RIS
Revista de Inteligencia y Seguridad

NÚMERO 2
(ENERO-JUNIO 2023)

CIBERSEGURIDAD NACIONAL

ISSN EN TRÁMITE
www.inap.mx/ris

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

68 AÑOS
mejorando a las Instituciones Públicas
1955-2023

RIS

Revista de Inteligencia y Seguridad

Número 2
(enero-junio 2023)

CIBERSEGURIDAD NACIONAL

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

68 AÑOS
mejorando a las Instituciones Públicas
1955-2023

Revista de Inteligencia y Seguridad, No. 2, enero-junio 2023, es una publicación semestral digital (www.inap.mx/ris), editada por el Instituto Nacional de Administración Pública, ubicado en Km. 14.5 Carretera México-Toluca No. 2151, Col. Palo Alto, C.P. 05110, Alcaldía de Cuajimalpa, Ciudad de México. Teléfono (55) 5081 2657. www.inap.mx, contacto@inap.org.mx
Editor responsable: José Rafael Martínez Puón.
Reserva de Derechos al Uso Exclusivo No. 04-2023-032713274000-102, otorgado por Instituto Nacional del Derecho de Autor.
ISSN: En Trámite.

Consejo Directivo 2020-2023

Luis Miguel Martínez Anzures
Presidente

Olga María del Carmen Sánchez Cordero
Vicepresidenta

Carlos Eduardo Flota Estrada
Vicepresidente para los IAPs de los Estados 2023-2024

CONSEJEROS
Rina Aguilera Hintelholher
Eber Omar Betanzos Torres
Esther Nissán Schoenfeld
David Villanueva Lomelí
Susana Libién Díaz González
Gerardo Felipe Laveaga Rendón
Fernando Álvarez Simán
Luis Humberto Fernández Fuentes

Selene Lucía Vázquez Alatorre
Secretaria del INAP

Rafael Martínez Puón
Director de la Escuela Nacional de Profesionalización Gubernamental

Ricardo Corral Luna
Director del Centro de Consultoría en Administración Pública

Luis Armando Carranza Camarena
Director de Administración y Finanzas

CONSEJO DE HONOR

Luis García Cárdenas
José Natividad González Parás
Alejandro Carrillo Castro
José R. Castelazo
Carlos Reta Martínez

IN MEMORIAM

Gabino Fraga Magaña
Gustavo Martínez Cabañas
Andrés Caso Lombardo
Raúl Salinas Lozano
Ignacio Pichardo Pagaza
Adolfo Lugo Verduzco

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

REVISTA DE INTELIGENCIA Y SEGURIDAD
N° 2 (enero-junio 2023)

CIBERSEGURIDAD NACIONAL

COORDINACIÓN EDITORIAL

COMITÉ EDITORIAL

REVISTA DE INTELIGENCIA Y SEGURIDAD
No. 2
Enero-junio 2023

ÍNDICE

PRESENTACIÓN

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, este número de la RIS está dedicado 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 por 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, 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.

En efecto, el presente número aborda el ámbito del ciberespacio desde una perspectiva de la seguridad nacional. Se recupera el esfuerzo académico con el que colaboraron 5 destacados especialistas en la materia, ya sea desde la academia o desde la práctica profesional, en 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.

Estoy convencido, que como ha sucedido con los diversos números que la RIS 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.

Luis Miguel Martínez Anzures
Presidente del INAP

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

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 Latina (Centro LATAM Digital) [1], alojado en el Centro de Investigación y Docencia

* Secretaria General del Centro de Investigación y Docencia Económicas (CIDE)-Profesora Asociada de la División de Estudios Jurídicos del CIDE. Maestra en Dirección Internacional, Instituto Tecnológico Autónomo de México (ITAM)
** Profesora Investigadora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Doctora en Derecho, Universidad de París II, Panthéon-Assas (Francia)
*** Profesora Investigadora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Doctora en Derecho, Universidad de Salamanca, España

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 Información y 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.*

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

---

[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.

reducir 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 de la información "puede resumirse en la preservación de la tríada de confidencialidad, integridad y disponibilidad de la información de un

---

[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.

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].

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,

---

[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.

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; 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

[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.

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]

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].

[23] *Ídem.*

[24] *Ibidem*., pp. 48-111.

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 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].

[25] *Ibidem*, p. 115.
[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).

- 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].
- 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[34].
- 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[35].
- La capacidad de respuesta a las crisis o a incidentes en materia de seguridad informática, así como las posibilidades de abordar

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

las amenazas cibernéticas, son limitadas en los países de América Latina en general[36]. No obstante, algunos de ellos, como Colombia, ya cuentan con iniciativas maduras para atender incidentes del gobierno y del sector privado[37].

- 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[38]. Hoy por hoy, ya se han sumado Argentina, Chile, Costa Rica y Paraguay; a Colombia y Perú sólo les queda pendiente ratificar este instrumento internacional[39], 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

---

[36] *Ídem.*

[37] *Ídem.*

[38] 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).

[39] 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).

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.

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[40].

IV.1.b) Derecho aplicable

A la cuestión de determinar la autoridad competente en materia de

[40] 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.

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 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[41].

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

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

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 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[42]. 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[43] 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

---

[42] 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).

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

programas educativos. Se 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 [44]. Se debe procurar crear una verdadera cultura de ciberseguridad[45].

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" [46] de Venezuela y la campaña internacional Stop.Think.Connect[47].

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 plataformas que ayuden a

---

[44] 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.

[45] 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).

[46] 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).

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

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."[48] 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.

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[49]. Esta definición es fundamental para poder regular la materia de forma integral.

---

[48] 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).

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

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"[50].

Mary Ellen O´Connell[51] 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"*.[52]

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

---

[50] 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).

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

[52] Mary Ellen O'Connell, "Cyber Security without Cyber War", p. 209.

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).

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).

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

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

* 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]

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.

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 todas 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 casi la mitad del siglo XX,

[2] El interés por la historia de la inteligencia ha ido en aumento por parte de académicos civiles y militares alrededor del mundo, así como para los interesados en desarrollar una historia política internacional, como para los especialistas en épocas, países 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

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 intuición 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

---

Espías") y el hindú *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.

[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 especialistas 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 espías 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.

militares y del impresionante avance tecnológico. Con el inicio del siglo XX arrancó su reposicionamiento, en medio de la 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 obtenidos por SIGINT.[9] A contramano,

---

[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

[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

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.

---

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 esenciales del estado en los ámbitos político, económico o de seguridad. 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] *Ídem.*

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 intereses 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 especialistas de distintas disciplinas, para

---

[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 encriptación alemana con fama de indestructibles, frenando a la armada germana en el Atlántico, 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.

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. Así 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 encubiertas, contrainteligencia y, principalmente, de recolección y análisis de

[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] Arnold Wolfers, "National Security as an Ambiguous Symbol", *Press Discord 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 específicas 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]

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 traído 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, así como las corrientes de innovación y los flujos 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 especializado, y a canales digitales de expresión, intercambio y organización.

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

---

[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.

[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

(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.

---

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."[1]

Para ilustrar el dinamismo en internet Jarmon y Yannakogeorgos lo plasman como una ciudad compuesta por: [2]

> "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.[3] Esta gran ciudad digital con sus claroscuros, avanza hacia la integración de una

---

[1] 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].

[2] 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].

[3] 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

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"[4] con comportamientos hostiles. Es por eso que se requieren recursos de ciberinteligencia para comprender las tendencias 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.

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**."[5]

El trazo del binomio individuos–información de estos autores destaca la interdependencia alcanzada entre estos dos extremos, ya que

---

[4] "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]

[5] 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

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 capacidad de disrupción por su manejo especializado de lo cibernético. Las herramientas de ataque de todos ellos: códigos maliciosos o *malware*, virus, gusanos y troyanos, bots y bombas lógicas, entre otros.[6]

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

[6] 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]

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 traducirlo 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.[7]

d) **Funcionalidad y estabilidad.** Ciberataques dirigidos contra la infraestructura crítica nacional [8] 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.[9] En el

---

[7] 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.

[8] 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.

[9] 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)

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 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.[10]

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." [11]

Los tres tipos de operaciones de los servicios de inteligencia tendrían como objetivos en el ciberespacio los siguientes:[12]

---

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]

[10] 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]

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

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

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
c) **Operaciones encubiertas**.[13] 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 ciberoperaciones 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

[13] 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.

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 y seguro,*[14] que delimitó cuatro campos de acción conjunta para la construcción de capacidades de ciberseguridad de los Estados miembros: 1) ciberresiliencia[15], 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[16] Su división de Operaciones concentra las capacidades de *ciberinteligencia* para atender crímenes de alta tecnología, explotación sexual infantil vía online y fraude de pagos, principalmente. La División Estratégica del EC-3 tiene un área de

---

[14] 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]

[15] 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 Informáticas 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

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

análisis estratégico que diagnostica y evalúa las tendencias globales del cibercrimen y proyecta escenarios futuros.

Más adelante, la perspectiva sobre el ciberespacio se encuadró en el concepto paraguas de *amenazas híbridas*[17], 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."[18] 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."[19] Esto es, diagnosticar mediante procesos de inteligencia la multiplicidad de entornos, para enfrentar los desafíos de manera efectiva, entre ellos los de la ciberseguridad.

---

[17] En 2017 se creó un *Centro de Excelencia – Para la lucha contra las amenazas híbridas*», a cargo del gobierno de Finlandia y 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]

[18] 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]

[19] 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]

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 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.[20]

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:[21]

---

[20] 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]

[21] 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]

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

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: infraestructura 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, así como producir inteligencia de corto plazo para responder a los acciones de provocación de los adversarios."[22] Una base de este trabajo es la identificación y priorización de riesgos –una acción prioritaria que marca la Estrategia–[23] 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.

CUADRO 2
Análisis de las Intenciones y acciones rusas en las recientes

[22] 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." *Ibid.,* p. 32 [traducción propia]

[23] *Ibid.,* p. 13. [traducción propia]

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. [24]

Llama la atención que el trabajo de difusión 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.[25] 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; [26] Irán al que responsabiliza de actividades de espionaje para penetrar las redes de EEUU y países aliados, y Corea del Norte por ciberoperaciones de recolección de inteligencia o lanzar ciberataques contra *EEUU y Corea del Sur.*

[24] 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]

[25] 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]

[26] 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 información "detenida" de las computadoras. Ibid. P. 6

Por último, el documento apunta a que los terroristas están haciendo operaciones de recolección e inteligencia en apoyo 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:[27]

> "…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."[28]

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 respecto a 2016. Siete de cada diez mexicanos se conectan a través de un dispositivo *Smartphone.*[29]

---

[27] 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*

[28] 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]

[29] 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-

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.[30] 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.[31]

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 –veintiséis lugares por debajo de Estados Unidos (2º) y dieciséis de Canadá (9º)– este desequilibrio potencialmente lo hace un blanco atractivo para ataques hostiles.[32]

Como elementos básicos de ciberseguridad cabe hacer una anotación general, para posteriormente identificar los elementos de base que dieron lugar a su estrategia:[33]

Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid= [10-01-19]

[30] "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]

[31] 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]

[32] 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]

[33] 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 construcción de capacidades, y

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,[34] 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.[35]
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.[36]

---

cooperación, alianzas, marcos de cooperación y redes de intercambio de información. En ambos México no tuvo una evaluación mínima. *Ídem.*

[34] Cámara de Diputados, *Código 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

[35] 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.

[36] 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 Publica Federal contribuyan a la generación de la ENCS y den seguimiento a la misma mediante acciones generales y especificas 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*)[37]. Posteriormente, el derivado programa sectorial de seguridad nacional incluyó en la lista de amenazas 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, [38] intereses económicos, redes de información y capacidades de defensa", señalando como actores de riesgo a gobiernos, grupos criminales y organizaciones terroristas.[39]

Lo anterior fue el marco para la presentación cuatro años después (2017) de la *Estrategia Nacional de Ciberseguridad,* que se planteó el objetivo del aprovechamiento responsable de las TIC,[40] 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:

---

[37] 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]

[38] 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]

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

[40] 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]

> "Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales."[41]

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 etapa 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

[41] 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 la contrainteligencia, recuérdese que México ha sido un objetivo de inteligencia, incluyendo las operaciones de recolección masiva 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 presidencial 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 una inversión en formación para uso de métodos estandarizados de evaluación y procesamiento de información, para garantizar el

aprovechamiento 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 cosas 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 págs. Disponible en inglés:

http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

— Cámara de Diputados, *Código 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 págs. 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 págs. 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 págs. 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 Seguridada 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.

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL: AMENAZAS Y RETOS EN EL CIBERESPACIO

Anahiby Becerril Gil*

1. 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 de datos: en India, Aadhaar[6], considerado el

---

[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)

[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*

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

---

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 Accounts 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

[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

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

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

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)*,

---

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)

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 *cryptominers* 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 preocupación para la comunidad internacional. La Organización de Naciones Unidas (en adelante ONU) ha emitido diversas recomendaciones en donde enfatiza que "la

---

[14] De conformidad con ENSIA, el *cryptohacking* o *cryptomining* es un ejemplo del funcionamiento del cibercrimen como servicio (*Cybercrime-as-a Service)*, conceptualizando 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)

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 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

---

[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.

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 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]

---

[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)

[21] Thimoty L. Thomas, "Information Security Thinking: A Comparation of U.S., Russian and China Concepts, Foreign Military Studies Office, julio, 2001,

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 ejercicio de sus derechos y libertades, de la misma forma que lo hacen en el mundo físico[26]. La

---

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).

[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).

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

---

[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)

[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).

> "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 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.

---

[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)

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]

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].

---

[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)

[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:

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*"*.

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

---

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.

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 emplean 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 específicas 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 órdenes a la máquina de la víctima" con fines de

---

[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)

[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)

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:

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.

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

[44] Randall Dipert, "Other-than-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)

[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)

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

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 porque 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,

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 bloqueo o desfiguración de un sitio web ya sea

---

pp. 13-15, disponible en: http://www.highseclabs.com/data/foir2970.pdf (Consultado el 29 de enero de 2019)

[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)

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 responsable de todo[52]. Se contabilizaron al menos 128 ataques únicos *DDos*, dirigidos a los protocolos de Internet en Estonia durante

---

[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)

[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)

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.

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

---

[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)

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

---

[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] Ibid.

[62] Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), *Russia: Implications for UK defence and security*, House of Commons, Reino Unido, disponible en:

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 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 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.

---

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)

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 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.

---

[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)

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 *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

[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)

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 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

[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 Cybersecurity", Springer, Suiza, 2019, pp. 19-22 (19-46).

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.

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

---

[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.

[71] 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)

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.

5. 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

---

[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.

[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)

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.

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.

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

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.

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)

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

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 Military 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

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

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:

CUARO 2. Gasto militar mundial en 2018

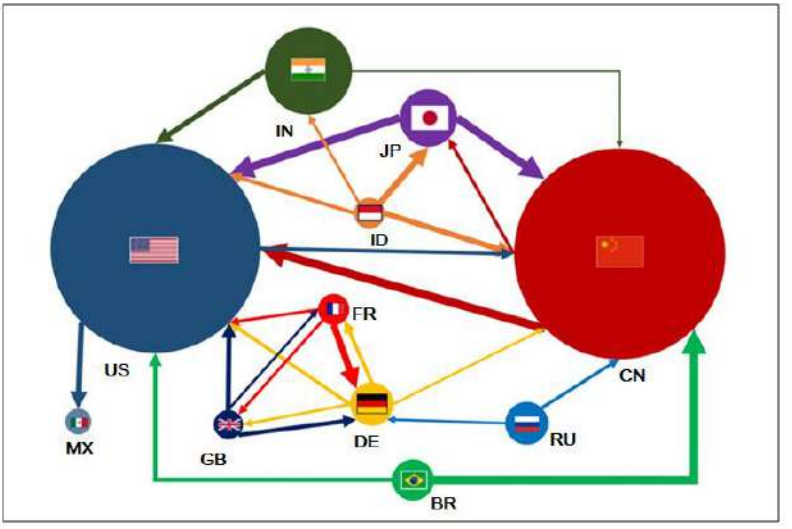
RANK	PAÍSES	GASTO (USD BN)	% PIB
1	Estados Unidos	649	3.2
2	China	250	1.9
3	Arabia Saudita	68	8.8
4	India	67	2.4
5	Francia	64	2.3
6	Rusia	61	3.9
7	Reino Unido	50	1.8
8	Alemania	49	1.2
9	Japón	47	0.9
10	Corea del Sur	43	2.6
11	Italia	28	1.3

12	Brasil	28	1.5
13	Australia	27	1.9
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 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

[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

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,

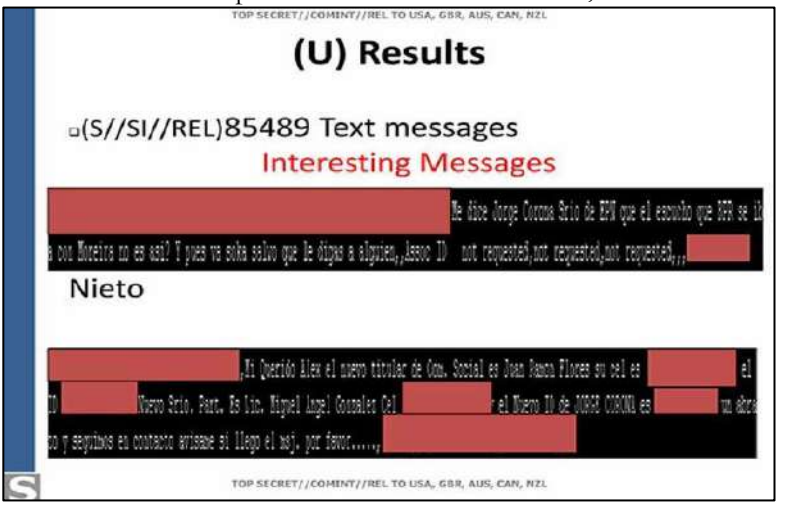
Boeing, Northrop Grumman, General Dynamics, BAE Systems, etcétera. Asimismo, en capital humano, la planeación y ejecución de las estrategias se llevan a cabo por consultoras privadas tales como Booz Allen Hamilton, Leidos, McKinsey, entre otras.

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, Japón y México. 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: "México 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

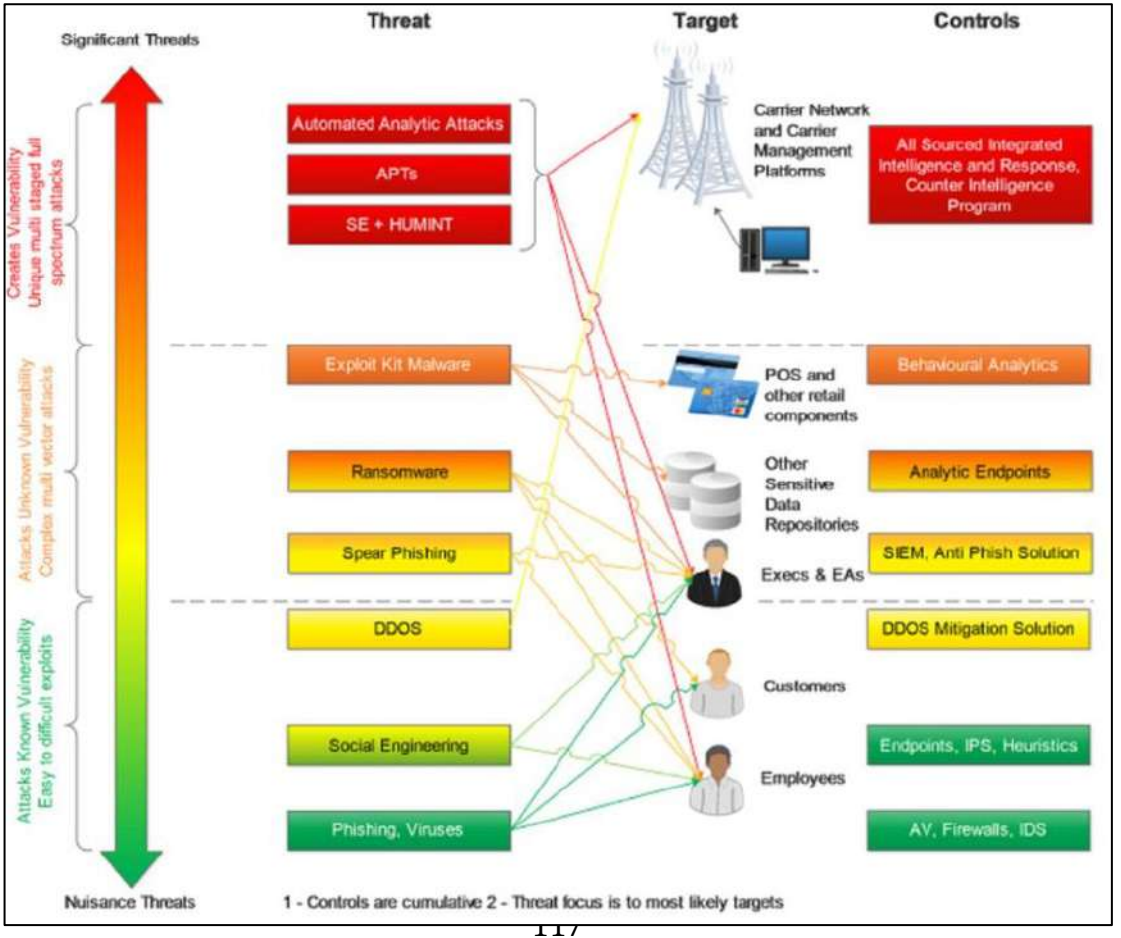
Debe observarse que cuando menos el 85% de estas Infraestructuras Críticas se encuentran en empresas del sector privado, por lo cual resulta indispensable la sinergia de esfuerzos. Algunas tendencias que incrementan los riesgos en estos sectores son: interdependencia entre los mismos sectores, proliferación 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


Threat
Target
Controls
Significant Threats
Creates Vulnerability
Unique multi staged full spectrum attacks
Attacks Unknown Vulnerability
Complex multi vector attacks
Attacks Known Vulnerability
Easy to difficult exploits
Nuisance Threats
Automated Analytic Attacks
APTs
SE + HUMINT
Exploit Kit Malware
Ransomware
Spear Phishing
DDOS
Social Engineering
Phishing, Viruses
Carrier Network and Carrier Management Platforms
POS and other retail components
Other Sensitive Data Repositories
Execs & EAs
Customers
Employees
All Sourced Integrated Intelligence and Response, Counter Intelligence Program
Behavioural Analytics
Analytic Endpoints
SIEM, Anti Phish Solution
DDOS Mitigation Solution
Endpoints, IPS, Heuristics
AV, Firewalls, IDS
1 - Controls are cumulative 2 - Threat focus is to most likely targets

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].

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

REGÍMENES PARA LA CIBERSEGURIDAD[*]

Alejandro Pisanty[**]

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.

[**] 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 Sólido, 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.a 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.b 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.c Problemas

Algunos problemas característicos de la ciberseguridad son los siguientes:

2.c.i 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.c.ii 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.c.iii 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.c.iv Confianza

Bajo el rubro "confianza" encontraremos una enorme cantidad de problemas; cuando menos los siguientes:

2.c.iv.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 ciberespacio.

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.c.iv.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.c.iv.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.c.iv.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.c.v 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 general mente 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.a Multilateral

3.a.i 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.a.ii 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.a.iii**).

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.a.iii 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.oxfordmartin.ox.ac.uk/cybersecurity/)

3.b 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.c 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.

5. 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.

Referencias / 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