Quantum Sci. Technol. 3, 035004 (2018).
[31] R.L. Rivest, A. Shamir, and L.M. Adleman. Cryptographic communications system and method. Patent US4405829A (filed on 14/Dec/1977, anticipated expiration on 20/Sep/2009).
[32] Gauss, Carl Friedrich; Clarke, Arthur A. Disquisitiones Arithemeticae (Second, corrected edition, translation from Latin to English). Springer (1986).
[33] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, vol. 6, pp. 35365-35381 (2018) doi: 10.1109/ACCESS.2018.2836950
[34] https://www.ted.com/talks/anne_milgram_why_smart_statistics_are_the_key_to_fighting_crime
[35] N.J. Nilson. The quest for Artificial Intelligence. Cambridge University Press (2010).
[36] Venegas-Andraca, S.E., Cruz-Santos, W., McGeoch, C., and Lanzagorta, M., "A cross-disciplinary introduction to quantum annealing-based algorithms", Contemporary Physics 59(2), 2018, pp. 174-196.
[37] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S., "Quantum machine learning", Nature 549, 2017, pp. 195-202.
[38] Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. Contemporary Physics 56(2), pp. 172-185.
[39] M. Lanzagorta, O. Jitrik, J. Uhlmann, S.E. Venegas-Andraca. Quantum Synthetic Aperture Radar. SPIE Defense + Security 2017, Anaheim, CA, EE UU. Proc. of SPIE Vol. 10188, 101880D, Radar Sensor Technology XXI (April 2017); doi: 10.1117/12.2262645.

[40] M. Lanzagorta and S.E. Venegas-Andraca. Algorithmic Analysis of Quantum Radar Cross Sections. Proc. SPIE 9461 Radar Sensor Technology XIX; and Active and Passive Signatures VI, Quantum Radar, 946112-946112-8, doi:10.1117/12.2177238 (2015).

[41] C Freier, M Hauth, V Schkolnik, B Leykauf, M Schilling,H Wziontek, H-G Scherneck, J Müller, and A Peters, "Mobile quantum gravity sensor with unprecedented stability", 8th Symposium on Frequency Standards and Metrology, Journal of Physics: Conference Series 723, 2016, 012050.

[42] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. Science vol. 362, Issue 6412, eaam9288 (2018). DOI: 10.1126/science.aam9288

[43] USA Congress. National Quantum Initiative Act. Recuperado el 31/marzo/2019 de la dirección https://www.congress.gov/bill/115th-congress/house-bill/6227

[44] Estrategia Nacional de CIberseguridad (2018). Gobierno de los Estados Unidos Mexicanos 2012-2018. Recuperado el 08/abril/2019 del sitio https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[45] Tendencias de Seguridad Cibernética en América Latina y el Caribe. Organización de los Estados Americanos (2014). Recuperado el 08/abril/2019 del sitio https://www.sites.oas.org/cyber

Revista de Administración Pública

INAP

Atlas de riesgos para la Seguridad Nacional Cibernética en México

Carlos Estrada Nava

Resumen: La Seguridad Nacional Cibernética es una "zona híbrida" entre conocimientos de ingeniería de programación, así como de actualidad de los temas de geopolítica mundial. Adicionalmente, existe una simbiosis entre Seguridad Cibernética y el Cómputo Forense, el cual se encarga de obtener y procesar evidencias digitales sobre incidentes informáticos. En México para abordar el campo de la "Seguridad Nacional Cibernética", la Secretaría de la Defensa Nacional recientemente creó el primer Comando Cibernético. Nuestro aporte consiste en la elaboración del primer Atlas Nacional de Riesgos Cibernéticos, los cuales pueden ser mitigados por ISO 2700, así como medidas concretas de este documento.

Palabras clave: Seguridad Nacional Cibernética, Infraestructuras Críticas, BlockChain.

Atlas of risks for National Cyber Security in Mexico

Abstract: National Cyber Security is a "hybrid zone" among programming engineering knowledge, as well as topical issues of global geopolitics. Additionally, there is a symbiosis between Cyber Security and Forensic Computing, which is responsible for obtaining and processing digital

evidence on computer incidents. In Mexico to address the field of "National Cyber Security", the Ministry of National Defense recently created the first Cyber Command. Our contribution consists in the elaboration of the first National Atlas of Cyber Risks, which can be mitigated by ISO 2700, as well as concrete measures of this document.

Keywords: National Cyber Security, Critical Infrastructures, BlockChain.

Fecha de recepción: 22 de mayo de 2019
Fecha de aceptación: 7 de junio de 2019

Revista de Administración Pública

INAP

Atlas de riesgos para la Seguridad Nacional Cibernética en México

Carlos Estrada Nava*

Introducción

Si bien el año de 2018 ha sido el peor en ataques cibernéticos en México, con pérdidas en gobierno y empresas por más de 1,200 millones de pesos, en 2019 y el porvenir de la tendencia prevista incluye más riesgos, debido a que no se han corregido ninguno de los 5 principales problemas estructurales del país.

Aunado a ello, el tema de la Seguridad Nacional Cibernética en México se encuentra en estado embrionario debido a que se trata de un campo híbrido, y el mayor riesgo actualmente lo constituyen posibles ataques a las Infraestructuras Críticas del país, como lo es la red eléctrica nacional, misma que ya ha tenido fallas masivas durante 2019.

* Licenciatura en Ciencias Políticas y Administración Pública por la Facultad de Ciencias Políticas y Sociales de la UNAM. Master in Business Administration (MBA) por University of Phoenix, Arizona, USA. Estudios de Ingeniería en Desarrollo de Software. Técnico en Computación profesional, y perito privado ante Ministerio Público de la Procuraduría General de Justicia de la Ciudad de México. Consultor de análisis de datos, cómputo forense y seguridad cibernética en corporaciones mexicanas y americanas de seguridad e inteligencia como: Kroll Inc., Ernst & Young (EY), así como FTI Consulting. Actualmente socio de firma privada Vestiga Consultores, al servicio de Gobierno, Bancos, Minería, Construcción y otras industrias. Ha impartido conferencias de tecnología en los congresos internacionales de la Asociación Mexicana de Ciencias Políticas (AMECIP), y participado en la materia de Seguridad Nacional en Universidad Anáhuac.

Primeramente, resulta indispensable comprender los desarrollos tecnológicos que, día a día, crean nuevas amenazas digitales, más porque en los últimos 5 años existe una explosión en el desarrollo de códigos de programación, debido al crecimiento exponencial del *Open Source* (programas de código abierto), ya que las plataformas de *Big Data* y *Machine Learning* se basan fundamentalmente en código abierto.

Además, se requiere una comprensión de la lógica geopolítica, así como de relaciones internacionales, bajo la cual operan muchos de estos desarrollos, ya sea para atacar o defender la infraestructura de los países y sus empresas.

En nuestro caso en particular, tenemos el objetivo de desarrollar un primer "Atlas Nacional de Riesgos Cibernéticos" de la República Mexicana, lo cual implica analizar riesgos potenciales en contra de las instalaciones estratégicas públicas y privadas, como pueden ser: plantas eléctricas, gasoductos, transporte público, hospitales, escuelas, entre otras.

Asimismo, para poder analizar, diagnosticar y anticipar eventos de Seguridad Cibernética, resulta indispensable emplear elementos técnicos básicos de su disciplina hermana, el Cómputo Forense.

Sobre la actualidad de la Seguridad Cibernética

Junto con la democratización de las tecnologías de la información, debido a la posibilidad de su acceso para cada vez mayores sectores de la población mundial, también se generalizó el acceso global a Internet, convirtiéndose esta red en una plataforma donde por primera vez pueden interactuar por igual Gobiernos, Organizaciones públicas y privadas, así como los individuos en lo particular.

Esta apertura y universalización de las tecnologías multiplicó a su vez los riesgos y vulnerabilidades de los usuarios de las mismas, al tratarse muchas veces de entornos no regulados. Si bien los errores de programación o de hardware, así como los virus informáticos han existido desde el origen de la computación, en el inicio del siglo XXI, a nivel empresas se ha consolidado una industria conocida como "Crimeware", pero a nivel gobierno los ataques

cibernéticos se enmarcan en las llamadas "guerras de cuarta generación", caracterizadas por usar herramientas no convencionales y ocultas, para atacar por sorpresa al enemigo, siendo que se le desestabiliza al grado de poder derrotarlo.

Primeramente, la Seguridad de la Información se encuentra enfocada hacia los procesos y prácticas organizacionales para proteger el entorno de una empresa; este concepto se consolidó en octubre de 2005 por la *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*, quienes aprobaron y publicaron como estándar internacional de seguridad de la información la serie ISO 27000, siguiendo el modelo de la serie ISO 9000, comenzando con el ISO/IEC 27001:2005 (Calder, 2009, p. 29).

A diferencia de esta noción de "Seguridad de la Información", la "Seguridad Cibernética" engloba todos aquellos elementos que pudieran representar un riesgo para la integridad digital de alguna entidad en específico, como pueden ser: ataques de fuerza bruta contra claves de correos electrónicos, ingeniería social con *phishing*, distribución de malware que solicita el pago de un rescate por archivos encriptados, intervención de dispositivos móviles o líneas telefónicas, así como hackeo en general de equipos de cómputo.

En cuanto al desarrollo conceptual del término "Seguridad Cibernética", Tim Stevens (2015, p. 11) desarrolla 3 diferentes planos: a nivel ontológico, su definición posee una connotación de buscar una condición de liberación ante la "inseguridad cibernética", esto es, evitar los riesgos y amenazas propias de la proliferación de las tecnologías de la información, de las cuales dependen nuestras sociedades actuales; en su lado procedimental, la Seguridad Cibernética implica abarcar un rango de prácticas tecnológicas y políticas, desde lo defensivo y proteccionista, hasta lo ofensivo y subversivo; finalmente, la Seguridad Cibernética constituye un medio no sólo de protección y defensa de la sociedad y sus infraestructuras de información, sino también un medio para perseguir políticas nacionales e internacionales mediante instrumentos informáticos-tecnológicos.

Debe ponerse especial atención en que a partir de los recientes 5 años se han disparado los ataques cibernéticos en todo el mundo, impulsados por diferentes procesos paralelos:

1. La explosión y consolidación del *Open Source* frente a Software por licencia, orillando a empresas tradicionales a abrir sus códigos, como Microsoft con Azure o Apple con Swift; debido a que los desarrolladores prefieren programas libres (gratuitos), con la consecuencia de que se descuidan las vulnerabilidades del código (por ejemplo, hay más *hackeos* en celulares con código abierto de Android, pero muy pocos en el código privado de iOS del iPhone)
2. El auge del *Big Data* y el nuevo *Machine Learning* (basados fundamentalmente en Open Source), aumentando el poder analítico y de procesamiento, lo cual también eleva la sofisticación de los ataques digitales
3. Irrupción de las *Crypto Currencies*, basadas en la tecnología *BlockChain*, las cuales impiden rastrear el destino final de las transacciones, promoviendo con ello los delitos cibernéticos

Ante esta nueva actualidad de la Seguridad Cibernética en el mundo, han surgido nuevos enfoques que ayudan a organizaciones públicas y privadas a lograr la ahora llamada "Resiliencia Cibernética", esto es, la capacidad de una entidad para prevenir, anticipar, responder, recuperarse e incluso contraatacar ante un incidente cibernético, y así evitar con ello que se ponga en riesgo la continuidad de su operación.

De las opciones para evaluar la Resiliencia Cibernética de una organización, se encuentran las pruebas de penetración (*pentesting*), mismas que pueden incluir: *denial of Service* (DoS), *out-of-band attacks*, *applications security testing*, *wireless networks analysis*, *mapping* and OS *fingerprinting*, *vulnerability scanning/analysis* (*Spoofing*, *Network sniffing*, *Trojan*, *Brute force attack*, etcétera), entre otros.

Cómputo forense como complemento de la seguridad cibernética en general

En la última década del siglo XX, a nivel global, la industria de la computación vivió un periodo de consumo masivo de equipos de cómputo personales y para nivel corporativo, esto debido fundamentalmente al empaquetamiento de diferentes ambientes de trabajo, como lo han sido los sistemas operativos de Windows, Apple o de código abierto como Linux.

El uso cada vez más generalizado de estas tecnologías, derivó en la necesidad de obtener evidencias informáticas para poder apoyar procesos legales, todo ello en la disciplina de las ingenierías de sistemas, bajo el paraguas del llamado Cómputo Forense. Bajo este campo teórico y práctico, es posible obtener, documentar, procesar y presentar, de manera científica, toda aquella evidencia obtenida de equipos de cómputo, susceptible para usarse en peritajes y dictámenes informáticos.

La rama del Cómputo Forense tiene una naturaleza intrínsecamente científica, debido a que las evidencias recabadas son susceptibles de replicarse, obteniendo en todos y cada uno de los casos los mismos resultados, debido al carácter digital de sus elementos. Adicionalmente, este proceso puede auditarse por un tercer actor interesado, aplicando los métodos de comprobación necesarios, tras lo cual obtendría los mismos resultados del reporte forense original. De esta manera, es posible documentar con Cadenas de Custodia, evidencias forenses de equipos de cómputo en general (escritorio, laptops, servidores), así como realizar análisis forense de redes, datos y dispositivos móviles.

Entre las capacidades básicas de Cómputo Forense podemos encontrar la recuperación profunda de información borrada, análisis del código de archivos, registros de sistema operativo, historiales de navegación por Internet, contenido y encabezados de correos electrónicos, dispositivos móviles, redes de trabajo, entornos de *Cloud*, bases de datos, así como expresiones regulares en el universo de datos en particular, entre otras.

Infraestructuras críticas como nuevo teatro de operaciones de la Seguridad Nacional

Desde nuestra práctica profesional, actualmente nos encontramos en el desarrollo de un primer "Atlas Nacional de Riesgos Cibernéticos" de México. A nivel mundial, países líderes de estas iniciativas han sido Singapur, China, India, Inglaterra, Israel y Estados Unidos. En los países referidos, se definen legislaciones y políticas públicas nacionales sobre seguridad cibernética, las cuales incluyen un análisis generalizado sobre los riesgos potenciales que enfrentan sus instalaciones estratégicas públicas y privadas, como lo son: plantas eléctricas, gasoductos, transporte, hospitales, escuelas, etcétera.

Siendo el Departamento Militar de Innovación Tecnológica de Estados Unidos (DARPA o Defense Advanced Research Projects Agency), el creador del Internet, en aquel país desde hace cuando menos 3 décadas, se ha considerado a la Seguridad Cibernética como uno de los más urgentes problemas que deben enfrentar los gobiernos y las organizaciones públicas y privadas. Como parte del debate legislativo estadounidense, a la "Seguridad Nacional Cibernética" se le considera como el grupo de actividades estratégicas relacionadas con los "sistemas de información electrónicos", conocidos también como "infraestructuras de información", sobre todo aquellas que implican una amplia gama de activos económicos y de seguridad para los sectores públicos y privados (John Rollins, 2009).

Debe mencionarse que dentro del "teatro de operaciones cibernético", para el Pentágono americano, un ataque digital equivale a un ataque físico, por lo cual todo ciberataque requiere una respuesta, ya sea digital o física.

En este documento, se considera el término "teatro de operaciones" o "teatro de guerra", bajo el concepto de "área de operaciones", usado en el diccionario militar del Departamento de la Defensa americano y la OTAN (Organización del Tratado del Atlántico Norte), entendido como "la porción de un área de guerra necesaria para las operaciones militares y para la administraciones de tales operaciones" (Departamento de la Defensa, 1987, p.34).

De esta manera, como fue expuesto anteriormente, los ataques cibernéticos se enmarcan en las llamadas

"guerras de cuarta generación", caracterizadas por usar herramientas no convencionales y ocultas, para atacar por sorpresa al enemigo, siendo que se le desestabiliza al grado de poder derrotarlo. La diferencia a comparación de las guerras anteriores, consiste en que el nuevo "teatro de operaciones cibernético" se lleva a toda la extensión del Internet.

El mayor ejemplo de ello a la fecha, y que se considera la primer arma cibernética, fue el desarrollo del malware "Stuxnet", por parte de Estados Unidos, con el apoyo de la Unidad 8200 de Israel, símil de la NSA (National Security Agency) americana, con el objetivo de atacar los procesadores Siemens de las centrales nucleares de Irán, logrando detener por más de 10 años que alcanzaran la capacidad de enriquecer uranio.

No obstante, esta caja de Pandora se ha extendido hasta la aparición de "filtradores" (*leakers*) que obtienen estas herramientas cibernéticas y las publican o venden abiertamente, como ha sido el caso de "ShadowBrokers" y el grupo "Lazarus", quienes han estado detrás del ataque de bancos y organizaciones mexicanas, incluyendo a la Bolsa Mexicana de Valores. A nivel global, también desarrollaron el *ransomware* famoso llamado "WannaCry", que infectó cientos de miles de computadoras de más de 100 países; este malware usaba sólo 2 herramientas "zero-day" (desconocidas para el público al momento de su ataque) por parte de la NSA, pero desarrollos más recientes como "EternalRocks", usan hasta 7 zero-days.

El impacto de los ataques cibernéticos no ha sido sólo contra la infraestructura o sistemas financieros de los países, porque a partir de 2016 se han documentado estrategias globales para atacar a gobiernos democráticos. El caso político más conocido es el de Rusia, quien habría estado atacando procesos electorales en Estados Unidos, Francia, Alemania e Italia, cuando menos. Esta operación global incluye: *hackeo* directo de políticos, organizaciones, universidades y *think tanks*; campañas digitales de propaganda empleando información obtenida de los *hackeos*; y la creación de "fake news" dirigidas específicamente al núcleo de apoyo electoral de candidatos opuestos a las políticas de Moscú.

Para enfrentarse a los incidentes de los ciberdelincuentes, desde 2004 se estableció a nivel internacional el Convenio de Budapest, bajo el cual a la fecha existen 62 países firmantes, siendo México un país observador. En este Convenio también concurre un comité integrado por representantes de la Unión Europea, G7, Interpol, OCDE, OEA, ONU y Unión Africana. Aunque este instrumento de relaciones internacionales busca ser el marco para resolver litigios y extradiciones, en los hechos resulta inoperante, debido a que están ausentes los países de donde provienen la mayor cantidad de ataques en contra de occidente: Norcorea, China, Rusia, India, Irán, Indonesia, Nigeria y Brasil.

A pesar de sus limitaciones, la Convención de Budapest establece el precedente para prevenir y establecer litigios en contra de delitos cibernéticos como son: robo de identidad, ataque a infraestructuras críticas, *spam*, *malware*, *botnets*, terrorismo y ataques DDOS.

En el caso de México, en el año de 2017 el Gobierno Federal publicó el documento rector a la fecha llamado "Estrategia Nacional de Ciberseguridad" (Presidencia de la República, 2017), el cual fue el resultado de mesas de trabajo con el apoyo de la Organización de Estados Americanos, mediante su Comité Antiterrorismo, debido a que se sabe que un 80% de países no cuentan con estrategias de ciberseguridad o planes de protección de infraestructura crítica. Este documento, como sucede con muchas iniciativas de gobierno o privadas, también confunde los esquemas de "seguridad informática" (programas e infraestructura), con respecto a "seguridad de la información" (organización y actividades humanas).

El más reciente esfuerzo a nivel internacional por regular el "teatro de operaciones" de las ciberguerras actuales, ocurrió en noviembre de 2018, en el Foro de Gobernanza de Internet de la UNESCO, donde el presidente de Francia Emmanuel Macron lanzó el "Llamado de París" para la confianza y la seguridad en el ciberespacio. Esta declaración de alto nivel a favor del desarrollo de principios comunes para asegurar el ciberespacio ya ha recibido el respaldo de 552 partidarios oficiales: 66 países, 139 organizaciones internacionales y de la sociedad civil y 347 entidades del sector privado. Entre los objetivos del "Llamado de París" se enlistan:

- aumentar la prevención y la resistencia a la actividad maliciosa en línea;
- proteger la accesibilidad e integridad de Internet;
- cooperar para prevenir la interferencia en los procesos electorales;
- trabajar juntos para combatir las violaciones de propiedad intelectual;
- mejorar la seguridad de los productos y servicios digitales, así como la "higiene cibernética" de todos los usuarios;
- reprimir las actividades mercenarias en línea y las acciones ofensivas de actores no estatales; entre otras.

Si bien se requiere un tratado internacional para regular las actividades de las guerras cibernéticas actuales, el "Llamado de París" fue rechazado de inmediato por Rusia, China y Estados Unidos, los 3 principales países involucrados en los conflictos cibernéticos a la fecha (Archer, 2018).

Para comprender la utilidad de los tratados entre países, es necesaria una distinción entre el tipo de ataques, para determinar si se trata de una motivación política o no (Kim Andreasson, 2012, capítulo 13). A detalle, en el caso de los ataques sin motivación política, los acuerdos internacionales y la cooperación con el sector privado ayudan a mitigar las amenazas, como son: aquellas de motivación financiera, como las cometidas por ciberdelincuentes, el robo de propiedad intelectual, el fraude digital, así como el hackeo por retribución, diversión o por empleados molestos.

En cambio, será mucho más difícil poder lidiar con amenazas de motivación política, aquellas realizadas por gobiernos o con su apoyo, como son: la ciberguerra, el ciberterrorismo, espionaje y "hacktivismo" (hackeo con fines políticos). Un caso reciente de este tipo ocurrió contra la embajada de México en Guatemala, en este año de 2019, la cual fue víctima de un "hackeo", donde más de 4,800 documentos fueron comprometidos, incluyendo copias de pasaportes, visas y cartas confidenciales de ciudadanos y diplomáticos mexicanos que viven en la capital guatemalteca (Ruiz, 2019).

De la unipolaridad a un mundo de cuatro potencias

Cuando se analiza la cantidad de Infraestructuras Críticas de Información y Telecomunicaciones de los diferentes países en el mundo, puede observarse una correlación directamente proporcional con respecto a aquellas naciones protagonistas en el "teatro de operaciones" cibernético.

Uno de los principales elementos de soberanía en telecomunicaciones consiste en la operación de satélites para uso militar o de gobierno. Al momento de la elaboración del presente documento, existe un aproximado de 2,062 satélites en operación en la órbita terrestre, de los cuales 992 corresponden a satélites activos de uso militar, de gobierno o compartido entre ambos, con uso civil o comercial, cuyos países encargados de su operación son los siguientes:

Cuadro 1
Satélites activos de uso militar, de gobierno o compartido

RANK	PAÍS	SATÉLITES	PORCENTAJE
1	EUA	333	34%
2	China	218	22%
3	Rusia	123	12%
4	India	51	5%
5	Japón	35	4%
6	Multinacional	23	2%
7	Agencia Europea	22	2%
8	Alemania	14	1%
9	Francia	12	1%
10	Reino Unido	11	1%
11	Corea del Sur	9	1%
12	España	9	1%
13	Israel	9	1%
14	Italia	8	1%
15	Arabia Saudita	6	1%
	TOTAL	**992**	**100%**

Elaboración propia, Vestiga Consultores, mayo 2019. Con base en datos de satélites de la Union of Concerned Scientists (UCS), marzo 2019.

En caso de que continuáramos el listado, México aparece hasta el lugar 28, con sólo 2 satélites de uso militar o de gobierno: Mexsat-3 (Mexsat Bicentenario, desarrollado por Orbital Sciences Corp, número Norad 39035) y Mexsat3 (Morelos-3, desarrollado por Boeing Satellite Systems, número Norad 40946). Dadas las características y necesidades de telecomunicaciones en el país, como ha sido el llamado de la nueva administración federal para proveer de Internet a todo el territorio nacional, México requeriría cuando menos de 4 satélites adicionales, independientemente de las redes de fibra óptica y las antenas instaladas por parte de las compañías de telefonía e Internet en el país.

Como puede observarse en la tabla anterior de infraestructura de satélites en operación, los cuatro países con mayor presencia también son las 4 potencias que disputan actualmente las principales estrategias geopolíticas en el mundo: Estados Unidos, China, Rusia e India.

Estas cuatro naciones también tienen un papel destacado en el gasto militar mundial en 2018, el cual ha sido el año de mayor inversión militar en la historia:

Cuadro 2
Gasto militar mundial en 2018

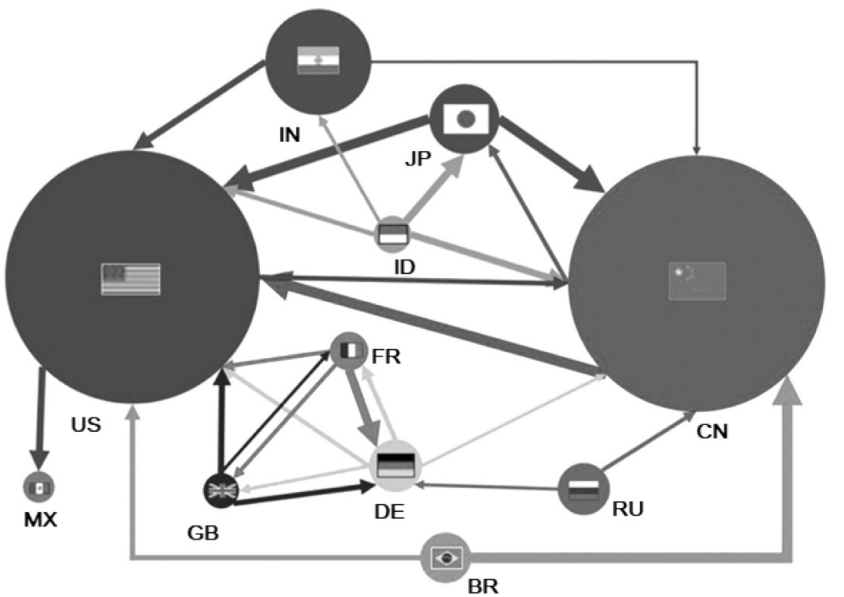
RANK	PAÍSES	GASTO (USD BN)	% PIB
1	Estados Unidos	649	3.2
2	China	250	1.9
3	Arabia Saudita	68	8.8
4	India	67	2.4
5	Francia	64	2.3
6	Rusia	61	3.9
7	Reino Unido	50	1.8
8	Alemania	49	1.2
9	Japón	47	0.9
10	Corea del Sur	43	2.6
11	Italia	28	1.3
12	Brasil	28	1.5
13	Australia	27	1.9

RANK	PAÍSES	GASTO (USD BN)	% PIB
14	Canadá	22	1.3
15	Turquía	19	2.5
	Total mundial	**1,822**	**2.1**

SIPRI (Stockholm International Peace Research Institute), en: Nan Tian, *et. al.*, *Trends in World Military Expenditure.*

Para comprender la dinámica e interdependencia actual entre las potencias mencionadas, hemos elaborado un diagrama con las principales relaciones comerciales entre estos países. En este diagrama, mientras el tamaño de los círculos representa la dimensión de cada economía (por paridad de poder adquisitivo), el tamaño de las fLechas indica el tipo de relación comercial (importaciones o exportaciones), así como el valor de las mismas.

Figura 1
Relación comercial de 11
principales economías exportadoras



Elaboración propia, Vestiga Consultores. Con base en datos del *Factbook 2012* de la Agencia Central de Inteligencia, Estados Unidos.

Esta correlación de fuerzas cambiará poco en las próximas décadas. De acuerdo a la firma PriceWaterhouseCoopers (PwC, febrero 2015), junto con Indonesia y Nigeria, México es una de las 3 economías emergentes que integrarán el listado de las 10 principales economías entre 2030 y 2050:

Figura 2
Proyección de 10 principales economías 2050

	2014		2030		2050	
PPP rank	*Country*	*GDP at PPP (2014 US$bn)*	*Country*	*Projected GDP at PPP (2014 US$bn)*	*Country*	*Projected GDP at PPP (2014 US$bn)*
1	China	17,632	China	36,112	China	61,079
2	United States	17,416	United States	25,451	India	42,205
3	India	7,277	India	17,138	United States	41,384
4	Japan	4,788	Japan	6,006	Indonesia	12,210
5	Germany	3,621	Indonesia	5,486	Brazil	9,164
6	Russia	3,559	Brazil	4,996	Mexico	8,014
7	Brazil	3,073	Russia	4,854	Japan	7,914
8	France	2,587	Germany	4,590	Russia	7,575
9	Indonesia	2,554	Mexico	3,985	Nigeria	7,345
10	United Kingdom	2,435	United Kingdom	3,586	Germany	6,338
11	Mexico	2,143	France	3,418	United Kingdom	5,744

PwC, febrero 2015. PIB proyectado en PPP.

Debido a estas proyecciones, se sabe que aumentará el valor geopolítico de México ante el mundo, y por tanto, podrían aumentar los ataques cibernéticos en contra del país y sus intereses comerciales.

Estado del arte en México y problemas estructurales

Bajo el contexto mundial que aborda el presente documento, el 1 de junio de 2016 en México se crea el Centro de Operaciones del Ciberespacio de la Secretaría de la Defensa Nacional. Parte de las capacidades ampliadas del gobierno mexicano se ha reflejado recientemente, por ejemplo, en operativos de la Secretaría de Marina, para el arresto de líderes de cárteles del narcotráfico, los cuales se habrían logrado mediante la intercepción de comunicaciones de aplicaciones de mensajería, tales como Whatsapp y Telegram, apoyados por tecnología americana e israelí,

como puede ser aquella que se basa en explotar las vulnerabilidades del código SS7, técnica reciente que usan los hackers de élite mundial para romper la "doble autentificación" de los usuarios.

Un esquema básico del sistema de ciberseguridad nacional, fue presentado recientemente para el Instituto de Investigaciones Estratégicas de la Armada de México[1], como puede verse a continuación:

Figura 3
Posible organigrama de la Seguridad Nacional Cibernética en México

Adolfo Arreola (2018), Secretaría de Marina.

A nivel mundial el esquema de defensa cibernética que se sigue es el establecido por los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), los cuales surgen como respuesta de DARPA ante el primer

1 Adolfo Arreola García, Ciberseguridad Nacional en México y sus desafíos. Instituto de Investigaciones Estratégicas de la Armada de México, Secretaría de Marina. Septiembre 2018, pp. 28

malware de la historia en 1988 (“Morris worm”, el cual infectó casi 10% de las 66 mil computadoras que en aquel entonces conformaban Internet).

> En un trabajo reciente de Rodrigo Riquelme (2018), se explica que:
> en el mundo sólo existen dos CERT como tal: uno es el CERT/CC (CERT Coordination Center), que forma parte del Instituto de Ingeniería en Software de la Universidad de Carnegie Mellon, en Pennsylvania, Estados Unidos, y el otro es el US-CERT, el equipo de respuesta del Departamento de Seguridad Nacional estadounidense.
>
> En todos los demás países del mundo, a los equipos de ciberseguridad se les denomina Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por su sigla en inglés), los cuales al obtener la certificación que ofrece la Universidad de Carnegie Mellon pueden incluir en su nombre la sigla CERT. Además, es necesario distinguir entre los CSIRT que pertenecen a instituciones públicas, como es el caso del CERT - UNAM, y aquellos que forman parte de la oferta de empresas privadas, como puede ser el CERT - IQSec.

De esta manera, tenemos la siguiente lista de defensas cibernéticas de México:

CSIRTs públicos (Equipo de Respuesta ante Incidentes de Seguridad Informática):

1. CSIRT de la Universidad Nacional Autónoma de México (CERT UNAM)
2. CSIRT de la Policía Federal (CERT MX)
3. CSIRT de la Universidad Autónoma de Chihuahua (CERT UACH)
4. CSIRT del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (CERT Infotec)

CERTs privados (Equipos de Respuesta ante Emergencias Informáticas):

1. CSIRT de Scitum (Scitum CERT)
2. CSIRT de IQSec (IQSec CERT)

3. CSIRT de Total Sec (CERTDSI Totalsec)
4. CSIRT de Netrix (CERT Ntx)
5. CSIRT de Global CyberSec (GCS CERT)
6. CSIRT de Mnemo (Mnemo CERT)
7. CSIRT de TIC Defense (TIC CERT)

A pesar de la existencia de los once centros de monitoreo cibernético mencionados, con base en diez años de experiencia con participación personal directa en investigaciones o análisis post-mortem de incidentes cibernéticos, podemos considerar que México se enfrenta cuando menos a los siguientes problemas estructurales particulares.

A. Ausencia de capital humano

A nivel de todas las ingenierías, se sabe que México tiene un déficit de 2 millones de profesionistas, el cual sería cubierto hasta dentro de 14 años. Por esta razón, el país es el principal importador de mano de obra calificada de toda Iberoamérica.

En la industria de seguridad cibernética, esta carencia de personal calificado deja expuestas a las organizaciones públicas y privadas. Este factor se agrava cuando en algunas industrias no se comparte la información suficiente sobre nuevos riesgos. El caso más reciente fue el hackeo a Bancomext, con un monto defraudado por 30 millones de dólares. Este ataque fue realizado por el colectivo Lazarus, y dado a conocer hasta enero de 2018. De acuerdo a las autoridades mexicanas, al menos durante 500 días más de 30 equipos de cómputo habrían sido infectados por el mismo malware que usó este colectivo para atacar a la empresa Sony, así como a otros bancos en el sudeste asiático. En México, de acuerdo a contactos de la industria, dos años antes del ataque a Bancomext, cuando menos 2 bancos privados ya tenían conocimiento de los intentos de ataque en el país, pero los detalles técnicos no fueron compartidos a tiempo.

B. Cárteles de crimen organizado

Debido a la proliferación de actividades de los grupos de crimen organizado en México, desde hace más de una década se sabe que varias células de los mismos están dedicadas al secuestro o reclutamiento de grupos de ingenieros o empleados de empresas de sectores clave,

como son las entidades financieras del país. El mayor caso al respecto ha sido el hackeo al sistema de SPEI (Sistema de Pagos Electrónicos Interbancarios) en el primer semestre de 2018. De acuerdo a información interna de algunas de las empresas afectadas, sabemos que cuando menos 3 mil cuentas de cada banco fueron empleadas en toda la República Mexicana, las cuales en promedio tenían más de 4 años de existencia, para poder distribuir el dinero que se fue extrayendo de la alteración a la operación del SPEI. En muchos de estos casos, más que un hackeo externo, existe complicidad por parte de empleados que son contratados o extorsionados por los cárteles del narcotráfico. Fue ahora en mayo de 2019 que habría sido capturado el líder de la célula que organizó esta operación, con cuentas y activos físicos por 250 millones de pesos.

C. Robo de identidad

Un problema recurrente en el país es el robo de identidad, e incluso las entidades financieras se enfrentan al reto de poder comprobar la documentación que presentan los clientes para "aperturar" nuevas cuentas. Este tema afecta en particular a las empresas dedicadas a otorgar préstamos o créditos, ya sea financieros o para adquirir algún inmueble o bien mueble. Hasta donde tenemos entendido, las compañías reciben documentación que incluso es oficial, pero no corresponde a la identidad real de la persona. Al respecto, al interior del INE (Instituto Nacional Electoral), instancia que otorga el principal documento de identificación en México, existe una deliberación con respecto a cómo mejorar los procesos de comprobación de identidad, así como del almacenamiento de la misma. En años recientes, una de las principales tecnologías que ayudarían al respecto es el BlockChain (Cadena de bloques): existen programas de Naciones Unidas, como el de entrega de alimentos, donde se apoyan en registros biométricos, para asignar un BlockChain infalsificable, por ejemplo, a desplazados de zonas de guerra que ya no poseen documentación oficial alguna.

D. Carencia de estándares ISO 27000 (ISO/IEC 27001:2005)

De un enfoque heurístico, el elemento de mayor riesgo en la seguridad cibernética lo representa el factor humano,

y para el caso de México las organizaciones se enfrentan a la baja educación tecnológica. A ello debe añadirse el desconocimiento de las mejores prácticas de seguridad de la información del ISO 27000 (ISO/IEC 27001:2005). Prueba de ello lo representan los casos de ataque tipo "spear-phishing", los cuales son los mayores tipo de defraudación en el país, donde el atacante envía un correo apócrifo haciéndose pasar por una persona u organización legítima, con tal de solicitar un pago o transferencia bancaria. Técnicamente, para evitar este engaño, basta con analizar el código fuente del correo electrónico recibido, para determinar si se trata de un servidor legítimo; no obstante, es muy reducido el número de usuarios con la capacidad para realizar dicho análisis.

Actual monitoreo sobre México desde el Pentágono

A nivel de industria, la clasificación del nivel de severidad de un ataque cibernético es parecida a los 5 niveles con que se clasifica la fuerza de un huracán, siendo el nivel 5 el de mayor afectación a la infraestructura crítica de un país, donde puede quedar sin energía eléctrica en regiones del mismo o en todo su territorio, como ha sucedido en Ucrania.

El ataque que sufrió Bancomext recientemente se califica entre los niveles 2 y 3. México no ha recibido un ataque de mayor potencia debido a que las infraestructuras críticas del país son protegidas por el Comando Norte de Estados Unidos (United States Northern Command), el cual incluye a toda la Unión Americana y Canadá. El anterior encargado de esta zona militar fue el general John Kelly, anterior jefe de gabinete del Presidente Donald Trump.

A nivel digital, Estados Unidos cuenta con el Comando Cibernético (US Cyber Command), el cual fue creado en 2009 para funcionar bajo el cobijo de la NSA. El Cibercomando americano centraliza las operaciones del gobierno en el ciberespacio, ya sea para organizar recursos cibernéticos o coordinar la defensa y ataque de redes militares.

A partir de la llegada de la actual administración de Estados Unidos, existen 3 cambios radicales en la política de Seguridad Nacional Cibernética de este país:

1. Comando Cibernético (US Cyber Command)
   - El Cibercomando es elevado de rango, al nivel de una Secretaría, con lo cual sale de la esfera de la NSA.
   - Este Comando ya cuenta con autorización para realizar ataques preventivos y no sólo de monitoreo o reacción.
2. Departamento de Seguridad Nacional (Department of Homeland Security)
   - Se crea una Unidad especial dedicada a la protección de las Infraestructuras Críticas del país.
   - Se presta especial interés a las instalaciones eléctricas.
3. Fuerza Espacial (Space Force)
   - Se destina un presupuesto y personal para la defensa satelital, frente a los posibles ataques fuera de órbita de Rusia, China o India.
   - Se enfoca el calendario de la NASA para tener misiones tripuladas tanto a la Luna como a Marte en la presente década.

Estas estrategias de Seguridad Cibernética Nacional de Estados Unidos están apoyadas con una red de empresas líderes de la industria de armamento y seguridad, como son: Lockheed Martin, Raytheon, Boeing, Northrop Grumman, General Dynamics, BAE Systems, etcétera. Asimismo, en capital humano, la planeación y ejecución de las estrategias se llevan a cabo por consultoras privadas tales como Booz Allen Hamilton, Leidos, McKinsey, entre otras.

Además, dichas estrategias de Seguridad Cibernética Nacional, están acompañadas por la guerra comercial de Estados Unidos en contra de China. Debe mencionarse que las medidas en contra de empresas chinas no comenzaron con el gobierno de Donald Trump: desde 2016 el Pentágono prohibió el uso de laptops Lenovo, por contener microcomponentes de espionaje; en 2017 se restringió la venta del antivirus Kaspersky incluso en tiendas como BestBuy, porque su creador reconoció el robo de secretos

militares americanos; y han sido más difundidos desde 2018 las medidas en contra de Huawei, desde la captura de su CFO e hija del fundador, así como el reciente bloqueo de suministros a esta empresa por parte de tecnológicas americanas como Google o Intel.

Para el caso de México, tanto los ex presidentes Felipe Calderón así como Enrique Peña, junto con otros 35 líderes mundiales, fueron intervenidos en sus comunicaciones por parte de la NSA (mediante su unidad SATC), lo cual fue revelado en una serie de documentos filtrados por el ex ingeniero de esta agencia, Edward Snowden.

Figura 4
Documento filtrado por Edward Snowden
Publicado por Electronic Frontier Foundation, 2013

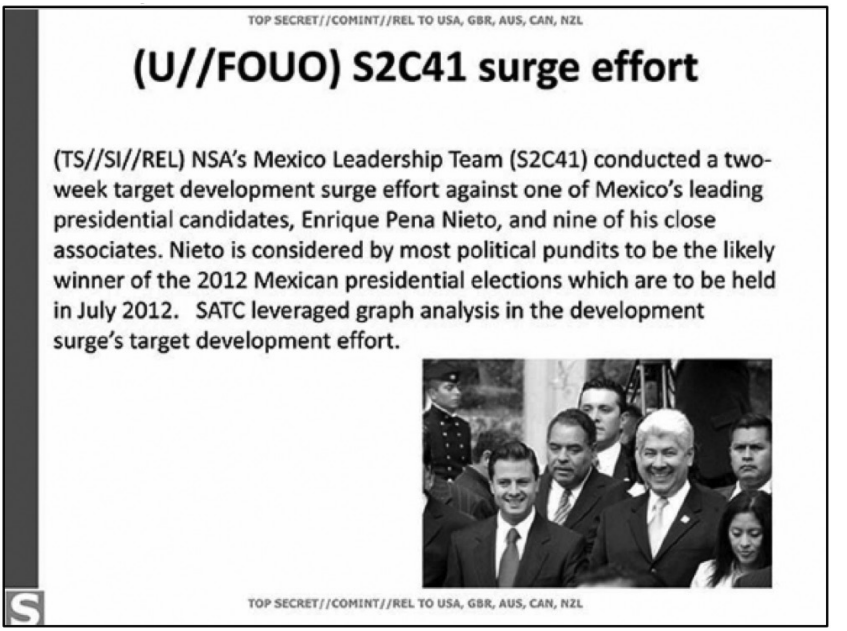
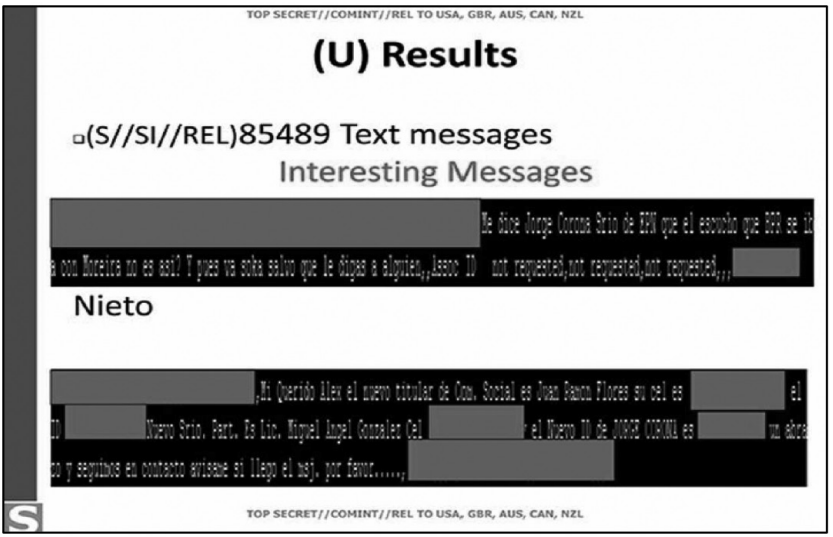


Figura 5
Documento filtrado por Edward Snowden
Publicado por Electronic Frontier Foundation, 2013



Como puede verse en la evidencia anterior, diversos mensajes de México fueron interceptados, en este caso sobre un encuentro con el entonces Gobernador de Coahuila, Humberto Moreira, con respecto al señor Jorge Corona, en su momento secretario auxiliar del entonces Gobernador Enrique Peña, y actualmente diputado federal.

Esta información de inteligencia obtenida por la NSA es compartida con los "FiveEyes": Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda, con quienes el gobierno americano comparte más información.

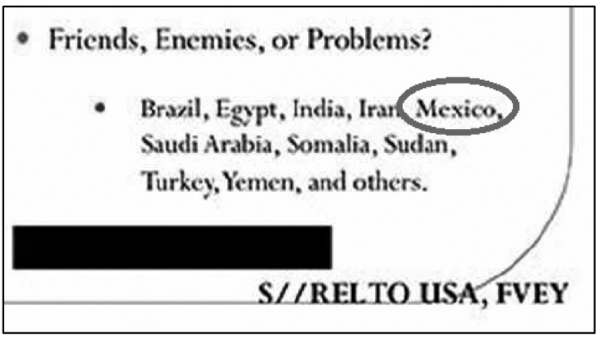
En el mismo documento publicado por la Electronic Frontier Foundation (2013, p.19), puede leerse un apartado llamado "Geopolitical Trends: Key Challenges", en donde se describe el objetivo del monitoreo sobre México:

> Algo que une a todos estos países es su importancia para intereses económicos, de comercio y defensa de Estados Unidos (...) (esta división) se enfoca

> principalmente en la política exterior y actividades comerciales de Bélgica, Francia, Alemania, Italia y España, así como Brasil, Japon y Mexico. Los reportes de esta División también proveen información clave sobre actividades militares y de inteligencia en algunos de estos países.

Además, en el apartado "Factores de estrés sobre la estabilidad regional/Ascenso de nuevos actores", al país se describe de la siguiente manera: "Mexico está estresado, e impacta en nuestra frontera". Debido a este contexto, en la proyección que maneja la NSA, a nuestra nación se le ubica en un bloque entre posibles "amigos, enemigos o problemas":

Figura 6
Documento filtrado por Edward Snowden
Electronic Frontier Foundation, 2013



Finalmente, debe señalarse que la función de la NSA no ha sido sólo de monitoreo: de acuerdo a la información obtenida por Edward Snowden, y revelada en diferentes entrevistas (como lo ha sido la producción de Oliver Stone, y una serie de 4 horas de entrevistas de Stone con el Presidente de Rusia), parte de la información obtenida por la NSA ha sido usada por Estados Unidos no sólo por temas de seguridad nacional, sino para negociaciones de tratados comerciales; adicionalmente, la NSA contaría con dispositivos y códigos al interior de las infraestructuras críticas de varios de sus "aliados" (como son Alemania, Japón y México), para sabotear la energía o telecomunicaciones de estos países en caso de una disputa con Estados Unidos.

Propuestas de Reformas periodo 2018-2024

En México han existido cuatro relevantes momentos en el desarrollo de una estructura de seguridad cibernética, con la creación de diferentes dependencias en los siguientes años:

- 2001: PFP, «Policía Cibernética Federal»
- 2013: CDMX, «Policía Cibernética»
- 2016: Ejército, «Centro de Operaciones del Ciberespacio»
- 2017: PGR, «Unidad de Investigaciones Cibernéticas»

No obstante, estas iniciativas siguen rezagadas, al menos con respecto a los años de creación de los principales referentes en Estados Unidos:

1952: National Security Agency (criptografía)
1978: FISA (Foreign Intelligence Surveillance Act)
2009: United States Cyber Command

Parte de los retos en México parten desde el Poder Legislativo, debido a la ausencia de una Ley federal de delitos cibernéticos, frente al debate actual que existe en Inglaterra y China, en donde están aprobando nuevas leyes sobre ámbito de seguridad cibernética (con respecto a exigir "back doors" a las empresas tecnológicas, o ampliar la recolección de "meta data" de los habitantes).

Recién en marzo de 2019 en el Senado de la República, la fracción del partido Morena hizo pública una propuesta de "Ley de Seguridad Informática" (Senadora Lucía Trasviña, 2019). En esta iniciativa se plantea la creación de una Agencia Nacional de Seguridad Informática (ANSI), la cual proteja la "Infraestructura Información (sic) Esencial", ante posibles actos de: espionaje, sabotaje, terrorismo, rebelión o "traición a la patria". En este sentido, se incluyen como agravantes aquellos ataques en contra del "Estado", así como en contra de entidades financieras, con multas de hasta 136 mil pesos. En un primer análisis de esta iniciativa, y a reserva de que el debate parlamentario modifique su esencia y alcances, de nueva cuenta se parte de una concepción que confunde la "seguridad informática" con respecto de la "seguridad de la información", y no se

detallan cuáles serían aquellas infraestructuras críticas a proteger.

Una de las leyes más avanzadas en la materia se aprobó este año en India, donde se obliga a las empresas extranjeras de tecnología (como Amazon, Google, Facebook, etc.), a procesar los datos de los usuarios locales en servidores ubicados físicamente en territorio de la India. De esta manera, la nueva Ley de la India aumenta su "soberanía cibernética", al permitir la realización de procesos legales en contra de las empresas de tecnología ante alguna disputa comercial, de protección de datos, etc. Esta situación no ocurre actualmente en México, debido a que la "extra territorialidad" bajo la que operan estas empresas, obliga a que los usuarios mexicanos presentaran las demandas pero en Estados Unidos.

Elementos para primer atlas de riesgos cibernéticos

Las dependencias potencialmente involucradas en una nueva estrategia de seguridad nacional cibernética requieren mejorar su nivel de tecnología y recursos humanos, para salir de un momento de desmantelamiento que han padecido cuando menos en las recientes 3 administraciones federales.

Existen casos dramáticos que documentan esta situación: en 2015 se filtraron los archivos de una empresa de ciberseguridad italiana "HackerTeam", en cuyos correos internos hicieron mofa de que los servidores del CISEN (Centro de Investigación y Seguridad Nacional) ni siquiera contaban con un FireWall instalado; para la tercera captura del narcotraficante Joaquín "Chapo" Guzmán en 2016, el operativo de la Marina tuvo en todo momento el apoyo de la DEA (Drug Enforcement Administration), pero con intercepción de mensajes y llamadas desde Estados Unidos; desde 2016 se hicieron públicas filtraciones de contratos de dependencias como PGR (Procuraduría General de la República), PFP (Policía Federal Preventiva) o el propio CISEN, para usar software de espionaje de la empresa de Israel NSO (famosa por el malware "Pegasus"), cuyos resultados en México fueron limitados, pero costosos.

Para establecer una primera línea de fuego ante los riesgos de seguridad nacional cibernética en México, se

requiere instrumentar el esquema C4ISR, por sus siglas en inglés, que implica: Comando, control, comunicaciones, computadoras e inteligencia, vigilancia y reconocimiento. En el documento más reciente de Estrategia de Defensa Nacional de Estados Unidos (Departamento de la Defensa, 2018), se establece como prioridad el fortalecimiento del C4ISR, entendida esta estrategia como el desarrollo de redes y ecosistemas de información resilientes, constantes, a nivel federal, desde el nivel táctico hasta la planificación estratégica. Esta estrategia también da prioridad a las capacidades para obtener y explotar información, negarles a los competidores las mismas ventajas, y permitan proporcionar atribuciones para responsabilizar a los actores estatales o no estatales culpables durante los ataques cibernéticos.

Adaptándose a la nueva realidad internacional, México necesita establecer un mapa de los siguientes sectores que son definidos como críticos:

Sectores de Infraestructuras Críticas

1. Entidades financieras
2. Instalaciones de comercio y logística
3. Parques críticos de manufacturas
4. Dependencias de gobierno
5. Hospitales y centros de salud
6. Universidades y escuelas
7. Defensa y seguridad nacional
8. Instalaciones eléctricas
9. Abasto energético y gasoductos
10. Sistemas de telecomunicaciones
11. Sistemas de transporte
12. Cobertura de red satelital
13. Plantas de químicos y petroquímica
14. Servicios de emergencias
15. Centrales de represas e hidroeléctricas
16. Sistemas de aguas y tratamiento
17. Producción de alimentos
18. Centros nucleares y de materiales peligrosos

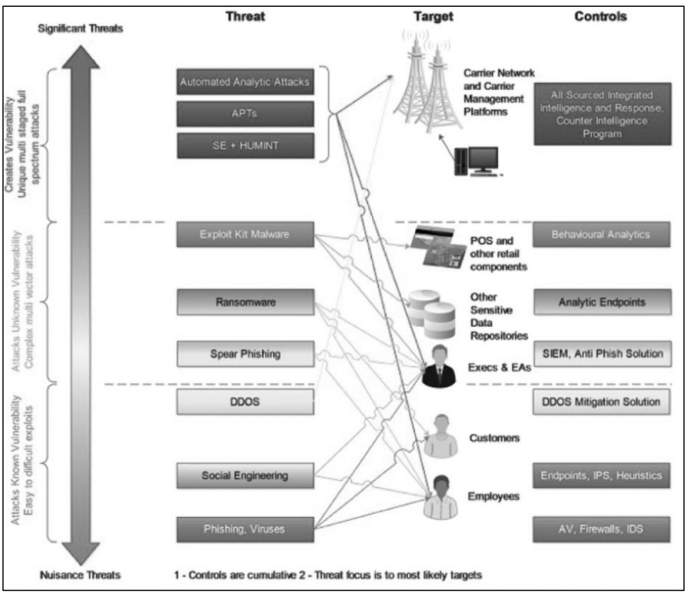
Debe observarse que cuando menos el 85% de estas Infraestructuras Críticas se encuentran en empresas del sector privado, por lo cual resulta indispensable la sinergia de esfuerzos. Algunas tendencias que incrementan los

riesgos en estos sectores son: interdependencia entre los mismos sectores, proliferación de puntos expuestos, y concentración de activos.

Como ejemplo de algunos de los elementos del Atlas Nacional de Riesgos Cibernéticos, hemos integrado un listado de las organizaciones, escuelas, empresas y gobiernos estatales más atacados por *hackers* en México. Para ello, parte de nuestra metodología se apoya en el análisis de Cómputo Forense de diferentes campañas de *phishing* y *malware* que han atacado a usuarios nacionales, así como la revisión de directorios con muestras de ataques cibernéticos a servidores mexicanos en los últimos 5 años.

El Atlas de riesgos cibernéticos resulta indispensable para poder mapear las amenazas a todas las Infraestructuras Críticas del país. Los ataques pueden venir desde la parte más alta del sistema, directamente en contra de la infraestructura física, o con ataques sobre los usuarios de la misma, como puede apreciarse en el siguiente diagrama:

Figura 7
Controles según cada tipo de amenaza cibernética



Greg Reith, *Recorded Future,* 2017.

Para poder proteger a las infraestructuras críticas del país, se requiere instrumentar en todas las dependencias de gobierno directamente relacionadas las siguientes capas de seguridad cibernética:

Capas de seguridad cibernética

1. Dispositivos (seguridad Endpoint, cifrados)
2. Aplicativos (BMS, bases de datos, web)
3. Datos (control de acceso, autenticación, administración de claves)
4. Red (firewalls, DMZs, VPNs, segmentaciones)
5. Perimetral (filtros de Internet, monitoreo de amenazas)
6. Física (guardias, candados)

Conclusiones

Como se ha expuesto en el presente documento, el papel geopolítico de México seguirá creciendo en valor en las próximas décadas, debido a su relación comercial con las principales potencias del mundo. Debido a ello, resulta previsible un aumento en los ataques en contra de las Infraestructuras Críticas del país. Si bien actualmente muchos de estos activos se encuentran bajo monitoreo de diferentes dependencias de Estados Unidos, existen problemas estructurales específicos que aumentan el nivel de riesgo en México, como lo es la presencia de grupos de crimen organizado y la falta de personal altamente capacitado.

Adicionalmente, existen elementos indispensables para la elaboración de un primer Atlas de riesgos para la Seguridad Nacional Cibernética:

- Taxonomía de incidentes cibernéticos frecuentes en México
- Medidas para prevenir y combatir incidentes cibernéticos
- Prácticas de ISO 27000 (desde ISO/IEC 27001:2005) para resiliencia e higiene cibernéticas
- Documentación y protocolos para protección legal
- Nueva Protección de Datos de Unión Europea (GDPR)

- Nueva iniciativa nacional para la educación en Ciberseguridad (NICE, por sus siglas en inglés), del National Institute of Standards and Technology (NIST), del Departamento de Comercio de los Estados Unidos

La cooperación entre sectores será una de las principales vías en la cual México pueda aumentar su resiliencia cibernética, como lo es: a nivel Gobierno, fortalecer sus capacidades de reacción, defensa y contraataque, para proteger las Infraestructuras Críticas; a nivel de Universidades, se requiere mayor investigación y capacitación de profesionistas; a nivel de Empresas, se necesita ampliar la cantidad de programas de monitoreo e innovación, así como promover la autoeducación como primera línea de defensa de la nación.

BIBLIOGRAFÍA

Agencia Central de Inteligencia. *The CIA World Factbook*. Virginia, Estados Unidos [Consultado en https://www.cia.gov/library/publications/the-world-factbook/].

Agencia de Seguridad Nacional (unidad SATC). *Intelligently filtering your data: Brazil and Mexico case studies*. Maryland, Estados Unidos. Difundido en el sitio de *Electronic Frontier Foundation* [Consultado en https://www.eff.org/files/2013/11/15/20130903-globo-satc.pdf].

Andreasson, Kim. *Cybersecurity: Public Sector Threats and Responses*. Florida, Estados Unidos. CRC Press. 2012, pp. 392.

Archer, Joseph. "US, Russia and China refuse to back French cybersecurity initiative". *The Telegraph*. Noviembre, 2018 [Consultado en https://www.telegraph.co.uk/technology/2018/11/12/us-russia-china-refuse-back-french-cybersecurity-initiative/].

Arreola García, Adolfo. "Ciberseguridad Nacional en México y sus desafíos". México. Instituto de Investigaciones Estratégicas de la Armada de México, Secretaría de Marina. Septiembre 2018, pp. 28 [Consultado en https://www.researchgate.net/publication/329253059].

Budapest Convention, *The Convention on Cybercrime of the Council of Europe*. Consejo de Europa. 2004 [Consultado en https://www.coe.int/en/web/cybercrime/the-budapest-convention].

Calder, Alan. *Information Security based on ISO 27001/ISO 27002*, Londres, Reino Unido. Van Haren Publishing. 2009, pp. 102.

Departamento de la Defensa. *2018 National Defense Strategy*. Estados Unidos, Virginia. 2018 [Consultado en: https://dod.defense.gov/Portals/1/ Documents/ pubs/2018-National-Defense-Strategy-Summary.pdf].

Departamento de la Defensa. *The Military Dictionary (Dictionary of Military and Associated Terms)*. Virginia, Estados Unidos. DIANE Publishing. 1987, pp. 399.

France Diplomatie. *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Paris, 2018 [Consultado en: https://www.diplomatie.gouv.fr/en/ french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in].

Presidencia de la República. *Estrategia Nacional de Ciberseguridad*. México, 2017 [Consultado en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf].

PriceWaterhouseCoopers. *The World in 2050. Will the shift in global economic power continue?*, febrero 2015, pp. 46 [Consultado en https://www.pwc.com/gx/en/issues/ the-economy/assets/world-in-2050-february-2015.pdf].

Reith, Greg. "Prioritizing Cyber Threats With Real-Time Threat Intelligence". Recorded Future. Agosto, 2017 [Consultado en https://www.recordedfuture.com/ prioritizing-cyber-threats/].

Riquelme, Rodrigo. "¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?". *El Economista*. Enero, 2018 [Consultado en https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html]

Rollins, John. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. Washington DC, Estados Unidos. DIANE Publishing. Marzo 2009, pp. 18.

Ruiz, Claudia. "Embajada de México en Guatemala es víctima de un hackeo". *CNET*. Abril 2019 [Consultado en https://www.cnet.com/es/noticias/embajada-de-mexico-en-guatemala-es-victima-de-un-hackeo-reporte/].

Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge, Reino Unido. Cambridge University Press. 2015, pp. 269.

Tian, Nan, et. al., *Trends in World Military Expenditure*. SIPRI (Stockholm International Peace Research Institute). Abril, 2019.

Trasviña, Lucía. *Propuesta de Ley de Seguridad Informática.* México, Senado de la República, 2019, pp. 17 [Consultado en http://blog.derecho-informatico.org/wp-content/uploads/2019/03/20190319_PropuestaMorena_LSI.pdf].

Union of Concerned Scientists (UCS), *UCS Satellite Database*, marzo 2019 [Consultada desde https://s3.amazonaws.com/ucs-documents/nuclear-weapons/sat-database/5-9-19-update/UCS_Satellite_Database_4-1-2019.xlsx].

Revista de Administración Pública

INAP

Ciberseguridad y la gobernanza multistakeholder

Fátima Cambronero

Resumen: La relación existente entre la gobernanza de Internet y la ciberseguridad puede centrarse en la aplicación de los principios que rigen al primer concepto y extrapolarlos a la gobernanza de la ciberseguridad: la participación en pie de igualdad de los múltiples actores interesados en las discusiones y toma de decisiones, en procesos de abajo hacia arriba basados en el consenso, en una estructura horizontal de administración.

En el presente trabajo se analizarán las políticas públicas y las estrategias nacionales de ciberseguridad a la luz de los principios de la gobernanza multistakeholder, teniendo en cuenta que la ciberseguridad emerge como uno de los grandes temas contemporáneos que atraviesan la agenda de la gobernanza de Internet, así como los sectores de seguridad de diversos países. Encontrar un equilibrio y armonización entre los intereses de ambos regímenes, resulta fundamental para la promoción de una tecnología a favor de los derechos humanos y la innovación.

Palabras clave: gobernanza, multistakeholder, políticas, privacidad, ciberseguridad.

Cybersecurity and multistakeholder governance

Abstract: The relationship between Internet governance and cybersecurity can focus on the application of the principles that govern the first concept and extrapolate them to cybersecurity governance: the equal participation of the multiple actors interested in discussions and taking decisions, in bottom-up processes based on consensus, in a horizontal administration structure.

In this paper, public policies and national cybersecurity strategies will be analyzed in the light of the principles of multistakeholder governance, taking into account that cybersecurity emerges as one of the great contemporary issues that cross the Internet governance agenda, as well as the security sectors of various countries. Finding a balance and harmonization between the interests of both regimes is essential for the promotion of technology in favor of human rights and innovation.

Keywords: governance, multistakeholder, policies, privacy, cybersecurity.

Fecha de recepción: 11 de febrero de 2019
Fecha de aceptación: 25 de marzo de 2019

Revista de Administración Pública

INAP

Ciberseguridad y la gobernanza multistakeholder

Fátima Cambronero*

1. Gobernanza de Internet y ciberseguridad: delimitando el ámbito de análisis

La gobernanza de Internet permite realizar paralelismos con la ciberseguridad por diferentes razones que se expondrán en el presente trabajo. Una de ellas, se encuentra referida a los principios que rigen la gobernanza de Internet y que son relevantes para este ámbito y que pueden ser aplicados a la gobernanza de la ciberseguridad: la participación en pie de igualdad de los múltiples actores interesados en las discusiones y toma de decisiones, en procesos de abajo hacia arriba basados en el consenso, en una estructura horizontal de administración. Es decir, hablar

* Abogada y responsable de Derecho Informático de R10S Abogados, trabaja en temas de gobernanza de Internet, privacidad, protección de datos personales, derechos de los consumidores y nombres de dominio. Es docente en Diplomados y Especializaciones sobre temas de gobernanza de Internet, protección de datos personales y comercio electrónico en ISDI, Universidad Panamericana Guadalajara, Universidad Anáhuac México Sur, entre otras.
Se ha desempeñado en organizaciones nacionales, regionales e internacionales vinculadas a la gobernanza de Internet, tales como el Comité Asesor At-Large (ALAC) de ICANN, en representación de LACRALO (Latin American and the Caribbean Regional At-Large Organization); del Grupo Asesor Multisectorial (MAG) del Foro de Gobernanza de Internet como representante de la sociedad civil; miembro del Comité Asesor del Global Forum on Cyber Expertise (GFCE); del Comité del Programa del LACIGF (Foro de Gobernanza de Internet para América Latina y Caribe) y del Comité del Programa de GigaNet (Global Internet Governance Academic Network); Vice Presidenta del Capítulo Mexicano de la Internet Society (ISOC), entre otros.

de la gobernanza de la ciberseguridad implica pensar en modelos *multistakeholders*, lo cual será profundizado en los siguientes párrafos.

A continuación se realizará un análisis de los principales conceptos a desarrollarse, la tensión existente entre los mismos y la dificultad de trabajar con definiciones uniformes y universalmente aceptadas. Luego se hará un repaso de los principios y normas que deberían informar las políticas de ciberseguridad, las guías y recomendaciones que se han elaborado para diseñar estrategias nacionales de ciberseguridad basadas en modelos *multistakeholders*, poniendo mayor atención en la elaboración de la Estrategia Nacional de Ciberseguridad en México, analizando si la misma ha respetado dicho modelo *multistakeholder*, y el estado actual en el que se encuentra la mencionada estrategia. A continuación se revisarán las implicaciones de la ciberseguridad en cuanto a la privacidad y protección de datos personales de los titulares –ciudadanos digitales–, cerrando el presente trabajo con algunas reflexiones finales, e invitando a los lectores a seguir investigando y desarrollando material relacionado con los temas centrales del mismo.

Como punto de partida, es importante destacar que resulta complicado entender posibles escenarios de análisis y estudio si no se parte de una definición de los conceptos que se van a explorar. Esto se vuelve aún más difícil cuando los conceptos que se intentan definir no son entendidos de la misma manera por los diferentes actores involucrados, cuando en sí mismos son complejos, diversos y con cargas valorativas implícitas diferentes para cada comunidad.

En consecuencia, se vuelve necesario tomar prestadas definiciones de diferentes disciplinas que permitan delimitar el campo de análisis, las cuales serán expuestas en el presente trabajo.

Para entender qué significa la gobernanza de Internet, es necesario remontarse hasta la Cumbre Mundial de la Sociedad de la Información (CMSI, 2003-2005). Si bien en sentido estricto, gobernanza de Internet y gobernanza *multistakeholder* no son conceptos intercambiables, para la definición del segundo, se tomarán las características y elementos centrales del primero.

Vale aclarar que la traducción al español de la expresión "*Internet governance*", de la cual se origina el presente concepto, ocasionó dificultades, en primer lugar, al traducir "*governance*" como gobierno, cuando hay importantes diferencias entre ambos. La expresión "gobierno" hace referencia a una estructura vertical y burocrática de administración, donde se involucra en la misma a un solo actor –gobierno– y donde las decisiones son tomadas por ese solo actor, en procesos de arriba hacia abajo (*top down*), mientras que "gobernanza" implica una estructura horizontal y transversal de administración, involucra la participación de múltiples actores interesados ("*stakeholders*", aquellos que tienen un "*stake*" en juego, un interés) en un pie de igualdad y donde la toma de decisiones se realiza basada en el consenso y en procesos de abajo hacia arriba (*bottom up*).

A los fines de una simplificación, se entenderá como Internet[1], a la red de redes autónomas, comunicadas entre sí con un lenguaje común, el cual es el protocolo TCP/IP.

Para analizar la definición de gobernanza de Internet brindada por el Grupo de Trabajo de Gobernanza de Internet (GTGI), es importante recordar que, en el año 2000, la Organización de las Naciones Unidas (ONU) convocó a la Cumbre del Milenio, la cual consagraba entre sus objetivos aquellos relacionados con la reducción de la pobreza en el mundo, y dentro de las acciones a tomar se incluía la reducción de la brecha digital. Dentro de este contexto y con el apoyo de la Cumbre del Milenio, se llevó a cabo la Cumbre Mundial sobre la Sociedad de la Información, en el seno de las Naciones Unidas y a cargo de su realización por la Unión Internacional de las Telecomunicaciones (UIT).

La UIT recibió de la Asamblea General de la ONU el mandato de realizar la Cumbre Mundial sobre la Sociedad de la Información en dos fases: una en Ginebra en 2003

1 A consideración de la autora y teniendo en cuenta las convenciones adoptadas por la comunidad internacional, al referirse a Internet, siempre se lo hará con letra mayúscula y sin artículo precedente –es una sola red de redes– por entender que escribir "internet" –con letra minúscula– podría hacer referencia a distintas "internets" y a la posibilidad de fragmentación de la red de redes que dicha expresión lleva implícita.

y otra en Túnez en 2005, invocando la participación del sector privado y de la sociedad civil.

En Octubre de 2004 se creó el Grupo de Trabajo de Gobernanza de Internet, formado por convocatoria del Secretario General de la ONU y con mandato de la Asamblea General, a estar integrado por miembros provenientes de los diversos sectores, explícitamente de todos los *stakeholders* en un proceso abierto e inclusivo. Después de unos meses de deliberaciones, el GTGI preparó un informe que sirvió de base para las negociaciones realizadas en la segunda fase de la CMSI, llevada a cabo en Túnez. Los resultados más importantes de la fase de Túnez fueron, por un lado, haber elaborado una definición operacional o de trabajo de gobernanza de Internet, a propuesta del GTGI, que es tomada posteriormente por los foros e iniciativas donde participan los distintos actores involucrados en ella[2]. Dicha definición de gobernanza de Internet quedó plasmada en el párrafo 34 de la Agenda de Túnez para la Sociedad de la Información, donde se establece:

> *34. Una definición de trabajo de la gobernanza de Internet es desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet (Agenda de Túnez para la Sociedad de la Información, 2005).*

Hubo consenso en la comunidad internacional, en entender que en esos momentos, ésta fue la mejor definición a la que se podía arribar y acordaron revisar la misma en futuros trabajos, por esto fue entendida como una definición operacional o de trabajo. Sin embargo, a quince años de dicha definición, no ha logrado ser superada por ninguna otra, aun cuando también haya consenso en entender que la misma pueda ser deficiente o incompleta y cuando se hayan creado diferentes grupos de trabajo para ocuparse de este asunto.

2 Cambronero, F. (14 de mayo de 2013). *El MAG y el IGF.* [Mensaje en un blog]. Fatima Cambronero. [Online] Recuperado de https://fatimacambronero.com.ar/2013/05/14/el-mag-y-el-igf/

Entre algunas de aquellas críticas respecto de la definición bajo análisis, se ha indicado que en la misma no se incluye a todos los *stakeholders* –sólo se hace referencia a los gobiernos, al sector privado y a la sociedad civil–; que no queda claro qué significa "en el desempeño de sus respectivos papeles"; que si entonces los diferentes espacios dedicados a atender temas vinculados a la gobernanza de Internet sólo se refieren a mecanismos de toma de decisiones, entre otros puntos.

Enfocarse en analizar estos diferentes cuestionamientos excede el objetivo del presente trabajo, por lo que sólo se mencionará un aspecto de los mismos.

En relación a los diferentes *stakeholders* involucrados en la definición de gobernanza de Internet provista por el GTGI, es importante recordar lo que establece el párrafo 35 de la citada Agenda de Túnez para la Sociedad de la Información, que dispone:

> *35. Reafirmamos que la gestión de Internet abarca cuestiones técnicas y de política pública y que en ella deberían participar todas las partes interesadas y las organizaciones intergubernamentales e internacionales relevantes.*
> *[…] (Agenda de Túnez para la Sociedad de la Información, 2005).*

Es decir, si bien en la definición incluida en el referido párrafo 34, no se menciona a la comunidad técnica, sería absurdo no reconocerla con dicha calidad. Lo mismo para las organizaciones intergubernamentales e internacionales y la comunidad académica, que en muchos espacios sigue estando asociada a la comunidad técnica.

En años recientes, algunos grupos de actores participantes de la *Internet Corporation for Assigned Names and Numbers* (ICANN), han insistido en incluir además, y como un *stakeholder* separado de la sociedad civil organizada, a los usuarios finales de Internet. Si bien no hay consenso en adoptar esta categoría independiente, los argumentos para sostener dicha separación han ido ganando peso en espacios como el *At-Large Advisory Committee* (ALAC) de ICANN, donde se discuten temas vinculados a la

gobernanza de Internet, en particular, desde la perspectiva de los usuarios finales de Internet.

Hablar entonces de gobernanza de Internet, implica referirnos a la participación de los diferentes actores interesados, gobiernos, sociedad civil, sector privado, comunidad técnica y académica, tanto en la discusión como en la toma de decisiones, de principios, normas, reglas, procedimientos, políticas, que permiten la evolución y el uso de Internet.

Habiendo delimitado el concepto de gobernanza de Internet, corresponde hacer lo propio con el concepto de ciberseguridad.

Definir qué se entiende por ciberseguridad puede resultar aún más complejo que arribar a una definición de gobernanza de Internet.

En primer lugar, pareciera ni siquiera haber consenso en cómo escribir la palabra en sí misma. Algunos autores y expertos en la materia, usan la expresión ciber-seguridad, otros ciber seguridad y finalmente –como el caso de la autora– ciberseguridad. Parafraseando a Alexander Klimbur (2017), escribir "ciber seguridad", como dos palabras separadas, implica que se trata sólo de otra forma de seguridad, y no un concepto especial para nada. Según dicho autor, escribir "ciberseguridad", en una sola palabra, implica algo nuevo, no sólo extensión de lo viejo, aunque también entiende que existe un rechazo general a esta expresión entre algunas partes de la comunidad técnica civil –para diferenciarla de la comunidad técnica militar– respecto de la cual se enfoca para referirse principalmente en estrategias ofensivas de ciberseguridad.

Asimismo, al intentar definir qué se entiende por ciberseguridad aparecen otros conceptos que se encuentran inmediatamente asociados con ella, tales como ciberespacio y ciberpoder, respecto de los cuales, encontrar una definición adecuada, se torna una tarea aún más difícil.

Es importante destacar que el lector podrá obtener diversas definiciones de "ciberespacio" –desde su origen vinculado a la ciencia ficción hasta las propuestas más actuales– que

le permitan formarse un marco de referencia[3]. A los fines del presente trabajo, se tomará la definición brindada por Joseph M. Elbaum (2008, pág. 76), quien parte de una definición brindada por Gordon England, que dispone:

> *El ciberespacio es un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de tecnología de la información, que incluye Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados4 (Elbaum, 2008).*

Asimismo, y siguiendo al mismo autor (Elbaum, 2008, pág. 77) quien se sustenta en la definición brindada por el Dr. Dan Khuel, se entiende por ciberpoder a:

> *….la capacidad de usar el ciberespacio para crear ventajas e influenciar eventos en todos los entornos operativos y en todos los instrumentos de poder[5].*

Como se ha mencionado previamente, ambos conceptos están intrínsecamente relacionados, ya que, en la Cumbre de la OTAN que se llevó a cabo en Varsovia en el año 2016, se reconoció al ciberespacio como un nuevo dominio de las operaciones, junto con los definidos por la tierra, el mar, el aire y el espacio.

Es importante destacar que cualquiera que sea la definición en la que se base el lector, y aun cuando se las use de manera intercambiable, Internet y ciberespacio no son sinónimos, sino que éste último abarca mucho más que Internet, conforme ha sido expuesto previamente de acuerdo a las definiciones brindadas de ambos conceptos.

Como se puede apreciar, intentar definir qué se entiende por ciberseguridad, no resulta tan simple.

3 Algunas definiciones adicionales podrán encontrarse en Ciberespacio (2019). En Wikipedia. Recuperado el 22 de marzo de 2019 de https://es.wikipedia.org/wiki/Ciberespacio; ECURED (sin fecha). *Ciberespacio*. [Online] Recuperado de https://www.ecured.cu/Ciberespacio; Pérez Porto, J. y Gardey, A. (2016-2017). Definicion.de: *Definición de ciberespacio*. [Online] Recuperado de https://definicion.de/ciberespacio/.

4 Traducción de la autora.

5 Ídem.

Uno de los primeros obstáculos que hay que sortear, es la confusión con otros conceptos que pueden aparecer como similares. Como lo expresa el citado autor Alexander Klimburg (2017, pág. 70), lo anterior sucede con conceptos como seguridad de la información y seguridad informática, con lo cual –indica– se confunde a los usuarios y a los expertos en seguridad y no permite ver las diferencias críticas entre ambas disciplinas. Asimismo, sostiene Klimburg, que la ciberseguridad comprende un amplio rango de prácticas, herramientas y conceptos estrechamente relacionados con los de seguridad informática y operacional, donde –concluye diciendo– la ciberseguridad se distingue por su inclusión del uso ofensivo de las tecnologías de la información para atacar a los adversarios. Es decir, dicho autor incluye dentro del ámbito de la ciberseguridad a la dimensión referida a una estrategia ofensiva de la ciberseguridad.

En este sentido, es importante traer a colación dos definiciones de ciberseguridad que han tenido una importante recepción en la comunidad internacional. Una de ellas, es la provista por el National Initiative for Cyber Security Careers and Studies (NICCS)[6], quienes la entienden de la siguiente manera:

> *La ciberseguridad es la actividad o proceso, habilidad o capacidad o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizados o explotación (Traducción de la autora).*

La segunda definición provista, es la que se encuentra incluida en la Recomendación UIT-T X.1205[7] sobre los aspectos generales de la ciberseguridad, emitida por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de las Telecomunicaciones (UIT-T), en la cual se entiende a la ciberseguridad como:

6 Official website of the Department of Homeland Security (2018). National Initiative for Cybersecurity Careers and Studies. Glossary. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. [Online] Recuperado de https://niccs.us-cert.gov/about-niccs/glossary

7 International Telecommunication Union (2018). X.1205: Overview of cybersecurity. *Recommendation X.1205 (04/08)*. [Online] Recuperado de https://www.itu.int/rec/T-REC-X.1205-200804-I/en

> *El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.*

Se complementa lo anterior con la definición que en dicha Recomendación se brinda al ciberentorno, incluyendo a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

Como se puede apreciar, en ambas definiciones, el foco está puesto en la dimensión defensiva del concepto, y en ninguno de los casos se hace hincapié en el uso ofensivo de las tecnologías de la información para atacar a los adversarios al que hace referencia Klimburg.

A los fines del presente análisis, se utilizarán las definiciones mencionadas y centradas en los aspectos defensivos de la ciberseguridad, sin desconocer la existencia de este otro inmenso enfoque –estrategias ofensivas de ciberseguridad– por exceder los objetivos de este trabajo.

Habiendo delimitado los conceptos centrales del presente análisis –gobernanza de Internet y ciberseguridad– se vuelve indispensable desarrollar la relación que existe entre ambos, los principios y las normas ("cibernormas") que deben informar las políticas de ciberseguridad, la elaboración de las estrategias nacionales de ciberseguridad y las implicaciones en cuanto a la privacidad y a la protección de datos personales para determinar si en dichas construcciones, mecanismos y/o espacios, es posible contar con la participación y las contribuciones de los múltiples actores interesados.

2. Principios, normas y estrategias nacionales de ciberseguridad

2.1 Principios y normas que deberían informar las políticas de ciberseguridad

Vishik, Matsubara y Plonk[8] citando al libro blanco adoptado por diferentes asociaciones de la industria en Europa, Asia y Estados Unidos referido a las recomendaciones de la industria y el gobierno para continuar con el crecimiento y la seguridad en el ciberespacio[9], refieren que todos los *stakeholders* (gobiernos, industria, academia y sociedad civil) deben trabajar de manera conjunta para asegurar que los beneficios del ciberespacio sean accesibles para los ciudadanos y que se aborden los principales desafíos.

Para lograr lo anterior, es necesario entonces que los diferentes *stakeholders* participen, de manera conjunta y en un pie de igualdad, en la elaboración de los principios que deberían informar a las políticas referidas a la ciberseguridad. Es decir, la participación de los diferentes actores interesados debe realizarse en esta primera capa, que permita determinar cuáles son para ellos, los principios de las políticas que se deban respetar en materia de ciberseguridad.

La elaboración de estos principios podrá realizarse a nivel global o si por el consenso de dichos *stakeholders* resultara más conveniente, más enfocado y más apropiado debido a los diversos escenarios en que se puedan aplicar, a nivel regional o local.

8 Claire Vishik, Mihoko Matsubara, Audrey Plonk, "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms", *International Cyber Norms: Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), Tallin, NATO CCD COE Publications, 2016, 221-242.

9 BSA The Software Alliance, DIGITAL EUROPE, Information Technology Industry Council, Japan Electronics and Information Technology Industries Association, Korea Internet Corporations Association (2013). *Moving Forward Together: Recommended Industry and Government Approaches to the Continued Growth and Security of Cyberspace*. [Online] Recuperado de https://www.itic.org/dotAsset/9/d/9dede1e6-0281-4c19-84c5-00b8209b7bea.pdf

En este sentido, es importante recordar los principios establecidos en las Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad[10] a los que también se refieren Vishik, Matsubara y Plonk (2016), donde enumera entre dichos principios, a los siguientes:

i. Concienciación: Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
ii. Responsabilidad: Todos los participantes son responsables de la seguridad de los sistemas y redes de información.
iii. Respuesta: Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
iv. Ética: Los participantes deben respetar los intereses legítimos de terceros.
v. Democracia: La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.
vi. Evaluación del riesgo: Los participantes deben llevar a cabo evaluaciones de riesgo.
vii. Diseño e implementación de la seguridad: Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
viii. Gestión de la Seguridad: Los participantes deben adoptar una visión integral de la administración de la seguridad.
ix. Reevaluación: Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

10 Organisation for Economic Co-operation and Development (2004). España: *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*. [Online] Recuperado de; http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm y http://www.oecd.org/sti/ieconomy/34912912.pdf

Si bien estas Directrices ya tienen algunos años –son del 2012– a consideración de la autora, varios de estos principios pueden ser tomados –y en su caso, adaptados– para elaborar una lista de los principios que informen a las políticas de ciberseguridad y que se encuentren *aggiornados* a la actualidad, ya que los mismos cubren varios aspectos importantes al ser tenidos en cuenta, al momento de gestionar la seguridad en diferentes ambientes.

También es importante considerar los principios de ciberseguridad que se encuentran enumerados en la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro emitido en la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones[11], del año 2013, donde se mencionan los siguientes:

i. Los valores esenciales de la Unión Europea lo son tanto en el mundo físico como en el digital, es decir, las leyes y normas que se aplican en el ámbito físico, también son aplicables en el ciberespacio.
ii. Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad. La ciberseguridad se debe basar en los derechos fundamentales, en las libertades y en el respeto a la normativa en materia de protección de datos personales.
iii. Acceso para todos, lo que implica asimismo garantizar la integridad y la seguridad de Internet para lograr un acceso seguro para todos.
iv. Gobernanza multilateral democrática y eficaz, lo cual hace referencia a la participación de los múltiples actores interesados en la gestión diaria de los recursos, protocolos y normas de Internet y en su futuro desarrollo.

11 United Nations, General Assembly (24 June 2013). Sixty-eighth session Item 94 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98). [Online] Recuperado de http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

v. Garantizar la seguridad: una responsabilidad compartida, es decir que, todas las partes interesadas deben reconocer esta responsabilidad compartida, tomar medidas para protegerse y, en caso necesario, ofrecer una respuesta coordinada para reforzar la ciberseguridad.

Estos principios, *mutatis mutandis*, también deberían poder aplicarse para elaborar una lista de los principios que informen a las políticas de ciberseguridad, con la participación de los diferentes *stakeholders*.

Adicionalmente, a consideración de la autora, también deberían ser objeto de análisis los principios de diseño o de la arquitectura de Internet, que permitan extrapolarse para aplicarse a la ciberseguridad, entre ellos, el de apertura, descentralización, extremo a extremo, mejor esfuerzo, modelo de capas e innovación sin pedir permiso, ya que los mismos son parte de la esencia de Internet, lo que le permite ser Internet y no otra cosa diferente, y cuya conservación y respeto a través del tiempo ha permitido la existencia de Internet tal como se la conoce en la actualidad; analizar dichos principios desde la perspectiva de la ciberseguridad, podría brindarle a ésta última, ciertas condiciones de permanencia en el diseño de estrategias que se generen respecto de la misma.

Una vez definidos estos principios de las políticas de ciberseguridad, con la participación de gobiernos, sociedad civil, sector privado y comunidad técnica y académica, se debería trabajar en elaborar las normas, estándares y buenas prácticas que resulten aplicables a los diferentes escenarios que se encuentran transversalizados por la problemática que implica la ciberseguridad.

Recordando nuevamente a Vishik, Matsubara y Plonk (2016, pág. 224) es importante destacar lo que señalan en el artículo citado:

> *El enfoque típico (y constructivo) en los esfuerzos de múltiples partes interesadas en la ciberseguridad es proponer principios comunes de políticas de alto nivel y garantizar que las normas técnicas se desarrollen de acuerdo con ellas. Esta perspectiva de arriba hacia*

abajo conduce a resultados positivos para acordar las normas de la industria.

Es decir, si bien se ha insistido a lo largo del presente trabajo en la participación y compromiso de los múltiples actores interesados, principalmente en la elaboración de los principios que van a informar a las normas, debido a que la problemática que plantea la ciberseguridad es multisectorial y, por lo tanto, necesita de contribuciones de todos los *stakeholders*, tampoco se puede negar que para ciertas normas, principalmente aquellas técnicas que requieren de conocimientos especializados, el asunto se torna meritocrático, es decir, sólo algunos actores interesados se encontrarán en condiciones de participar en su elaboración y obtener la aprobación de los demás miembros de dicha comunidad. Lo anterior no invalida la necesidad de contar, en la mayor medida posible, con la participación de los múltiples actores interesados en las diferentes etapas del proceso bajo análisis.

Relacionado con lo expuesto previamente, también se encuentra el hecho de enfrentarse con una dificultad al intentar regular el ciberespacio y elaborar cibernormas que le resulten aplicables, debido a que el mismo comprende tanto ambientes virtuales como ambientes físicos, lo cual resulta complicado al momento de determinar, entre otros, la identidad de los usuarios, su ubicación geográfica y la atribución de autoría a las acciones –u omisiones– realizadas en dicho entorno y, en consecuencia, la dificultad para determinar la ley y la jurisdicción aplicable. Sin embargo, todo esto, también deberá ser tenido en cuenta al momento de establecer los principios de políticas que se apliquen a la ciberseguridad, lo cual será el punto de partida para trabajar en la elaboración de estrategias nacionales de ciberseguridad, lo cual será analizado en el siguiente apartado.

3. Cómo diseñar estrategias nacionales de ciberseguridad con base en un modelo *multistakeholder*

Habiendo establecido, con la participación de los múltiples actores interesados, los principios que deben informar las políticas de ciberseguridad, y habiendo determinado un primer grado de madurez en la comunidad local de

determinado país como consecuencia de dichos trabajos previos, es posible comenzar a diseñar una estrategia nacional de ciberseguridad.

Para ello, y reconociendo que no existen recetas universalmente aceptadas y probadas en su eficacia que puedan funcionar en todas las comunidades, se han elaborado y publicado diferentes guías que pueden resultar útiles para estos fines.

En particular, conforme al objetivo de este trabajo –demostrar la relación entre la gobernanza de Internet y la ciberseguridad– y a consideración de la autora, resulta relevante analizar la guía y características emitidas por *Global Partner Digital* identificada como *Multistakeholder Approaches to National Cybersecurity Strategy Development*[12] –que se enfoca precisamente en la relación planteada en el presente trabajo– sin desconocer la existencia de importantes modelos elaborados para desarrollar estrategias nacionales de ciberseguridad, tanto por organizaciones internacionales como regionales[13].

En primer lugar, el trabajo de *Global Partner Digital*, considera las características que debe tener un enfoque *multistakeholder*, y enumera entre ellas, a las siguientes:

i. Abierto y accesible: con ello se hace referencia, al grado en que se comunican debidamente, las oportunidades de participación de las partes interesadas relevantes (a través de la participación en

12 Global Partner Digital. Matthew Shears, Daniela Schnidrig, Lea Kaspar (June 2018). London: *Multistakeholder Approaches to National Cybersecurity Strategy Development*. [Online] Recuperado de https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

13 Entre ellos, puede revisarse el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), con las diferentes recomendaciones y guía que ha realizado al respecto y cuya documentación se encuentra disponible en su página de Internet, cuya dirección electrónica es https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx. También se sugiere revisar la Guía para la elaboración de una estrategia nacional de ciberseguridad producida por la Unión Internacional de Telecomunicaciones y asociados de organizaciones intergubernamentales e internacionales, la cual se encuentra disponible en la siguiente dirección electrónica https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf.

comités, talleres, redacción de sesiones, consultas, etc.) y a través de los canales pertinentes, y se realizan esfuerzos para abordar cualquier obstáculo que pueda impedir o desalentar la participación.

ii. Inclusión de los puntos de vista de las diferentes partes interesadas: se refiere al grado en que los actores interesados relevantes tienen la posibilidad de contribuir, son escuchados, se consideran y se toman en cuenta las diferentes opiniones e intereses de los mismos, se hacen públicos los insumos y se informan las deliberaciones que se encuentran basadas en evidencia.

iii. Basado en el consenso: hace alusión al grado en el que las diferentes partes interesadas pueden acordar formas de avanzar y encontrar un propósito común.

iv. Transparente y con rendición de cuentas: se refiere a la medida en que los procedimientos y mecanismos están claramente definidos y son transparentes. Se debe incluir aquí, la expresión de intereses y afiliaciones de los actores interesados –y en consecuencia, la existencia de posibles conflictos de interés–, claridad de los mecanismos de rendición de cuentas, y aquellos indispensables para asegurar que las discusiones y decisiones estén completamente documentadas.

Finaliza el reporte bajo análisis –en el apartado correspondiente a las características de un enfoque *multistakeholder*– expresando que, mientras más abierto sea este proceso, se va a facilitar un diálogo más informado que permita que los actores interesados contribuyan con sus puntos de vista y experiencia. Este diálogo asimismo, ayuda a generar confianza entre las partes interesadas, lo cual es un requisito previo clave para la colaboración y la toma de decisiones por consenso. Adicionalmente, un compromiso con la transparencia y la rendición de cuentas, genera confianza en el proceso de desarrollo de la estrategia y en el resultado final y en su implementación[14].

14 Nota de la autora: lo anterior es traducción del trabajo citado de Global Partner Digital por parte de la autora.

Asimismo, el referido reporte de *Global Partner Digital* define las etapas en el proceso de desarrollo de una estrategia nacional de ciberseguridad. A consideración de la autora, es importante complementar estas etapas con lo establecido en el *Framework for multistakeholder cyber policy development*, también elaborado por *Global Partner Digital*[15], con los ajustes propuestos en el presente trabajo.

La primera etapa que deberá atravesar la elaboración de una estrategia nacional de ciberseguridad, es la del proceso de formación de políticas o también identificada como de alcance. En esta instancia se deberá obtener una comprensión completa y precisa del panorama de ciberseguridad existente en el país.

Para ello, se vuelve indispensable identificar a los actores interesados relevantes, entendidos como aquellos que no sólo tienen un *stake* en juego, sino además porque su participación es importante por sus conocimientos y experiencia en la temática y que además tengan capacidad para involucrarse de manera activa en este proceso. A consideración de la autora, también se deberá evitar en esta etapa, posibles conflictos de interés en los actores interesados participantes, siendo imprescindible requerirles a los mismos, una declaración de interés que permita identificar a qué sector u organización representan y qué intereses tienen en juego –en lo personal o por parte de las entidades que representan– en la elaboración de la estrategia nacional de ciberseguridad. Coincide la autora con el *Framework* de *Global Partner Digital*, en el entendido de que, mientras se hayan expresado las afiliaciones e intereses de los actores interesados relevantes, no se les deberá poner obstáculos a su participación en dicho proceso, y, en caso de que haya dudas al respecto, no sólo se deberá tener en cuenta el nivel de representación, sino también el grado de legitimidad con que cuentan dichas partes interesadas para convertirse en actores relevantes en la elaboración de la estrategia de marras.

Adicionalmente, en esta fase, luego de haber identificado a los actores interesados relevantes, es muy importante

15 Global Partner Digital. Matthew Shears, Lea Kaspar (March 2018). London: *Framework for Multistakeholder Cyber Policy Development*. [Online] Recuperado de https://www.gp-digital.org/publication/multistakeholder-framework/

implementar mecanismos tendientes a evitar que alguno de ellos capture el proceso de desarrollo de la estrategia nacional de ciberseguridad, ya sea porque algún *stakeholder* en particular pretenda controlarlo o manipular a las demás partes interesadas, porque un mismo actor interesado esté representando intereses de más de un sector, o porque los intereses en juego sean demasiado relevantes y se estén esperando obtener determinadas recompensas al finalizar la elaboración de la mencionada estrategia. Para evitar esta captura, es que aparece como necesario contar con la referida declaración de interés mencionada en los párrafos precedentes y que haya un control por pares, es decir, que las mismas partes interesadas puedan señalar estas situaciones en caso de presentarse en este proceso.

Finalmente, dentro de esta primera etapa, se deberá avanzar a la fase de formación de la estrategia propiamente dicha. Aquí se deberán establecer la visión, las metas, los objetivos y definir la estructura y los procesos que se van a emplear para lograr los primeros. Teniendo en cuenta lo establecido en el reporte bajo análisis, en esta etapa también se deberá determinar el enfoque general que tendrá la estrategia nacional de ciberseguridad, pudiendo definirse un marco de alto nivel o una estrategia detallada de ciberseguridad con políticas y prácticas adecuadamente elaboradas. Asimismo, es en esta fase donde cobra sentido haber identificado a los actores interesados relevantes, ya que son ellos quienes deberán llevar a cabo la definición de la visión, alcance y objetivos de la estrategia y de los roles y responsabilidades de cada uno, incluidos los encargados de definir los términos que serán utilizados, revisar el marco jurídico y las buenas prácticas existentes y desarrollar el texto de la estrategia; todo esto, enriquecido con un amplio debate basado en sus conocimientos y experiencias. Es decir, estos actores relevantes deberán determinar en esta etapa, las reglas de participación y los mecanismos para arribar a resultados, acordar un marco de tiempo y establecer hitos y entregables, e implementar mecanismos del proceso, liderazgo y toma de decisiones.

A consideración de la autora, esta primera etapa, debe contar con una amplia difusión a nivel local, en los diferentes medios de comunicaciones, tanto los tradicionales, como los basados en las nuevas tecnologías, para lograr que, si alguno de los actores interesados relevantes no fueron

convocados a participar de este proceso, puedan enterarse de que el mismo se está llevando a cabo, y participar e involucrarse en dicho desarrollo.

Siguiendo el reporte y el *Framework* de *Global Partner Digital*, a continuación se deberá desarrollar la segunda etapa, que consiste en la redacción del primer borrador de esta estrategia. Es probable que para la escritura de determinados apartados del texto de la estrategia, sea necesario que participen algunos de los actores interesados relevantes con determinados conocimientos o experiencia técnicos y que no sea posible involucrar a todos los *stakeholders* en la redacción de la misma. Esto es especialmente importante para lograr un texto que sea preciso y de valor en aquellos sectores de la estrategia que así lo requieran. Sin embargo, esto no significa excluir a los demás actores interesados. Por el contrario, su rol será muy importante en controlar si el texto que quede plasmado, es al que se ha arribado previamente, basado en las discusiones de las demás partes interesadas y principalmente, en el consenso entre las mismas.

Luego de haberse alcanzado este primer borrador del texto de la estrategia, es recomendable que el mismo sea sometido a comentarios públicos de la comunidad más amplia posible a nivel local. Esto enriquecerá el texto y podrá hacer los ajustes correspondientes e incluso adicionar aspectos que puedan haber sido pasados por alto por las partes interesadas que intervienen en el proceso de desarrollo previo de la estrategia. Incluso puede volverse necesario en esta etapa, convocar a mesas o foros de discusión, principalmente para aquellos aspectos de la estrategia que sean más controvertidos o respecto de los cuales no se esté pudiendo alcanzar el consenso de los actores interesados intervinientes. Este proceso de consulta pública podrá realizarse las veces que se considere necesario hasta arribar al texto final de la estrategia nacional de ciberseguridad.

Adicionalmente, es recomendable publicar los comentarios recibidos y que los mismos sean de libre acceso para los interesados en conocerlos. Esto contribuirá a la transparencia a la que se hace referencia en los párrafos precedentes y permitirá controlar a los actores interesados participantes, si efectivamente dichos comentarios recibidos, fueron incluidos en el texto de la estrategia.

Finalmente, la última etapa de este proceso, es lograr un acuerdo del texto final de la estrategia nacional de ciberseguridad y la puesta a disposición de la misma en manos de los responsables de aprobarla y/o adoptarla como marco o legislación vigente aplicable, ya sea el Poder Legislativo o el Poder Ejecutivo del país.

A consideración de la autora, en las etapas previas de este proceso, también se debió haber definido quién o quiénes serían los actores interesados encargados de implementar esta estrategia nacional de ciberseguridad para evitar que luego de su aprobación, la misma se diluya al no conocer de manera concreta quién o quiénes deben ser los encargados de implementarla, y también se debería haber obtenido un compromiso de los actores interesados relevantes, en participar de esta siguiente etapa de implementación, al menos en un rol de control, para revisar de manera periódica, que se están cumpliendo con los consensos alcanzados en la etapa de desarrollo de dicha estrategia.

Para complementar lo anteriormente expresado, se considera importante también incluir en el proceso de desarrollo tanto de políticas de ciberseguridad como de la estrategia nacional de ciberseguridad, las características que establece Internet Society[16] para lo que llama seguridad colaborativa, debiendo respetarse los siguientes principios:

i. Fomentar la confianza y proteger las oportunidades: el objetivo de la seguridad es fomentar la confianza en Internet y garantizar el éxito continuo de Internet como motor de la innovación económica y social.
ii. Responsabilidad colectiva: los participantes de Internet comparten una responsabilidad con el sistema en general.
iii. Propiedades y valores fundamentales: las soluciones de seguridad deben ser compatibles con los derechos fundamentales y las propiedades fundamentales de Internet: las invariantes de Internet.
iv. Evolución y consenso: vínculos de seguridad eficaces en pasos evolutivos ágiles basados en

16 Internet Society (12 April 2015). Improving Technical Security. *Collaborative Security: An approach to tackling Internet Security issues*. [Online] Recuperado de https://www.internetsociety.org/collaborativesecurity/approach/

la experiencia de un amplio conjunto de partes interesadas.

v. Piensa globalmente, actúa localmente: es a través de la autoorganización voluntaria de abajo hacia arriba que es probable que lleguen las soluciones más impactantes.

Aun cuando en el presente trabajo se ha insistido en la participación en un pie de igualdad en el desarrollo de la estrategia nacional de ciberseguridad de todos los actores interesados relevantes identificados, es importante destacar que el principal compromiso para el éxito de dicha estrategia, es el del gobierno, a implementar la misma, y a adoptar el desarrollo de la mencionada estrategia, como una política pública y no como una política del gobierno de turno, principalmente para que la estrategia nacional de ciberseguridad tenga continuidad en su implementación, luego de haber sido desarrollada y aprobada por los órganos encargados de dicha función.

Como se ha expresado previamente, ésta no es una "receta de cocina" para elaborar una estrategia nacional de ciberseguridad. Es simplemente una guía, que deberá irse adaptando y ajustando, entre otros factores, conforme al grado de madurez de la comunidad local involucrada en asuntos relacionados a la ciberseguridad, al escenario de ciberseguridad del país, al grado de involucramiento de los actores relevantes locales y al grado de compromiso del poder político de turno de otorgarle legitimidad al producto desarrollado en un proceso *multistakeholder* a nivel local.

4. Implicaciones a nivel nacional: elaboración de la Estrategia Nacional de Ciberseguridad (ENCS) en México

El 17 de marzo de 2017, se comenzó a trabajar en México en el desarrollo de la Estrategia Nacional de Ciberseguridad (ENCS), asumiendo el Gobierno de la República el rol de facilitador de la misma, y con el apoyo y auspicio de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos

(OEA), a través de su Programa de Ciberseguridad, y dicha estrategia fue dada a conocer públicamente en noviembre de 2017[17].

A consideración de la autora, es importante analizar la ENCS a la luz de las características y guía expuestos en el apartado anterior, para valorar si la misma ha sido desarrollada con base a un modelo *multistakeholder* nacional, con la aclaración de que la autora del presente trabajo, formó parte de las mesas de discusión y foros que se llevaron a cabo dentro del proceso de elaboración de la mencionada estrategia y en determinada fase de su implementación.

En primer lugar, es importante destacar, que en principio, siempre es más relevante contar con una estrategia nacional de ciberseguridad *ad hoc*, elaborada a nivel local –aun con el apoyo de organizaciones internacionales–, con la participación de actores interesados relevantes locales y atendiendo a la realidad y al escenario de ciberseguridad local, aun con las deficiencias o áreas de oportunidad que se puedan identificar, a no tener dicha estrategia o tener una estrategia exportada que no resulte aplicable a México.

Con este contexto, y en líneas generales –analizar a profundidad la ENCS excedería el objetivo del presente trabajo– es interesante considerar los siguientes puntos:

i. se desconocen cuáles fueron los criterios empleados para determinar quiénes eran las partes interesadas relevantes en México, para haberlos invitado a participar de este proceso;
ii. a dichos participantes no se les solicitó que elaboraran, presentaran y publicaran una declaración de interés y que manifestaran su afiliación para evitar potenciales situaciones de conflictos de interés y/o captura del proceso por un mismo actor interesado o sector, con lo cual pareciera no haberse respetado las características de transparencia y rendición de cuentas;

17 gob.mx (13 de noviembre de 2017). [Página de Internet del Gobierno de México]. México: *Estrategia Nacional de Ciberseguridad*. [Online] Recuperado de https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad.

iii. relacionado con el punto anterior, pareciera que conforme a los mecanismos empleados para cursar las invitaciones correspondientes –que al menos no fueron identificados públicamente por la autora–, no fue posible determinar si estuvieron involucrados en el proceso de desarrollo de la ENCS, todos los actores interesados relevantes que deberían haber participado, y en consecuencia, tampoco se podría afirmar que este proceso haya sido abierto y accesible;
iv. técnicamente, no hubo un llamado al consenso de todos los actores interesados relevantes, al momento de arribar al texto final de la ENCS, con lo cual tampoco se habría cumplido con la característica de que se encuentre basado en el consenso;
v. en la ENCS se definieron:
   - Objetivo general: identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político, que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano;
   - Cinco objetivos estratégicos: sociedad y derechos; economía e innovación; instituciones públicas; seguridad pública y seguridad nacional;
   - Tres principios rectores: perspectiva de derechos humanos; enfoque basado en gestión de riesgos, y colaboración multidisciplinaria y de múltiples actores;
   - Ocho ejes transversales: cultura de ciberseguridad; desarrollo de capacidades; coordinación y colaboración; investigación, desarrollo e innovación TIC; estándares y criterios técnicos; infraestructuras críticas; marco jurídico y autorregulación; medición y seguimiento;
   - La Comisión Intersectorial para el Desarrollo del Gobierno Electrónico (CIDGE), a través de la Subcomisión de Ciberseguridad, como la encargada de coordinar al Gobierno de la República y articular los esfuerzos de los diferentes actores para la implementación y seguimiento de la ENCS.
vi. en relación a quiénes participaron en la redacción del texto de la ENCS, no se ha difundido

públicamente, aunque es importante destacar que esta fase estuvo apoyada por el CICTE;

vii. hubo llamado a realizar comentarios públicos y se publicó un documento denominado Consolidación de las consultas a actores nacionales[18];

viii. luego de haber finalizado el texto de la ENCS, se crearon grupos de trabajo en relación a los ejes transversales para trabajar en su implementación. Se presentaron los documentos de trabajo de dichos grupos aunque no se continuó ni se profundizó en la implementación de la ENCS;

ix. un sector de la industria, sostuvo en diferentes espacios, la necesidad de crear un organismo especializado de ciberseguridad para coordinar e implementar la ENCS.

Lamentablemente, a la fecha del desarrollo del presente trabajo, la nueva administración a nivel nacional no ha realizado ningún anuncio referido a la ENCS ni al tema de ciberseguridad.

Antes de la asunción de funciones del actual gobierno, circuló en los medios de comunicación, la información de que, dentro de la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes (SCT), se crearía una Subsecretaría TIC que, además, agregaría una Unidad de Planeación y Políticas, un área de infraestructura de redes críticas y ciberseguridad y una Unidad Habilitadora para vincularse con el sector educativo[19].

Sin embargo, a la fecha, habiéndose anunciado el Plan Nacional de Desarrollo (PND 2019-2024)[20], donde se

18 Secretaría General de la Organización de los Estados Americanos (2 de agosto de 2017). [Página de Internet de la Organización de los Estados Americanos]. *Hacia una Estrategia Nacional de Ciberseguridad: Consolidación de las Consultas a Actores Nacionales*. [Online] Recuperado de https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf

19 Juárez Escalona, C. (7 de octubre de 2018), *Subsecretaría TIC incluirá áreas de redes y de ciberseguridad*. EL ECONOMISTA. [Online] Recuperado de https://www.eleconomista.com.mx/empresas/Subsecretaria-TIC-incluira-areas-de-redes-y-de-ciberseguridad-20181007-0098.html

20 Monroy, J. (17 de marzo de 2019), *Presentan ejes del Plan Nacional de Desarrollo 2019-2024*. EL ECONOMISTA. [Online] Recuperado de https://www.eleconomista.com.mx/politica/Presentan-ejes-del-Plan-Nacional-de-Desarrollo-2019-2024-20190317-0012.html

incluyen como sus tres ejes principales a la Justicia y Estado de Derecho; Bienestar y Desarrollo Económico, así como a sus ejes trasversales Igualdad de Género, No Discriminación e Inclusión; Combate a la Corrupción y Mejora a la Gestión Pública; así como Territorio y Desarrollo Sustentable, en principio, y con la información disponible al momento del desarrollo del presente trabajo, no se hace mención a la continuidad en la implementación de la ENCS de la administración anterior. Solamente se ha publicado un estudio sobre los hábitos de los usuarios en ciberseguridad en México 2019[21] en el cual se indica:

> *Como plan para mejorar la educación y capacitación de la sociedad civil en aspectos de ciberseguridad, con apoyo de la Organización de los Estados Americanos (OEA) y recursos del Gobierno del Reino Unido, la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes (SCT) realizó este estudio, con el fin de coadyuvar a identificar la situación actual de la ciberseguridad en México con miras a generar estrategias para fortalecer la confianza y la utilización segura de los servicios de telecomunicaciones y radiodifusión, incluyendo la banda ancha e Internet, en el país.*

Sin embargo, luego de la publicación de dicho estudio, se desconoce cuál ha sido el seguimiento y cuáles serán las acciones que se implementarán a partir de los resultados obtenidos en el mismo, y quién será la entidad responsable de ejecutar las correspondientes acciones.

En este escenario, llama mucho la atención, que los demás actores interesados que participaron en el desarrollo de la ENCS, no estén requiriendo públicamente a la nueva administración, la continuidad de dicha estrategia, con lo cual pareciera demostrarse que entonces, en el momento de su elaboración, la comunidad local no estaba madura para asumir este compromiso a largo plazo ni de exigir públicamente el respeto por el desarrollo de un

21 Secretaría de Comunicación y Transporte (8 de marzo de 2019).gob.mx. México: *Publican estudio sobre hábitos de los usuarios en ciberseguridad en telecomunicaciones y radiodifusión*. [Online] Recuperado de https://www.gob.mx/sct/prensa/publican-estudio-sobre-habitos-de-los-usuarios-en-ciberseguridad-en-telecomunicaciones-y-radiodifusion?tab=

proceso que aparentemente fue el producto de un modelo *multistakeholder* a nivel local, habiendo quedado, al menos por el momento, dicha ENCS, en letra muerta. Prueba de ello es que ni siquiera participaron todos los *stakeholders* en la definición del glosario que se incluyó en el texto final de la ENCS; glosario que reflejara un vocabulario común a nivel local que trascendiera/superara las diferencias o diversidades de sectores y/o culturales que se encontraban representadas en dicha estrategia. No se lo hizo en México como punto de partida para la ENCS ni como primer ejercicio, cuando se podría haber realizado entre todos los actores interesados en un trabajo multidisciplinario.

Adicionalmente, tampoco se conoce a la fecha si la Comisión Intersectorial para el Desarrollo del Gobierno Electrónico (CIDGE), a través de la Subcomisión de Ciberseguridad, sigue existiendo, y si sigue teniendo entre sus atribuciones la tarea de "coordinar al Gobierno de la República y articular los esfuerzos de los diferentes actores para la implementación y seguimiento de la ENCS".

Es decir, al menos al momento de desarrollarse el presente trabajo, no ha habido una participación de las múltiples partes interesadas más allá del diseño de la ENCS.

En consecuencia, a la fecha se desconoce si la nueva administración le va a dar continuidad a esta ENCS, o como ha sucedido en otros asuntos, se hará "borrón y cuenta nueva". Ni siquiera hay una dependencia a la que se le haya asignado el tema de ciberseguridad en el ámbito federal. Sería importante preguntarnos en estos momentos, quién se ocupa de temas de ciberseguridad a nivel nación en nuestro país, al menos, desde un enfoque defensivo de la ciberseguridad.

5. Implicaciones en cuanto a la privacidad y protección de datos personales

Una problemática estrechamente vinculada a la ciberseguridad, es la referida a la privacidad y a la protección de datos personales, siendo la misma no exclusiva de nuestro país sino principalmente a nivel global y con impacto local, precisamente por la masificación del uso de las nuevas herramientas tecnológicas, el mayor acceso a las mismas por parte de los usuarios con un abaratamiento de los costos

no sólo de los dispositivos sino también de los servicios de acceso a Internet, lo cual se encuentra asimismo relacionado con el reconocimiento en muchas legislaciones nacionales y/o regionales, del acceso a Internet, a banda ancha o a las tecnologías de la información y las comunicaciones, como un derecho humano o en su caso, como un derecho fundamental y la obligación de los Estados de garantizar el acceso a los mismos.

En este sentido es regulado el acceso a Internet en el artículo 6 Constitucional, el cual, en el párrafo correspondiente, establece:

> *El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.*

Asimismo, el derecho a la protección de datos personales, o también reconocido como el derecho a la autodeterminación informativa, ha sido reconocido en el artículo 16 Constitucional, como un derecho humano:

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

En este escenario, donde el acceso a las tecnologías de información y comunicación, a banda ancha y a Internet deben ser garantizados por el Estado en virtud de un mandato constitucional, y donde la privacidad y la protección de datos personales han sido reconocidos como un derecho humano en nuestro país, se vuelve indispensable contar con políticas públicas de ciberseguridad y al menos con una adecuada estrategia nacional de ciberseguridad que ya se encuentre implementada. Lamentablemente, como ha sido expuesto previamente, dichas regulaciones no existen en nuestro país. Se comenzó a trabajar en ello

aunque la nueva administración a nivel nacional, no le ha dado continuidad, al menos hasta la fecha de desarrollo del presente trabajo.

¿Cómo puede entonces un Estado garantizar el acceso a Internet al mismo tiempo que protege los datos personales de los usuarios, si no cuenta con políticas públicas de ciberseguridad?

Lamentablemente, de continuarse por este camino –sin adecuadas políticas de ciberseguridad, con capacidad de implementación demostrada y que funcionen– se corre el riesgo de convertir en letra muerta los mandatos constitucionales referidos.

Esto se torna aún más grave, si revisamos los incidentes de seguridad en entornos digitales ocurridos en los últimos años, no sólo a nivel global por los gigantes tecnológicos, sino en especial por dependencias federales e incluso por empresas locales, donde se han producido brechas de datos personales de una enorme cantidad de titulares de dichos datos, demostrando que también con el tiempo la delincuencia digital se ha ido perfeccionando al mismo tiempo que se tratan de encontrar soluciones efectivas para la protección de la información.

En este contexto, resulta necesario realizar algunas aclaraciones. En primer lugar, es importante tener mucha precaución en cuanto a requerir más legislación con el argumento de que resulta necesario para regular situaciones nuevas y en entornos digitales o como se ha expresado previamente, en el ciberespacio.

En cuanto a la protección de datos personales, en nuestro país existen al menos dos leyes importantes, que resultan aplicables, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), las cuales cubren tanto el ámbito privado como el público del tratamiento de los datos personales de los titulares.

En ambas leyes se regula el deber de seguridad que tienen los responsables –tanto públicos como privados– en el tratamiento de los datos personales de los titulares, estableciendo la obligación de implementar medidas de seguridad físicas, técnicas y administrativas para resguardar los datos que están tratando y evitar cualquier tipo de vulneración de seguridad sobre los mismos, previendo sanciones para los responsables en los casos que se incumpla con esta obligación y se produzcan dichas vulneraciones de seguridad, con capítulos específicos donde se regulan las infracciones y sanciones. Asimismo, la LFPDPPP tiene un capítulo específicamente dedicado a regular los delitos en materia del tratamiento indebido de datos personales. Sumado a lo anterior, existe en nuestro país un órgano constitucional autónomo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que tiene la competencia atribuida por mandato constitucional para aplicar estas leyes y, específicamente, para determinar si los responsables del tratamiento de los datos personales de los titulares, están cumpliendo con la obligación de implementar medidas de seguridad respecto de dicho tratamiento, ya sea que el mismo se realice en soporte físico o electrónico.

Con lo expuesto, se refuerza la recomendación de que, previo a requerir más legislación en nuestro país, se tome conocimiento de las normativas que actualmente existen, y lo que es aún más importante, cualquier legislación que se emita al respecto, deberá cuidar de regular o en su caso sancionar, las conductas humanas y no el medio en el cual las mismas se llevan a cabo.

En consecuencia, el desafío es, entonces, ver de qué manera va a hacer frente el gobierno a este asunto de la ciberseguridad sin afectar los derechos y libertades fundamentales de los usuarios, teniendo en cuenta que las cuestiones relacionadas con la privacidad/protección de datos personales y ciberseguridad no son cuestiones exclusivamente de derechos ni exclusivamente de Internet o del ciberespacio, sino que deben ser abordadas por todas las partes interesadas, incluidos los gobiernos, el sector privado, la sociedad civil, la academia y la comunidad técnica.

Para dar cierre a este apartado, resulta relevante incluir lo manifestado por Internet Society[22] al referirse al enfoque de la seguridad colaborativa, cuando expresa:

> *Creemos que este enfoque de seguridad colaborativa para abordar los problemas de seguridad de Internet es fundamental para garantizar el futuro de la Internet abierta como motor de la innovación social y económica. Como una red de redes sin control centralizado, ninguna entidad u organización puede mantener la seguridad de Internet. Es importante que estas cuestiones sean abordadas por todas las partes interesadas en un espíritu de colaboración y responsabilidad compartida de manera que no se menoscabe la arquitectura global de Internet ni se reduzcan los derechos humanos. Internet es para todos: trabajemos juntos para alcanzar su máximo potencial.*

6. Algunas reflexiones finales

Conforme a lo que ha sido expuesto en el presente trabajo, la gobernanza de Internet y la ciberseguridad son conceptos que se encuentran íntimamente relacionados, ya que el modelo *multistakeholder* característico del primer concepto, basado en la participación en pie de igualdad de las múltiples partes interesadas –gobiernos, sociedad civil, sector privado y comunidad técnica y académica–, y con decisiones adoptadas con base en el consenso de los mismos, ha sido un mecanismo utilizado en diferentes espacios y sobre algunos asuntos de la gobernanza de Internet que ha demostrado su eficacia, al otorgarle una mayor efectividad a los resultados obtenidos de esta manera.

En otras palabras, si no se tienen en cuenta la visión, los aportes y la experiencia de los diferentes *stakeholders*, tanto para la elaboración de cualquier política pública de ciberseguridad como para el diseño, desarrollo e implementación de una estrategia nacional de ciberseguridad, se corre el riesgo de que el ciberpoder del Estado se diluya y pierda legitimidad, y en consecuencia, tienda a no ser respetado por aquellos a quienes se tiene que aplicar, o,

22 Internet Society (12 April 2015). Improving Technical Security. *Collaborative Security: An approach to tackling Internet Security issues*. [Online] Recuperado de https://www.internetsociety.org/collaborativesecurity/approach/

por el contrario, migre hacia el extremo opuesto, donde dicho ciberpoder del Estado crezca, de manera de detentar el mismo, un control absoluto y sin límites, en detrimento de los demás *stakeholders*.

Como ha sido expuesto, la ciberseguridad emerge como uno de los grandes temas contemporáneos que atraviesan la agenda de la gobernanza de Internet, así como los sectores de seguridad de diversos países. Encontrar un equilibrio y armonización entre los intereses de ambos regímenes, resulta fundamental para la promoción de una tecnología a favor de los derechos humanos y la innovación.

En el presente trabajo se han analizado guías y características que debiera tener el desarrollo de una estrategia nacional de ciberseguridad basado en un modelo con la participación de las múltiples partes interesadas, o dicho en otras palabras, con una gobernanza *multistakeholder*. Se insiste, que sólo son guías, recomendaciones y no brindan en sí mismas garantías acerca del éxito de las mismas –principalmente si en dicho desarrollo no se tienen en cuenta las particularidades de la comunidad local hacia la cual va dirigida– reconociendo, asimismo, que existen diferentes documentos que han sido publicados y compartidos tendientes también a allanar este camino hacia la elaboración de una estrategia de ciberseguridad de este tipo.

Se ha analizado también la ENCS y se ha expresado las ventajas de contar con ella, aun cuando la misma tenga áreas de oportunidad para mejorar y cuando, a consideración de la autora, es probable que la comunidad local vinculada a temas de ciberseguridad no se haya encontrado madura en dicho momento para el diseño de la misma. Sin embargo, la actual administración a nivel nacional, aún no ha anunciado si le dará continuidad a la misma o no, ni quién será la dependencia u organismo a nivel nacional encargado de llevar los temas vinculados a la ciberseguridad. Se espera al menos un poco más de claridad en los próximos meses, en particular teniendo en cuenta la agenda que ya se ha compartido públicamente, respecto de la intención de brindar conectividad a Internet a todo el territorio mexicano. Sobra decir, que una política de mejora de la conectividad, indudablemente debe ir de la mano con políticas públicas adecuadas de ciberseguridad,

en particular para proteger a los nuevos ciudadanos digitales que se incorporen al ciberespacio, velando asimismo por la protección del derecho a la autodeterminación informativa de dichos ciudadanos.

Lo anterior, sin olvidar que, como sostiene Internet Society[23], existe una responsabilidad colectiva respecto de la seguridad en Internet, y que la colaboración transfronteriza de múltiples partes interesadas es un componente esencial para lograr la misma. Sirva la presente reflexión, para invitar al lector a seguir investigando sobre estos temas y produciendo material relacionado a los mismos, en particular desde la perspectiva local aunque pensando globalmente.

Como reflexión final, cualquier política pública que desarrolle un gobierno, en este caso particular, vinculada a la ciberseguridad, debe estar centrada en el usuario – incluidas las herramientas y mecanismos para facilitar su concienciación y capacitación-, debe elaborarse con base en mecanismos de gobernanza, con un enfoque *multistakeholder* y respetar los principios arquitectónicos o de diseño de Internet de forma tal de promover la apertura, innovación y la confianza.

BIBLIOGRAFÍA

Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*, JOIN(2013) 1 final, Bruselas, 7 de febrero de 2013.

Bravo, J. (15 de marzo de 2019), Plan Nacional de Desarrollo de telecomunicaciones y el apestado. *EL ECONOMISTA*. [Online] Recuperado de https://www.eleconomista.com.mx/opinion/Plan-Nacional-de-Desarrollo-de-telecomunicaciones-y-el-apestado-20190315-0041.html

23 Ibidem.

BSA The Software Alliance, DIGITAL EUROPE, Information Technology Industry Council, Japan Electronics and Information Technology Industries Association, Korea Internet Corporations Association (2013). *Moving Forward Together: Recommended Industry and Government Approaches to the Continued Growth and Security of Cyberspace*. [Online] Recuperado de https://www.itic.org/dotAsset/9/d/9dede1e6-0281-4c19-84c5-00b8209b7bea.pdf

Cambronero, F. (14 de mayo de 2013). El MAG y el IGF. [Mensaje en un blog]. Fatima Cambronero. [Online] Recuperado de https://fatimacambronero.com.ar/2013/05/14/el-mag-y-el-igf/

Ciberespacio (2019). En Wikipedia. Recuperado el 22 de marzo de 2019 de https://es.wikipedia.org/wiki/Ciberespacio.

Constitución Política de los Estados Unidos Mexicanos. Publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, México, D.F., 25 de junio de 2014.

Craigen, Dan; Diakun-Thibault, Nadia; Purse, Randy (October 2014). Technology Innovation Management Review. *Defining Cybersecurity*. [Online] Recuperado de https://timreview.ca/article/835

ECURED (sin fecha). *Ciberespacio*. [Online] Recuperado de https://www.ecured.cu/Ciberespacio.

Elbaum, Joseph M., *Cyber power in the 21st century*, US, thesis presented to the Faculty Department of Electrical & Computer Engineering, Graduate School of Engineering and Management Air Force Institute of Technology, Air University, Air Education and Training Command, AFIT/GCO/ENG/09-01, [sin editorial], 2008.

García Barrera, Myrna Elia, *Manual de Derecho de las Nuevas Tecnologías*, Ciudad de México, Tirant lo Blanch, 2018.

Global Partner Digital. Shears, Matthew; Schnidrig, Daniela; Kaspar, Lea (June 2018). London: *Multistakeholder Approaches to National Cybersecurity Strategy Development*. [Online] Recuperado de https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

Global Partner Digital. Shears, Matthew; Kaspar, Lea (March 2018). London: *Framework for Multistakeholder Cyber Policy Development*. [Online] Recuperado de https://

www.gp-digital.org/publication/multistakeholder-framework/

gob.mx (13 de noviembre de 2017). [Página de Internet del Gobierno de México]. México: *Estrategia Nacional de Ciberseguridad*. [Online] Recuperado de https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

International Telecommunication Union (2015). Cumbre Mundial sobre la Sociedad de la Información. Ginebra 2003 – Túnez 2005. *Documentos finales de la CMSI*. [Online] Recuperado de http://www.itu.int/net/wsis/index-es.html y https://www.itu.int/net/wsis/outcome/booklet-es.pdf

International Telecommunication Union (2018). X.1205: Overview of cybersecurity. *Recommendation X.1205 (04/08)*. [Online] Recuperado de https://www.itu.int/rec/T-REC-X.1205-200804-I/en

Internet Society (8 de agosto de 2016). *Generar confianza. Un marco de políticas para una Internet abierta y de confianza*. [Online] Recuperado de https://www.internetsociety.org/es/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/

Internet Society (12 April 2015). Improving Technical Security. *Collaborative Security: An approach to tackling Internet Security issues*. [Online] Recuperado de https://www.internetsociety.org/collaborativesecurity/approach/

Juárez Escalona, C. (7 de octubre de 2018), Subsecretaría TIC incluirá áreas de redes y de ciberseguridad. *EL ECONOMISTA*. [Online] Recuperado de https://www.eleconomista.com.mx/empresas/Subsecretaria-TIC-incluira-areas-de-redes-y-de-ciberseguridad-20181007-0098.html

Klimburg, Alexander, *The darkening web*, New York, Penguin Press, 2017.

Lara, F. Propuesta de crear organismo de ciberseguridad sigue vigente: Canieti. *MILENIO*. [Online] Recuperado de https://www.milenio.com/negocios/propuesta-crear-organismo-ciberseguridad-vigente-canieti

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Publicada en el Diario Oficial de la Federación el 5 de julio de 2010, México, D.F., 27 de abril de 2010.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Publicada en el Diario Oficial de la

Federación el 26 de enero de 2017, Ciudad de México, 13 de diciembre de 2016.

Monroy, J. (17 de marzo de 2019), Presentan ejes del Plan Nacional de Desarrollo 2019-2024. *EL ECONOMISTA*. [Online] Recuperado de https://www.eleconomista.com.mx/politica/Presentan-ejes-del-Plan-Nacional-de-Desarrollo-2019-2024-20190317-0012.html

North Atlantic Treaty Organization (27 September 2016). DEEP: Cybersecurity - A Generic Reference curriculum. *Cybersecurity: A generic reference curriculum*. [Online] Recuperado de https://www.nato.int/cps/en/natohq/topics_157591.htm

Official website of the Department of Homeland Security (2018). National Initiative for Cybersecurity Careers and Studies. Glossary. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. [Online] Recuperado de https://niccs.us-cert.gov/about-niccs/glossary

Organisation for Economic Co-operation and Development (2004). España: *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*. [Online] Recuperado de http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm y http://www.oecd.org/sti/ieconomy/34912912.pdf

Organización de los Estados Americanos (2019). Seguridad Cibernética: *Documentos*. [Online] Recuperado de https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx.

Pérez Porto, J. y Gardey, A. (2016-2017). Definicion.de: *Definición de ciberespacio*. [Online] Recuperado de https://definicion.de/ciberespacio/.

Sánchez Onofre, J. (19 de agosto de 2017), Así perfila la OEA al Coordinador para la Estrategia de Ciberseguridad. *EL ECONOMISTA*. [Online] Recuperado de https://www.eleconomista.com.mx/tecnologia/Asi-perfila-la-OEA-al-Coordinador-para-la-Estrategia-de-Ciberseguridad-20170819-0003.html

Secretaría de Comunicación y Transporte (8 de marzo de 2019).gob.mx. México: *Publican estudio sobre hábitos de los usuarios en ciberseguridad en telecomunicaciones y radiodifusión*. [Online] Recuperado de https://www.gob.mx/sct/prensa/publican-estudio-sobre-habitos-de-los-usuarios-en-ciberseguridad-en-telecomunicaciones-y-radiodifusion?tab=

Secretaría General de la Organización de los Estados Americanos (2 de agosto de 2017). [Página de Internet de la

Organización de los Estados Americanos]. *Hacia una Estrategia Nacional de Ciberseguridad: Consolidación de las Consultas a Actores Nacionales*. [Online] Recuperado de https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf

SUN (12 de diciembre de 2018), La SCT planea cinco ejes estratégicos en telecomunicaciones. *INFORMADOR.MX*. [Online] Recuperado de https://www.informador.mx/mexico/La-SCT-plantea-cinco-ejes-estrategicos-en-telecomunicaciones-20181212-0114.html

Téllez Valdés, Julio, *Derecho Informático*, México, McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V., 2009, Cuarta edición.

Unión Internacional de Telecomunicaciones (UIT), Banco Mundial, Secretaría de la Commonwealth (Comsec), Organización de Telecomunicaciones de la Commonwealth (CTO), Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad*. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). [Online] Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf.

United Nations, General Assembly (24 June 2013). Sixty-eighth session Item 94 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98). [Online] Recuperado de http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

Vishik, Claire; Matsubara, Mihoko; Plonk, Audrey, "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms", *International Cyber Norms: Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), Tallin, NATO CCD COE Publications, 2016, 221-242.

Revista de Administración Pública

INAP

Regímenes para la ciberseguridad

Alejandro Pisanty

Resumen: En el presente trabajo se problematiza la definición de Ciberseguridad Nacional, considerando el estado del arte en la consideración de actores nacionales y no nacionales, y las relaciones con actividades como las del delito organizado y la posible negación de gobiernos sobre la actuación de actores no nacionales que los impliquen o favorezcan. Se describen los regímenes aplicables a la gobernanza de la ciberseguridad: el multilateral o intergubernamental, el multisectorial o "multistakeholder" que se ha formado especialmente en gobernanza de Internet, y un régimen híbrido o ecléctico que impera en el ámbito operativo actual. Se comparan las características de dichos regímenes, como las Cibernormas y la Medidas Constructoras de Confianza, para concluir atendiendo a la acción de estados poderosos que apalancan acciones en unos y otros regímenes para ganar espacios estratégicos. Finalmente se atrae la atención del Estado mexicano a esta temática en beneficio de los intereses nacionales.

Palabras clave: Ciberseguridad, Seguridad Nacional, gobernanza de Internet, gobernanza multisectorial, gobernanza "multistakeholder"

Cybersecurity regimes

The definition of National Cybersecurity is scrutinized, considering the state of the art in the study of national and non-national actors, and relationships with activities such as organized cybercrime and the possible plausible deniability of governments with respect to non-national actors who implicate or favor them. Regimes applicable to cybersecurity governance are described: multilateral or intergovernmental; multistakeholder as has emerged in Internet governance; and a hybrid or eclectic regime which applies to the present operational environment. The characteristics of these regimes are compared, as are Cybernorms and Confidence Building Measures, to finish attending to the action of powerful states which leverage their actions from one regime to the other thus gaining strategic spaces. Finally, the attention of the Mexican state is attracted to this problem in benefit of the national interest.

Keywords: Cybersecurity, National Security, Internet governance, multistakeholder governance

Fecha de recepción: 11 de marzo de 2019
Fecha de aceptación: 9 de abril de 2019

Revista de Administración Pública

INAP

Regímenes para la ciberseguridad*

Alejandro Pisanty[1]

1. Introducción

En el presente texto intento reflejar conceptos de la teoría de regímenes internacionales sobre la gestión de la ciberseguridad, especialmente en lo que se refiere a seguridad nacional. Con ello propongo proveer un marco de referencia para la toma de decisiones que considere las diferentes formas de organización que existen en torno a la seguridad en sistemas computacionales y redes de telecomunicaciones, así como la gobernanza de Internet y permita orientar a diferentes organismos del Estado y de la sociedad en su actuación.

* Esta investigación se llevó a cabo con apoyo del Departamento de Física y Química Teórica y de la Coordinación de Asignaturas Sociohumanísticas de la Facultad de Química de la UNAM. La Lic. Fátima Cambronero, de la Internet Society y la firma Ríos Abogados, S.C. hizo una lectura crítica de una versión inicial del presente artículo, que contribuyó a lo poco bueno que el mismo podrá ofrecer. Asumo la responsabilidad del resultado agradeciendo a la vez su colaboración.

1 Doctor en Química por la Universidad Nacional Autónoma de México y profesor de tiempo completo de la Facultad de Química de la UNAM. Estudios postdoctorales en el Instituto Max-Planck de Investigaciones sobre el Estado Sóido, Stuttgart, Alemania. Su actividad se refiere a la gobernanza de Internet y de la tecnología en general; relaciones ciencia-tecnología-sociedad; Sociedad de la Información, e-gobierno y educación o e-learning; y estrategias digitales nacionales, regionales y locales. Ha impartido cursos en la UNAM, el INAP, el ITAM, INFOTEC y el CIDE. Ha sido funcionario de la UNAM y de organismos internacionales como ICANN y la Internet Society.

La seguridad de las sociedades actuales enfrenta nuevos riesgos con el desarrollo y acceso generalizado a Internet. El término "ciberseguridad" se utiliza para describir el complejo de interacciones entre el ciberespacio y la seguridad personal, pública y nacional. En el presente trabajo describo los regímenes dominantes para el análisis de la ciberseguridad (multilateral y multisectorial o "multistakeholder") y añado a consideración otros dos, el de "Administración de TI" y el de "Cibernormas", explicando su relación con los dos primeros. Describo la efectividad relativa de cada uno de ellos en el tratamiento de la ciberseguridad en diferentes planos. Previamente y para entender mejor esa evaluación, describo algunos problemas que son específicos a la ciberseguridad, como la ventaja estructural del atacante sobre la defensa, el problema de atribución del origen del ataque, y algunos problemas emergentes. Finalmente oriento la discusión para que el análisis realizado en el texto sirva a la formulación y ejecución de estrategias de ciberseguridad a nivel nacional aunque también en formas aplicables a las regionales y locales, en contraste con las propuestas de organismos internacionales como la Organización de Estados Americanos (OEA).

2. Ciberseguridad

2.1 Definiciones

Sería conveniente empezar con una definición de "ciberespacio" y aun esta tarea aparentemente sencilla encuentra muchas dificultades. En una época no lejana el ciberespacio estaba definido por computadoras, ante todo, algunas de ellas conectadas a redes. Hoy es casi sinónimo de Internet, aunque preferimos reservar este nombre para la interconexión global de redes accesibles unas desde otras, utilizando un sistema normalizado (el protocolo IP) y un espacio único de direcciones numéricas IP (IPv4 o actualmente también IPv6). Muchas lecturas del término "Internet" abarcan también los recursos computacionales, los dispositivos móviles, los sistemas de información e incluso a los usuarios y sus prácticas.

¿Y el ciberespacio? "casi lo mismo pero más", el universo de sistemas y personas conectados por medio de telecomunicaciones (digitales en su mayoría), del que

Internet sería vehículo (en la definición restrictiva), subconjunto (en la definición más lata) y paradigma, en una definición de ciberespacio asimilada a la de Sociedad de la Información de Castells.

La palabra "ciberseguridad" engloba significados muy diferentes para distintos actores sociales, y su polisemia varía a lo largo del tiempo. Puede referirse a la seguridad de los sistemas informáticos o a toda afectación de la seguridad (física, personal, pública o nacional) que provenga de sistemas informáticos y computacionales o de Internet. Puede ser considerada materia de trabajo de los técnicos informáticos o de las representaciones nacionales en la ONU, motivo de angustia por el futuro de los niños o materia de frío análisis actuarial en una compañía de seguros.

En este artículo dejaré jugar esta polisemia, acotándola al avanzar pero dejando una "ambigüedad creativa", como el experto diplomático Markus Kummel (2004) caracteriza a amplios campos del lenguaje diplomático. Una definición oficial de referencia es "la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada" (México, Gobierno de, 2011). Esta definición se ha considerado tanto más general como más particular que la de "seguridad de la información", lo cual ilustra las dificultades que estamos discutiendo.

Para fines operacionales, desde luego, las definiciones mejor acotadas se refieren a los activos de información, de cuya protección deriva el diseño de la protección de los datos y documentos, las bases de datos, los sistemas de información computacionales, las computadoras y las redes. Los atributos de la información que deben ser administrados en esta protección son, en la definición más ceñida generalmente aceptada, integridad, autenticidad y confidencialidad; definiciones más amplias incluyen ciertamente la disponibilidad y en muchos casos el no-repudio (Daltabuit, 2007)

Las dificultades actuales para acotar la definición de ciberseguridad provienen que conforme más y más

sistemas humanos y sociales dependen de la computación y de Internet, es posible afectar objetos físicos, personas, sistemas de la sociedad y sociedades enteras a través de la afectación o manipulación de sistemas informáticos. Características específicas de Internet facilitan aún más esta interacción entre lo "cíber" y el resto de los sistemas de las sociedades: apertura, masificación, capacidad de ocultar u ofuscar la identidad, carácter transjurisdiccional, reducción de barreras y reducción de fricción. Cada una de éstas tiene efectos positivos universalmente apreciados, y aspectos que en distintas sociedades son mayor o menormente considerados negativos.

En muchos casos los efectos de Internet en la seguridad (personal, pública, nacional; patrimonial, reputacional, física) se deben además a las "affordances" o "prestaciones" descritas por Nancy Baym (Baym, 2015) como alcance, estructura temporal, colapso contextual, y amplificación. En este nivel estamos hablando de "psyops" ("operaciones psicológicas"), "guerras de información" como las descritas por Arquilla y Ronfeldt ((Arquilla, 1993) en la corporación RAND, o, en términos más llanos, de propaganda y subversión.

Otro factor que complica el tratamiento de la ciberseguridad, especialmente en tanto que seguridad nacional, es que la mayor parte del conocimiento existente sobre seguridad nacional parte de la premisa de que ésta se dirime entre Estados. En ciberseguridad el papel de actores no estatales (Kello, 2013) en la ejecución o como blanco de acciones hostiles llega a condicionar las capacidades del Estado. Ejemplos de este condicionamiento o de capacidad activa son: el delito organizado, el terrorismo, empresas privadas que poseen capacidades e información necesarios para la acción del Estado, empresas cuyos activos son el blanco de acción de actores estatales y grupos de la sociedad civil o de la comunidad técnica, sin cuya participación el Estado no tiene la capacidad de actuar defensivamente.

Es imprescindible añadir que el enfoque generalmente aceptado para administrar la seguridad es el de gestión o administración de riesgos (Corona, 2019), (Kure, 2018). La palabra "seguridad" tiene una alta carga emotiva

que obnubila los análisis. La gestión de riesgos, por el contrario, permite enunciar explícitamente los riesgos, cuantificarlos en probabilidad e impacto, y aplicar diversas técnicas como evasión, reducción, transferencia del riesgo, la detección de eventos, respuesta, mitigación, ejecución de planes de contingencia y recuperación de la continuidad de las operaciones. En una gestión racional las medidas siguen un principio de proporcionalidad con base en una relación costo-beneficio.

2.2 Ámbitos

Una de las dificultades que derivan del uso polisémico de la palabra "ciberseguridad" es que abarca ámbitos muy diversos, en los cuales los actores, los problemas y las soluciones son diferentes. No está exento de complicaciones el hecho de que estos ámbitos estén concatenados y si bien algunos problemas se pueden definir claramente como pertenecientes a cada uno de los ámbitos, las fronteras entre éstos no son tajantes.

Los principales ámbitos de la ciberseguridad son seguridad personal, seguridad pública y seguridad nacional. En el primero imperan la confidencialidad, la intimidad, la protección de datos personales, el patrimonio y la reputación; en el segundo la palabra clave es "delito" y por lo tanto prevención, persecución, legislación, procedimientos policiales, judiciales y penales, investigación forense; la seguridad nacional, por último, se refiere, al hablar de ciberseguridad, a la estabilidad del Estado y la seguridad de la nación, su independencia y autonomía, la preservación de la soberanía, la funcionalidad, estabilidad y seguridad de las infraestructuras críticas y la capacidad de operación de la sociedad en su conjunto y la del Estado y el gobierno en particular. Más que en los tradicionales dominios de tierra, mar, aire y espacio, en ciberseguridad las infraestructuras y operaciones críticas incluyen entes privados, como banca e industria.

Como se señaló en un párrafo anterior estos ámbitos están concatenados. Una afectación a cuentahabientes de la banca mediante "phishing" puede afectar sólo a unos cuantos y constituir un problema de seguridad personal y quizás de seguridad pública. El mismo ataque, llevado a

gran escala, puede llevar a suspender el funcionamiento de las estructuras financieras de un país, por muchos días, y generando no sólo su suspensión, sino incertidumbre acerca de su estabilidad; en un caso así el ataque ya no sólo afecta a las personas o a los negocios sino al país entero y se convierte en un problema de seguridad nacional. En dirección inversa, un ataque delictivo masivo puede ser propiciado por un Estado pero éste podrá negar su intervención, culpando a delincuentes no controlados. El ataque a las infraestructuras de Estonia (Ottis, 2008), que ya ha alcanzado estatura de histórico, es un buen ejemplo.

2.3 Problemas

Algunos problemas característicos de la ciberseguridad son los siguientes:

2.3.1 Ventaja estructural del atacante

La naturaleza de Internet (Pisanty, Principios fundamentales y gobernanza de Internet, 2016), (Pisanty, Llámame Internet, 2018;) da una ventaja estructural al atacante (Gartzke, 2015), Internet como dominio bélico es diferente de los dominios terrestre, naval, aéreo y espacial, ya que es un medio íntegramente construido por el hombre, y cuyas estructuras y reglas son por tanto un producto humano. Esta consideración invitaría a preguntar si es posible reestructurar Internet para que favorezca al defensor o al menos reduzca la ventaja del atacante. Lamentablemente –para el lector que se ponga del lado de la defensa– no hay esperanza alguna de revertir la situación en ningún horizonte temporal razonable. Sí son posibles algunas inversiones de la ventaja del atacante, pero hasta ahora temporales y locales.

La ventaja del atacante en Internet se basa en que es posible tener acceso a la red y operar en ella sin que se exija identificación o autenticación alguna, y por ello sea fácil amplificar los recursos del ataque en múltiples puntos, así como ocultar o al menos ofuscar –como se dice en la jerga técnica– la identidad del atacante, de tal manera que éste se considera exento de riesgo de respuesta o castigo y por ello está fuera del alcance de la disuasión. En cambio los recursos que interesa atacar están centralizados o al menos ubicados en posiciones fijas y conocidas– el sitio Web o

los sistemas informáticos internos de un banco, de un gobierno, de un ejército– están montados en computadoras y éstas se identifican mediante direcciones IP que terminan por ser conocidas, ya por ser públicas por necesidad del servicio, ya por ser posible identificarlas mediante sucesivas operaciones de reconocimiento de la red por parte de los atacantes.

Otro factor decisivo que da ventaja al atacante es que en muchos tipos de ataque, el atacante instala software en los sistemas del defensor con antelación y sin que sea detectado. En el momento del ataque el software es activado con una señalización simple y subrepticia. Las actividades preparatorias del ataque pueden pasar desapercibidas o ser subestimadas.

En otros sentidos –en capas más altas de la arquitectura de Internet– se reproduce la ventaja del atacante sobre el defensor. Los dispositivos de acceso a Internet y a las operaciones matemáticas necesarias para violar las barreras criptográficas son a la vez cada vez más poderosos, cada vez más baratos, cada vez más accesibles aun para los inexpertos, y cada vez más dispersos y fáciles de ocultar (esto último utilizando, por ejemplo, la red TOR (McCoy, 2008), originalmente concebida para proteger el anonimato de personas que pudieran estar en situaciones de persecución política). En cambio el defensor protege sistemas cada vez más complejos, cada vez más expuestos, dependientes de cada vez más usuarios cuya capacitación es insuficiente, con activos de valor e importancia crecientes, sin un aumento proporcional de presupuestos y personal capacitado, en otras palabras, exponiendo una superficie de ataque cada vez mayor.

Cuando las defensas mejoran y en consecuencia incrementan el costo del ataque directo, el atacante recurre a la ingeniería social (Allen, 2001) o se resigna a realizar un ataque de negación de servicio. Mientras cada atacante está obsesivamente dedicado a una función específica y altamente especializada en el ecosistema criminal, y el número de atacantes se multiplica, el número de defensores apenas crece y desde luego no lo hace en proporción a los activos que defiende ni al número de atacantes. Los defensores, además, deben

ocuparse de todos los posibles ataques. Los factores de escala son totalmente desfavorables a la defensa. Una combinación particularmente perversa de ataque propiamente cibernético e ingeniería social se presenta en el "ransomware" (Richardson, 2017)) que "secuestra", toma como rehén, criptográficamente los sistemas de la víctima y ofrece –sin necesariamente cumplirlo– devolver a la víctima el control de sus recursos a cambio de un pago.

La naturaleza de los ataques informáticos favorece la existencia de un amplísimo espectro de atacantes, entre criminales o incluso aficionados individuales y actores estatales de pleno derecho. Entre estos extremos se cuentan atacantes avanzados y bien financiados que pueden atacar a nombre de un Estado, por encargo de éste, o para favorecerlo sin previo acuerdo.

El delito organizado en el ciberespacio se estructura en líneas similares al del espacio físico (estando, además, cada vez más imbricados ambos aspectos); son característicos: actores especializados, funciones separadas, células herméticas y escasamente comunicadas (Stanislakwski, 2004), condiciones de acceso que levantan una barrera casi intraspasable para su penetración por fuerzas del orden.

El uso de espacios y canales secretos de comunicación, el cambio constante de ubicación (virtual o física), el establecimiento de confianza mediante mecanismos de fuerza entre personas intrínsecamente no confiables (como lo ha documentado magistralmente Diego Gambetta (Gambetta, 2009). El uso de criptomonedas y otras aplicaciones de las cadenas de bloques, son otras constantes comunes entre el delito cibernético y el delito organizado en espacio físico.

2.3.2 Cyber-to-physical

Se podría plantear una visión "inocente" de la ciberseguridad en la que se considerara que los activos informáticos no alcanzan el valor crítico de los activos físicos de las sociedades, una visión que Lucas Kello llama "clausewitziana" (Kello, 2013), en la que el territorio, las personas y las instalaciones son los objetos de la actividad

bélica, y los sujetos son ejércitos bajo mandos nacionales. En esta visión el ciberespacio y la ciberseguridad serían irrelevantes o de importancia secundaria. Sin embargo, de manera creciente la actividad en el cibersepacio tiene alcances en el territorio, las personas y las instalaciones físicas.

No se trata solamente de amenazas relativamente abstractas –la dificultad para el pago de nóminas en todo el país sigue siendo considerada, para sorpresa de este autor, como un problema menor que la pérdida parcial de control territorial– sino también de la posibilidad de que los atacantes impidan el funcionamiento de las redes eléctrica o de agua, produzcan explosiones o liberación de substancias tóxicas en fábricas y ductos, dirijan el funcionamiento de dispositivos médicos contra los pacientes, produzcan colisiones en el transporte público masivo, y otras formas de afectar físicamente a la población y reducir el control del gobierno sobre el territorio (véase, por ejemplo, Yampolsky, 2015).

A esto debe añadirse el uso bidireccional cíber-físico-cíber, es decir, apoderarse del control de dispositivos físicos como cámaras de videovigilancia para usar sus procesadores y conexiones a la red como vehículos para ataques cibernéticos, como ha pasado en 2017 en algunos casos muy sonados de *botnets* (Kolias, 2017).

El "problema de atribución" (Tsagourias, 2012) es uno de los puntos torales de la ciberseguridad, que la hace enormemente diferente de las consideraciones conocidas para la seguridad en espacio físico, y complica especialmente el nivel de seguridad nacional.

Atribuir un ataque a un agresor es la premisa fundamental de la defensa y de la retaliación. Si no se sabe quién ataca es muy difícil defenderse, pero sobre todo es muy difícil realizar un contraataque o una acción contra otros activos que sirva como medida para infligir daño al enemigo. El contraataque debe ser creíble, pronto y eficaz para que su sola posibilidad disuada a posibles atacantes. En delito cibernético, la atribución es extremadamente importante para iniciar y hacer efectiva la acción legal contra el delincuente; en seguridad nacional, la atribución no sólo debe identificar al individuo o grupo atacante, sino que

debe poder asociar su acción a la de un Estado contra el cual dirigir el contraataque o los recursos diplomáticos pertinentes.

En los siguientes párrafos vamos a explorar la posibilidad y consecuencias de atribuir un ataque que ya ha ocurrido a una persona en específico y determinar las acciones que un Estado debe emprender en consecuencia, para entender las limitaciones de la atribución y las consecuencias de dichas limitaciones.

En general los medios técnicos de Internet sólo permiten rastrear de manera fidedigna el origen de un ataque hasta una dirección IP. Ésta, suponiendo primero que no haya sido falsificada ("spoofeada" en el argot técnico), habrá sido asignada a un ISP (proveedor de servicios de acceso a Internet), del cual suele ser posible conocer su identidad y nacionalidad. El ISP puede o no compartir con un investigador forense más información, como los datos del cliente que tuvo asignada la dirección IP en el momento de interés y la ubicación física del equipo, dependiendo de la capacidad técnica del ISP, disponibilidad de la información, retención de datos, y legislación y prácticas de protección de datos personales (que impide compartir información) y de colaboración con las autoridades (que lo permite). Todo esto asume que se ha logrado atravesar la que puede ser una espesa barrera de indirección que oculta la dirección IP real desde la que se origina un ataque.

En la hipótesis de que se conozca la información descrita en el párrafo anterior, el problema de atribución puede haber quedado acotado pero no necesariamente estará resuelto. Incluso cuando se tiene la fortuna de contar con información fidedigna acerca del equipo específico del que efectivamente partió la acción informática del ataque, los medios técnicos por sí solos no bastan para atribuir a una persona específica el ataque, ya que el equipo puede haber estado comprometido y bajo control de alguien externo, o no puede comprobarse quién usó el equipo en el momento en cuestión.

Y aun suponiendo que, ahora combinando métodos informáticos y técnicas policiales y de inteligencia, se pueda atribuir el ataque a una persona u organización, ésta podrá negar haber actuado bajo órdenes de un Estado,

si cuenta con la suficiente "plausible deniability" (Office of the Historian, 1946). La investigación puede continuar por años pero la respuesta puede ser exigida en un corto plazo. Además, incluso en el caso de que el Estado capture el dispositivo, como ha ocurrido en actos de terrorismo o subversión cometidos desde dentro del territorio, el Estado puede estar sujeto a que un particular (el fabricante del teléfono) pueda y quiera aplicar medidas criptográficas para revelar el contenido de las comunicaciones relacionadas con la investigación. Peor aún, en muchos casos esta información no existe, simple y llanamente, por diseño de los protocolos y de los servicios.

Resulta así que el gobierno de un país puede tener identificado un ataque sufrido por entes en su territorio y no estar en condiciones de atribuirlo de manera suficientemente precisa a un actor estatal externo como para emprender una acción que dé respuesta en especie; y al no existir esta amenaza en forma contundente y en corto plazo, el Estado atacado tiene escaso poder de disuasión sobre posibles atacantes.

2.3.3 Definición de actos de guerra

La respuesta a un ataque por parte de un gobierno o Estado depende no sólo del problema de atribución, sino también en la definición de un acto de guerra en el ciberespacio, o a partir de éste, y la doctrina que rige la respuesta.

La definición de actos de guerra en el ciberespacio está a debate al momento de realizar la presente investigación. Diversos organismos internacionales, entes académicos y gobiernos están tratando de alcanzar definiciones claras pues de esta claridad dependerá la precisión de la doctrina de defensa y contraataque de las partes atacadas. Una referencia común en esta materia es el "Manual de Tallinn" (Manual, 2017).

Como en párrafos anteriores, la definición de un acto de guerra se ve complicada por la diversidad de posibles agresores y su relación con un gobierno determinado (Klimburg, 2017). Depende además de cuán crítico consideren distintas entidades que debe ser un ataque de origen cibernético para considerarlo un acto de guerra.

Se suele ilustrar el espectro de posibles definiciones haciendo mención de ejemplos como que el ataque interrumpa o altere el funcionamiento de los equipos de un hospital de tal manera que ocasione pérdida de vidas; ésta podría ser una consecuencia no sólo de un ataque enfocado a los dispositivos sino algo mucho más genérico, una interrupción en el abasto eléctrico.

Otros posibles actos bélicos serían la suspensión de servicios vitales como el abasto de agua, electricidad o combustibles, o transporte. La interferencia con las elecciones está también sometida a consideración. ¿Cuándo es esto un acto de guerra, cuándo se puede afirmar que es un acto promovido o realizado por un gobierno al que habrá que considerar hostil? El ataque pudo venir desde un territorio cuyo gobierno esté combatiendo a los atacantes, y el país destino y el país origen del ataque podrían identificar un enemigo común en lugar de considerarse uno a otro como hostiles.

Debe considerarse también una distinción que induce un momento de sobriedad: algunos ataques a la soberanía de una nación se pueden propagar a través del ciberespacio, incluso hacerlo en formas inéditas e insidiosas, pero deben ser analizados como propaganda, operaciones psicológicas, intervención, subversión, y deben ser tratados a partir de esa naturaleza fundamental. El tratamiento de estas actividades en el ciberespacio debe estar supeditado a las leyes, tratados, políticas y prácticas pertinentes de forma sustantiva, y referirse a las redes solamente como medio comisivo. La amplificación, la facilidad de acceso, el ocultamiento del origen, etc., se tratarán como agravantes o atenuantes según el caso.

2.3.4 Confianza

Bajo el rubro “confianza” encontraremos una enorme cantidad de problemas; cuando menos los siguientes:

2.3.4.1 Confianza entre Estados

La base de todas las consideraciones en materia de ciberseguridad en tanto seguridad nacional es la ausencia de confianza total entre los Estados. De existir

esta confianza, ningún país percibiría que está en riesgo de agresión por un tercero, y si lo estuviera, disiparía sus dudas por vías pacíficas. En cambio, la competencia entre países por motivos económicos o políticos, las diferencias ideológicas o religiosas, versiones diferentes de la historia sobre la autoridad sobre un territorio, motivos de raíz étnica y muchísimos otros, las múltiples raíces históricas, económicas, políticas, sociales y culturales de la guerra, se manifiestan en la ausencia de confianza como base de las relaciones internacionales.

La historia es también fuente de lecciones para la construcción de confianza y de relaciones entre actores que no se pueden basar en plena confianza. Desde luego una de las bases de estas últimas es la identificación y persecución de objetivos comunes, como puede ser la subsistencia del sistema en su conjunto, la ausencia de conflicto bélico de gran escala, etc.

La Guerra Fría proveyó nuevas lecciones de construcción de relaciones con base en desconfianza o confianza limitada, mediante la disuasión proveniente de la ”doctrina MAD”, “destrucción mutua asegurada”, entre las potencias nucleares, que a su vez dio lugar a un gran sistema de alianzas de alcance global. Como lo han señalado Klimburg y otros autores, la analogía con la amenaza nuclear no se puede extrapolar fielmente al ciberspacio.

La señalización de las intenciones de los actores es mucho menos clara en el ciberespacio y por ello, y las otras razones ya descritas en este texto como las capacidades de los actores subnacionales, la impredecibilidad del alcance de los ataques, etc., no ha sido posible todavía construir un sistema estable de relaciones basadas en confianza limitada. Una importante escuela en el régimen de Cibernormas (Pawlak y Barmpalou, 2017) y el trabajo del “Best Practice Forum” sobre Ciberseguridad del Foro sobre Gobernanza de Internet de la ONU, (Hoorenbeck, 2018) dedica esfuerzos extraordinarios al diseño de CBM, “confidence building measures” o medidas de construcción de la confianza, para acotar el riesgo de daños que escalen rápidamente hasta quedar fuera de control en el caso de una confrontación en el ciberespacio.

2.3.4.2 Confianza entre ciudadanos y autoridades del Estado

En todas las condiciones de potencial agresión al Estado, sea ésta por otro Estado o por actores subnacionales propios o ajenos, la capacidad de acción del Estado depende de la confianza, el control, o ambos, con el que cuente en su relación con los actores internos. En ciberseguridad la acción encubierta (y descubierta) del Estado contra los ciudadanos, como la intervención no autorizada de comunicaciones, la provocación y engaño a través de "bots", "trolls" y otras herramientas, y su ocultamiento, erosiona corrosivamente esta base de confianza, de manera especialmente crítica ya que ocurre en el mismo dominio operacional de Internet, redes y computadoras.

La continuidad entre las acciones relacionadas con el delito cibernético, la seguridad personal y pública, y las acciones de agresión contra la nación y el Estado diluye la sensación de seguridad del ciudadano ante el Estado, y su confianza en el mismo. El argumento que expresa "si no tienes nada que ocultar no tienes nada que temer", o "si se solicita la intervención de las comunicaciones o la penetración de las actividades de una persona u organización es que están efectuando acciones presumiblemente delictivas" pierde su poder cuando se considera que el Estado, el gobierno, o alguna parte de éste actúa fuera de la ley. En países como México donde no hay una tradición sólida de confianza en el imperio del Estado de Derecho, y donde se conoce la penetración de las autoridades y los cuerpos policíacos por elementos delictivos, se vuelve difícil alcanzar acuerdos nacionales sobre ciberseguridad basados en confianza.

2.3.4.3 Confianza entre los sectores

Para la gobernanza multisectorial del ciberespacio, como la indican las prácticas probadas y los mandatos de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la construcción de confianza entre los sectores privado, social, público, académico y técnico es fundamental. En su ausencia es difícil que construyan acuerdos sólidos, operables y de la profundidad necesaria.

Entre otras medidas de construcción de confianza para las estrategias nacionales y locales de ciberseguridad, son indispensables la transparencia, la declaración de conflictos de interés y la vigilancia constante. Al mismo tiempo es también indispensable llevar a cabo eventos y acciones con resultados que prueben las bases de la confianza y permitan que ésta se profundice y arraigue, y vuelvan inaceptables los costos de faltar a ésta.

2.3.4.4 Confianza entre actores críticos

Un nexo que no puede faltar en la construcción de ciberseguridad es la confianza entre ciertos sectores críticos que deben compartir información y actuar conjuntamente para la preparación y la respuesta a incidentes. Los CERTs (equipos de respuesta a emergencias en cómputo) y CSIRTs (equipos de respuesta a incidentes de seguridad en cómputo), la banca, las áreas de seguridad informática de las empresas y de entes públicos y de la sociedad civil, la prensa, los proveedores de servicios especializados y las fuerzas del orden deben contar con mecanismos de comunicación y coordinación en los cuales cuenten con la confianza de transmitir información de amenazas y ataques, vulnerabilidades de software, sistemas y redes, y acciones.

La dificultad de construir esos espacios de confianza se acentúa dado que por un lado esa confianza no existe respecto a otras acciones hostiles, como el delito en espacio físico, y por otro lado, los medios de comunicación y coordinación son informáticos, también doblemente sujetos a riesgos.

2.3.5 Tecnologías exponenciales

En algunas esferas se conoce como "tecnologías exponenciales" a las que significativamente amplifican capacidades del ser humano, como la inteligencia artificial, la impresión 3D, la robótica, y tecnologías no informáticas como la manipulación genética (López-Portillo Romano, 2018).

Éstas tienen el potencial de transformar los análisis y las acciones de ciberseguridad tanto del lado del defensor como del atacante; por ejemplo algunas

formas de Inteligencia Artificial ya existentes pueden contribuir a identificar patrones que conduzcan a detectar vulnerabilidades técnicas, físicas o humanas en el blanco de un ataque, o, *contrario sensu*, ayudar al defensor a identificar patrones y anomalías en el tráfico de Internet que le permitan iniciar una alerta por un posible ataque y así evitarlo.

3. Regímenes

Entre muchas posibles definiciones de régimen seleccionamos la de Krasner (1082): "conjunto de principios, normas, reglas y procedimientos para la toma de decisiones, implícitos o explícitos, alrededor de los cuales convergen las expectativas de los actores en un área dada de las relaciones internacionales".

Se puede simplificar el estudio de los regímenes aplicables a la ciberseguridad reduciéndolo a dos, el multilateral y el multisectorial ("multistakeholder" o MSH en este texto), que ha sido reconocido entre otros autores como Franda (2001). Sin embargo, por razones que me propongo hacer evidentes en el texto, se gana precisión y riqueza de análisis si consideramos cuatro regímenes: el multilateral o intergubernamental; el de la administración de TI (tecnología de información, o TICs, tecnologías de información y comunicación); el de cibernormas (que es en parte una extensión del multilateral, con variaciones importantes), y el multisectorial característico de la gobernanza de Internet. Es aportación original del presente trabajo reconocer como un régimen específico el de Administración de TI.

El régimen multilateral es parte fundamental de nuestra realidad contemporánea. Lo definen los principios de soberanía e identidad territorio-nación y los mecanismos de la diplomacia y los tratados. En años recientes y desde los otros regímenes también se le llama "de Westfalia" (Scholte, 2017), en referencia al tratado del mismo nombre que hace unos siglos definió las bases ya citadas, o "de Clausewitz" para al menos un autor notable, (Kello, op. Cit.) que reconoce también a la conducción de la guerra como un asunto exclusivo de los Estados. Son característicos de este régimen los instrumentos bilaterales y multilaterales de acuerdo entre países y

organismos como la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA) (característico de los organismos regionales) o la Unión Internacional de Telecomunicaciones (característica de los organismos especializados), así como la Organización para la Cooperación y el Desarrollo Económico (OCDE), organismo emblemático de los "clubes" u organismos basados en afinidad.

Me refiero al "régimen de Administración de TI" para describir el conjunto de entidades, operaciones, decisiones y políticas que se presentan en el nivel operacional de la seguridad informática como generalmente se practica en gobiernos, empresas, universidades y otras organizaciones. Éste no es un régimen formalmente constituido a pesar de que lleva la principal carga de proteger los recursos informáticos de la sociedad. Miles de técnicos, abogados, administradores y directivos organizan las políticas internas de las empresas, adquieren y desarrollan software y sistemas de información, capacitan personal, adquieren, instalan y operan sistemas de detección y de prevención de intrusiones, administran y operan redes, servidores, servicios en la "nube", contratos de tercerización, se certifican ante entidades públicas y privadas, y un sinfín de otras actividades. Frecuentemente encuentran en las leyes un obstáculo donde deberían encontrar un apoyo. Parte de este sistema se formaliza en entidades llamadas CERT (Computer Emergency Response Team) y CSIRT (Computer Security Incident Response Team) y en los departamentos de seguridad informática, o a cargo de la misma, en gobiernos, empresas y organizaciones civiles. Lo caracterizan el dinamismo, el pragmatismo y su orientación a la solución de problemas.

El régimen de Cibernormas es una extensión del régimen multilateral, que incorpora partes del de Administración de TI, de la academia, y del "multistakeholder". Se centra en la búsqueda de normas internacionales que rijan a los Estados en su conducta internacional en materia de ciberseguridad, con algunas analogías a la Convención de Ginebra y a acuerdos de limitación de las armas nucleares y otros conducentes al control de armamentos. Se presenta en organizaciones y mecanismos multilaterales no globales como el de Cooperación de Shanghai (formado por China, Rusia,

Uzbekistán y Kazakhistán, con adiciones y observadores como Pakistán e India, y más recientemente México), y al interior de la ONU mediante el GGE (Grupo de Expertos Estatales) formado por la Asamblea General y que tuvo un sonado fracaso en junio de 2017 (Henriksen, 2019), complemento a los Estados, proviene de académicos distinguidos como, de manera ejemplar, Ronald Deibert y el fallecido Roger Hurwitz (Hurwitz, 2013-14); (Hollis, 2002); (Osula, 2016) y (Klimburg, 2017), las universidades en las que trabajan, gobiernos como el de los Países Bajos y algunas otras organizaciones.

El régimen multisectorial o "multistakeholder" caracteriza especialmente a la gobernanza de Internet. Lo constituyen numerosos mecanismos y organizaciones en los que fundamentalmente se distinguen agrupamientos de gobiernos, industria, sociedad civil, academia y comunidad técnica; en algunas organizaciones estos dos sectores se consideran bien dentro de la sociedad civil, bien transversalmente a los otros. Dependiendo del tema del que se ocupan, estas organizaciones y mecanismos tienen diversos grados de formalización. Así por ejemplo ICANN (Internet Corporation for Assigned Names and Numbers), a cargo de la coordinación técnica de los identificadores centralmente coordinados de Internet (nombres de dominio, direcciones IP y parámetros de protocolos técnicos), se constituye como un organismo privado no lucrativo, basado íntegramente en instrumentos consensuales del derecho privado, con mecanismos formales de toma de decisiones, elección o designación de funcionarios, recurso y reversión de decisiones, y penalización por faltas a sus propias norma. En cambio el IGF (Internet Governance Forum o Foro sobre Gobernanza de Internet) requiere un aparato normativo menos complejo, ya que se limita a organizar un evento anual y debates a lo largo del año entre los distintos sectores. Los mecanismos de este régimen se caracterizan por una aspiración de agilidad, relevancia y equidad, sin oponerse a las leyes y mecanismos multilaterales o de cibernormas, y dando un amplio reconocimiento a la comunidad operacional, como la descrita como "administración de TI" en párrafos anteriores. Se orienta a la solución de problemas, convoca a todos los actores relevantes, y si bien enfrenta un conocido problema de "déficit democrático", lo compensa mediante apertura, transparencia y rendición de cuentas. Basa su

legitimidad en la combinación de eficacia y reconocimiento de las partes interesadas. Le rigen además un principio de subsidiaridad y uno de racionalidad técnica.

Una caracterización reciente del régimen que rige en gobernanza de Internet ha sido provista por Scholte (2017) y la describe como transescalar, transectorial, difusa, fluida, con mandatos superpuestos, jerarquías ambiguas y la ausencia postsoberana de una autoridad única y consistente. A esta caracterización se debe añadir el factor heurístico y que la selección natural evolutiva entre los mecanismos y organizaciones activos en gobernanza de Internet se base en un criterio de legitimidad, fundado a su vez en la efectividad de las organizaciones para cumplir con sus mandatos.

Las características citadas se describen brevemente de la manera siguiente:

1. Transescalar: atraviesan múltiples escalas, por ejemplo desde la de un número limitado de servidores raíz del DNS (13) o de países (alrededor de 200) hasta los más de 3 millones de personas conectadas, o el incontable número (posiblemente decenas de millones) de dispositivos o de cuentas de servicio.
2. Transectorial: en gobernanza de Internet participan los sectores público, privado y social, con un papel específico también para las comunidades generadoras y operadoras de tecnología ("comunidad técnica") y la comunidad académica, que pueden ser transversales a los sectores citados y ello en forma variable según el país y con el paso del tiempo. Dentro de cada uno de estos sectores hay subdivisiones, por ejemplo en el sector privado distinguimos intereses complementarios y contrapuestos entre los operadores de redes, los proveedores de servicios en línea, las empresas que utilizan Internet para sus negocios, etc.
3. Difusa: la gobernanza de Internet tiene fronteras difusas en tanto que algunos asuntos son resueltos en formas inmediatas y locales y de manera informal mientras que su escalamiento ante diversos factores puede llevar a mecanismos más formales, en otras geografías, etc.

4. Fluida: el "locus" y la forma de organización para resolver diversos problemas en gobernanza de Internet varía rápidamente en el tiempo y según las partes involucradas. Organizaciones como ICANN han sufrido varias reestructuraciones y cambios de reglas tan fundamentales como abandonar su dependencia de la supervisión del gobierno de Estados Unidos en tan solo 20 años; la IETF ha modificado sus métodos y estructura, los registros de nombres de dominio nacionales y muchas otras entidades se reorganizan y adaptan constantemente. Surgen estructuras nuevas como el APWG en el momento en que son requeridas y se abandonan cuando dejan de ser útiles o son substituidas por otras que lo sean más.
5. Mandatos superpuestos: no es infrecuente que diversas organizaciones o mecanismos tengan mandatos simultáneamente en determinados asuntos. Así, por ejemplo, hay una superposición entre ICANN, los registros de nombres de dominio, la OMPI, organizaciones arbitrales, asociaciones de empresa, autoridades nacionales de propiedad industrial e intelectual, y la OMC, para temas de propiedad industrial en nombres de dominio.
6. Jerarquía difusa: no hay una jerarquía definida ni permanente entre las organizaciones y mecanismos de gobernanza de Internet. Así por ejemplo en materia de nombres de dominio los ccTLDs reciben autoridad delegada de ICANN, pero no requieren reconocerla para todas sus actividades, tratando en muchos casos los asuntos directamente con sus gobiernos y comunidades nacionales. En algunos casos ICANN actúa reconociendo formal o implícitamente la autoridad de la IETF (para el establecimiento de estándares); en otros la IETF confía plenamente en la autoridad delegada en ICANN (para la asignación de parámetros y el registro de sus valores, en la unidad llamada IANA).
7. Ausencia postsoberana de una autoridad única y consistente. No existe una autoridad única para todos los asuntos de Internet. El sistema en operación está conformado por diversas entidades, cada una de las cuales tiene algún grado de autoridad –a veces sólo poder de convocatoria para debates,

como el IGF– en un ámbito específico, como se menciona en la característica de superposición de ámbitos de competencia, y en otras es subordinada. En algunos casos la autoridad es formal como en la ISO-3166-MA que a su vez deriva su lista de parámetros de la Oficina de Estadística de la ONU; en otros, informal como el APWG. Sólo algunas entidades de alcance nacional pueden reclamar una autoridad legal delegada por un proceso parlamentario y elecciones de un gobierno.

8. Heurística: a las características identificadas por Scholte, añado la muy importante de que las organizaciones y mecanismos de gobernanza de Internet se diseñan y operan alrededor de la solución de un problema o conjunto pequeño de problemas a cuya solución pueden contribuir eficazmente: la IETF para la normalización técnica de Internet; W3C para la Web; ICANN para eliminar la discrecionalidad y descentralizar la gestión de los identificadores coordinados; APWG para atacar el "phishing", y así sucesivamente.
9. Legitimidad basada en efectividad: la otra característica de los mecanismos de gobernanza de Internet que añado a la lista de Scholte es la legitimidad por vía de la efectividad. Siguiendo quizás el viejo "mantra" de la IETF "no tenemos presidentes ni reyes ni votos, sólo tenemos consensos fuertes y programas funcionando", la legitimidad de las organizaciones –cuya aceptación se demuestra por el acatamiento de sus mandatos, el recurso a sus decisiones, la participación en sus procesos– se basa en su capacidad de resolver de manera efectiva los problemas. Para mantener su legitimidad las organizaciones y mecanismos deben evolucionar constantemente y asegurar la participación de las partes interesadas de manera completa y a través de representaciones efectivas, así como tener procesos, archivos y operatividad conmensuradas con las características deseadas de las soluciones, como certeza, velocidad, amplitud de consulta, capacidad de implementarlas, y otras.

Otras organizaciones de este régimen involucradas en ciberseguridad son la IETF (Internet Engineering Task Force); el M3AAWG (Messaging, Malware and Mobile Anti

Abuse Working Group) y el APWG (Anti-Phishing Working Group), así como ISOC (Internet Society) (Pisanty, The vexing problem of oversight, 2015)

Ciberseguridad bajo los distintos regímenes

TI. En el régimen de Administración de TI, la ciberseguridad es una consideración constante en un número creciente de formas. Pasó de ser una característica superpuesta a las actividades en Internet a ser una consideración de diseño desde el principio de cada desarrollo de sistemas. En licitaciones y contratos, así como en instrucciones internas, se considera a la seguridad de los sistemas como una de los principales "requerimientos no funcionales" de los desarrollos.

El gobierno de la función de ciberseguridad en este régimen está basado principalmente en experiencia, comunicación entre las partes, acuerdos para compartir información, desarrollo de capacidades, normas técnicas y normas organizacionales. Los estándares de la familia ISO 27000, los de gestión informática como COBIT e ITIL, los del NIST (National Institute of Standards and Technology, de Estados Unidos), la norma MAAGTIC-SI (Manual Administrativo de Aplicación General en Tecnologías de la Información y Comunicación y Seguridad Informática, del Gobierno Federal mexicano) y otros relacionados dan normas de conducta a los administradores de redes y sistemas que les permiten mantener seguros sus sistemas, desde el desarrollo de software y la adquisición de sistemas hasta las operaciones más sensibles, pasando por los contratos de tercerización para servicios administrados, "cómputo en la nube", contratación y promoción de personal, aseguramiento de calidad y numerosos otros aspectos.

El marco normativo de esta gobernanza tiene múltiples fuentes: leyes como las cláusulas de Colaboración con las Autoridades de la Ley Federal de Telecomunicaciones y Radiodifusión (México) y las de Protección de Datos Personales; los Decretos de Austeridad del Gobierno Federal mexicano desde el año 2000, que orientan a la tercerización de servicios informáticos; contratos colectivos del personal en empresas y gobiernos; reglamentos y políticas de gobiernos nacionales y

subnacionales; contratos con proveedores y clientes; normatividad sectorial, como es el caso en banca, sector salud en algunos países, leyes fiscales; normas técnicas internacionales generalmente aceptadas y sus versiones y variantes nacionales; políticas públicas como la EDN (Estrategia Digital Nacional) y el acuerdo de colaboración informal y permanente que forma parte fundamental del tejido de Internet ((Sullivan, 2016).

3.1 Multilateral

3.1.1 Unión Internacional de Telecomunicaciones (UIT)

La gobernanza de la ciberseguridad en el marco de la UIT se puede considerar centrada en la Resolución 45 de Doha, 2006 (UIT, 2006), que es a su vez una evolución de los acuerdos para el combate al correo electrónico comercial no solicitado ("spam"), y que ha pasado por versiones y revisiones en las Conferencias y Asambleas de la UIT sobre telecomunicaciones internacionales (WCIT), normalización técnica (WTSA) y sobre Desarrollo (WTDC) así como el cauce al que éstas llevan, las Conferencias de Ministros Plenipotenciarios conocidas también como Plenipots o PP-xy donde xy es el número abreviado del año de la Conferencia, por ejemplo PP-10 se llevó a cabo en 2010.

Debe recordarse que la gobernanza de la UIT reside en los Estados Miembros, cuyas decisiones son las únicas resolutivas. En años recientes se ha transferido una parte de la capacidad de decisión a los sectores (Telecomunicaciones, Radio y Desarrollo), incrementado la participación de los Miembros Sectoriales, y ampliado el alcance de organizaciones que pueden presentarse a las Asambleas y Conferencias y participar en los Grupos de Estudio, pero las decisiones finales son intergubernamentales. Otro objeto de fricción con otros sectores proviene de que los documentos de la UIT son accesibles solamente para miembros autorizados mediante claves celosamente custodiadas, a diferencia de los de las organizaciones de la comunidad Internet, disponibles ampliamente.

El alcance de estas Resoluciones se traduce a nivel nacional a través de la naturaleza vinculante o no de los

instrumentos normativos de la UIT, su Constitución y sus Reglamentos como el Reglamento de Telecomunicaciones Internacionales. La traducción entre el nivel global y el nacional se transmite también a través de organismos regionales como CITEL (Conferencia Interamericana de Telecomunicaciones) y sus contrapartes en otras regiones del mundo.

Los puntos contenciosos para el desarrollo de estas resoluciones derivan de aspectos estratégicos, aspectos tácticos, aspectos técnicos y aspectos políticos. Los aspectos técnicos se refieren a la capacidad de los Miembros Sectoriales y los Países Miembros de implementar las medidas, considerando que los Miembros Sectoriales son operadores de redes de telecomunicaciones que no siempre son los ISPs. Los aspectos políticos están determinados por factores como la formación de bloques regionales, la formación de bloques de afinidad de países y Miembros Sectoriales promotores de un modelo de mercado abierto y competitivo contra otros basados en proteccionismo, y su imbricación con la formación de bloques y negociaciones en asuntos ajenos a la UIT. Los aspectos estratégicos y tácticos pasan del interés en la substancia de las Resoluciones a la persecución de fines como la obtención de votos para los cargos de elección de la Unión y otros organismos.

En la historia de la Resolución 45 han sido contenciosos diversos asuntos: las referencias a la libertad de expresión, que para Estados Unidos y países afines es un valor fundamental que la propia ciberseguridad debe contribuir a preservar, pero a la vez puede verse limitado por la inspección de comunicaciones requerida para algunos proyectos de seguridad, y que por otra parte, para otros países no debe ni ser mencionada en este contexto; las referencias a la privacidad, tema en el que Estados Unidos se opone al enfoque normativo europeo basado en leyes de protección de datos personales y más recientemente el “derecho al olvido”, mientras que por otra parte, numerosos gobiernos incluido el de Estados Unidos se oponen al enfoque de países como China, Vietnam y el bloque árabe que no prevé llevar la protección a la privacidad a este nivel; la mención de y colaboración con otros organismos, especialmente los multisectoriales como la IETF o ICANN; y el carácter

vinculante de las resoluciones. El personal y algunos líderes de la UIT se empeñan en reafirmar en cada párrafo la preeminencia de la Unión en el seguimiento de la Cumbre Mundial sobre la Sociedad de la Información y en citar a la Unión a la vez que excluyen a la UNESCO y otras organizaciones y ramas de la ONU.

El resultado es una resolución extensa en antecedentes y parca en extremo en contenido propiamente resolutivo: "*Resuelve instruir al Director de la Oficina de Desarrollo de las Telecomunicaciones:* 1. Organizar, en conjunto con el Programa 3 y con base en contribuciones de los miembros, reuniones de Estados Miembros y Miembros Sectoriales para discutir maneras de aumentar la ciberseguridad, incluyendo, *inter alia*, un memorándum de entendimiento para reforzar la ciberseguridad y combatir el spam entre Estados Miembros interesados; 2. Informar de los resultados de estas reuniones a la conferencia plenipotenciaria de 2006."

El impacto de hecho sobre la ciberseguridad es muy limitado, ya que depende de que los gobiernos de los Estados Miembros y los Miembros Sectoriales efectivamente den operación a las Resoluciones. Generalmente la comunidad de los regímenes multisectorial y de Administración de IT no las requieren y las Resoluciones sólo se utilizan para justificar leyes y decisiones gubernamentales en algunos países, más frecuentemente en los que tienen una operación gubernamental menos participativa o abiertamente autoritaria.

3.1.2 ONU

La ONU presta atención creciente a Internet, la Sociedad de la Información y el ciberspacio a través de muchos de sus organismos. En la década 1990-2000 el Programa de las Naciones Unidas para el Desarrollo tuvo un papel activo en la promoción del acceso a Internet. La UNESCO ha competido con la UIT por el liderazgo en materia de Sociedad de la Información, en el que actualmente se ocupa de temas como acceso al conocimiento, libertad de prensa y de expresión, y educación, mientras que la UIT obtuvo y conserva el liderazgo a través de su control sobre la Cumbre Mundial sobre la Sociedad de la Información (2003-2005) y sus mecanismos de

seguimiento. Las Relatorías Especiales sobre Libertad de Expresión y más recientemente sobre Privacidad han tenido incidencia importante al menos a nivel declarativo sobre estos temas, con paralelos productivos en regiones como la de las Américas, en este caso a través de la OEA (sobre la cual se trata en el punto 3.1.3).

En la Asamblea General de la ONU y tanto en el Primer como en el Segundo Comité, y en sus órganos administrativos como ECOSOC, se presta también atención al uso pacífico del ciberespacio. Para abreviar referiremos solamente el trabajo del GGE, Grupo de Expertos Gubernamentales, que ha buscado establecer un conjunto mínimo de reglas de coexistencia pacífica y de limitación del alcance sobre seguridad nacional de las acciones en el ciberespacio. El GGE es un grupo cerrado que emite poca información acerca de los resultados de su trabajo y casi nula sobre sus procesos. De acuerdo con noticias internacionales, en junio de 2017 interrumpió sus trabajos ante la imposibilidad de alcanzar acuerdos.

Los acuerdos que se buscaban en el GGE, para alimentar posibles resoluciones de la Asamblea General, se orientan a reglas para la coexistencia en el ciberespacio, la definición de los actos bélicos y la prohibición o autorización de determinadas acciones entre los Estados. Buscan además limitar el daño que las acciones bélicas en el ciberespacio pueden producir sobre la población civil; por ejemplo, prohibirían el ataque a redes y sistemas de instalaciones hospitalarias y escolares. Establecerían un marco para la determinación de atribución de origen de ataques y para la pertinencia, oportunidad, necesidad y proporcionalidad de las medidas de respuesta de los Estados cuyos territorios o sistemas fueran atacados. Las limitaciones a la propaganda y a la subversión, a la intercepción de comunicaciones y al espionaje, y a la interferencia en la vida privada o en el ejercicio de derechos ciudadanos parecen ser los obstáculos que han resultado insalvables. Con miembros como Estados Unidos, Rusia, China y Cuba, el contraste entre expresiones a favor de la vigencia del Derecho Internacional en el ciberespacio o en contra de la militarización del mismo, algunas sustanciales y otras retóricas, es posible apreciar que este Grupo haya encontrado dificultades para avanzar.

3.1.3 Organismos regionales y especializados

Entre los organismos regionales de interés para las propuestas multilaterales de gobernanza del ciberespacio cabe destacar para los fines de este trabajo a la Organización de Cooperación de Shanghai, ya mencionada y a la OEA. También son importantes la OCDE, la Unión Europea, APEC y ASEAN; en beneficio de la extensión del trabajo no serán tratadas.

La Organización de Cooperación de Shanghai parte de una reunión entre China (que la lidera), Rusia, Uzbekistán y Kazakhiztán para explorar reglas de convivencia multilaterales entre países afines, a iniciativa de China. Se han reunido al menos dos veces en forma amplia y pública y ha incorporado a India y Pakistán como miembros, estableciendo así un territorio amplio y sobre todo una población cercana en número a la mitad de la humanidad. Otros países, entre ellos México, se han incorporado como observadores. El propósito explícito de la Organización es el orden basado en reglas en el ciberespacio, plasmado en un Código de Conducta para la Seguridad de la Información acordado entre sus miembros (sin que haya entrado en vigencia hasta ahora).

Aquí la palabra clave es "seguridad de la información"; su insidiosa polisemia será analizada en la sección de conclusiones.

Como se puede ver en la declaración de esta organización después de su reunión de 2017 en Xinhua (y una nueva reunión, la 4ª. Conferencia Mundial en Wuzhen llevada a cabo en diciembre de 2017) el alcance que China busca es mucho más amplio que la cooperación para la seguridad de la información; propone reformas sustantivas a la gobernanza del ciberespacio y de Internet, con un fuerte sesgo multilateral (honrando sólo de manera nominal al multisectorial) con el propósito de limitar a los actores no gubernamentales a nivel global y servir de marco legitimador de legislación, políticas y acciones coercitivas en el plano nacional. China intenta, además, extender su visión desde el mecanismo de Shanghai a los BRICS (asociación formada por Brasil, Rusia, India, China y Sudáfrica) y otros espacios donde su presencia es asimétricamente relevante.

Por su parte la OEA se ha aproximado al tema de ciberseguridad en al menos dos proyectos, no independientes, el mecanismo CICTE contra el terrorismo (Comité Interamericano contra el Terrorismo) y el impulso a la creación, país por país, de una Estrategia Nacional de Ciberseguridad (ENCS). El CICTE extiende sus alcances en el ciberespacio a la vigilancia e intercepción de comunicaciones potencialmente relacionadas con el terrorismo y por ello se expande al ámbito del delito organizado.

El programa para promover las ENCS está a cargo de la Gerencia para la Seguridad Cibernética de la OEA y se distingue por una actividad constante en eventos regionales y locales, la promoción de un texto normalizado para que alimente y constituya el documento de ENCS en cada país, la contratación y publicación de un diagnóstico del estado de madurez de seguridad cibernética de cada país de la región, y una activa alianza con las grandes empresas transnacionales que dominan los mercados de equipo para redes y de software. Hasta ahora ha logrado la incorporación de Jamaica y Colombia en la emisión de sus respectivas ENCS.

Es importante también mencionar a la GCCS (Global Conference on Cyberspace, Conferencia Global sobre el Ciberespacio) cuyo origen es multilateral, y cuyo trabajo se trata más adelante en el rubro de Cibernormas.

También es indispensable mencionar el Convenio de Budapest o Convención Europea contra el Delito Cibernético, un instrumento multilateral por excelencia para la cooperación internacional para prevenir y perseguir el delito cibernético. Éste, como ya lo hemos expuesto, no se debe identificar con la ciberseguridad pero ciertamente es un componente importante, y el Convenio de Budapest es un instrumento valioso intrínsecamente y un experimento en marcha del que se puede aprender mucho para otros aspectos de la ciberseguridad entendida como seguridad nacional.

En los últimos cinco años también ha cobrado importancia la actividad del Ministerio del Exterior del Reino Unido, y de organismos constituidos en ese país que colaboran con dicho Ministerio, como el Global Cyber

Security Capacity Center (GCSCC) que opera en la Universidad de Oxford (GCSCC 2018, https://www.oxford-martin.ox.ac.uk/cybersecurity/)

3.2 Multistakeholder y gobernanza de Internet

El concepto de gobernanza "multistakeholder" alcanzó sus actuales niveles de publicidad a partir de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), al convertirse la participación de todos los sectores, en pie de igualdad, en la norma deseable para la gobernanza de Internet. De hecho la gobernanza de Internet ya constituida seguía esta norma desde tiempo atrás, sin invocarla necesariamente por su nombre; y los procesos de gobernanza multisectorial se han aplicado a muchos otros ámbitos como el medio ambiente, el deporte, las finanzas, algunos productos agrícolas y alimentos, la pesca y la ganadería. Con fuertes raíces en el trabajo de Elinor Ostrom para la gobernanza de los bienes comunes, y con modificaciones para dar lugar a la intervención de los gobiernos formalmente constituidos y para adaptarse a la existencia de derechos de propiedad, la gobernanza multisectorial ha logrado avances significativos. tanto en la teoría como en la práctica, en la última década y es un horizonte ineluctable hacia el futuro.

En materia de ciberseguridad, los procesos multisectoriales se alimentan del régimen de Administración de TI y sus actores, y de mecanismos y organizaciones novedosos como la IETF (Internet Engineering Task Force) o ICANN. Los aprendizajes de las últimas dos décadas nos indican que las organizaciones y mecanismos multisectoriales exitosos son heurísticos, acotados a problemas definidos, plurales, abiertos y adaptables. Combinan reglas formales e informales, procuran el consenso más que la unanimidad o la votación por mayorías simples, se mantienen dentro del marco de las legislaciones existentes a la vez que pueden impulsar su armonización e innovaciones normativas, y se revisan a sí mismos con frecuencia para asegurar que su legitimidad por reconocimiento de los actores relevantes y por la eficacia de sus resultados se preserven y expandan.

El ejemplo más elaborado de gobernanza multisectorial de Internet es ICANN (ICANN, 2019, https://icann.org).

Esta organización, encargada de la coordinación central de las políticas que afectan al Sistema de Nombres de Dominio, la distribución de direcciones IP y el registro de parámetros de protocolos de la IETF, reúne a comunidad técnica, gobiernos, empresas, sociedad civil, y academia. Las empresas a su vez aparecen agrupadas en función de la estructura del mercado de nombres de dominio, en "constituencies" de registros (operadores de bases de datos centrales de nombres de dominio de primer nivel), registradores (empresas que comercian con esos registros), intereses de propiedad intelectual y marcas, operadores de redes y empresas usuarias de los nombres de dominio. En el marco de los nombres de dominio los intereses no comerciales, principalmente institucionales y de la sociedad civil organizada, se presentan en dos grupos que constituyen el grupo rector no-comercial; y respecto a un marco más amplio, los usuarios, comerciales o no, participan a través de la comunidad "At Large". Los gobiernos se agrupan en el GAC, Comité Asesor Gubernamental, y la comunidad técnica forma parte de diversos grupos asesores específicos como el de Seguridad y Estabilidad y el de operadores de servidores raíz, además de la representación formal de la IETF y grupos afines en funciones de enlace en el Consejo Directivo.

ICANN produce políticas que reducen las posibles arbitrariedad y discrecionalidad en la gestión de la raíz del Sistema de Nombres de Dominio, mediante procesos formales cuyos efectos tienen impacto global en diversos negocios a lo largo y ancho de Internet. Por ello, cuenta además con procedimientos que pueden llevar a la revisión e incluso reversión de algunas de sus decisiones. Atendiendo a la naturaleza global de Internet, sus procesos de decisión combinan reuniones en diversos lugares del mundo con discusiones a través de Internet que evitan favorecer asimétricamente a los participantes con mayores recursos económicos.

La incidencia directa de ICANN en ciberseguridad se da a través de la estabilidad, seguridad y resiliencia del Sistema de Nombres de Dominio a su cargo; de la seguridad en la asignación y uso de las direcciones IP; y en la promoción de tecnologías como DNSSEC y otras que permiten dar seguridad a la operación de Internet en general. Además,

el desarrollo y cumplimiento de las políticas de ICANN contribuye a limitar los abusos de los nombres de dominio que acompañan a diversos delitos como el "phishing" y el comercio fraudulento.

La IETF, por su parte, ha incluido consideraciones de seguridad en el desarrollo de los protocolos técnicos de Internet desde sus tiempos fundacionales, y los formalizó como requisito en 2003 (Rescorla) En el origen, Internet estaba orientada ante todo a la comunicación entre nodos de la red. La seguridad de la información fue considerada siempre una prioridad y, en una paradoja que sólo es aparente, por ello no se convirtió en un principio de diseño como sí lo fueron la interoperabilidad y la apertura. El principio "de punta a punta" establece que criterios como la seguridad deben ser atendidos en los nodos, no en la red, abreviado como "red tonta, orilla inteligente". Internet se usó desde un principio para conectar sitios que procesaban información sensible; los mecanismos para protegerla evolucionaban rápidamente, como lo hacían también aquellos orientados a atacarla. Insertar los mecanismos de defensa en el interior de la red obligaría a reemplazos constantes para sobrevivir a fuerzas progresivamente superiores en el ataque. Por ello las consideraciones de seguridad se introdujeron sólo cuando fue posible proveerlas de una manera más estable. Así en la actualidad la IETF ha normalizado numerosos mecanismos que impiden diversos ataques, como los "de hombre en medio" la escucha pasiva permanente de canales por intervenciones no autorizadas (Farrel). En extensión de estas consideraciones, la gobernanza multisectorial de la ciberseguridad es la ruta al futuro.

Diversas funciones pueden conllevar un peso y participación mayor de un grupo de actores; por ejemplo, la persecución de delitos debe seguir a cargo de las fuerzas del orden legítimas y legales, la intervención de comunicaciones debe seguir pautas legales (además de principios de necesidad y proporcionalidad), la operación de redes debe continuar a cargo de las empresas autorizadas, y el desarrollo de sistemas residir en la comunidad técnica. La sociedad civil puede realizar contribuciones muy diversas, desde marcar la agenda en temas de privacidad hasta vigilar que la acción de las autoridades se mantenga dentro de la legalidad. La operación de CERTs y CSIRTs, cuyo origen está en el régimen de Administración de TI y es orgánico a

la comunidad Internet, puede también ser multisectorial, con diversos pesos para los participantes en las decisiones según se trate de entidades a cargo de la seguridad nacional, académicas, bancarias, etc.

3.3 Cibernormas

El régimen de Cibernormas es una variante del régimen multilateral en el que diversas fuentes, además de algunos gobiernos, impulsan la creación de un orden normativo para las relaciones entre Estados en el ciberespacio. El producto deseado por estos promotores es un conjunto de instrumentos normativos internacionales que regulen qué pueden hacer los Estados ante posibles hostilidades. Como se ha mencionado antes, un tratado global o varios regionales o multilaterales, de naturaleza vinculante, limitarían los alcances de las acciones hostiles, preservarían la vida y salud de la población civil, asegurarían la necesidad, debida atribución y proporcionalidad de medidas defensivas y retaliatorias ante ataques presuntos o comprobados, controlarían el comercio de software y dispositivos de posible uso hostil a la manera del Tratado de Wassenaar (Granick, 2017), y otros beneficios. La diferencia con el régimen estrictamente multilateral estriba en la inclusión, en diversos grados, de actores no gubernamentales. Hasta ahora éstos residen principalmente en instituciones académicas del ámbito de las Relaciones Internacionales, donde los análisis de la hostilidad en el ciberespacio llevan a conclusiones alarmantes y a un llamado a la acción para evitar las peores consecuencias. Hace falta tiempo para asimilar la revolución tecnológica que representa el ciberespacio y explorar la posibilidad de construir una arquitectura de disuasión similar a la que originaron las armas nucleares. Las comunidades técnica y de gobernanza de Internet observan con cierto escepticismo estos esfuerzos ya que aprecian que se encuentran lejos de los teatros operacionales ya existentes y resulta difícil que se alimenten mutuamente ambas perspectivas. Un resumen de la situación en la intersección de los regímenes de gobernanza de Internet y de Cibernormas ha sido producido por Hinojosa (Hinojosa, 2016).

Un evento distintivo en este régimen es la GCCS (Conferencia Global sobre el Ciberespacio) que se inició en Londres, y que en su sesión de La Haya en 2015 se

abrió con particular amplitud a la participación de todos los sectores (si bien conservó sesiones cerradas exclusivas para representantes gubernamentales; de manera notable, entre éstos se encuentran autoridades policiales y de procuración de justicia, no sólo del ámbito de relaciones exteriores). La sesión de 2017 se llevó a cabo en India, con un perfil internacional más bajo que las anteriores. Se preveía que India aprovecharía la Conferencia para desplegar su visión política que favorece nominalmente al enfoque multisectorial en la coordinación de recursos centrales de Internet y otros aspectos donde hay lugar para la flexibilidad, pero insiste en la autoridad gubernamental y multilateral en los temas que afectan directamente a sus intereses nacionales. Esto ocurrió efectivamente, conjuntamente con una tendencia de otros países, como Rusia y China, a manifestarse también en favor de los controles nacionales

4. Consideraciones conjuntas sobre ciberseguridad, regímenes y estrategias nacionales

Hemos señalado arriba la necesidad de problematizar el uso de la categoría "seguridad de la información" en las discusiones sobre ciberseguridad. Los especialistas en seguridad informática se refieren a la seguridad de la información como el valor determinante de su actividad; como dijimos arriba, es a partir de ésta que se determinan las estrategias de protección de su integridad, autenticidad, confidencialidad y disponibilidad, y a partir de ello la seguridad de las bases de datos, sistemas de información, computadoras y redes. Sin embargo en el contexto internacional la misma categoría representa un significado diferente, la regulación del espionaje y el acceso no autorizado de extranjeros a la información protegida del país propio, y de los nacionales bajo tutela del Estado a información, generalmente proveniente del extranjero, a cuya difusión al interior del país el Estado se opone.

La popularidad del término "ciberseguridad" ha tenido vaivenes importantes en distintos contextos. Así, en el Foro sobre Gobernanza de Internet tuvo uso intensivo en 2010, en boca y documentos de la delegación de Rusia, y posteriormente desapareció varios años para, por un lado, aparecer en la Asamblea General de la ONU y por otro, realizar un gradual regreso al IGF. Este fenómeno podría

ser explicado mediante una aplicación de la teoría agente-principal, entendiendo que Rusia habría estado buscando delegar en el IGF como agente la ejecución de su agenda de ciberseguridad, y al no tener el éxito buscado habría cambiado de foro a la Asamblea General con mejores esperanzas de avanzar en ese espacio exclusivamente intergubernamental.

Entre otras conclusiones importantes que han emergido de las discusiones y la literatura reciente (véase especialmente a Klimburg y a Kello, ya citados abundantemente) destacan:

a) Las ENCS deben orientarse a la gestión de riesgos. Con ello procede identificar los activos que la Estrategia busca proteger, los ámbitos en que se encuentran y los procedimientos de gestión de riesgos específicos aplicables a cada uno, para integrarlos en una estrategia de alcance global.
b) Las ENCS deben hacer participar orgánicamente a todos los sectores.
c) Es necesario distinguir entre delito cibernético y ciberseguridad, evitando reducir la segunda a lo primero pero sin desconocer su conexión, como se ha expuesto en el presente texto.

En años recientes se llevaron a cabo trabajos para formular en México una ENCS. Al igual que en otros países, una ENCS es parte y complemento importante para una Agenda Digital como la Estrategia Digital Nacional, que contiene elementos de seguridad desde su formulación en 2013.

El impulso propio de la OEA y sus aliados empresariales ha sido resistido correctamente por el gobierno mexicano en busca de una formulación mejor arraigada y adaptada a las necesidades del país. Se ha emitido una estrategia puntual para el sector financiero, en acuerdo con el Gobierno Federal a través de la Secretaría de Hacienda y Crédito Público (Gobierno de México, 2017; Gobierno de México, 2017), a la que falta mucho para incorporar orgánicamente una construcción multisectorial. También está a debate la adhesión de México al Convenio de Budapest.

Conclusiones

En el más breve resumen de conclusiones podemos decir lo siguiente:

1. La Ciberseguridad Nacional es un problema espinoso, de difícil definición y solución. Entre otros factores que lo vuelven complejo está la continuidad entre afectaciones a la seguridad informática de los sectores privado y público y la continuidad entre las acciones delictivas, propias del marco de la seguridad pública, y las que ponen en riesgo la viabilidad de la nación. La influencia de actores no estatales y la posibilidad de que ésta sea producto de intención o tolerancia de actores estatales capaces de negar creíblemente su participación, se complica con el "problema de atribución" que hace difícil asignar el origen de un ataque a un individuo u organización específicos de manera inequívoca en un tiempo razonable para una respuesta del Estado nacional a otros Estados.
2. Los regímenes tradicionales –multilateral o intergubernamental– no proveen marcos suficientes para la gestión de la Ciberseguridad Nacional. Es importante que el Estado mexicano reconozca el régimen multisectorial y el régimen ecléctico en el que se desarrollan sus propias operaciones y sus relaciones con la sociedad en materia de informática, gobierno electrónico, economía digital, banca, industria y otros sectores.
3. El papel de la sociedad civil organizada, las sociedades profesionales especializadas, y la comunidad técnica de Internet y en general del ramo de Tecnologías de Información y Comunicación, transversal a gobierno, industria y sociedad civil, es indispensable para el avance en Ciberseguridad Nacional.
4. En compañía de todos los sectores, el Estado debe atender a los movimientos de las grandes potencias y otros actores competentes en los regímenes multilateral y multisectorial para evitar que algunos de estos actores encubran o apalanquen sus actividades en uno de los regímenes con las que llevan a cabo directamente o a través de aliados y afines en otro régimen, en detrimento de nuestros intereses.

BIBLIOGRAFÍA

Allen, M. (2001). Social Engineering: a Means to Violating a Compute System. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/paper/529

Arquilla, J. y. (1993). *Cyberwar is Coming!* Santa Monica, CA, US: Rand Corporation. Retrieved from https://www.rand.org/pubs/reprints/RP223.html

Baym, N. (2015). *Personal Connections in the Digital Age* (2 ed.). Politi Press.

Corona, P. (2019). *Guía Práctica para la Gestión de Riesgos en Ciberseguridad.* México: en prensa.

Daltabuit, E. M. (2007). *La Seguridad de la Información.* México: Limusa.

Farrel, S. y. (n.d.). *RFC 7258.* Retrieved from https://tools.ietf.org/html/rfc7258

Franda, M. (2001). *Governing the Internet: the Emergence of an International Regime.* Boulder, CO, EUA: Lynne Rienner Pubs.

Gambetta, D. (2009). *Codes of the Underworld: How Criminals Communicate.* Princeton, NJ, EUA: Princeton.

Gartzke, E. y. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies, 24*(2), 316-348. doi:10.1080/09636412.2015.1038188

Gobierno de México. (2017). Retrieved from https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad?idiom=es

Granick, J. (2017). *Changes to export control arrangements apply to computer exploits and more.* Retrieved from https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more

Henriksen, A. (2019). The end of the road for the GGE process: the future regulation of cyberspace. *Journal of Cybersecurity*, 1-9. doi:10.1093/cybsec/tyy009

Hollis, D. (2002). Private Actors in Public International Law: Amicus Curiae and the Case for the Retention of State Sovereignty. *B.C. Int'l Comp L. Rev, 235*.

Hoorenbeck, M. A. (2018). *Cybersecurity Culture, Norms, and Values - Internet Governance Forum, Best Practice Forum on Cybersecurity.* United Nations Organization. Retrieved from https://www.academia.edu/37417784/Cybersecurity_Culture_Norms_and_Values

Hurwitz, R. (2013-14). Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs: International Engagement*

on Cyber III: State Building on a New Frontier, 17-28. Retrieved from https://www.jstor.org/stable/43134319

Kello, L. (2013, Fall). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security (Quarterly Journal), 38*(2), 7-40.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* London, UK: Penguin Press.

Kolias, G. K. (2017). DDos in the IoT: Mirai and Other Botnets. *Computer*, 80-84.

Krasner, S. (1982). Rebimes and the limits of realism: regimes as autonomous variables. *International Organizations*, 497-510.

Kummer. (2004). *Personal communication.*

Kure, H. S. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Science, 8*(898), 1-29. doi:doi:10.3390/app8060898

López-Portillo Romano, J. R. (2018). *Retos y oportunidades del cambio tecnológico exponencial.* México, México: Fondo de Cultura Económica (FCE).

Manual, T. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, UK: Cambridge.

McCoy, D. B. (2008). Shining Light in Dark Places: Understanding the TOR Network. In N. y. Borisov, *Privacy Enhancing Technologies, PETS 2008, Lectures in Computer Science vo. 5134.* Berlin y Heidelberg: Springer.

México, Gobierno de. (2011). *Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published.* Retrieved from Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published: Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published

Office of the Historian, U. G. (1946). *National Security Council Directive on Office of Speical Projects.*

Osula, A.-M. y. (2016). *International Norms: Legal, Policy & Industry Perspectives.* Tallinn: NATO CCDCOE.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.

ECIW2008 - Proceedings of the 7th European Conference on Information Warfare.

Pawlak, P. y. (2017). Politics of Cybersecurity Capacity Building: Conundrum and Opportunity. *Journal of Cyber Policy*, 123-144. doi:10.1080/23738871.2017.1294610

Pisanty, A. (2015). The vexing problem of oversight. In W. Drake, *The Working Group on Internet Governance - 10th Anniversary Reflections.* Berlin y Johannesburgo: Springer y APC.

Pisanty, A. (2016). Principios fundamentales y gobernanza de Internet. In J. e. Thumfart, *Pensar Internet.* México: Universidad Iberoamericana.

Pisanty, A. (2018). *Llámame Internet.* México: Secretaría de Cultura - EDUCAL.

Rescorla, F. y. (n.d.). *RFC 3552.* Retrieved from https://tools.ietf.org/html/rfc3552

Richardson, R. y. (2017). Ransomware; Evolution, Mitigation and Prevention. *International Management Review, 13*(1). Retrieved from https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

Scholte, A. (2017). The Net and the Nation State. In U. Kohl, *The Net and the Nation State: Multidisciplinary Perspectives in Internet Governance.* Cambridge. doi:10.1017/9781316534168

Stanislakwski, B. H. (2004). Transnational "Bads" in the Globalized World: The Case of Transnational Organized Crime. *Public Integrity*, 155-170.

Sullivan, A. (2016). "The Internet is made with carrots, not sticks". *TechCrunch*. Retrieved from https://techcrunch.com/2016/04/07/the-internet-is-made-with-carrots-not-sticks/

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and security Law*, 229-244. doi:https://doi.org/10.1093/jcsl/krs019

UIT. (2006). Retrieved from
https://www.itu.int/ITU-D/cybersecurity/docs/WTDC06_resolution_45-e.pdf

Xinhua. (n.d.). Retrieved from http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_4.htm

Yampolsky, A. H. (2015). A language for describing attacks on cyber-physical systms. *International Journal of Critical Infrastructure Protection, 8*, 40-52. doi:https://doi.org/1.1016/j.ijcip.201409.003

Revista de Administración Pública

INAP

Las constituciones locales mexicanas durante la Cuarta Transformación: un análisis prospectivo

Eduardo de Jesús Castellanos Hernández

Resumen: A partir de la denominada Cuarta Transformación de la República, iniciada como propaganda electoral y convertida en eje rector de las políticas de Estado, de gobierno y de las políticas públicas, con motivo del cambio de titular del ejecutivo federal, se plantea la posibilidad y se proponen procedimientos legislativos ante una eventual nueva Constitución General de la República. Se trata de un ejercicio de prospectiva constitucional en el que se reúnen las herramientas de la administración pública con los principios de la teoría jurídica de la constitución, al tiempo que se estudian los elementos del sistema político mexicano en su composición actual, cuyas posibilidades de cambio se sitúan en un plano formal en la nueva mayoría legislativa que apoya al ejecutivo desde las cámaras federales y congresos locales, en principio suficientes para lograr la aprobación de una nueva Constitución.

Palabras clave: Prospectiva constitucional, populismo, presidencialismo, transformaciones jurídicas, control democrático.

Mexican local constitutions in the Fourth Transformation: a prospective analysis

Abstract: From the so-called Fourth Transformation of the Republic, initiated as electoral propaganda and become the guiding axis of State, government and public policies, on the occasion of the change of head of the federal executive, the possibility arises and they propose legislative procedures before a possible new General Constitution of the Republic. It is an exercise in constitutional prospective in which the tools of public administration meet the principles of the legal theory of the constitution, while studying the elements of the Mexican political system in its current composition, whose possibilities for change they are placed in a formal plane in the new legislative majority that supports the executive from federal chambers and local congresses, in principle sufficient to achieve the approval of a new Constitution.

Keywords: Constitutional prospect, populism, presidentialism, legal transformations, democratic control.

Fecha de recepción: 16 de mayo de 2019
Fecha de aceptación: 14 de junio de 2019

Revista de Administración Pública

INAP

Las constituciones locales mexicanas durante la Cuarta Transformación: un análisis prospectivo[1]

Eduardo de Jesús Castellanos Hernández[2]

¿Qué es la prospectiva?

El *Diccionario de la Lengua Española* define a la prospectiva como el "conjunto de análisis y estudios realizados con el fin de explorar o predecir el futuro, en una determinada materia"[3]. Ciertamente, se trata de un término propio de las ciencias económico-administrativas, por lo que no es frecuente encontrarlo en el Derecho Constitucional ni en la mayor parte de las ramas del derecho en las que, sin

1 Una versión inicial de este texto fue presentada durante los trabajos del **IV Seminario en Derecho Constitucional Oaxaca 2019. 97 aniversario de la Constitución de 1922**, organizado por la LXIV Legislatura del H. Congreso del Estado Libre y Soberano de Oaxaca, la Suprema Corte de Justicia de la Nación a través de la Dirección General de Casas de la Cultura Jurídica, Casa de la Cultura Jurídica Oaxaca, y la Red de Juristas Pro-Oaxaca, en la ciudad de Oaxaca de Juárez, Oaxaca, los días 6 y 7 de abril de 2019.

2 Profesor e Investigador adscrito al Instituto Interdisciplinario de Investigaciones de la Universidad de Xalapa. Investigador Nacional, Nivel I. Miembro del Registro CONACYT de Evaluadores Acreditados. Área 5, Sociales y Económicas. Licenciado en Derecho (UNAM), Maestro en Administración de Empresas (UAEMéx), Doctorado en Estudios Políticos (U. de París), Especialidad en Justicia Electoral (TEPJF), Posdoctorado en Control Parlamentario y Políticas Públicas (U. de Alcalá). Autor de diversos libros de derecho público, privado y social. Se ha desempeñado como servidor público en los tres órdenes de gobierno, así como en los poderes Ejecutivo y Legislativo, incluidas ambas cámaras del Congreso de la Unión, el Congreso del estado de Oaxaca y la Asamblea Constituyente de la Ciudad de México.

3 *Diccionario de la Lengua Española*, Real Academia Española, Vigésima primera edición, h-z, p. 1680.

embargo, es habitual encontrar las nociones de proceso y de procedimiento como un conjunto de actividades reguladas para la consecución de un fin que normalmente es la sentencia definitiva o una resolución interlocutoria, o bien, una ley o decreto al final del proceso legislativo.

También en el caso del proceso administrativo público, por ejemplo, donde como lo he mostrado en diversas publicaciones[4], se trata de una sucesión de actividades orientada hacia el futuro, prevista expresa y puntualmente en la Constitución y en las leyes secundarias que lo regulan. De tal manera que la construcción de escenarios de futuro, como podemos apreciar, finalmente, no resulta tan ajena a la práctica del derecho.

Más aún, existen disposiciones constitucionales expresas que regulan el Sistema Nacional de Planeación Democrática y –desde 2014– también *deliberativa*[5] del desarrollo nacional, por lo que a partir del mes próximo el Plan Nacional de Desarrollo deberá ser aprobado por la Cámara de Diputados. Así que existen también tanto una ley federal como 32 leyes locales de planeación del desarrollo; por cierto, sin reformar aún para dar cuenta de su nueva versión deliberativa entre ambos poderes, Legislativo y Ejecutivo.

En este contexto, estimo oportuno comentar que aunque antes, al estudiar la maestría en Administración, la materia *Planeación Estratégica* capturó mi atención, me acerqué por primera vez al concepto *prospectiva* al leer el libro de Lucien Sfez –mi director de tesis en la Universidad de París, hoy profesor emérito de La Sorbona– *L'administration prospective*[6].

En principio, la administración habla de actividades cotidianas y la prospectiva del futuro, de tal suerte que a partir de la previsión a mediano y a largo plazo, la programación y la actitud prospectiva de todos los grupos humanos –en los que siempre se enlazan la historia, el mito

4 Consultar: Castellanos Hernández, Eduardo de Jesús, "El proceso administrativo público. Fundamento constitucional", publicado en: *Revista de Administración Pública 134*, Volumen XLIX, No. 2 (mayo-agosto 2014) y en *Buen Gobierno*, Revista No. 18 semestral, Enero-Junio 2015.

5 *Diario Oficial de la Federación* de 10 de febrero de 2014.

6 Librairie Armand Colin, Paris 1970.

y la utopía para llegar, finalmente, a la prospectiva–, Sfez puso el énfasis en los métodos específicos de la administración prospectiva: la informática, la *rationalisation des choix budgetaires* (PPBS[7]) y el plan, para llegar a los procedimientos y los órganos de la administración prospectiva.

Yehezkel Dror, en su ensayo sobre *Un modelo general de planeación*[8] sostiene que la clasificación de los modelos desarrollados en las ciencias sociales corresponden a tres clases principales: modelos matemáticos, en los que se expresan con fórmulas matemáticas las relaciones recíprocas entre las distintas variables; los modelos cualitativos que buscan determinar esas relaciones recíprocas entre variables sin fórmulas matemáticas o cuantitativas y, finalmente, los modelos analíticos que se centran en el diagnóstico de las variables principales y su investigación sistemática.

Russel L. Ackoff en su libro *Un concepto de planeación de empresas*[9], señala que sin duda la planeación es un proceso de toma de decisiones pero que se caracteriza por ser una toma de decisiones anticipadas e interdependientes; distingue entre planeación táctica y planeación estratégica, y atribuye a ésta decisiones de efectos duraderos y difícilmente reversibles, es una planeación a largo plazo que en tanto más actividades de las funciones de la organización afecte, más estratégica será; en tanto que la planeación táctica se refiere a la selección de medios para perseguir objetivos específicos, la planeación estratégica se orienta tanto a los fines como a los medios.

Para Tomás Miklos y María Elena Tello, en su libro *Planeación Prospectiva*[10], planear significa elegir, definir opciones frente al futuro y proveer los medios necesarios para alcanzarlo; el papel de la prospectiva en este proceso implica mirar hacia adelante o imaginar el futuro deseado como un ejercicio necesario en dicho proceso de toma de decisiones. Para dichos coautores, la prospectiva implica

7 Planning, Programming and Budgeting System, *presupuesto por programas* en su versión nacional.
8 Facultad de Ciencias Políticas y Sociales, UNAM, México 1980.
9 Editorial Limusa, México 1979.
10 Centro de Estudios Prospectivos Fundación Javier Barrios Sierra, A. C., Editorial Limusa, México 2018, pp. 59-60.

una visión holística que incluye pasado, presente y futuro; una perspectiva desde el futuro; la conformación de futuros alternativos y la confrontación entre futuros, así como las estrategias y requerimientos para lograr el futuro seleccionado por sobre los simplemente tendenciales. En donde se tiene, por lo tanto, un futuro deseable, pero no probable ni posible; un futuro deseable y posible; un futuro probable y posible pero no deseable, así como esfuerzos, requerimientos y estrategias.

Mi profesor en la Universidad de París, M. Jacques Attali, en su libro *Breve historia del futuro*[11] se refiere a las siguientes olas del futuro: la primera ola, el *hiperimperio*, en el que se "desmantelará primero los servicios públicos, luego la democracia y finalmente los Estados y las naciones", esto es, una primera fase del futuro con un mercado mundial unificado y sin Estados. Luego vendrían –supone– "una serie de guerras de extremada violencia que conducirán a un *hiperconflicto*. Finalmente, ante el fracaso del hiperimperio y del hiperconflicto, nuevos valores conducirán a un nuevo equilibrio, a escala mundial, entre democracia y mercado, a una *hiperdemocracia* planetaria.

No puedo dejar de citar su prospectiva sobre América Latina y sobre México:

> Brasil se propondrá dominar el hemisferio sur de las Américas; Venezuela se esforzará por disputarle ese papel e intentará conseguir la alianza de los países andinos con la intención de echar a los Estados Unidos de la región; México y Argentina no se dejarán marginar. En México, se desatarán importantes revueltas políticas y sociales que pondrán de nuevo en entredicho la alianza con Estados Unidos. Canadá, en cambio, procurará permanecer neutral. Las exigencias de la lucha contra los narcotraficantes impuesta por Estados Unidos exigirán a su vez un refuerzo importante del potencial militar mexicano.

Debemos, pues, o intentemos al menos, imaginar el contenido futuro de las constituciones locales de México –pero también el de la Constitución Federal– en este proceso

11 Ediciones Paidós Ibérica, Barcelona 2007.

mundial y nacional –y no solo local, desde luego– de toma de decisiones político institucionales constructoras de escenarios alternativos de futuro en donde se encuentra inserto.

Antecedentes de la prospectiva constitucional

El análisis prospectivo de las constituciones particulares de las entidades federativas corresponde e involucra, obvia y necesariamente, tanto la perspectiva común que hacia el futuro tienen todas las constituciones de las entidades federativas del país, incluida la más reciente, la de la Ciudad de México[12]; como, de otra parte, la actualización de todas ellas a la luz de la nueva situación política e institucional que vive el país, con motivo de la renovación del Poder Ejecutivo federal, de ambas cámaras federales y de diecinueve legislaturas en otras tantas entidades federativas, ocurrida el año anterior. No podemos dejar de recordar que un día los presidentes, al asumir el cargo, protestan guardar y hacer guardar la Constitución Federal y, a los días siguientes, empieza el desfile de iniciativas de reforma constitucional iniciadas por él o por los legisladores y grupos parlamentarios que lo apoyan.

Durante las campañas electorales del proceso que culminó con la jornada electoral del primero de julio del año pasado, el candidato presidencial de la coalición *Juntos Haremos Historia*, hoy Presidente de la República, propuso al electorado una "cuarta transformación de la república". Se trataba, entonces, de una oferta electoral que, con motivo de la contundente victoria, se ha convertido ahora en el eje rector de las políticas públicas del gobierno federal y en su horizonte prospectivo necesario.

La Cuarta Transformación de la República (4T) tiene como antecedentes la independencia nacional que culminó, si asumimos dichas transformaciones desde una perspectiva constitucional, con la Constitución Federal de 1824; la guerra de reforma, que tuvo como rasgo distintivo la segunda Constitución federal de 1857, y la revolución mexicana que a su vez encontró su justificación e instrumento

12 Publicada en la *Gaceta Oficial de la Ciudad de México* del 5 de febrero de 2017. Se caracteriza por una amplia carta de derechos sin señalar la manera de financiar su materialización.

de cambio con la Constitución vigente de 1917. No es extraño, por lo tanto, que finalmente la Cuarta Transformación que ahora presenciamos y que de alguna manera u otra todos los ciudadanos y ciudadanas mexicanos –por acción u omisión– protagonizamos, desemboque en un nuevo texto constitucional. Mi primera hipótesis, por lo tanto, es que la Cuarta Transformación habrá de culminar en una nueva constitución federal cuyo contenido desconocemos, desde luego, pero que nada impide realizar aquí y ahora el ejercicio prospectivo sobre su contenido deseable y posible.

Ha habido otras constituciones, todos lo sabemos –1814, 1836, 1843 y 1847[13]– además de congresos constituyentes disueltos y dos estatutos imperiales[14]. Pero, sólo la Constitución de 1917 lleva ya, hasta el día de hoy, más de 700 reformas a su articulado mediante 235 decretos de reforma, varias de las cuales entrañan en sí mismas sendas transformaciones de la vida republicana del país; las tres más recientes, publicadas[15], son de la actual Legislatura.

La modificación a profundidad más reciente del texto constitucional, sin duda, es el conjunto de reformas comprometidas y suscritas al inicio del gobierno federal anterior en el documento conocido como *Pacto por México*[16]. Pero tenemos otras, por ejemplo, las reformas de 1996 durante el gobierno del presidente Ernesto Zedillo[17], y que éste llamó "la reforma electoral definitiva", que de alguna manera lo fue, porque permitió la primera alternancia partidista en el Poder Ejecutivo F-Federal.

13 Constitución de Apatzingán, Siete Leyes Constitucionales, Bases Orgánicas, y Acta de Reformas y Restauración del Federalismo y la Constitución de 1824, respectivamente.

14 Consultar: Castellanos Hernández, Eduardo de Jesús; Gómez Galvarriato Freer, Aurora (Coordinadores), *Antecedentes históricos y constituciones políticas de los Estados Unidos Mexicanos*, Secretaría de Gobernación, Cuarta edición octubre de 2009, Segunda reimpresión agosto de 2011, México.

15 *Diario Oficial de la Federación* de 14 y 26 de marzo y de 12 de abril de 2019 (Guardia nacional, extinción de dominio y prisión preventiva oficiosa), respectivamente.

16 Consultar: Zamitiz Gamboa, Héctor (Coordinador), *Pacto por México. Agenda legislativa y reformas 2013-2014*, UNAM, La Biblioteca, México 2016.

17 Consultar: Castellanos Hernández, Eduardo, *Las reformas de 1996*, Centro de Investigación Científica "Jorge L. Tamayo", México, 1998.

Si salimos del plano electoral[18] –donde, por cierto, no podemos olvidar otra gran transformación: la fundación del Partido Nacional Revolucionario[19] en 1929, es decir, la racionalización de la lucha por el poder político al interior del grupo revolucionario triunfante– y vamos al ámbito económico, la prolongada reconstrucción del país después de la guerra civil de 1910 tiene en el modelo económico del desarrollo estabilizador –y unos años antes en la expropiación petrolera–, el punto de arranque de un crecimiento económico sostenido con estabilidad cambiaria.

Aunque ya se tienen algunos indicios con la Ley de Ingresos y el Presupuesto de Egresos de la Federación del año en curso, es de suponerse que las transformaciones a profundidad contenidas en los programas sectoriales, regionales, especiales e institucionales –previstos en la *Ley de Planeación*– se describan en el *Plan Nacional de Desarrollo 2019-2024* que deberá ser discutido y aprobado en la Cámara de Diputados el mes próximo, a partir del proyecto que envíe el Presidente de la República. Tendremos entonces mayores elementos para evaluar los alcances, pertinencia y viabilidad del escenario prospectivo en que se materializará la Cuarta Transformación de la República.

Es de suponerse, también, que el documento *Proyecto de Nación 2018-2024* (Ejes principales: Política y Gobierno; Desarrollo Social; Economía y Desarrollo; Educación, Ciencia, Valores y Cultura), constituye el antecedente obligado del Plan Nacional de Desarrollo 2019-2024, pues en su momento significó parte principal de la oferta electoral adoptada por la mayoría del electorado.

Populismo y presidencialismo

El final del periodo de desarrollo estabilizador se presenta con el llamado desarrollo compartido que, en la práctica, es un populismo económico que genera inflación y devaluaciones de manera recurrente, por diversas razones que no corresponde analizar ahora, pero que son perfectamen-

18 Consultar: Castellanos Hernández, Eduardo de Jesús, *Nuevo Derecho Electoral Mexicano*, UNAM, Trillas, México 2014.

19 Más tarde: Partido de la Revolución Mexicana y, actualmente, Partido Revolucionario Institucional.

te recordadas por los lectores mexicanos, sea porque hayan estudiado ese periodo, porque lo hayan vivido o porque hayan escuchado la historia oral del mismo.[20]

Es oportuno recordar que en el *Diccionario de Política* coordinado por Norberto Bobbio *et al*, se consignan varias definiciones de *populismo*, caracterizadas por la ambigüedad conceptual del término –que desde luego es difícil resolver–, por ejemplo: "todo credo y movimiento basado en la siguiente premisa principal: la virtud reside en el pueblo auténtico que constituye la mayoría aplastante y en sus tradiciones colectivas"; "la legitimidad reside en el pueblo", o bien, el populismo "se basa en dos principios fundamentales: la supremacía de la voluntad del pueblo y la relación directa entre el pueblo y el liderazgo". En rigor, el autor de la voz populismo en el *Diccionario* –Ludovico Incisa– sostiene que "se pueden reagrupar los movimientos populistas en tres categorías: nacional-populista, populista revolucionario y populistas democráticos o pluralistas".

Enrique Cárdenas, en su libro *La política económica en México, 1950-1994*[21], dedica un capítulo al estudio de "El populismo económico mexicano, 1972-1981", caracterizado porque "Las políticas expansionistas a través del gasto público excesivo, tanto corriente como de inversión, se financian a través de emisión monetaria o por endeudamiento externo, lo cual permite impulsar la actividad económica en el corto plazo, con un impacto favorable en el nivel de empleo, pero también con efectos inflacionarios posteriores".

Cuando después de severos programas de ajuste para el pago de la deuda externa por fin se abandona el proteccionismo arancelario de la industria nacional y se abre el mercado nacional a la competencia internacional –donde el momento culminante es la negociación y firma del Tra-

20 Consultar y cfr.: Rivera Ríos, Miguel Ángel, *Desarrollo económico y cambio institucional* (UNAM, Facultad de Economía, Juan Pablos Editor, México 2009); Romero Sotelo, María Eugenia (Coordinación), *Historia del pensamiento económico en México. Problemas y tendencias (1821-2000)* (Trillas, 2005); Núñez Zúñiga, Rafael (Compilador), *La economía mexicana, de la sustitución de importaciones a la promoción de exportaciones* (Trillas, 2014); Garrido, Celso, *Desarrollo económico y procesos de financiamiento en México,* UAM Azcapotzalco, Siglo XXI Editores, México 2005.

21 El Colegio de México, Fondo de Cultura Económica, México 1996, pp. 86-117.

tado de Libre Comercio para América del Norte, renegociado y renombrado como T-Mec, pero que espera todavía la aprobación del congreso americano–, entramos al periodo que algunos con optimismo llamaron de *liberalismo social* y otros, despectivamente, de *neoliberalismo*. Recientemente, por cierto, el Presidente de la República anunció la terminación oficial del periodo neoliberal.

Independientemente de la denominación que pueda darse a los diferentes periodos que he mencionado –aunque no de manera exhaustiva, desde luego, porque puede haber varias transformaciones más dependiendo de los indicadores o parámetros que adoptemos para el análisis, como nuevamente veremos en seguida–, en todos los casos hablamos de un Estado nacional, federal, con economía mixta y con una mayor o menos intervención estatal en la economía que va desde la promoción y atracción de inversiones extranjeras –como sucedió durante el gobierno del general Porfirio Díaz[22]– pasando por el monopolio estatal en ciertas actividades económicas –antes en correos o ferrocarriles, después en Pemex y Comisión Federal de Electricidad–, hasta la función estatal de regular y garantizar la libre competencia en una economía de mercado abierta al exterior. Y no tengo duda de que es aquí donde estamos todavía ahora, aunque a veces parezca que se quiere salir hacia otro escenario económico aún por definir, sin que se pueda modificar de golpe, desde luego, la estructura económica a la que hemos llegado hasta hoy.

Hay un libro reciente de José Roldán Xolpa, *La ordenación constitucional de la economía. Del Estado regulador al Estado garante*, publicado por el Fondo de Cultura Económica[23] con una presentación de José Ramón Cossío, cuya lectura no puedo dejar de recomendar de manera entusiasta para estudiar la etapa actual hasta antes de los intentos de cambio.

Por su vinculación habitual con el populismo, me refiero ahora, de entre las muchas clasificaciones que hay del

22 Consultar: Ávila Ortiz, Raúl; Castellanos Hernández, Eduardo de Jesús; Hernández, Pilar (Coordinadores), *Porfirio Díaz y el derecho. Balance crítico*, Cámara de Diputados, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, México 2015.

23 México, 2018.

presidencialismo latinoamericano, a la formulada por Jorge Carpizo[24] en un artículo publicado *post mortem* donde señala que la tipología del *presidencialismo latinoamericano* debe contemplarse desde tres ángulos o perspectivas: la de la norma constitucional, la de la realidad constitucional y la de la interacción de la norma con la realidad constitucional.

Desde la perspectiva de la norma constitucional distingue cinco tipos: presidencialismo puro, predominante, atemperado, con matices parlamentarios y parlamentarizado. En tanto que desde la perspectiva de la realidad constitucional distingue tres: hegemónico, equilibrado y débil.

Desde la perspectiva de la interacción de la norma con la realidad constitucional la tipología se forma con los señalados en las otras dos perspectivas, de manera que los presidencialismos puro, predominante, atemperado y con matices parlamentarios pueden ser hegemónicos, equilibrados o débiles. Para Carpizo el presidencialismo parlamentarizado sólo puede ser hegemónico o débil pues su naturaleza excluye el tipo equilibrado.

Concluyo este acápite refiriéndome a otro libro de Jorge Carpizo, *El presidencialismo mexicano*[25], escrito durante el periodo de la anterior hegemonía presidencial y partidista, en el que identifica las siguientes facultades que denomina *metaconstitucionales* del Presidente de la República: jefatura real del partido gobernante, designación de su sucesor, designación de los gobernadores y remoción de los gobernadores.

La posterior etapa de los gobiernos divididos nos enseñó que dichas facultades metaconstitucionales tenían un origen, a su vez, perfectamente identificable: la mayoría absoluta y calificada que en ambas cámaras federales y en las legislaturas locales poseía el partido político del que el presidente era el jefe real.

24 "Propuesta de una tipología del presidencialismo latinoamericano", publicado en: Vázquez Ramos. Homero (Coordinador), *Cátedra Nacional de Derecho Jorge Carpizo. Reflexiones Constitucionales*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, México 2014.

25 Siglo Veintiuno Editores, Cuarta edición, México 1984.

Las transformaciones jurídicas

No puedo dejar de referirme a los indicadores o temas estrictamente jurídicos, recientes, de transformación del ordenamiento, de los ordenamientos y de la manera de aplicarlos e interpretarlos. Para ello debo referirme a un estudio académico, coordinado por Héctor Fix Fierro y Diego Valadés en el Instituto de Investigaciones Jurídicas de la UNAM, publicado en 2015[26], con una propuesta de texto reordenado y consolidado de la Constitución Política de los Estados Unidos Mexicanos, en el que se señalan las siguientes materias más importantes para dichos investigadores en las que ha sido reformada la Constitución:

- Control de la constitucionalidad de las leyes
- Autonomía de gobierno y administración de los municipios
- Sistema electoral y representativo (federal y local)
- Derechos fundamentales, tanto individuales como sociales, y sus medios de protección
- Derechos y autonomía de los pueblos indígenas
- Propiedad y justicia agrarias
- Transparencia y acceso a la información pública gubernamental
- Sistemas de justicia penal y seguridad pública
- Presupuesto, control del gasto público y rendición de cuentas
- Relaciones del Estado con las iglesias y las comunidades religiosas
- Independencia, gobierno y carrera judiciales
- Rectoría del Estado sobre el desarrollo nacional y sistema de planeación democrática
- Explotación de recursos energéticos y empresas productivas del Estado

Me refiero ahora a cinco aspectos fundamentales actuales, vigentes, de la transformación jurídica que se vive hoy en México:

- El nuevo proceso penal acusatorio y oral que ha modificado la distribución de competencias en ma-

26 *Constitución Política de los Estados Unidos Mexicanos. Texto reordenado y consolidado. Estudio académico*, LXII Legislatura de la Cámara de Diputados, UNAM, Instituto de Investigaciones Jurídicas, México: julio de 2015.

teria adjetiva y, previsiblemente, también sustantiva, habiendo dado paso, por lo menos, a cuatro leyes nacionales (nueva manera de llamar a la federalización o centralización de antiguas facultades concurrentes entre Federación y entidades federativas): el Código Nacional de Procedimientos Penales[27], la Ley Nacional de Mecanismos Alternativos de Solución de Controversias en Materia Penal[28], la Ley Nacional de Ejecución Penal[29]y la Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes[30].

- Los procedimientos para favorecer la competencia económica resueltos por nuevos organismos constitucionales autónomos, la Comisión Federal de Competencia Económica y el Instituto Federal de Telecomunicaciones, así como en materia de energía por los órganos reguladores coordinados en la materia, la Comisión Reguladora de Energía y la Comisión Nacional de Hidrocarburos.
- Las reformas constitucionales en materia de fiscalización, transparencia y rendición de cuentas que culminaron con la reforma constitucional[31], el diseño e implementación del Sistema Nacional Anticorrupción. No puedo dejar de sugerir la lectura de los cuatro tomos –el quinto está en prensa– de la colección *Fiscalización, Transparencia y Rendición de Cuentas*, publicada por la Unidad de Evaluación y Control de la Comisión de Vigilancia de la Auditoría Superior de la Federación de la Cámara de Diputados, en cuya redacción he participado con mis contribuciones personales en cada tomo. Igualmente, sugiero la lectura del libro colectivo más reciente en el que participo, publicado este año en España por tirant lo Blanch, de Valencia, *Rendición de cuentas, control parlamentario y políticas públicas en México*[32].

27 *Diario Oficial de la Federación* de 5 de marzo de 2014.
28 *DOF* de 29 de diciembre de 2014.
29 *DOF* de 16 de junio de 2016.
30 *DOF* de 16 de junio de 2016.
31 *Diario Oficial de la Federación* de 27 de mayo de 2015.
32 Moreno Espinosa, Roberto; Escobar Roca, Guillermo; Covarrubias Moreno, Óscar Mauricio (Editores), Valencia 2019.

- La reforma constitucional en materia laboral[33] que, gracias a la presión internacional, particularmente la proveniente de nuestro vecino del norte, finalmente encontrará al parecer muy pronto su regulación secundaria, y
- Todo lo que implica el nuevo modelo de control difuso *ex officio* de constitucionalidad y convencionalidad, para cuyo estudio no puedo dejar de sugerir la lectura de dos libros de César Astudillo intitulados *El bloque y el parámetro de constitucionalidad en México*[34] y *El funcionamiento de la Suprema Corte de Justicia de la Nación como tribunal constitucional*[35].

Hasta aquí la historia y el presente del desarrollo constitucional nacional, al interior o a partir del cual es necesario construir los escenarios de futuro del contenido de nuestras leyes fundamentales, la federal y las locales.

Hipótesis centrales y suposiciones auxiliares

Después de estos antecedentes que me parecen obligados e ilustrativos trataré ahora de formular varias hipótesis más sobre el futuro previsible y deseable de las constituciones locales de las entidades federativas del país.

En primer lugar, como ya lo he señalado, es necesario identificar o definir la nueva situación política en la que nos encontramos. Sostengo que el gobierno del presidente Andrés Manuel López Obrador es un gobierno populista nacionalista de izquierda y también un presidencialismo hegemónico que rescata las facultades metaconstitucionales del anterior periodo hegemónico. He adelantado ya algunos conceptos y elementos para justificar estas denominaciones, tarea que realizo con mayor amplitud en el libro que actualmente preparo intitulado *Populismo, Cuarta Transformación y Control Democrático del Poder en México hoy*, del cual adelanto en este artículo algunos elementos.

Las reformas constitucionales recientes, en curso o anunciadas, pero correspondientes ya al gobierno federal

33 *Diario Oficial de la Federación* de 27 de junio de 2017.
34 UNAM, tirant lo blanch, México 2014.
35 UNAM, tirant lo blanch, México 2019.

actual y su mayoría parlamentaria –Guardia Nacional, extinción de dominio, prisión preventiva oficiosa, revocación del mandato, reforma educativa, cinco nuevos integrantes de la Suprema Corte de Justicia de la Nación y, al parecer, supresión del Consejo de la Judicatura Federal– sostengo también como hipótesis central que no impiden ni cancelan la posibilidad de una nueva Constitución federal.

En su libro *2018 La Salida. Decadencia y renacimiento de México*[36], el entonces candidato presidencial Andrés Manuel López Obrador no se refiere a ninguna reforma constitucional, ni gradual ni integral. Propone, en cambio, las siguientes "Decisiones básicas para el renacimiento económico y social de México": 1) El rescate del campo y de su importancia social, ambiental y cultural y la autosuficiencia alimentaria; 2) Rescate del sector energético y su utilización como palanca del desarrollo; 3) Impulso al crecimiento y generación de empleos; 4) Estado de bienestar; 5) Sociedad segura; 6) Una República fraterna.

Me parece que a todos nos queda muy claro que la tercera alternancia en el Poder Ejecutivo Federal, pero ahora –a diferencia de las dos anteriores– con 30 millones de votos, una amplia mayoría en ambas cámaras federales y en diecinueve legislaturas locales, nos ha hecho transitar del gobierno dividido –un Ejecutivo sin mayoría en las cámaras– a un *neopresidencialismo* mexicano ya no sustentado solamente en un partido hegemónico sino, además, en un liderazgo carismático que, tal vez, me atrevo a afirmar, ningún presidente anterior había logrado alcanzar, aunque pudo haber varios que lo hayan intentado.

En mi libro *Técnica legislativa, control parlamentario y gobiernos de coalición*[37], publicado el año pasado, hice notar el riesgo de que un gobierno de coalición con amplia mayoría en las cámaras pudiera banalizar o superar los controles parlamentarios propios de un sistema democrático. Sostengo ahora que dicho peligro es todavía mayor en el *neopresidencialismo* donde no existen los contrapesos políticos propios de un gobierno de coalición.

36 Primera edición en formato epub: febrero de 2017; primera edición en formato impreso: febrero de 2017; primera reimpresión en este formato (Editorial Planeta): mayo de 2018, pp. 177-270.

37 Instituto Internacional del Derecho y del Estado, Editorial Flores, México 2018.

Más aún, mediante reformas constitucionales como las que ya se han anunciado –elevar en cinco el número de integrantes de la Suprema Corte–, no sólo los controles políticos sino también los controles constitucionales y convencionales pueden ser superados.

Cabe precisar que en el supuesto caso de una reforma constitucional integral o de la convocatoria a un congreso constituyente para la Cuarta Transformación de la República que pase o incluya una modificación y actualización constitucional, de cualquier forma, el control constitucional y convencional vía amparo es improcedente, pero también vía acción de inconstitucionalidad o controversia constitucional o mediante algún medio de impugnación en materia electoral.

Regreso a las constituciones locales: sostengo ahora que la reforma de cualquier otra entidad federativa, en el supuesto previsible –no sé si deseable, lo veremos en seguida– de una reforma integral de la Constitución Federal de 1917 o de una nueva constitución federal, estaría totalmente en función de la modificación federal que pudiese haber. A esta hipótesis general agrego una suposición auxiliar: ante este escenario, difícilmente el gobernador de un estado o la jefa de gobierno de la Ciudad de México podrían emprender o auspiciar o aceptar una reforma de fondo en este momento a sus ordenamientos constitucionales locales.

Esta afirmación nos obliga a regresar al plano constitucional nacional y a formular propuestas viables y útiles como consecuencia de la hipótesis central: la Cuarta Transformación tendrá su propia Constitución y hay que formular propuestas al efecto.

Paulatinamente, academia, organizaciones no gubernamentales, partidos políticos, organizaciones sindicales y patronales, y demás grupos sociales, habrán de bosquejar algunas, pero antes es necesario dejar claro que el modelo económico de economía mixta con intervención, regulación y garantía estatal es un modelo económico que sólo tiene, en mi opinión, alguno de los siguientes cursos de actualización: pasar a un mayor intervencionismo estatal, pasar a una mayor regulación y garantía o plantear una ruptura con el pasado inmediato mediante una ruptura de alianzas geopolíticas estratégicas.

Vayamos ahora al plano político. Me sustento aquí en el libro clásico de Karl Loewenstein, *Teoría de la Constitución*, cuando se refiere a los controles horizontales y verticales del poder político. Los controles verticales, sostiene, son intraórganos –en el gobierno y en el parlamento– e interórganos –controles del parlamento frente al gobierno, controles del gobierno frente al parlamento, de los tribunales frente al gobierno y el parlamento, y del electorado frente al gobierno y el parlamento–, y los verticales –federalismo, garantías de las libertades individuales (derechos humanos y sus garantías, para usar nuestra fraseología nacional actual) y pluralismo–. Pero el primero y fundamental control democrático del poder político, afirma Loewentein, es una constitución democrática.

En su libro *El control del poder*, Diego Valadés estudia dicho control desde una triple perspectiva: como problema (legitimidad democrática y sistema representativo), como fenómeno (función, responsabilidad, Estado de derecho y orden) y como proceso (en España, Estados Unidos y México). Propone al efecto la siguiente tipología de los controles: materiales y formales; unidireccionales y bidireccionales; organizativos y funcionales; preventivos y correctivos; perceptibles e imperceptibles; constitucionales y paraconstitucionales. Propone finalmente otras posibilidades de encuadramiento: de acuerdo con su naturaleza: obligatorios y potestativos; con su objeto: constructivos y limitativos; con sus efectos: vinculatorios e indicativos; con su frecuencia: sistemáticos y esporádicos; con su forma: verbales y formales; con sus agentes: colectivos y selectivos; con sus destinatarios: generales o singulares; con su oportunidad: previos, progresivos y posteriores.

Consecuentemente, sea a través de una reforma integral apoyada en el procedimiento de reformas previsto en el artículo 135 constitucional vigente[38] o sea mediante la

38 "La presente Constitución puede ser adicionada o reformada. Para que las adiciones o reformas lleguen a ser parte de la misma, se requiere que el Congreso de la Unión, por el voto de las dos terceras partes de los individuos presentes, acuerden las reformas o adiciones, y que éstas sean aprobadas por la mayoría de las Legislaturas d ellos Estados y de la Ciudad de México".

convocatoria a un congreso constituyente[39], las opciones fundamentales económicas a elegir ya han sido planteadas, en tanto que la forma de gobierno tendría que iniciar por la elección entre presidencialismo, semipresidencialismo[40] o parlamentarismo, y las modalidades que pudiera tener el formato constitucional de gobierno adoptado. Sin dejar de tener en cuenta la adopción o modificaciones que pudieran surgir a las reformas a que ya me he referido.

Conclusiones y propuestas

Sostengo y propongo, en consecuencia, desde una perspectiva cualitativa pero también analítica, que ante una eventual nueva Constitución federal para materializar el modelo político, económico y social que propone la denominada Cuarta Transformación, se analicen, con rigor y objetividad, e incluyan todas las instituciones y procedimientos necesarios para asegurar la eficacia, eficiencia y efectividad del sistema productivo que permitan el crecimiento económico y el desarrollo social, para cerrar la brecha de la terrible desigualdad social existente, donde más de la mitad de los mexicanos vive en pobreza o pobreza extrema. La permanencia y viabilidad de México como país democrático sólo puede fincarse en la inmediata reducción y futura desaparición de dicha desigualdad lacerante entre las y los mexicanos.

El control más efectivo del electorado frente al gobierno y el parlamento es el diseño del sistema de representación y del sistema electoral y, en el caso de este último, la elección sólo puede ser entre sistemas de mayoría, de representación proporcional pura y sistemas mixtos. La Asamblea Constituyente de la Ciudad de México fue formada a partir

39 Las reformas integrales a las constituciones locales se han basado en un artículo equivalente al 135 federal citado. La nueva Constitución de la Ciudad de México provino de una reforma al artículo 122 constitucional federal que regulaba el gobierno local del entonces Distrito Federal; el diseño y convocatoria al Congreso Constituyente respectivo quedaron establecidos en los artículos transitorios del decreto de reforma correspondiente.

40 El semipresidencialismo estuvo vigente de 1993 a 1996 en el texto de la Constitución federal para efecto de gobierno local de la hoy Ciudad de México; antes, el jefe del departamento administrativo encargado del gobierno local del entonces Distrito Federal era nombrado y removido libremente por el presidente de la república. Actualmente, se mantiene el modelo presidencialista para el gobierno local de la Ciudad de México, mediante la elección por separado del jefe de Gobierno de la Ciudad y de los diputados a su Asamblea Legislativa.

de un sistema mixto complejo con elección directa, indirecta y designación personal que muy poco tuvo de democrático y que no debe repetirse[41]. Luego, entonces, sostengo que la representación proporcional pura es el único sistema electoral idóneo para que la voluntad popular se exprese en esta circunstancia de definición del contenido de la Constitución.

Consecuentemente, por lo que entraña para el rumbo futuro de la nación y porque en las tres transformaciones anteriores fueron convocados otros tantos congresos constituyentes, la elección entre una u otra alternativa no podría darse por el Constituyente Permanente de la República o Poder Revisor de la Constitución previsto en el 135 constitucional, sino sólo por un Congreso Constituyente integrado –propongo– con por lo menos 500 diputados constituyentes electos a partir del principio de representación proporcional pura, pero en el que 300 hubiesen sido postulados por partidos políticos nacionales y locales, pero 200, necesariamente, autopostulados como candidatos independientes auténticamente ciudadanos, en número proporcional a la población de la entidad federativa en la que fuesen electos.

Una palabra más sobre el proyecto de Constitución. Para la Ciudad de México, el Jefe de Gobierno envió un proyecto de Constitución que, con algunas modificaciones, finalmente fue aprobado[42]. La Constitución federal vigente de 1917 surgió del proyecto, reformado, enviado

41 Artículos Transitorios del Decreto publicado en el Diario Oficial de la Federación el día 29 de enero de 2016 Artículo Séptimo. La Asamblea Constituyente de la Ciudad de México se compondrá de cien diputados constituyentes, que serán elegidos conforme a lo siguiente: A. Sesenta se elegirán según el principio de representación proporcional, mediante una lista votada en una sola circunscripción plurinominal . B. Catorce senadores designados por el voto de las dos terceras partes de los miembros presentes de la Cámara, a propuesta de su Junta de Coordinación Política . C. Catorce diputados federales designados por el voto de las dos terceras partes de los miembros presentes de la Cámara, a propuesta de su Junta de Coordinación Política D. Seis designados por el Presidente de la República. E. Seis designados por el Jefe de Gobierno del Distrito Federal.

42 Consultar: Castellanos Hernández, Eduardo de Jesús, "Evaluación *ex ante*, *in itinere* y *ex post* de la norma y del ordenamiento como política pública y técnica legislativa. Un estudio de caso: la Constitución Política de la Ciudad de México", publicado en: Moreno Espinosa, Roberto, Escobar Roca Guillermo, Covarrubias Moreno, Óscar Mauricio (Editores), tirant lo blanch, Valencia 2019, España.

por el Primer Jefe del Ejército Constitucionalista, en un momento de reposo de la lucha armada y de los atentados entre jefes revolucionarios. El proyecto de una eventual nueva Constitución federal sólo puede surgir del debate democrático entre los diputados constituyentes electos por el pueblo, como nació la Constitución de 1857.

En este plano político-electoral, la Constitución de la Cuarta Transformación sólo puede ser de fortalecimiento de los controles democráticos del poder político, y aquí han quedado expuestos algunos de los que han sido clasificados en la doctrina especializada. Durante los últimos cuarenta años, la transición mexicana a la democracia nos trajo a un punto en el que se permitió la alternancia partidista por tres veces en el Ejecutivo federal y muchas más en los ejecutivos y legislativos locales. Este resultado del ejercicio soberano de la ciudadanía no puede menos que ser ampliamente fortalecido por una eventual nueva constitución, que surja e impulse la cuarta transformación prometida por la nueva élite gobernante y que el pueblo le demande, elija y apruebe.

BIBLIOGRAFÍA

Ackoff, Russel L, *Un concepto de planeación de empresas,* Editorial Limusa, México 1979.

Astudillo, César, *El funcionamiento de la Suprema Corte de Justicia de la Nación como tribunal constitucional,* UNAM, tirant lo blanch, México 2019.

_____, *El bloque y el parámetro de constitucionalidad en México,* UNAM, tirant lo blanch, México 2014.

Attali, Jacques, *Breve historia del futuro,* Ediciones Paidós Ibérica, Barcelona 2007.

Ávila Ortiz, Raúl, Castellanos Hernández, Eduardo de Jesús, Hernández, Pilar (Coordinadores), *Porfirio Díaz y el derecho. Balance crítico*, Cámara de Diputados, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, México 2015.

Cárdenas, Enrique, *La política económica en México, 1950-1994,* El Colegio de México, Fondo de Cultura Económica, México 1996.

Carpizo, Jorge, "Propuesta de una tipología del presidencialismo latinoamericano", publicado en: Vázquez Ramos.

Homero (Coordinador), *Cátedra Nacional de Derecho Jorge Carpizo. Reflexiones Constitucionales*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, México 2014.

_____, *El presidencialismo mexicano,* Siglo Veintiuno Editores, Cuarta edición, México 1984.

Castellanos Hernández, Eduardo de Jesús, "Evaluación *ex ante*, *in itinere* y *ex post* de la norma y del ordenamiento como política pública y técnica legislativa. Un estudio de caso: la Constitución Política de la Ciudad de México", publicado en: Moreno Espinosa, Roberto, Escobar Roca, Guillermo, Covarrubias Moreno, Óscar Mauricio (Editores), *Rendición de cuentas, control parlamentario y políticas públicas en México,* tirant lo blanch, Valencia, España 2019.

_____, *Técnica legislativa, control parlamentario y gobiernos de coalición,* Instituto Internacional del Derecho y del Estado, Editorial Flores, México 2018.

_____, "El proceso administrativo público. Fundamento constitucional", publicado en: *Revista de Administración Pública 134*, Volumen XLIX, No. 2 (mayo-agosto 2014) y en *Buen Gobierno*, Revista No. 18 semestral, Enero-Junio 2015, México.

_____, *Nuevo Derecho Electoral Mexicano*, UNAM, Trillas, México 2014.

_____, *Las reformas de 1996*, Centro de Investigación Científica "Jorge L. Tamayo", México 1998.

_____, Gómez Galvarriato Freer, Aurora (Coordinadores), *Antecedentes históricos y constituciones políticas de los Estados Unidos Mexicanos*, Secretaría de Gobernación, Cuarta edición octubre de 2009, Segunda reimpresión agosto de 2011, México.

Diario Oficial de la Federación.

Diccionario de la Lengua Española, Real Academia Española, Vigésima primera edición.

Dror, Yehezkel, *Un modelo general de planeación,* Facultad de Ciencias Políticas y Sociales, UNAM, México 1980.

Fix Fierro, Héctor, Valadés, Diego (Coordinadores), *Constitución Política de los Estados Unidos Mexicanos. Texto reordenado y consolidado. Estudio académico*, LXII Legislatura de la Cámara de Diputados, UNAM, Instituto de Investigaciones Jurídicas, México: julio de 2015.

Gaceta Oficial de la Ciudad de México.

Garrido, Celso, *Desarrollo económico y procesos de financiamiento en México,* UAM Azcapotzalco, Siglo XXI Editores, México 2005.

López Obrador, Andrés Manuel, *La salida. Decadencia y renacimiento de México,* Primera edición en formato epub: febrero de 2017; primera edición en formato impreso: febrero de 2017; primera reimpresión en este formato (Editorial Planeta): mayo de 2018.

Miklos, Tomás, Tello, María Elena, *Planeación Prospectiva,* Centro de Estudios Prospectivos Fundación Javier Barrios Sierra, A. C., Editorial Limusa, México 2018, pp. 59-60.

Núñez Zúñiga, Rafael (Compilador), *La economía mexicana, de la sustitución de importaciones a la promoción de exportaciones*, Editorial Trillas, México 2014.

Rivera Ríos, Miguel Ángel, *Desarrollo económico y cambio institucional*, UNAM, Facultad de Economía, Juan Pablos Editor, México 2009.

Roldán Xolpa, José, *La ordenación constitucional de la economía. Del Estado regulador al Estado garante,* Fondo de Cultura Económica, México 2018.

Romero Gudiño, Alejandro, Bolaños Cárdenas, Leonardo (Coordinadores), *Fiscalización, transparencia y rendición de cuentas* (4 tomos), Cámara de Diputados, Comisión de Vigilancia de la Auditoría Superior de la Federación, Unidad de Evaluación y Control, México, 2014, 2015, 2016 y 2017.

Romero Sotelo, María Eugenia (Coordinación), *Historia del pensamiento económico en México. Problemas y tendencias (1821-2000),* Editorial Trillas, México 2005.

Sfez, Lucien, *L'Administration Prospective*, Librairie Armand Colin, Paris 1970.

Zamitis Gambia, Héctor (Coordinador), *Pacto por México. Agenda legislativa y reformas 2013-2014*, UNAM, La Biblioteca, México 2016.

Revista de Administración Pública

INAP

La evolución del pensamiento sobre la "administración pública" a la luz de los clásicos: un breve recorrido histórico (siglo XVI al siglo XX)

José Joel Peña Llanes

Resumen: El objetivo de este artículo es presentar una breve descripción de la evolución del pensamiento sobre la "administración pública" a partir de lo expuesto por pensadores clásicos de occidente que publicaron sus obras entre el siglo XVI y las primeras décadas del siglo XX. Lo anterior, a efecto de comprobar que la administración pública es un elemento intrínseco de las relaciones entre la sociedad y el Estado y que su estudio ha evolucionado de manera paralela al desarrollo de los propios Estados-nación, especialmente en el contexto de conflictos bélicos. Para cumplir dicho objetivo, el artículo incluye una tabla que concentra las definiciones de administración pública en orden cronológico, así como los años de nacimiento y fallecimiento de los pensadores que las dilucidaron y su formación académica y profesional.

Palabras clave: administración pública, pensadores administrativistas, Estado-nación.

The evolution of thinking about "public administration" in the light of the classics: a brief historical journey (16th to 20th century)

The objective of this article is to present a brief description of the evolution of thinking about "public administration" based on the works published by classical thinkers from the West between the 16th century and the first decades of the 20th century. The foregoing, in order to confirm that public administration is an intrinsic element of the relation between society and the State and that its study has evolved parallel to the development of States, especially in the context of armed conflicts. To accomplish its purpose, the article includes a table containing the definitions of public administration in chronological order, as well as the years of birth and death of thinkers who elucidated those definitions and their academic and professional training.

Keywords: public administration, administrative thinkers, Nation-State.

Fecha de recepción: 20 de febrero de 2019
Fecha de aceptación: 19 de marzo de 2019

Revista de Administración Pública

INAP

La evolución del pensamiento sobre la "administración pública" a la luz de los clásicos: un breve recorrido histórico (siglo XVI al siglo XX)*

José Joel Peña Llanes**

1. Introducción

El objetivo de este artículo es presentar una breve descripción de la evolución del pensamiento sobre la "administración pública" a partir de las aportaciones de pensadores clásicos de occidente (Europa, México y Estados Unidos) que publicaron sus obras entre el siglo XVI y las primeras décadas del siglo XX. Lo anterior, a efecto de comprobar que la administración pública es un elemento intrínseco de las relaciones entre la sociedad y el Estado y que su estudio ha evolucionado de manera paralela al desarrollo de los propios Estados-nación, especialmente en el contexto de conflictos bélicos. Es por ello que, aun cuando nuestra intención principal es explicar la evolución conceptual, a lo largo del texto se hace referencia a ciertos hechos históricos que, a nuestro juicio, influyeron de manera especial en dicho desarrollo cognitivo.

* Fecha de elaboración: junio de 2018

** Licenciado en Relaciones Internacionales y Maestro en Estudios en Relaciones Internacionales, ambos grados por la Universidad Nacional Autónoma de México (UNAM). Actualmente, cursa el Doctorado en Administración Pública en el Instituto Nacional de Administración Pública, A.C. (INAP). Funcionario adscrito a la Dirección General de Asuntos Internacionales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Profesor de asignatura adscrito al Centro de Relaciones Internacionales de la Facultad de Ciencias Políticas y Sociales de la UNAM.

Para cumplir con el objetivo planteado, el artículo incluye una tabla con las definiciones y aportaciones sobre la administración pública que han realizado distintos autores, la cual está ordenada de manera cronológica e incluye datos biográficos de los propios autores para comprobar que su contexto y formación académica y profesional tienen una relación directa con su visión sobre la materia que nos ocupa.

En cuanto a la estructura del texto, se decidió recurrir a dos criterios específicos: el orden cronológico de las aportaciones de los autores referidos y el país o región geográfica a la que pertenecen. Por lo tanto, el recorrido histórico inicia necesariamente en Europa, para después retomar a los autores mexicanos y finalmente a los de origen estadounidense, quienes desarrollan una perspectiva novedosa de la administración pública utilizando conceptos de la administración privada.

Finalmente, es importante aclarar que los autores que se exponen en este artículo se seleccionaron en virtud de sus aportaciones para la construcción de la ciencia de la administración pública. Sin embargo, la lista es enunciativa, más no limitativa, pues existen muchos otros pensadores, particularmente administrativistas, de diferente procedencia que también podrían considerarse como "clásicos" porque realizaron contribuciones igual de importantes a este campo de estudio pero que no se incluyeron por cuestiones de espacio.

2. Breve recorrido histórico de la conceptualización de la administración pública en Europa

Iniciaremos este apartado haciendo alusión a Jean Bodin, un jurista francés proveniente de una familia acomodada, que, adelantándose a la creación formal de los Estados-nación, escribió, en plena época renacentista (a mediados del siglo XVI), que existe una diferencia entre el Estado y la sociedad, pues el primero detenta el poder soberano y, por ende, le corresponde mantener unificada a la sociedad.

Dos siglos después, Johann Heinrich Gottlob von Justi y Karl vom Stein de origen alemán y prusiano respectivamente, desarrollaron una disciplina denominada ciencia de la policía que tenía la encomienda de arreglar todas las

cosas relativas al Estado con el fin último de mejorar a la sociedad para que sus miembros alcancen la felicidad. El advenimiento de esta ciencia, la cual retoma la tarea que Bodin le asignó al Estado, marcó el inicio de lo que después se reconocería como administración pública.

Por su parte, Wilhelm von Humboldt se refirió no sólo al alcance de la actividad del Estado en términos de todo aquello que puede realizar en bien de la sociedad, sino que puntualizó la necesidad de definir, al interior de cualquier Estado, la verdadera organización del gobierno y las instituciones que se propongan mantener o fomentar el bienestar físico de la nación.

En Francia, durante la época de la Ilustración, concretamente después de la Revolución Francesa de 1789, un grupo de juristas y políticos criticaron los fundamentos que sostenían a la sociedad del Antiguo Régimen, argumentando que la razón humana podía combatir los gobiernos tiránicos y, de esta forma, allegarse de bienes para satisfacer las necesidades personales y sociales.

Así, en el contexto ilustrado surge la figura de Charles-Jean Baptiste Bonnin, quien escribió, entre muchos otros libros, uno titulado "Doctrina Social, textualmente formada por las declaraciones de los derechos franceses y americanos". En dicha publicación, que data de 1820 y cuyo contenido no es específicamente de administración pública, destaca el siguiente fragmento:

> Es bueno que el padre se ocupe de la administración de su familia y se ocupe de la atención doméstica, ya que tiene la atribución de sus intereses, la confianza que su esposa merece y que él tiene en ella; porque esta supervisión es un deber así como un alivio, y pertenece al gobierno de la familia, al mantenimiento de la unión y a la preservación de la propiedad: la indiferencia o el orgullo que descuida esta vigilancia y estos cuidados, es un olvido de sus deberes, de los cuales uno es castigado por el vacío y el aburrimiento en su casa, y frecuentemente por el trastorno de su fortuna.[1]

1 Charles-Jean Baptiste Bonnin, *Doctrine Sociale, textuellement formée des déclarations de droits françaises et américaines*, París, Paulin, 1833, p. 146.

Una de las aportaciones de Bonnin, quien es considerado por muchos estudiosos como el padre de la administración pública, fue precisamente encontrar un símil entre el deber de un padre para con su familia y el del gobierno para con su pueblo a través de la administración pública. No obstante, el autor va más allá de esta concepción cuando establece un vínculo inherente entre la administración y la sociedad misma.

> La administración es una consecuencia natural del estado social, como este lo es da la sociabilidad natural del hombre: su naturaleza es un resultado de la comunidad, pues desde el momento en que existe pacto social, hay administración: así es, que siempre encontramos la naturaleza, ha en el despotismo. Es, pues, evidente, que la administración no toma su principio en convenios humanos, sino que es un fenómeno procedente de la existencia misma de la sociedad, sin que los convenios o leyes sirvan más que para organizarla, es decir, para determinar su modo de existir, pues su existencia procede de los mismos principios que la de la sociedad. [...] Definiré pues así la administración pública: es una potencia que arregla, corrige y mejora cuanto existe y da una dirección más conveniente a los seres organizados y a las cosas. Como ciencia, tiene su doctrina propia, determinada por la naturaleza de los objetos que abraza; como establecimiento social tiene sus elementos legislativos, derivados de la naturaleza de las cosas que arregla. Instituida para velar en los pueblos sobre las personas y bienes en sus relaciones públicas y hacerlos concurrir a la común utilidad, es el gobierno de la comunidad en su acción ejecutiva directa de aplicación [...].[2]

En efecto, de acuerdo con Bonnin, la administración pública, en su vertiente de ciencia y arte, al nacer de la propia comunidad, tiene como fin último conservar a los individuos y sus relaciones, es decir, a la sociedad misma, mediante la conjugación del interés público y los intereses particulares y a través de la institución de la

2 Charles-Jean Baptiste Bonnin, *Compendio de los Principios de Administración*, Madrid, Imprenta de Don José Palacios, 1834, pp. 14 y 37.

administración: el gobierno. Dicho de otro modo, la acción social es el carácter de la administración pública y la ejecución de las leyes para mantener el orden y garantizar el bien público es su atribución.

A diferencia de los pensadores mencionados hasta el momento, Bonnin ya no se refiere al Estado como el garante del bienestar social, sino sólo a una parte de éste que denomina administración pública y que conforma una estructura compleja y abarcadora que, como veremos más adelante, se diferencia de la justicia y de la política.

Otros dos pensadores franceses, M. R. Gandillot y M. Macarel, cuya biografía se desconoce, o al menos es de difícil acceso, también hicieron contribuciones importantes. Gandillot señala que el derecho administrativo es una demostración de los deberes de la sociedad para con los ciudadanos y de éstos hacia la sociedad, lo cual nos refiere a la relación simbiótica entre la sociedad y la administración y, por ende, al hecho de que una no puede existir sin la otra.

Por su parte, M. Macarel afirma que la administración es la acción vital del gobierno y el brazo de la sociedad. Esta metáfora sirvió para argumentar que, independientemente del Estado del que se trate, la administración está basada en reglas generales y absolutas que, de acuerdo con Macarel, se refieren a la protección y seguridad, a la beneficencia pública, a la educación pública y a las vías de comunicación, como elementos que deberá proveer el gobierno para garantizar el bienestar social.

Ahora es momento de referirnos a los autores españoles, pues su pensamiento, aun cuando se originó durante un período de problemas internos muy complejos debido a crisis internas e invasiones extranjeras, tuvo una gran influencia en la concepción actual de la administración pública como ciencia, particularmente en México y en América Latina por su presencia permanente aun después de las guerras de independencia.

Javier de Burgos, Pedro Sainz de Andino, Alejandro Oliván, Manuel Ortiz de Zúñiga, José de Posada de Herrera y Manuel Colmeiro escribieron textos que enriquecieron el contenido de la ciencia de la administración porque

tenían formación jurídica y, algunos de ellos, ocuparon cargos públicos. Javier de Burgos, por ejemplo, se refiere a la administración como la más útil de las ciencias morales que se encarga de velar por el interés público del hombre desde su nacimiento y aún después de su muerte. Esta concepción le otorga a nuestro objeto de estudio la característica de omnipresencia.

Pedro Sainz de Andino, al igual que Bonnin, señala que la administración civil pública actúa de forma paternal, pues usa todo aquello que está a su alcance para que pueda ser aprovechado en beneficio de los hombres, mientras que Alejandro Oliván aclara que la administración no es una atribución de supremacía que ejerce el gobierno, sino una responsabilidad que tiene como fin último el cuidado de la cosa pública y, de esta manera, ordenar y proteger a la sociedad. Además, agrega que, administrando, se gobierna.

Esta distinción que hace Oliván sobre la administración como una responsabilidad y no como una atribución de supremacía responde claramente al contexto de su época, pues en 1843, cuando escribió su obra cúspide ("De la administración pública con relación a España"), inició la sucesión de intentos para crear el Estado liberal español, al cual se opuso un movimiento de índole tradicional y católico encabezado por Carlos de Borbón, quien quería usurpar el trono de la Reina Isabel II.

En el mismo sentido, Manuel Ortiz de Zúñiga le confiere aún más responsabilidad al gobierno como el protector de todos los objetos de la sociedad cuando señala que éste es el alma de la administración. Al igual que Macarel, se refiere al gobierno como el pensamiento que dirige y a la administración como el brazo que ejecuta.

Por su parte, José de Posada de Herrara señala que la administración, más allá de ser una responsabilidad exclusiva del gobierno, es la vida misma de la sociedad o, dicho de otro modo, es la sociedad en acción. Esta reflexión tiene una similitud con Gandillot, quien afirmaba que la administración es una responsabilidad compartida entre los ciudadanos y la sociedad.

Finalmente, Manuel Colmeiro, recurriendo al formalismo que lo caracterizaba por su formación de jurisconsulto y

economista, define a la administración pública como el conjunto de principios y reglas que determinan la acción del poder público encargado de promover y fomentar el bien común. Su aportación permite relacionar perfectamente a la administración con el derecho público, sobre todo a partir del derecho administrativo[3], tema central de su producción literaria.

Como se puede advertir, existe una influencia marcada de Bonnin en el pensamiento español, así como de otros pensadores franceses. Omar Guerrero señala que "podría afirmarse, casi sin temor a equívoco, que la ciencia de la administración francesa, la de Bonnin, influyó más en España que en la propia Francia, toda vez que los autores peninsulares estudiaron en tierra gala, o leyeron los trabajos de sus vecinos, o los tradujeron al castellano."[4]

Ahora bien, durante la segunda mitad del siglo XIX tuvieron lugar diferentes movimientos bélicos e intelectuales en Europa que pretendían agrupar, por un lado, a los estados que conformaban el Sacro Imperio Romano Germánico y, por el otro, a los diversos estados en los que estaba dividida la península italiana.

En el caso de Alemania, Estado que se unificó hacia 1871 después de una guerra que enfrentó al Segundo Imperio Francés de Napoleón III y a la Prusia de Guillermo I, es preciso referirnos a 5 intelectuales que estuvieron influenciados por un período de transición que inició con una Alemania devastada y concluyó con el advenimiento de una potencia mundial.

En primer lugar, Robert von Mohl, quien fue uno de los primeros en referirse al Estado constitucional, definió la administración pública como la exposición sistemática de los principios relativos al empleo de las instituciones auxiliares individuales del Estado para vencer los eternos obstáculos prepotentes. Von Mohl veía a la estructura estatal como "[...] la formación más armónica posible de

3 El Derecho administrativo es la rama del derecho público que tiene por objeto regular la actividad de la administración pública, encargada de satisfacer las necesidades esenciales de la colectividad.

4 Omar Guerrero Orozco, *Introducción a la administración pública*, México, Harla, 1985, p. 134.

todas las fuerzas humanas en cada individuo concreto. [Por tanto, el fin del Estado de derecho, y de la administración como parte de éste, es la] eliminación de los obstáculos que entorpecen el desarrollo completo de las fuerzas del ciudadano."[5]

Un segundo pensador de la época fue Lorenz von Stein, quien es considerado como el fundador de la "ciencia" de la administración pública que reemplaza a la antigua ciencia cameralista. Si bien la literatura de von Stein es muy amplia, solamente retomaremos su definición clásica de administración pública, a saber: actividad del Estado que tiene lugar mediante los órganos estatales y constituye, por lo tanto, la vida propiamente exterior del Estado.

Si esta definición no la tomamos de manera literal, podremos advertir que para von Stein la administración pública no es un conocimiento únicamente teórico, sino también práctico. De acuerdo con Manuel García-Pelayo, "[…] los acontecimientos de 1848 [(revolución alemana que pretendía terminar con el régimen jurídico de la nobleza)] han suscitado en la mente de von Stein la vinculación entre una preocupación teórica y una necesidad práctica."[6]

El tercer pensador de este período es Karl Marx, un jurista, filósofo, sociólogo, historiador y economista que se dedicó a estudiar la sociedad, la economía y la política de su época. Si bien sus aportaciones se reflejaron en otras ciencias y disciplinas, en su crítica al Estado capitalista como producto del carácter irreconciliable de las luchas de clases, definió a la administración pública como la actividad organizadora del Estado, de esa superestructura que responde a los intereses de la clase dominante.

Hacia finales del siglo XIX, ya en una Alemania unificada y constituida como un Estado de derecho liberal, Otto Mayer publicó distintas obras sobre derecho administrativo, el cual, según el propio autor, está condicionado por el

5 Joaquín Abellán, "Liberalismo alemán del siglo XIX: Roberto von Mohl", *Revista de Estudios Políticos (Nueva Época)*, n° 33, Madrid, Centro de Estudios Políticos y Constitucionales, 1983, pp. 143-144.

6 Manuel García-Pelayo, "La teoría de la sociedad en Lorenz von Stein", *Revista de estudios políticos*, no° 47, Madrid, Centro de Estudios Políticos y Constitucionales, 1949, p. 46.

derecho constitucional. De este modo, la administración es la actividad del Estado para el cumplimiento de sus fines, pero que tiene como límite las disposiciones contenidas en las leyes.

El quinto y último pensador alemán del período de estudio que abarca este trabajo es Max Weber. Al igual que sucede con Marx, las aportaciones de Weber tienen una mayor injerencia en la sociología; sin embargo, hizo contribuciones a la administración pública desde la óptica del estudio organizacional. Para los fines de esta investigación, basta señalar que Weber formuló la teoría de la burocracia, definida como una organización social que, basada en la racionalización de la actividad colectiva y en la profesionalización del personal, tiende al perfeccionamiento de la administración pública.[7]

En cuanto a los pensadores que vivieron durante la Italia unificada, destacan por sus aportaciones Carlo Francesco Ferraris y a Vittorio Wautrain Cavagnari. El primero de ellos, a sus 29 años de edad, publicó una obra titulada "Ensayos sobre la Ciencia de la Administración" en la que describe a la administración pública como las obligaciones y deberes del Estado en materia política y social. Es decir, es la acción social positiva y directa del Estado. Como se puede advertir, la influencia de Bonnin también permeo a la península itálica pues, como vimos anteriormente, el autor francés señaló que la acción social es el carácter de la administración pública.

Por su parte, Cavagnari, además de considerar a la administración como la acción del Estado, agrega que ésta se ocupa de la adquisición y uso correcto de los bienes económicos y servicios profesionales para lograr el mejoramiento de las clases sociales, como en su momento lo señaló Karl von Stein, pero ahora enfatizando que lo

7 Se recomienda revisar lo que escribió Max Weber sobre los tipos de dominación, específicamente la dominación legal con administración burocrática, en la siguiente referencia bibliográfica: Max Weber, *Economía y Sociedad. Esbozo de sociología comprensiva*, Madrid, Fondo de Cultura Económica de España, 2002, pp. 170-241.

deberá hacer en términos económicos, físicos, intelectuales y morales. [8]

3. La visión jurídica y social de la administración pública durante la conformación de la Nación Mexicana

En el caso mexicano, tenemos cuatro grupos diferenciados de pensadores administrativos de acuerdo a la clasificación realizada por José Juan Sánchez González[9]. Aquellos que produjeron sus obras durante la etapa histórica denominada "Independiente" (1820-1857), los pertenecientes a la etapa "Reformista" (1858-1876), los de la etapa "Porfiriana" (1877-1910), los de la etapa "Posrevolucionaria" y finalmente los del México contemporáneo (1940-1979), etapa que actualmente denominamos pasado reciente.

Sin embargo, con el objetivo de seguir un orden cronológico, por ahora nos enfocaremos en la etapa "Independiente" que incluye a cuatro mexicanos destacados en el campo de la política y el derecho. Nos referimos a Simón Tadeo Ortiz, Luis de la Rosa, Teodosio Lares y R.M. Veytia, quienes fueron claramente influenciados por los hechos vinculados con el surgimiento de México como país independiente y con la presencia de intelectuales españoles en el período de conformación del nuevo Estado-nación.

Simón Tadeo, el primer teórico de la administración pública en México, se refiere a la ciencia de la administración social como la autoridad pública que tiene como tarea principal

8 Por cuestiones cronológicas y de ubicación geográfica, no incluimos en el cuerpo del texto a dos pensadores administrativos europeos que tuvieron una influencia importante en el desarrollo de la disciplina. Nos referimos al suizo Gaspar Bluntschli (1807-1881) y al francés Henri Fayol (1841-1925). El primero concibió a la administración pública como un ejército de restricción que tiene un radio de acción en cualquier parte donde lo exijan la seguridad y las necesidades de la nación. Por su parte, Fayol, a pesar de su formación como ingeniero, compara a la administración pública con la administración privada, argumentando que ambas, para funcionar y ser eficientes, deben seguir un proceso administrativo que comprende las siguientes etapas: planificación, organización, dirección, coordinación y control. Además, introduce al léxico de la administración pública los principios de la administración (división del trabajo, autoridad, disciplina, unidad de mando, unidad de dirección, subordinación de intereses, remuneración, centralización, jerarquía, orden, equidad, estabilidad personal, iniciativa y espíritu de grupo).

9 José Juan Sánchez González, *Historia del estudio de la administración pública en México*, México, Porrúa, 2009, pp. 407-413.

otorgar empleo y promover los adelantos sociales mediante prácticas de industria y comercio. Esta definición, la cual se deduce de su obra "México considerado como una nación independiente", tiene una relación directa con su percepción de la realidad de un país en construcción que necesita, entre otras cosas, una reforma administrativa de gran calado para "desterrar los vicios que dejó la administración colonial, despótica, rapaz y desmoralizada."[10]

Luis de la Rosa, quien ocupó cargos como Presidente de la Suprema Corte de Justicia de la Nación, Secretario de Relaciones Exteriores y de Hacienda y Crédito Público, entre otros, consciente de los problemas vinculados con los gobiernos itinerantes de Antonio López de Santa Anna, sostuvo que la administración pública, para ser efectiva, debía avocarse a satisfacer las necesidades más imperiosas y exigentes de toda la sociedad y, para tal efecto, debía desarrollar todos los gérmenes de prosperidad del país para poner a la sociedad en un estado de animación, de vida y de progreso.

De manera contraria, Teodosio Lares, un abogado y político fiel al gobierno de Santa Anna y posteriormente al imperio de Maximiliano de Habsburgo, afirmaba que el derecho administrativo, considerado como una ciencia de la acción, era competencia del poder ejecutivo, de sus agentes y del tribunal administrativo. Esta postura sobre la competencia exclusiva, a diferencia de aquellas que conciben a la administración como un vínculo social y una responsabilidad del gobierno, tiene origen en los cargos que ocupó Lares a lo largo de su vida profesional. Basta mencionar que fue ministro de justicia durante la dictadura de Santa Anna, ministro de Justicia en las presidencias de Félix María Zuloaga y Miguel Miramón, claros oponentes al gobierno de Juárez, y, finalmente, presidente del Tribunal Supremo de Justicia y presidente del Consejo de Ministros durante el Segundo Imperio.

Cabe señalar que no estamos juzgando el pensamiento de Teodosio Lares, más bien coincidimos con la siguiente reflexión de Diego Valadés.

10 *Ibid.*, p. 83.

> El concepto de Lares es valioso examinado desde una perspectiva académica; pero su relevancia aumenta si se considera que fue formulado durante el gobierno de Mariano Arista. Dos años más tarde ocupó el ministerio de justicia en el último período de Antonio López de Santa Anna. Desde ahí, Lares procuró hacer efectivos los postulados de su doctrina; entendía que la administración debía sujetarse a los principios de legalidad, por lo que concernía a los órganos del poder, y de libertad y seguridad, por lo que atañía a los gobernados.[11]

Finalmente, R.M. Veytia, al igual que Teodosio Lares, considera que la administración o, mejor dicho, el derecho administrativo, se limita al poder ejecutivo, incluyendo a los ministros, y es la acción de sus diversas partes para garantizar el cumplimiento de las leyes. Como señala José Juan Sánchez González, "el objeto principal de la exposición del autor es jurídico y por tanto la administración pública se confina al derecho administrativo […]."[12] Esta precisión, la cual es muy importante porque relaciona la formación de los autores con su concepción de la administración pública, es la razón principal por la que decidimos incluir en la tabla los estudios que realizaron los pensadores administrativistas del ámbito jurídico.

Ahora corresponde referirnos a un autor de la etapa "Reformista" y a uno de la época porfiriana. José María del Castillo Velasco publicó en 1874 un texto titulado "Ensayo sobre el derecho administrativo mexicano" en el que concibe a la administración pública como un don del gobierno, concretamente del poder ejecutivo, en el que concurren los principios de todas las ciencias y los conocimientos humanos aplicados a efecto de conocer las causas sociales y, de este modo, producir el desarrollo de los pueblos o, en el peor de los casos, su decadencia y postración.

Esta noción es muy interesante porque es la primera vez que nos referimos a la administración pública como una acción que puede tener consecuencias negativas. En efecto, José María del Castillo Velasco estaba consciente de

11 Diego Valadés, "Comentario preliminar", en Nava Negrete, Alfonso, *Estudios administrativos*, México, UNAM, 2011, p. XIII.

12 J. J. Sánchez González, *op. cit.*, p. 121.

que una mala administración podría tener consecuencias funestas para la población, incluso vulnerando aquello que tradicionalmente se ubica como el fin último de la administración pública: la consecución del bien común.

Por esta razón, el autor agrega que "[…] las organizaciones administrativas deben cumplir dos condiciones indispensables para su funcionamiento. La administración debe estar en perfecta armonía con las instituciones políticas [y] la administración debe ser independiente, esencialmente activa y responsable […]."[13]

Manuel Cruzado, abogado de la época porfiriana, se refería a la administración pública como la institución que cuida del fomento y la conservación de los intereses de la sociedad por conducto de los funcionarios establecidos por la ley. Esta perspectiva jurídica, positivizada en reglas e instituciones, origina lo que en su momento se denominó ciencia de la organización administrativa que, hasta cierto punto, retoma algunas consideraciones hechas por Max Weber.

Años más tarde, saldrían a la luz las aportaciones de Gabino Fraga, representante de la época "Posrevolucionaria", y de Lucio Mendieta y Núñez, quien pertenece al período "Contemporáneo" o del pasado reciente.

Gabino Fraga, que en su momento se desempeñó como ministro de la Suprema Corte de Justicia de la Nación y como catedrático de la Universidad Nacional Autónoma de México, evitó encasillar a la administración pública como lo hicieron otros pensadores que lo antecedieron al definirla como el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales y para realizar sus actividades propias.

Por su parte, Lucio Mendieta y Núñez recurre a sus conocimientos como sociólogo para proponer una definición de administración pública que va más allá de su estructura y de funciones. Afirma que su actividad obedece a las necesidades sociales que, en esencia, consisten en responder a

13 J. J. Sánchez González, *op. cit.*, pp. 195-196.

exigencias internas de la vida colectiva y a exigencias que externas frente a otros grupos sociales. Por tanto, la administración se estructura de acuerdo con un plan que deriva de la sociedad misma o que le imponen los hechos sociales.

4. El pensamiento administrativo estadounidense: La incorporación del enfoque empresarial en un mundo tradicionalmente público

En Estados Unidos, después de la Guerra de Secesión (1861-1865), un conflicto en el que se enfrentaron los estados del Norte de la Unión y los Estados Confederados de América que provocó la muerte de más de un millón de personas, pero que a su vez puso fin a la esclavitud y permitió la unión de estados sujetos al poder federal, surgió de manera progresiva un grupo de intelectuales que estudiaron, desde sus respectivas disciplinas de formación, a la administración pública.

Un primer ejemplo es Thomas Woodrow Wilson, quien, además de ser el vigesimoctavo presidente de Estados Unidos, fue un estudioso del derecho y la ciencia política. En 1887, después de obtener el grado de doctor por la Universidad Johns Hopkins, escribió un ensayo titulado "El estudio de la administración" en el que define el concepto de administración púbica de manera clara y precisa, pero sin obviar su formación jurídica:

> La administración es la parte más obvia del gobierno; es gobierno en acción; es el lado ejecutivo, el operativo, el más visible del gobierno, y por supuesto es tan viejo como el propio gobierno. Es el gobierno en acción [...]. Una visión clara de la diferencia entre la provincia del derecho constitucional y la provincia de la función administrativa no debe dejar lugar a malentendidos; y es posible nombrar algunos criterios bastante definidos sobre los cuales se puede construir tal visión. La administración pública es una ejecución detallada y sistemática del derecho público. Cada aplicación particular de la ley general es un acto de administración. La evaluación y recaudación de impuestos, por ejemplo, el ahorcamiento de un criminal, el transporte y la entrega de los correos, el equipo y el reclutamiento del ejército y la marina, etc., son obviamente actos de administración; pero

> las leyes generales que ordenan que estas cosas se hagan están obviamente fuera de la administración y más allá de ella. Los amplios planes de acción gubernamental no son administrativos; la ejecución detallada de tales planes es administrativa.[14]

De manera complementaria, Frank Johnson Goodnow, un profesor de derecho contemporáneo de Wilson, escribió en 1900 un libro titulado "Política y administración. Un estudio en el gobierno". En dicha obra, Goodnow dedica un capítulo completo a las funciones de la administración, el cual inicia con la siguiente afirmación: "La función de ejecutar la voluntad del Estado ha sido llamada administración."[15] Más adelante, se refiere a otras funciones de la administración: cuasi judiciales; estadísticas y semi-científicas; y la función de establecer, preservar y desarrollar la organización gubernamental.

Por su parte, William Franklin Willoughby hace una distinción importante entre las funciones ejecutivas y las administrativas, pues existía una confusión no sólo al interior del gobierno sino en los centros de formación. Al respecto, señala lo siguiente:

> Con estas distinciones y requisitos en mente, se puede ver la diferencia esencial que existe entre el ejecutivo y la función administrativa, utilizando estos términos en su sentido técnico propio. La función ejecutiva es la función de representar al gobierno como un todo, y de ver que todas sus leyes se cumplan por sus diversas partes. La función administrativa es la función de administrar realmente la ley declarada por el legislativo e interpretada por los poderes judiciales del gobierno. Esta distinción generalmente se hace al declarar que la función ejecutiva es esencialmente de carácter político; es decir, una que tiene que ver con la determinación de políticas generales, y que implica el ejercicio del juicio en su uso; y la

14 Thomas Woodrow Wilson, "The study of administration", *Political Science Quarterly*, vol. 2, n° 2, Nueva York, Academy of Political Science, 1887, pp. 198 y 212

15 Frank Johnson Goodnow, *Politics and administration. A Study in Government*, Nueva York, The Macmillan Company, 1900, p. 72.

> función administrativa es la aplicación de políticas determinadas por otros órganos.[16]

Esta precisión, que podría oponerse a la concepción de Lares, Veytia y del Castillo Velasco de la administración pública como una facultad exclusiva del poder ejecutivo, nos permite corroborar que la administración pública no es privativa de uno de los poderes del Estado, sino que es una responsabilidad compartida entre el gobierno en su más amplia definición y la sociedad.

En las primeras décadas del siglo XX, también en Estados Unidos, un grupo amplio de intelectuales hicieron contribuciones importantes, y de carácter multidisciplinario, al estudio de la administración pública. A continuación, haremos una breve referencia de cada uno de ellos.

Mary Parker Follett, una trabajadora social especialista en relaciones humanas, señalaba que era importante favorecer la integración de grupos de trabajo para mejorar la eficacia no sólo de la administración pública, sino también de la administración privada; Elton Mayo, un sociólogo y psicólogo industrial, abonó a la teoría de la organización social afirmando que no se debe perder de vista que los individuos trabajan para satisfacer necesidades económicas, psicológicas y sociales.

En el mismo sentido, Chester Barnard, en su libro titulado "Las funciones de los elementos dirigentes" se refiere a la estructura de las organizaciones y al papel que desempeñan los cargos directivos.

Como se puede advertir, en aquella época se comenzó a estudiar a la administración pública ya no como un sistema cerrado perteneciente al Estado, sino como una estructura que, al igual que las empresas, está dividida en términos de sus recursos humanos y de su estructura organizacional. No obstante, Leonard D. White, Paul H. Appleby y Luther Gulick, a diferencia de los sociólogos, se enfocaron en el estudio de la administración pública en sus términos tradicionales.

16 William F. Willoughby, *An introduction of the study of the government of modern states*, Nueva York, The Century Co., 1919, p. 232.

Leonard D. White, en su libro titulado "Introducción al Estudio de la Administración Pública", retoma algunas nociones de Wilson, Goodnow y Willoughby para realizar una serie de aseveraciones clave para entender a la administración pública como una necesidad inherente al individuo en sociedad, a saber:

- Hasta donde llega la memoria humana, el arte de la administración ha sido una de las posesiones esenciales del hombre. La administración es un proceso común a todo esfuerzo de grupo, público o privado, civil o militar, en grande o en pequeña escala;
- La administración pública consiste en todas las operaciones que tienen por objeto la realización o la observancia forzosa de la política del Estado;
- Un sistema de administración pública es el compuesto de todas las leyes, reglamentos, prácticas, relaciones, códigos y costumbres que prevalecen en un momento y una jurisdicción para la realización o ejecución de la política del Estado;
- El arte de la administración es la dirección, coordinación y control de muchas personas para realizar algún propósito u objetivo;
- En consecuencia, un administrador es la persona que dirige, coordina y controla las actividades de los otros;
- La finalidad inmediata del arte de la administración pública es la utilización más eficaz de los recursos de que disponen los funcionarios y los empleados;
- La buena administración procura eliminar el despilfarro, conservar y usar eficazmente hombres y materiales, y proteger el bienestar y los intereses de los empleados;
- En su sentido más amplio, los fines de la administración son los objetivos últimos del Estado mismo: la conservación de la paz y el orden, la realización progresiva de la justicia, la instrucción de los jóvenes, la protección contra las enfermedades y la inseguridad, el ajuste y la transacción entre los grupos y los intereses antagónicos, en suma, la consecución de una vida buena.[17]

17 Leonard D. White, *Introducción al estudio de la Administración Pública*, México, Compañía General de Ediciones, 1964, pp. 1-3.

Paul H. Appleby, un teórico de la administración pública, señalaba que la administración es vista como el gobierno en acción directa en nombre de los ciudadanos y, al mismo tiempo, como una forma de contenerlos. La importancia de las aportaciones de Appleby radica en su concepción de la administración pública como el elemento central para mejorar la viabilidad de la democracia a gran escala. En ese sentido, afirma que, debido a la trascendencia de la administración pública, es impensable dejarla únicamente en manos de expertos administrativos, sino que requiere de la participación pública directa e indirecta. Como señalamos anteriormente, se trata de una responsabilidad compartida.

Por su parte, Luther Gulick, un destacado politólogo que se desempeñó como director del Instituto de Administración Pública de la Universidad de Columbia, manejó una concepción clásica de la administración pública al definirla como la parte de la ciencia de la administración que tiene que ver con el gobierno y que, por lo tanto, se ocupa principalmente del poder ejecutivo, aunque obviamente tiene relación con los poderes legislativo y judicial.

El último bloque de pensadores administrativos estadounidenses está conformado por Marshall E. Dimock, Dwight Waldo, Herbert A. Simon y Philip Selznick, quienes realizaron sus aportaciones más sobresalientes a partir de la segunda mitad del siglo XX. A continuación, se rescatan, de manera sucinta, sus contribuciones.

- Marshall E. Dimock: La administración pública es el cumplimiento o la ejecución de la política pública declarada por las autoridades competentes. La administración pública es la ley en acción. Es el lado ejecutivo de un gobierno;
- Dwight Waldo: Es la parte "empresarial" de un gobierno, continuamente activa, que se ocupa de llevar a cabo la ley tal como lo hacen los cuerpos legislativos (u otros agentes autorizados) e interpretada por los tribunales, a través del proceso de organización y gestión;
- Herbert A. Simon: Por administración pública se entiende el uso común, las actividades de las ramas ejecutivas de los gobiernos nacionales, estatales y locales;

- Philip Selznick: Sus contribuciones se enfocaron en el estudio de la burocracia como una estructura social adaptativa y dinámica que es condicionada, al interior de la organización, por una estructura informal.

Conclusiones

Como se puede advertir de este recorrido histórico, la administración pública es un elemento intrínseco de las relaciones entre la sociedad y el Estado, que, si bien en ciertas etapas respondía al poder ejecutivo o al gobierno, en la actualidad se vincula con toda la actividad del Estado, especialmente con aquellos de tradición democrática y constitucional.

Otro elemento que conviene destacar es la fuerte influencia de los pensadores franceses, especialmente de Charles-Jean Baptiste Bonnin, en la mayoría de las evocaciones sobre la administración pública, específicamente cuando se habla de su fin último: conservar a los individuos y sus relaciones o, dicho de otro modo, a la sociedad misma, y garantizar la satisfacción de las necesidades que permiten el desarrollo y la vida plena de los individuos.

En cuanto al concepto en sí mismo, se puede apreciar una evolución que responde a contextos históricos, especialmente a conflictos bélicos que derivaron en la adopción de textos normativos o en el surgimiento de nuevos Estados-nación. Es por ello que la administración pública se relacionó estrechamente con la actividad del gobierno, ya sea como una potestad reguladora o como la responsabilidad de atender las demandas sociales.

Asimismo, se hizo referencia a la administración pública como una escisión del derecho y de la política; sin embargo, conforme nos acercábamos al siglo XX, los pensadores se referían a estas ciencias como elementos diferenciados, pero íntimamente relacionados.

Finalmente, reconocemos que, en un inicio, la administración pública se estudiaba como un sistema cerrado que respondía a los intereses del Estado como condición previa a la satisfacción de los intereses colectivos. Sin embargo, los pensadores estadounidenses

nos enseñaron que la administración pública se puede estudiar como una estructura equiparable a las empresas en el sentido de que ambas necesitan, para garantizar su funcionamiento y eficiencia, elementos de planeación y organización interna, así como prestar atención a los responsables de su actividad: los funcionarios públicos o los empleados respectivamente.

Cuadro 1
Definiciones de Administración Pública y aportaciones al estudio de la ciencia (siglos XVI-XX)

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Jean Bodin	1530-1596	Francia	Jurista, escritor y politólogo	Señala la existencia de un poder público que desempeña el papel de unificador del orden social: concibe al Estado como la sede del poder soberano y, como tal, él lo diferencia de la sociedad.[1]
Johann Heinrich Gottlob von Justi	1717-1771	Alemania	Economista y politólogo	La ciencia de la policía consiste en arreglar todas las cosas relativamente al estado presente de la sociedad, en afirmarla, mejorarla y fortalecerla, que todo concurra a la felicidad de los miembros que la componen.[2]
Karl vom Stein	1757-1831	Prusia	Jurista, economista, historiador y político	Los propietarios de todas las clases sociales deberían involucrarse en el trabajo de la administración local a través de un nuevo sistema de órganos representativos (estados) a nivel distrital y provincial.
Wilhelm von Humboldt	1767-1835	Alemania	Estudioso de idiomas, filósofo, diplomático	A la vista de todo Estado nuevo debieran tenerse presentes siempre dos puntos, ninguno de los cuales puede pasarse por alto sin gran quebranto: uno es el de determinar la parte de la nación llamada a mandar y la llamada a obedecer, así como todo lo que forma parte de la verdadera organización del gobierno; otro, el determinar los objetivos a que el gobierno, una vez instituido, debe extender, y al mismo tiempo circunscribir, sus actividades. El verdadero alcance de la actividad del Estado abarca todo aquello que puede

1 [sin autor], "Qu'est-ce que l'État?", [en línea], París, *Vie-publique.fr*, 2018, Dirección URL: http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/qu-est-ce-que-etat.html, [consulta: 04 de junio de 2018].
2 Omar Guerrero Orozco, *Teoría administrativa del Estado*, México, Oxford University Press, 2000, p. 14.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Wilhelm von Humboldt	1767-1835	Alemania	Estudioso de idiomas, filósofo, diplomático	realizar en bien de la sociedad. El fin de Estado puede, en efecto, ser doble: puede proponerse fomentar la felicidad o simplemente evitar el mal, el cual puede ser, a su vez, el mal de la naturaleza o el de los hombres. Si se limita al segundo fin, busca solamente la seguridad, y permítaseme oponer este fin a todos los demás fines posibles que se agrupan bajo el nombre de bienestar positivo. Para tales efectos, se establecen instituciones del Estado que se propongan mantener o fomentar el bienestar fisico de la nación.[3]
Charles-Jean Baptiste Bonnin	1772-1846	Francia	Político	La administración pública es una potencia que arregla, corrige y mejora todo cuanto existe, y da una dirección más conveniente a los seres organizados y a las cosas.[4]
M. R. Gandillot		Francia	Jurista	El derecho administrativo es una demostración de los deberes de la sociedad para con los ciudadanos, y de los de estos hacia la sociedad.[5]
M. Macarel		Francia	Jurista	La administración es la acción vital del gobierno y brazo de la sociedad. La ciencia de la administración tiene por objeto investigar, en la fuente misma de las necesidades, las reglas de la vida práctica de las naciones, y los principios sociales que deben regir dentro de las relaciones de los administradores con los administrados. La ciencia de la administración está basada en reglas generales y absolutas, es decir, en los principios de la administración pública que implican protección y seguridad, beneficencia pública, educación pública y vías de comunicación.[6]

3 Wilhelm von Humboldt, *Los límites de la acción del Estado*, Madrid, Técnos, 2009, pp. 4, 21 y 23.
4 O. Guerrero Orozco, *Teoría administrativa del Estado*, *op. cit.*, p. 26.
5 M. R. Gandillot, *Curso de derecho administrativo*, Madrid, Imprenta de D. José Espinosa, 1835, p. 9.
6 Omar Guerrero Orozco, *La teoría de la administración pública*, México, Harla, 1986, pp. 162-164.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Javier de Burgos	1778-1849	España	Político, traductor y dramaturgo	La Administración es la más variada, la más vasta y la más útil de todas las ciencias morales. Ella preside el movimiento de la máquina social, precipita o modera su acción, arregla o modifica su mecanismo y protege así, y conserva o mejora todos los intereses públicos. Objeto de su solicitud es el hombre antes de nacer, y lo es después que ha cesado de existir.[7]
Pedro Sainz de Andino	1786-1863	España	Jurisconsulto, político y académico de la Real Academia de la Historia	La administración civil pública es una administración específica dentro de la noción más general de administración. Actúa en forma benéfica, consoladora y paternal. Las personas y las cosas son los objetos de la administración civil. Ella ve en cada individuo el objeto de su solicitud, su celo y sus providencias, porque debe conservarlo y aumentar su bienestar, apartarlo del mal, acercarlo al bien, criarlo, educarlo, nutrirlo, aliviar sus necesidades, darles goces y comodidades a sus expensas. Por cuanto a las cosas, la administración civil hace uso de ellas para, multiplicándolas y extendiendo su aplicación, puedan ser aprovechadas en beneficio de los hombres.[8]
Simón Tadeo Ortiz	1788-1833	México	Latinista y filósofo	La autoridad pública administrativa (ciencia de la administración social) tiene como tarea principal la dirección de la sociedad. Sus objetivos son abrir la puerta del trabajo, civilización, adelantos y mejoras sociales a los pueblos y que los gobiernos se desengañen. Esto consiste en medidas prácticas de industria y un ejercicio continuado de ocupaciones.[9]

7 [sin autor], *Las ideas de Administración de Javier de Burgos*, Madrid, Instituto Nacional de Administración Pública, 1987, s/p.
8 O. Guerrero Orozco, *La teoría de la administración pública*, *op. cit.*, pp. 100-101.
9 J. J. Sánchez González, *op. cit.*, pp. 82 y 84.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Alejandro Oliván	1796-1878	España	Militar, político y ensayista	Se ha convenido en considerarla científicamente en su acepción más lata, y en referirla constantemente al conjunto de cuidados que exige la cosa pública, no como atribución de supremacía, sino al contrario como gestión de responsabilidad. Porque en efecto, quien administra reconoce independencia. En este supuesto, la administración pública o de la cosa pública tiene por objeto la satisfacción de las necesidades interiores de la sociedad, la vigilancia sobre sus intereses, y el ordenado manejo de sus negocios en la intención del mejor estar de los asociados, y con sujeción a reglas de un superior. Este superior es el poder supremo o la personificación de la misma sociedad, y sus reglas son las leyes. El gobierno es el poder supremo considerado en su impulso y acción para ordenar y proteger la sociedad; y la administración constituye el servicio general o el agregado de medios y el sistema organizado para transmitir y hacer eficaz el impulso del gobierno, y para regularizar la acción legal de las entidades locales. De modo que administrando se gobierna.[10]
Robert von Mohl	1799-1875	Alemania	Jurista, político y diplomático	La exposición sistemática de los principios relativos al empleo de las instituciones auxiliares individuales del Estado, para vencer a los eternos obstáculos prepotentes.[11]
Luis de la Rosa	1804-1856	México	Político y abogado	La administración pública tiene por único objeto satisfacer las necesidades más imperiosas y exigentes de toda sociedad, el goce de todos los beneficios, de todas las comodidades y ventajas que proporciona al hombre la civilización: tales son los grandiosos e importantísimos objetos de la administración, y para llenarlos cumplidamente se necesita un vasto conocimiento de los recursos

10 Alejandro Oliván, *De la administración pública con relación a* España, Madrid, Boix Editor, 1843, p. 6.
11 O. Guerrero Orozco, *Teoría administrativa del Estado, op. cit.*, p. 23.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Luis de la Rosa	1804-1856	México	Político y abogado	y necesidades de un país. Una acertada administración, para cumplir los beneficios objetos con que ha sido establecida, necesita desarrollar todos los gérmenes de prosperidad de un país, poner a la sociedad en un estado de animación, de vida y de progreso.[12]
Teodosio Lares	1806-1870	México	Abogado y político	El derecho administrativo, así considerado, es la ciencia de la acción y de la competencia del poder ejecutivo, de sus agentes, y de los tribunales administrativos, en relación con los derechos e intereses de los ciudadanos, y con el interés general del Estado. La administración activa, se manifiesta en la protección de los intereses generales de la sociedad, vigilando la acción de cada ciudadano. Y entonces se dice que el ejecutivo administra. No hay administración sin acción, y esta se ejerce sobre las personas o sobre las cosas de los individuos.[13]
Manuel Ortiz de Zúñiga	1806-1874	España	Jurista	La acción protectora del gobierno, extendida a un mismo tiempo a todos los seres, a todos los objetos de la sociedad por medio de la multiplicidad de sus agentes y por la simultaneidad y extensión de sus ocupaciones. Es el poder que tiene acción y da impulso a cuanto existe en la sociedad. El gobierno es pues el alma de la administración, por cuyo resorte ella se mueve: el gobierno es el pensamiento que dirige, y la administración el brazo que ejecuta. Su objeto y atribuciones son amplísimos, y puede decirse, inconmensurables. En términos generales y absolutos promover la prosperidad, proteger los intereses generales, en una palabra, hacer bien es su incumbencia esencial.[14]

12 Luis de la Rosa, "Sobre la administración pública de México y medios de mejorarla", *Revista de Administración Pública*, n° 50, México, INAP, 1982, pp. 115-116.

13 Teodosio Lares, "El Derecho Administrativo. La ciencia de la Acción y de la Competencia del Poder Ejecutivo", *Revista de Administración Pública*, n° 50, México, INAP, 1982, pp. 80 y 86.

14 Manuel Ortiz de Zúñiga, "Idea general de la administración y del derecho administrativo", *Revista de Administración Pública*, Edición Especial en Memoria del Maestro y Primer Presidente del INAP Gabino Fraga, México, INAP, 1982, pp. 126, 127 y 129.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
M. Jean-Gaspard Bluntschli	1808-1881	Suiza	Jurista y político	La administración pública se basa en el derecho y el deber públicos. Llega tan lejos como el dominio del derecho público. La administración pública, es un ejército de restricción, tiene un radio de acción en cualquier parte donde lo exijan la seguridad y las necesidades de la nación. La administración pública es esencialmente general. Se extiende de modo uniforme sobre las clases de la sociedad y sobre todo el territorio o, por lo menos, sobre sus divisiones orgánicas: provincias, circulas, comunas. Tiene normas legales y ordenamientos magisteriales.[15]
José de Posada de Herrera	1814-1885	España	Jurista y político	La administración es la vida de la sociedad. Por ella obra, por ella se instruye, por ella piensa las leyes, por ella las ejecuta, por ella progresa, por ella entra en relación con los pueblos extranjeros, por ella se organiza, por ella se defiende, por ella en fin provee a todas sus necesidades y peligros. Es, en una palabra, la sociedad en acción, pensando, obrando, siguiendo el camino que le ha marcado la providencia en el espacio de los siglos. La administración es el número y distribución de los agentes que tiene el gobierno a su disposición para poder ejecutar las leyes. Derecho administrativo será el conjunto de leyes administrativas y ciencia de la administración será aquella ciencia que establece los principios y las relaciones que hay entre la sociedad y los miembros de que se compone. La administración abraza los intereses de la sociedad en masa y todo el cuerpo social de toda la nación, cualquiera que ella sea.[16]

15 M. Bluntschli, "La administración pública", *Revista de Administración Pública*, n° 42, México, INAP, 1980, pp. 127-128.
16 José de Posada de Herrera, *Lecciones de administración*, Tomo I, Madrid, Establecimiento tipográfico, 1843, pp. 9, 43-44.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Lorenz von Stein	1815-1890	Alemania	Economista y sociólogo	Actividad del Estado que tiene lugar mediante los órganos estatales y constituye, por lo tanto, la vida propiamente exterior del Estado, es lo que se llama administración del Estado.[17]
Karl Marx	1818-1883	Alemania	Filósofo, sociólogo, historiador, economista	La administración es la actividad organizadora del Estado.[18]
Manuel Colmeiro	1818-1894	España	Jurisconsulto y economista	La administración considerada como ciencia, o la administración pura es el conjunto de principios y reglas que determinan la acción del poder público encargado de promover y fomentar el bien común, en sus múltiples y variadas relaciones con los derechos e intereses particulares. El objeto, pues, de la administración son las necesidades materiales y morales de los pueblos: su fin satisfacerlas con la mayor amplitud y a costa de sacrificios tan leves cuanto fuere posible.[19]
José María del Castillo Velasco	1820-1883	México	Abogado y periodista	Lo que se ha llamado don de gobierno y es propiamente la ciencia administrativa, consiste en el conocimiento de las causas comunes a todas las naciones y de las particulares de cada una de ellas que pueden producir el desarrollo y adelantamiento de los pueblos o su decadencia y postración, así como de los medios propios para obtener aquellos bienes y evitar esos males. La ciencia administrativa busca la armonía absoluta entre todos los intereses sociales y entre todos los interese individuales. Así

17 Lorenz von Stein, *Movimientos Sociales y* Monarquía, Madrid, Centro de Estudios Constitucionales, 1981, p. 33.
18 Karl Marx, "Glosas críticas marginales al artículo: 'El Rey de Prusia y la reforma social' por un Prusiano", en Marx, Karl, *Escritos de juventud sobre el Derecho. Textos 1837-1847*, Barcelona, Anthropos, 2008, p. 123.
19 Manuel Colmeiro, *Derecho administrativo español*, Tomo I, Madrid, Imprenta y librería de Eduardo Martínez, 1876, pp. 7-8.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
José María del Castillo Velasco	1820-1883	México	Abogado y periodista	como la facultad de legislar corresponde exclusivamente al poder legislativo y la de juzgar, exclusivamente al poder judicial, así la facultad de administrar corresponde exclusivamente al poder ejecutivo.[20]
Henri Fayol	1841-1925	Francia	Ingeniero	Abarca no solo el servicio público, sino empresas de todos los tamaños y descripciones, de todas las formas y propósitos. Todos los proyectos requieren planificación, organización, comando, coordinación y control, y para funcionar correctamente, todos deben observar los mismos principios generales. Ya no se nos confunde con varias ciencias administrativas, sino con una sola, que puede aplicarse equitativamente a los asuntos públicos y privados.[21]
Otto Mayer	1846-1924	Alemania	Jurista	La administración es la actividad del Estado para el cumplimiento de sus fines.[22]
Manuel Cruzado	1847-1913	México	Abogado	Es la institución que cuida del fomento y la conservación de los intereses de la sociedad por conducto de los funcionarios establecidos por la Ley.[23]

20 José María del Castillo Velasco, *Ensayo sobre el derecho administrativo mexicano*, México, Taller de Imprenta de la Escuela de Artes y Oficios para Mujeres, 1874, pp. 5, 8 y 13.
21 Henri Fayol, "The administrative theory in the State", en Gulick, Luther y Urwick, L., eds., *Papers on the Science of Administration*, Nueva York, Institute of Public Administration, 1937, p. 101.
22 Otto Mayer, *Derecho administrativo alemán*, Tomo I, Buenos Aires, Editorial de Palma, 1949, p. 3.
23 Omar Guerrero Orozco, *Introducción a la administración pública*, *op. cit.*, p. 262.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Carlo Francesco Ferraris	1850-1924	Italia	Economista y jurista	La ciencia de la administración se refiere a las obligaciones, a los deberes, a los alcances del Estado en materia política, de un lado, y en la materia social, del otro. La ciencia de la administración es la injerencia del Estado en los hechos políticos y sociales. Comprende todas las misiones del Estado y su acción sobre la sociedad, para promover su desarrollo físico, económico e intelectual. Es la acción social positiva y directa del Estado.[24]
R. M. Veytia	1852	México	Jurisconsulto	Se limita al poder ejecutivo, y es la acción de sus diversas partes, o lo que es lo mismo, el conjunto de medios por los cuales las leyes se ejecutan.[25]
Thomas Woodrow Wilson	1856-1924	EE.UU.	Político, politólogo y abogado	La administración pública es una ejecución detallada y sistemática de la ley. Cada aplicación particular de la ley es un acto de administración. La administración es la parte más obvia del gobierno; es el gobierno en acción; es el lado ejecutivo, el operativo, el más visible del gobierno.[26]
Frank Goodnow	1859-1939	EE.UU.	Profesor, politólogo y jurista	La administración incluye la función de ejecutar la ley, así como las funciones semi-científicas, cuasijudiciales y cuasi-comerciales o comerciales.[27]

24 O. Guerrero Orozco, *La teoría de la administración pública*, *op. cit.*, pp. 260, 261 y 264.
25 O. Guerrero Orozco, *Introducción a la administración pública*, *op. cit.*, p. 248.
26 S. B. M. Marume, "Meaning of Public Administration", *Journal of Research in Humanities and Social Science*, vol. 4, issue 6, Quest Journals, 2016, p. 16.
27 *Ibid.*, p. 18.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Maximilian Weber	1864-1920	Alemania	Historiador, politólogo, filósofo, jurista, sociólogo y economista	Sus aportaciones se centran en la teoría de la administración de las burocracias, definidas como la racionalización de la actividad colectiva. Señala que el perfeccionamiento de la administración tiene que partir de la aplicación de un sistema burocrático ideal, profesionalizada y cualificada.
Vittorio Wautrain-Cavagnari		Italia		La ciencia de la administración deberá tener como objeto todas las materias que compendia el gobierno de un Estado. La ciencia de la administración tiene como objeto de su atención al Estado, más precisamente, la acción del Estado. La ciencia de la administración se ocupa de la adquisición y uso correcto de los medios (bienes económicos y servicios profesionales) para lograr el mejoramiento de las clases sociales bajo el cuádruple aspecto económico, fisico, intelectual y moral.[28]
William Franklin Willoughby	1867-1960	EE.UU.	Economista	El término administración puede emplearse en Ciencia Política en dos sentidos. En su sentido más amplio, denota el trabajo involucrado en la conducción real de los asuntos gubernamentales, independientemente de la rama particular del gobierno en cuestión. Es, por lo tanto, bastante apropiado hablar de la administración de la rama legislativa del gobierno, la administración de justicia o asuntos judiciales, o la administración del poder ejecutivo, así como la administración de los asuntos de la rama administrativa del gobierno, o la conducción de los asuntos del gobierno en general. En su sentido más estricto, denota las operaciones de la rama administrativa solamente.[29]

28 O. Guerrero Orozco, *La teoría de la administración pública*, *op. cit.*, pp. 267-268
29 S. B. M. Marume, *op. cit.*, p. 17.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Mary Parker Follett	1868-1933	EE.UU.	Socióloga	Sus aportaciones se centraron en la importancia de favorecer la integración de grupos de trabajo para mejorar la eficacia de la administración pública y privada, argumentando que las personas en grupos producen mejores resultados tanto en pensamientos como en acción.
Elton Mayo	1880-1949	EE.UU.	Sociólogo y psicólogo	Sus estudios se centraron en el desarrollo de la teoría de las relaciones humanas, haciendo énfasis en el papel de los recursos humanos y en reconocer que los individuos trabajan para satisfacer necesidades económicas, psicológicas y sociales.
Chester Barnard	1886-1961	EE.UU.	Economista	Sus aportes se relacionan con la teoría de la cooperación, la organización informal y la teoría de aceptación de la autoridad. En el caso específico de la teoría de la autoridad, señala que quienes realmente la ejercen son los trabajadores, pues ellos deciden si aceptan o no las órdenes de sus superiores.
Leonard D. White	1891-1958	EE.UU.	Politólogo e historiador	La administración pública consiste en todas aquellas operaciones que tienen por finalidad el cumplimiento o la aplicación de la política pública.[30]
Paul H. Appleby	1891-1963	EE.UU.	Politólogo y administrador público	La administración es vista como el gobierno en acción directa en nombre de y en contención de los ciudadanos.[31]

30 *Ibid*., p. 16.
31 Paul H. Appleby, *Policy and administration*, Birmingham, University of Alabama Press, 1949, p. 15.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Luther Gulick	1892-1993	EE.UU.	Politólogo	La administración pública es esa parte de la ciencia de la administración que tiene que ver con el gobierno y, por lo tanto, se ocupa principalmente del poder ejecutivo donde se realiza el trabajo del gobierno, aunque obviamente hay problemas en relación con los poderes legislativo y judicial.[32]
Lucio Mendieta y Núñez	1895-1988	México	Sociólogo y jurista	La actividad de la administración pública obedece a las necesidades sociales y éstas, a su vez, pueden ser clasificadas según su naturaleza. Toda sociedad humana, en cuando adquiere cierta importancia y complejidad, se organiza para responder a exigencias internas de la vida colectiva y a exigencias que pudiéramos llamar externas frente a otros grupos sociales. La administración se estructura de acuerdo con un plan que deriva de la sociedad misma o que le imponen los hechos sociales.[33]
Gabino Fraga	1899-1982	México	Abogado y político	La administración pública debe entenderse desde el punto de vista formal como el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales y que desde el punto de vista material es la actividad de este organismo considerado en sus problemas de gestión y de existencia propia tanto en sus relaciones con otros organismos semejantes como con los particulares para asegurar la ejecución de su misión.[34]

32 S. B. M. Marume, *op. cit.*, p. 17.
33 Lucio Mendieta y Núñez, La Administración Pública en México, México, UNAM, 1942, pp. 8 y 11.
34 Gabino Fraga, *Derecho administrativo,* México, Porrúa, 2000, p. 119.

Autor	Fecha	País	Formación	Definición de Administración Pública o aportación al estudio de la administración pública
Marshall E. Dimock	1903-1991	EE.UU.	Politólogo	La administración pública es el cumplimiento o la ejecución de la política pública declarada por las autoridades competentes. Se trata de los problemas y poderes de la organización y las técnicas de gestión involucradas en el cumplimiento de las leyes y políticas formuladas por las agencias de formulación de políticas del gobierno. La administración pública es la ley en acción. Es el lado ejecutivo de un gobierno.
Dwight Waldo	1913-2000	EE.UU.	Politólogo	La administración pública es el arte y la ciencia de la gestión aplicada a los asuntos del Estado. El proceso de administración pública consiste en las acciones involucradas en afectar la intención o el deseo de un gobierno. Por lo tanto, es la parte "empresarial" de un gobierno, continuamente activa, que se ocupa de llevar a cabo la ley tal como lo hacen los cuerpos legislativos (u otros agentes autorizados) e interpretada por los tribunales, a través del proceso de organización y gestión.[35]
Herbert A. Simon	1916-2001	EE.UU.	Economista y politólogo	Por administración pública se entiende el uso común, las actividades de las ramas ejecutivas de los gobiernos nacionales, estatales y locales.[36]
Philip Selznick	1919-2010	EE.UU.	Sociólogo	Aportaciones: a) la burocracia es una estructura social adaptativa y dinámica; por lo tanto, cuando un resultado no es el esperado, debe propiciarse una modificación de su estructura y definición; b) la burocracia debe analizarse desde un punto de vista estructural y funcional; c) dentro de una organización formal existe una estructura informal que impacta en las actividades burocráticas.

35 S. B. M. Marume, *op. cit.*, p. 17.
36 *Loc. cit.*

Fuente: Elaboración propia con información de las fuentes citadas a pie de página.

BIBLIOGRAFÍA

[sin autor], "Qu'est-ce que l'État?", [en línea], París, *Vie-publique.fr*, 2018, Dirección URL: http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/qu-est-ce-que-etat.html.

[sin autor], *Las ideas de Administración de Javier de Burgos*, Madrid, Instituto Nacional de Administración Pública, 1987.

Abellán, Joaquín, "Liberalismo alemán del siglo XIX: Roberto von Mohl", *Revista de Estudios Políticos (Nueva Época)*, n° 33, Madrid, Centro de Estudios Políticos y Constitucionales, 1983.

Appleby, Paul H., *Policy and administration*, Birmingham, University of Alabama Press, 1949.

Bluntschli, M., "La administración pública", *Revista de Administración Pública*, n° 42, México, INAP, 1980.

Bonnin, Charles-Jean Baptiste, *Compendio de los Principios de Administración*, Madrid, Imprenta de Don José Palacios, 1834.

_____, *Doctrine Sociale, textuellement formée des déclarations de droits françaises et américaines*, París, Paulin, 1833.

Castillo Velasco, José María del, *Ensayo sobre el derecho administrativo mexicano*, México, Taller de Imprenta de la Escuela de Artes y Oficios para Mujeres, 1874.

Colmeiro, Manuel, *Derecho administrativo español*, Tomo I, Madrid, Imprenta y librería de Eduardo Martínez, 1876.

De la Rosa, Luis "Sobre la administración pública de México y medios de mejorarla", *Revista de Administración Pública*, n° 50, México, INAP, 1982.

Fayol, Henri, "The administrative theory in the State", en Gulick, Luther y Urwick, L., eds., *Papers on the Science of Administration*, Nueva York, Institute of Public Administration, 1937.

Fraga, Gabino, *Derecho administrativo*, México, Porrúa, 2000.

Gandillot, M. R., *Curso de derecho administrativo*, Madrid, Imprenta de D. José Espinosa, 1835.

García-Pelayo, Manuel, "La teoría de la sociedad en Lorenz von Stein", *Revista de estudios políticos*, no° 47, Madrid, Centro de Estudios Políticos y Constitucionales, 1949.

Goodnow, Frank Johnson, *Politics and administration. A Study in Government*, Nueva York, The Macmillan Company, 1900.

Guerrero Orozco, Omar, *Introducción a la administración pública*, México, Harla, 1985.
_____, *La teoría de la administración pública*, México, Harla, 1986.
_____, *Teoría administrativa del Estado*, México, Oxford University Press, 2000.
Humboldt, Wilhelm von, *Los límites de la acción del Estado*, Madrid, Técnos, 2009.
Lares, Teodosio, "El Derecho Administrativo. La ciencia de la Acción y de la Competencia del Poder Ejecutivo", *Revista de Administración Pública*, n° 50, México, INAP, 1982.
Marume, S. B. M., "Meaning of Public Administration", *Journal of Research in Humanities and Social Science*, vol. 4, issue 6, Quest Journals, 2016.
Marx, Karl, "Glosas críticas marginales al artículo: 'El Rey de Prusia y la reforma social' por un Prusiano", en Marx, Karl, *Escritos de juventud sobre el Derecho. Textos 1837-1847*, Barcelona, Anthropos, 2008.
Mayer, Otto, *Derecho administrativo alemán*, Tomo I, Buenos Aires, Editorial de Palma, 1949.
Mendieta y Núñez, Lucio, La Administración Pública en México, México, UNAM, 1942.
Oliván, Alejandro, *De la administración pública con relación a* España, Madrid, Boix Editor, 1843.
Ortiz de Zúñiga, Manuel, "Idea general de la administración y del derecho administrativo", *Revista de Administración Pública*, Edición Especial en Memoria del Maestro y Primer Presidente del INAP Gabino Fraga, México, INAP, 1982.
Posada de Herrera, José, *Lecciones de administración*, Tomo I, Madrid, Establecimiento tipográfico, 1843.
Sánchez González, José Juan, *Historia del estudio de la administración pública en México*, México, Porrúa, 2009.
Stein, Lorenz von, *Movimientos Sociales y* Monarquía, Madrid, Centro de Estudios Constitucionales, 1981.
Valadés, Diego, "Comentario preliminar", en Nava Negrete, Alfonso, *Estudios administrativos*, México, UNAM, 2011.
White, Leonard D., *Introducción al estudio de la Administración Pública*, México, Compañía General de Ediciones, 1964.
Willoughby, William F., *An introduction of the study of the government of modern states*, Nueva York, The Century Co., 1919.

Wilson, Thomas Woodrow, "The study of administration", *Political Science Quarterly*, vol. 2, n° 2, Nueva York, Academy of Political Science, 1887.

Revista de Administración Pública

INAP

INDICACIONES PARA LOS COLABORADORES

1. Exclusividad

Los artículos enviados a la **Revista de Administración Pública** (RAP) deberán ser inéditos y no haber sido sometidos simultáneamente para publicación en otro medio.

2. Naturaleza y temática de los trabajos

Deberán ser de carácter eminentemente académico o relacionarse con uno o varios temas considerados de interés para las administraciones públicas de México y otros países.

3. Características de los trabajos

- Se entregarán, para su dictamen y publicación, en idioma español, totalmente concluidos. Una vez iniciado el proceso de dictaminación no se admitirán cambios.
- Deberán tener una extensión mínima de 12 cuartillas y máxima de 25, sin considerar cuadros, gráficas y lista de referencias bibliográficas utilizadas. En casos excepcionales, y a juicio de la RAP, se aceptarán trabajos con una extensión diferente.
- Deberán enviarse o entregarse en formato electrónico en Word de Microsoft Office en letra tipo Arial tamaño 12 con interlineado de 1.5 y márgenes superior-inferios 2.5 cms., decho-izquierdo 3 cms.

- Deberán contar con una estructura mínima de título, introducción, desarrollo, conclusiones y bibliografía, con las siguientes especificaciones mínimas:

a) El título del trabajo deberá ser breve y tener una clara relación con el contenido desarrollado.
b) Las siglas empleadas deberán tener su equivalencia completa al usarse por primera vez en el texto.
c) Las notas deberán aparecer numeradas al pie de página usando el orden que sigue para las referencias al pie:

- ***Para libro***: nombre, apellido, *título*, lugar de edición, editorial, año, intervalo de páginas.
  Ejemplo: Luis F. Aguilar Villanueva, *El gobierno del gobierno*, México, INAP, 2013.
- ***Para capítulo de libro***: nombre, apellido, "título del capítulo", *título de libro*, lugar de edición, Editorial, Año, intervalo de páginas.
  Ejemplo: Omar Guerrero, "Nuevos aportes a la teoría de la administración pública", en Luis Miguel Martínez Anzures (coord.), *Antología sobre teoría de la administración pública*, México, INAP, pp. 21-30.
- ***Para artículo***: nombre, apellido, "título del artículo", *nombre de la revista*, Volumen, número, Periodo y año, intervalo de páginas.
  Ejemplo: Luis Miguel Martínez Anzures, "Reflexión sobre la deontología del servidor público", *Revista de Administración Pública*, Vol. LII, Núm. 144, septiembre-diciembre de 2017, pp. 209-223.

d) La bibliografía final se ordenará alfabéticamente, siguiendo al formato anterior, pero invirtiendo el orden del nombre y apellido del autor (apellido, nombre). Si la fuente original no menciona alguno de los datos, deberá hacerse explícito usando las expresiones "sin pie de imprenta", "sin fecha" entre corchetes.
e) Los cuadros, gráficas, figuras y diagramas deben indicar la fuente completa correspondiente Los cuadros serán numerados con el sistema arábigo (cuadro 1, 2, 3, etc.) y romano para mapas planos, figuras, láminas y fotografías (figura I, II, III, etc.).

f) Las gráficas, cuadros, diagramas o figuras se incluirán en un archivo en cualquier programa de Microsoft Office

4. Dictaminación

Las colaboraciones se sujetarán a un proceso de dictamen imparcial y por pares ("*Peer System*") con carácter anónimo.

5. Resumen y abstract

En archivo separado se entregará un resumen del artículo con una extensión máxima de 150 palabras, tanto en español como en inglés. También se indicarán en ambos idiomas un mínimo de 3 y un máximo de 5 *palabras clave/ Keywords* que describan el contenido del trabajo.

6. Corrección y edición

La RAP se reserva el derecho de incorporar los cambios editoriales y las correcciones de estilo y de formato que considere pertinentes, de acuerdo con los criterios y normas editoriales generalmente aceptadas.

7. Difusión

El autor concede a la RAP el permiso automático y amplio para que el material que haya sido publicado en sus páginas se difunda en antologías, medios fotográficos o cualquier medio impreso o electrónico conocido o por conocerse.

8. Formas de entrega de los trabajos propuestos a publicación

- Los autores deberán enviar sus trabajos al correo electrónico:
  contacto@inap.org.mx

Revista de Administración Pública
Instituto Nacional de Administración Pública A.C.
Escuela Nacional de Profesionalización Gubernamental
Carretera Federal México-Toluca No. 2151 (Km. 14.5)
Col. Palo Alto, C.P. 05110 Cuajimalpa,
Ciudad de México, México

9. Identificación

- En el archivo del trabajo se indicarán la fecha de elaboración, el título, y nombre del autor
- En archivo por separado serán incluidos los siguientes datos:

a) Nombre completo del autor o autores; indicando para cada uno el máximo nivel de estudios alcanzado y, de ser el caso, los que haya en curso (incluyendo la disciplina e institución). Datos de contacto: domicilio, teléfono y correo electrónico.
b) Enviar breve currículum académico y profesional, incluyendo la actividad actual y centro de trabajo. Mencionar líneas actuales de investigación y la bibliografía completa de las últimas 3 ó 4 publicaciones, en su caso.

REVISTA DE ADMINISTRACIÓN PÚBLICA

148

Volumen LIV, No. 1
(enero-abril 2019)

Ciberseguridad Nacional

Se terminó de imprimir en septiembre de 2019
por Navegantes de la Comunicación
Gráfica S.A. de C.V.

La edición consta de 500 ejemplares

Distribución a cargo del INAP