NORTEAMÉRICA, Año 19, número 1, enero-junio de 2024
Recibido: 17/08/2023 Aceptado: 19/01/2024 • DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663

Rezago y asimetrías de las políticas nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: retos de cooperación para Norteamérica*

Disparities and Backlogs in Mexico's National and International Cybersecurity Policies *vis-à-vis* the United States and Canada: Challenges of Cooperation for North America

Juan Manuel Aguilar Antonio**

Resumen

En esta investigación se analiza la política nacional e internacional de ciberseguridad de Estados Unidos, México y Canadá. Se parte de la hipótesis de que el perfil de política exterior, de impacto regional e internacional, así como la trayectoria histórica individual, a lo largo de más de dos décadas, de Estados Unidos y Canadá, explican el nivel de consolidación de su política de ciberseguridad. Se trabajó con base en un conjunto ecléctico de teorías de relaciones internacionales como el realismo, el liberalismo, el constructivismo y la Teoría de la guerra para identificar elementos teóricos para abordar la política internacional y nacional de los tres países. Se concluye que tanto Estados Unidos, considerado una potencia global en ciberseguridad, y Canadá, potencia regional, poseen una política exterior activa de casi dos décadas, mientras que Mexico presenta un fuerte rezago en la materia, por lo que no cuenta con unas políticas nacional e internacional de ciberseguridad efectivas.

Palabras clave: ciberseguridad, Estados Unidos, México, Canadá, infraestructuras críticas, política nacional de ciberseguridad, delitos cibernéticos, protección de datos.

Abstract

The research analyzes the national and international cybersecurity policies of the United States, Mexico, and Canada. It is based on the hypothesis that the active foreign policy profile with regional and international impact, and the individual historical trajectory of more than two decades of the United States and Canada, can explain the level of consolidation in the development of their cybersecurity policy. An eclectic review of international relations theories such as realism, liberalism, constructivism, and the theory of war was conducted to identify theoretical

* Este artículo se realizó con apoyo del Programa de Becas Posdoctorales de la UNAM. El autor es becario del Centro de Investigaciones sobre América del Norte (CISAN), asesorado por Leonardo Curzio Gutiérrez.

** Programa de Becas Posdoctorales, Centro de Investigaciones sobre América del Norte (CISAN), Universidad Nacional Autónoma de México (UNAM); <alchemistffvii@hotmail.com>.

elements for the analysis of the international and national policies of the three countries. The conclusion shows that both the United States, considered a global power in cybersecurity, and Canada, a regional power, have an active foreign policy in the field, with a near-two-decade trajectory. Meanwhile, Mexico has a significant backlog in the field unrelated to an effective national and international cybersecurity policy.
Key words: cybersecurity, United States, Mexico, Canada, critical infrastructures, national cybersecurity policy, cybercrimes, data protection.

Introducción

En 2018, la renegociación del Tratado de Libre de Comercio de América del Norte (TLCAN) culminó con el Tratado entre México, Estados Unidos y Canadá (T-MEC). Esta nueva versión puso sobre la mesa temas emergentes en la agenda de cooperación multilateral de América del Norte (Aguirre Quezada, 2022).

En el artículo 19.15 del T-MEC, del capítulo 19 sobre comercio digital, se señala la ciberseguridad como un tema sensible que, de no atenderse, menoscabaría la confianza en el intercambio económico regional, por lo cual los países miembros se comprometen a desarrollar capacidades nacionales para responder a incidentes de ciberseguridad y fortalecer los mecanismos de colaboración para identificar y solventar aquéllos que se presenten en las redes o infraestructuras que involucran a los tres socios (Gobierno de México, s. a.).

En este artículo, se reconoce la naturaleza cambiante de las amenazas a la ciberseguridad y se propone que los países utilicen enfoques de análisis basados en riesgos relacionados con las normas consensuadas y las buenas prácticas para mitigar los efectos de las amenazas (Gobierno de México, s. a.). Por tanto, el artículo 19.15 se ha transformado en el primer marco de cooperación multilateral de ciberseguridad en Norteamérica; no obstante, éste es un concepto más amplio y holístico que no se limita al intercambio económico entre los socios. En los hechos, el diseño de una política de ciberseguridad se ha transformado en una piedra angular para la seguridad nacional, la política exterior, el desarrollo económico y la prosperidad de los Estados-nación en las dos primeras décadas del siglo XXI.

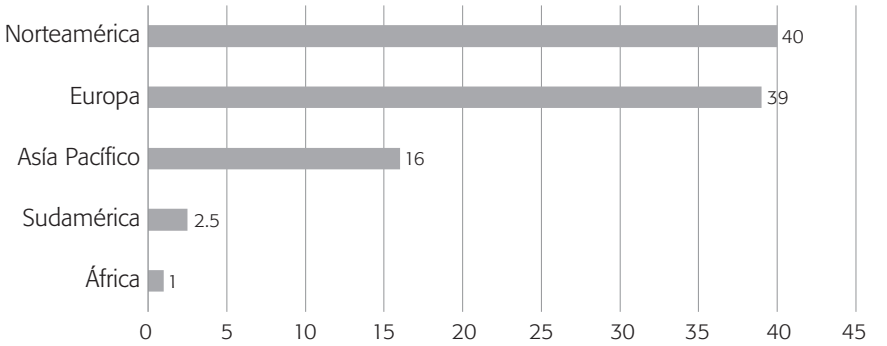
Asimismo, el avance de la digitalización, como consecuencia de la crisis global por Covid-19, impulsó la incidencia de ataques cibernéticos en todo el mundo, y esto se relaciona con el impulso de la internet suscitado por las condiciones que impuso la pandemia: se estima que entre 2020 y 2021 el número de usuarios se incrementó en 300 000 000, al pasar de 4 600 000 000 a 4 900 000 000 de personas (ITU, 2021b). También,

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

se estima que aumentará en 1 000 000 000 para 2025, lo que detonó el incremento del gasto en ciberseguridad por parte de los gobiernos.

En este sentido, Mordor Intelligence (2024) externa que el mercado de ciberseguridad para los gobiernos, empresas privadas y usuarios de internet crecerá un 378 por ciento en 2026. Esta información es vital cuándo se aborda a América del Norte. Por ejemplo, Intersog (2023) indica que la región concentra el 40 por ciento de los ciberataques a nivel internacional, y es la zona con el mayor nivel de incidencia, por encima de Europa, Asía Pacífico, Sudamérica y África. También prevé que esto se incrementará con el reciente auge de tecnologías como las redes 5G, la inteligencia artificial (IA) o el cómputo cuántico, que hacen aún más necesario la configuración de una política nacional y regional de ciberseguridad en Norteamérica.

Gráfica 1
NÚMERO DE CIBERATAQUES A NIVEL INTERNACIONAL
POR REGIONES (%)



Fuente: Intersog (2023).

Sin embargo, existen múltiples disparidades entre los socios del T-MEC como para consolidar una política regional en la materia, diferencias que pueden asociarse con el perfil y papel de cada uno como actor regional e internacional, así como al nivel de consolidación institucional y al proceso de creación de una política nacional de ciberseguridad. En ese sentido, la investigación parte de dos hipótesis: en primer lugar, que Estados Unidos y Canadá, al ser el primero una potencia global, y el segundo, regional, detentan un perfil de naciones con una política exterior activa de impacto regional e internacional en ciberseguridad, y, en segundo lugar, la trayectoria histórica individual de más de dos décadas de ambos explican el nivel de consolidación en el desarrollo de su política nacional de ciberseguridad frente a México.

Por esto, el presente artículo se divide en cuatro secciones: una discusión desde las mencionadas teorías de relaciones internacionales, aplicada al contexto de la ciberseguridad, para identificar con base en ellas qué tipo de perfil regional e internacional detenta cada uno de los tres países; enseguida, se analiza la política internacional de éstos a través de la revisión de métricas e índices internacionales que permitan ver su nivel de consolidación de capacidades cibernéticas, así como su papel en materia de ciberseguridad; luego, se explora la política nacional de cada socio a partir de su marco institucional interno en la materia para identificar y explicar las disparidades existentes, y, por último, se presentan las conclusiones.

Discusión con base en las teorías de relaciones internacionales aplicadas a la ciberseguridad

Los estudios sobre ciberseguridad pueden servirse de las teorías de relaciones internacionales para generar un marco de análisis que permita identificar y evaluar el nivel de desarrollo y consolidación de la política nacional en la materia. En esta sección se ofrece una propuesta que parte del Estado-nación, y se verá cómo éste, a través de su política nacional e internacional de ciberseguridad, puede consolidarse como nación líder o de vanguardia frente a otras.

La revisión teórica contempla los paradigmas realista, liberal, constructivista y de Teoría de la guerra. El ejercicio también sirve para identificar a los actores y dinámicas globales que se interrelacionan en el campo de la ciberseguridad desde la óptica de la política internacional.

Es importante recordar que esta propuesta es un ejercicio ecléctico que no se ajusta rígidamente a un paradigma de análisis o a un conjunto de supuestos, sino que se basa en lo expuesto por múltiples teorías, estilos e ideas para obtener amplios recursos a fin de complementar a la ciberseguridad con las dinámicas de cooperación y conflicto que pueden existir entre las naciones. De esta forma, en la gráfica 2 se presenta un modelo de análisis y abordaje teórico-metodológico para las dinámicas de la política nacional e internacional de los Estados-nación en materia de ciberseguridad. En él figuran actores y dinámicas globales.

A continuación, se exponen el enfoque y los temas que aborda cada paradigma, además de sugerirse algunas dinámicas que involucren a la ciberseguridad con la política nacional e internacional de los Estados-nación (véase la gráfica 2).

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Gráfica 2
PROPUESTA DE MODELO TEÓRICO-METODOLÓGICO DE ANÁLISIS DE LA CIBERSEGURIDAD PARA LAS POLÍTICAS NACIONAL E INTERNACIONAL DESDE LAS RELACIONES INTERNACIONALES

Fuente: Elaboración propia.

Paradigma realista

Incluye elementos teóricos del realismo clásico y del neorrealismo. Dos conceptos clave de este esquema de pensamiento son la lucha por el poder en el sistema internacional y la existencia de la anarquía global. Ambas ideas se relacionan con el concepto de ciberpoder, categoría de análisis propuesta por Joseph Nye Jr. (2011), según la cual el ciberespacio es el quinto dominio del poder de los Estados-nación para perseguir su interés. A su vez, el realismo se centra en calibrar el poder nacional de los países; para esto es importante mencionar que existen métricas internacionales que abordan el ciberpoder e incluso presentan propuestas para su medición, como el National Cyber Power Index (NCPI) y el Cyber Capabilities and National Power (CCNP), que abordaremos más adelante.

En este paradigma, desde el realismo clásico, el poder nacional de los estados está estrechamente relacionado con categorías como el poder duro (*hard power*), entendido como la capacidad de un país de influir ejerciendo coerción mediante su poderío militar, o con factores como la influencia política, económica y cultural, según

el neorrealismo (Nye Jr., 2004). Por último, el paradigma realista tiende puentes complementarios con el constructivismo y la Teoría de la guerra, para el análisis ecléctico, a la manera del diagrama de Venn, como se observa en la gráfica 2. Estos paradigmas expresan que los conflictos suponen la existencia de vías tangibles y aceptables para que las naciones alcancen su interés nacional y, en consecuencia, se superponen en algunas esferas con el paradigma realista.

Constructivismo

Este paradigma es un marco analítico que destaca por su propuesta de intersubjetividad para abordar fenómenos y sucesos internacionales. En él destaca el concepto de "identidad", presentado por Alexander Wendt, que permite identificar y ahondar en los procesos históricos y contextuales que explican el papel o dinámica que juegan los Estados-nación, organismos internacionales, o incluso conflictos o dinámicas de paz en el sistema internacional (Wendt, 1999).

Ayuda a explicar por qué países como Rusia o Estados Unidos se asocian con roles de potencias bélicas, mientras que Suiza o Costa Rica tienen una tradición pacifista (Wendt, 2004). También, el constructivismo es útil para entender la identidad de organismos internacionales como la ONU, la Organización de los Estados Americanos (OEA) o la Unión Europea (UE), que, si bien pueden clasificarse como instituciones supranacionales, esta denominación dista de su naturaleza, funciones y reputación internacional (Finnemore, 1993). Asimismo, al hablar de procesos de paz y conflicto, el constructivismo propone recurrir a elementos contextuales como las variables históricas, etnográficas, culturales y sociales para explicar las tensiones de países como Ucrania, Estonia y Georgia con Rusia, y como éstas, a su vez, son diferentes entre sí (Sürek, 2020).

Para su aplicación a la ciberseguridad, es importante mencionar que desde 2007, y como consecuencia de un ciberataque DDOS ejecutado desde Rusia a Estonia,[1] las naciones del mundo han desarrollado políticas nacionales de ciberseguridad que se reflejan en el diseño de estrategias nacionales, legislaciones o acuerdos de cooperación internacional en la materia (Aguilar Antonio, 2019). En ese sentido, el constructivismo es clave para ahondar en el perfil de cada país en este campo. Por ejemplo, no ejercen el mismo rol ni tienen la misma reputación internacional Estados Unidos, Rusia, China

[1] Un ataque DDOS (Distributed Denial of Service) es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red objetivo, incrementando de forma extraordinaria, a manera de avalancha, el tráfico de Internet. El objetivo es hacer que no esté disponible para sus usuarios previstos, causando interrupciones, pérdidas financieras o daños a la reputación.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

o Reino Unido, considerados las potencias globales en este tema, frente a naciones con un perfil más cooperativo como Estonia o Singapur (Wendt, 2004).

Asimismo, el constructivismo ayuda a explicar por qué una nación como Estonia hoy es una potencia en ciberseguridad, con capacidad de frenar agresiones provenientes de Rusia, mientras que Ucrania o Georgia no (Shackelford, 2009), por lo que este enfoque ayuda a entender desde el concepto de "identidad" el papel de un Estado-nación en el sistema internacional, los fines y objetivos de un tratado internacional o las causas y determinantes sociohistóricas y culturales que explican un conflicto prolongado en el contexto global. Por último, este esquema tiene puntos de encuentro con el paradigma realista, liberal y la Teoría de la guerra, con los cuales se complementa como instrumento reforzador de sus supuestos.

Paradigma liberal

El liberalismo presenta divergencias e incluso antagonismos con el realismo en la comprensión de la política internacional. Esto ocurre en razón de que promueve el multilateralismo y la cooperación desde la lógica de la diplomacia, y analiza la actuación de los Estados-nación con base en normas y tratados cimentados en el derecho internacional para la construcción de la gobernanza global (Barnett y Finnemore, 2004). Esta visión es claramente contraria a la procuración de intereses particulares y a la condición de anarquía global de la perspectiva realista.

Por otra parte, es importante destacar que este paradigma juega un trascendente papel al abrir espacios a nuevos actores de las relaciones mundiales como las empresas trasnacionales, los organismos internacionales y las organizaciones no gubernamentales (ONG) (Moravcsik, 1992). Fenómenos como la globalización y sus consecuencias en esferas como la economía y la cultura también son unidades clave para el estudio.

En el caso de la ciberseguridad, se indica que hay organismos internacionales que promueven la gobernanza del ciberespacio, como la Unión Internacional de Telecomunicaciones (International Telecommunications Union, ITU), a través del Global Cybersecurity Index (GCI) (ITU, 2021a; 2021b; 2019; 2017; 2014), o países como Estonia que mantienen una política en la materia y fomentan la construcción de capacidades cibernéticas con instrumentos como el National Cybersecurity Index (NCSI) (EGA, 2023). Ambos esquemas se centran en promover instrumentos que ayuden a las naciones a cumplir con los requerimientos internacionales mínimos para construir sus propias políticas o capacidades en pro de la ciberseguridad, y así contribuir a la gobernanza del ciberespacio (Keohane, 2012).

En este conjunto de acciones destacan iniciativas como el Convenio de Budapest —formalmente conocido como el "Convenio sobre la Ciberdelincuencia" (Consejo de Europa, 2001), tratado multilateral cuyo objetivo es promover la cooperación internacional, estableciendo un marco legal para dicho fin— y el Grupo de Expertos Gubernamentales sobre Ciberseguridad de las Naciones Unidas, otra iniciativa multilateral (Lewis, 2011).

Teoría de la guerra

Al igual que el constructivismo, tiende puentes con los tres paradigmas anteriores. En primera instancia, se empata con el núcleo más duro vinculado con el realismo prescriptivo que explora la supervivencia del Estado-nación como fin último y central del interés nacional, por lo que estudia los conflictos armados entre las naciones. En este cruce, también se establecen puentes con el constructivismo, debido a que es necesario identificar cómo se entiende y se ve a sí mismo cada país a través de la construcción de su identidad y sus capacidades en la política internacional, ante la perspectiva de entrar en un conflicto armado, y cómo un Estado-nación utiliza todos sus recursos en los diferentes dominios (entorno terrestre, marítimo, aéreo, espacial y el ciberespacio) frente a la posibilidad de librar una guerra (Sylvester, 2012).

Por otra parte, el núcleo suave de la Teoría de la guerra tiene una vertiente denominada "Teoría de la guerra justa", que se ajusta a los preceptos del derecho internacional humanitario para la valoración de los crímenes de guerra. Considera que las guerras entre los Estados-nación sólo acontecen cuando se han agotado todos los medios no bélicos en la búsqueda de un bien común, lo que se relaciona con la moral y ética imperantes en el contexto global (Marín, 2005).

En la última década, en el marco de conflictos, armados o no, se ha descubierto la importancia del ciberespacio, como en la invasión de Abjasia y Osetia del Sur (2008) por parte de Rusia, o más recientemente en las recurrencia a amenazas persistentes avanzadas (advanced persistent threat, APT) durante la invasión a Ucrania, a través de *malwares* (códigos dañinos) como Industroyer 2.0 y Wiper. Frente a esto, surge la necesidad de aplicar el derecho internacional humanitario y uno de los esfuerzos más destacados en este sentido es el "Manual de Tallin sobre Derecho Internacional Aplicable a los Conflictos Cibernéticos", redactado por un grupo de expertos en la materia, cuyo propósito es ofrecer orientación en el contexto de un conflicto armado (Schmitt, 2013).

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Metodología y materiales para la investigación

Nuestra estrategia metodológica es el estudio comparatista de corte cualitativo, pues permite identificar y revisar similitudes y diferencias entre los tres países (Tonon, 2011). César Colino (2009) indica que este método resulta ágil para un número acotado de unidades de estudio. Es importante señalar que el estudio se dividió en dos partes, en la primera se explora la política internacional y el papel a nivel global de cada país en ciberseguridad. A su vez, este análisis se subdivide en dos fases: en la primera se recurre al GCI y al NCSI para contrastar los niveles de desarrollo de sus capacidades cibernéticas, identificando las simetrías y asimetrías. Ambos índices se relacionan con una visión liberal de la ciberseguridad, porque muestran el nivel de compromiso de cada país con la cooperación multilateral y la gobernanza del ciberespacio. De esta forma, es necesario explicar cómo está integrado cada uno de estos índices.

El GCI muestra la cooperación internacional de actores estatales y no estatales organizados para garantizar la gobernanza y buena regulación del ciberespacio. El índice considera cinco aspectos fundamentales: el marco legal, las medidas técnicas, la estructura organizacional, el desarrollo de capacidades y la cooperación internacional. Ha realizado cuatro ejercicios, en 2014, 2017, 2018 (publicado en 2019) y 2020 (difundido en 2021), lo que permite ver los progresos y retrocesos de los 193 países (ITU, 2014; 2021a).

Por su parte, el NCSI evalúa las capacidades cibernéticas de los Estados-nación mediante doce indicadores: diseño de políticas, delimitación de amenazas, nivel de educación, aporte global, nivel de desarrollo digital, protección de servicios esenciales, identificación electrónica y confidencialidad de servicios, protección de datos personales, respuesta a incidentes cibernéticos (CIRC), gestión de crisis cibernéticas, política de lucha contra el ciberdelito y operaciones militares. El NCSI se aplicó por primera vez en 2017 y proporciona información sobre ciento sesenta y un países. Resulta valioso para evaluar la preparación e identificar lo que habría que mejorar en sus estrategias y capacidades (EGA, 2023).

Posteriormente, se describen las métricas cercanas al paradigma realista, en este contexto, conceptos como cooperación o multilateralismo se sustituyen con términos como ciberpoder o capacidades efectivas para alcanzar metas particulares en el quinto dominio:

El National Cyber Power Index (NCPI) fue creado por el Belfer Center de la John F. Kennedy Government School de la Universidad de Harvard. Su edición de 2020 (Voo *et al*., 2020) evalúa siete objetivos en treinta países, vinculados con la seguridad nacional y la política exterior, a saber: vigilancia y seguimiento de grupos internos; fortalecimiento y mejora de la ciberdefensa nacional; control y manipulación del entorno de información; recopilación de información en otros países con fines de inteligencia

para la seguridad nacional; la competencia comercial cibernética y tecnológica nacional, la destrucción o desactivación de la infraestructura y las capacidades de un adversario y la definición de normas técnicas y cibernéticas internacionales.

En su versión de 2022, el NCPI añadió un indicador: la capacidad de acumular riqueza y/o extraer criptomonedas. Este estudio del NCPI se ha realizado en dos ocasiones y es importante mencionar que resalta por su enfoque en las capacidades de defensa y ofensa de los países. La medida considera a Estados Unidos, China, Reino Unido, Rusia e Israel como potencias del ciberespacio; cabe aclarar que, por su metodología, sólo evalúa a naciones que así se asumen (Voo *et al*., 2022).

El estudio Cyber Capabilities and National Power (CCNP), publicado por el International Institute for Strategic Studies (IISS), proporciona una evaluación cualitativa de las capacidades cibernéticas de quince países y un marco cualitativo para clasificar dicha capacidad a nivel global. La metodología, además, informa sobre su contribución al poder nacional a través de factores como el ecosistema cibernético, la competencia económica y los asuntos militares. También destaca el contexto de creciente confrontación internacional en el ciberespacio, con ejemplos notables extraídos de declaraciones y acciones de potencias como China, Estados Unidos y Rusia (IISS, 2021), de las que destaca sus políticas y capacidades cibernéticas en el entorno de la seguridad internacional. El estudio ha sido publicado en dos ocasiones, la primera en 2021, en la que se analizaron quince países, mientras que el segundo, de 2023, se incluyó a Brasil, Estonia, Alemania, los Países Bajos, Nigeria, Arabia Saudita, Singapur, Sudáfrica, Turquía y los Emiratos Árabes Unidos hasta abarcar un total de veinticinco naciones.

Se realiza en siete categorías: estrategia y doctrina; gobernanza, comando y control; capacidad central de ciberinteligencia; empoderamiento y dependencia cibernéticos; seguridad y resiliencia cibernéticas; liderazgo global en asuntos cibernéticos y capacidad cibernética ofensiva. Por último, clasifica a los países en tres niveles de poder cibernético: en el primero están aquéllos con fortalezas sobresalientes en todas las categorías, en el segundo, los que destacan en algunas de ellas y, en el tercero, los que muestran fortalezas o potencial en algunos aspectos, pero debilidades significativas en otros (IISS, 2023).

Con estos cuatro índices (GCI, NCSI, NCPI y CCNP) se identifica el papel que se otorga en los ámbitos regional e internacional a cada país de América del Norte. Por otra parte, el NCSI también sirve para identificar sus áreas de convergencia y divergencia, por lo que realiza una revisión de fuentes abiertas gubernamentales que permitirían conocer la trayectoria de la política de ciberseguridad de cada nación y comparar los niveles de consolidación de sus políticas y capacidades cibernéticas.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Análisis de la política internacional de los países de Norteamérica. Métricas cercanas al paradigma liberal

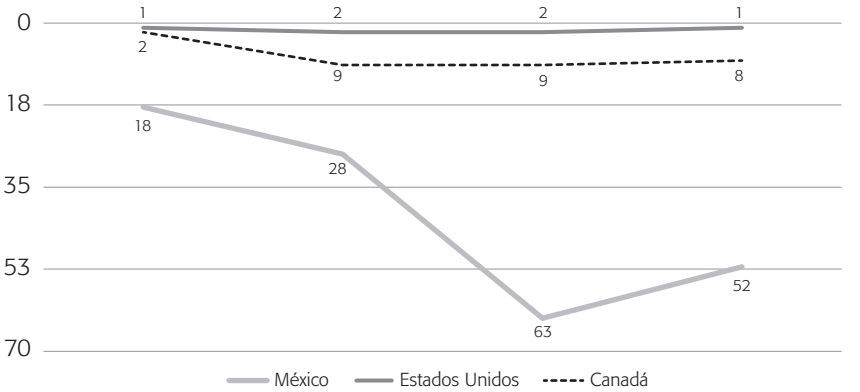
El continente americano constituye una de las zonas con mayores asimetrías en lo tocante al desarrollo de capacidades y políticas nacionales de ciberseguridad. Alberga potencias globales y regionales, como Estados Unidos y Canadá, mientras que el resto de las naciones presenta un fuerte rezago. En América Latina, considerando el territorio comprendido desde México hasta Argentina, los países ocupan la sexta posición a nivel global, entre un total de ocho regiones, sólo delante de África y Oceanía (Aguilar Antonio, 2020a). Se considera que existen otros que dan pasos estratégicos en la materia como Chile, Uruguay y Santa Lucía, países de desarrollo medio (México, Perú y Colombia) y algunos más con un claro rezago internacional, como Surinam, Trinidad y Tobago, entre otros (Aguilar Antonio, 2021).

Esta situación es más evidente cuando se observa a las tres naciones de Norteamérica empleando el GCI, donde Estados Unidos alcanza una calificación de 100/100 puntos; Canadá, de 97.6/100 y México, de 81.7/100. Esto muestra un claro rezago de este último frente a sus socios. Esa divergencia se ha profundizado en la última década, según se observa en los datos del GCI (de 2014 a 2020), mientras que Estados Unidos y Canadá se han mantenido entre las primeras posiciones.

Es notorio que la brecha que mantiene México era menor en 2014, cuando ocupaba la posición 18, mientras Canadá y Estados Unidos estaban en la 1 y 2, respectivamente. Para 2021, México se desplomó hasta la 52, mientras sus socios se mantienen entre los diez primeros puestos en desarrollo de capacidades cibernéticas a nivel internacional, como se observa en la gráfica 3.

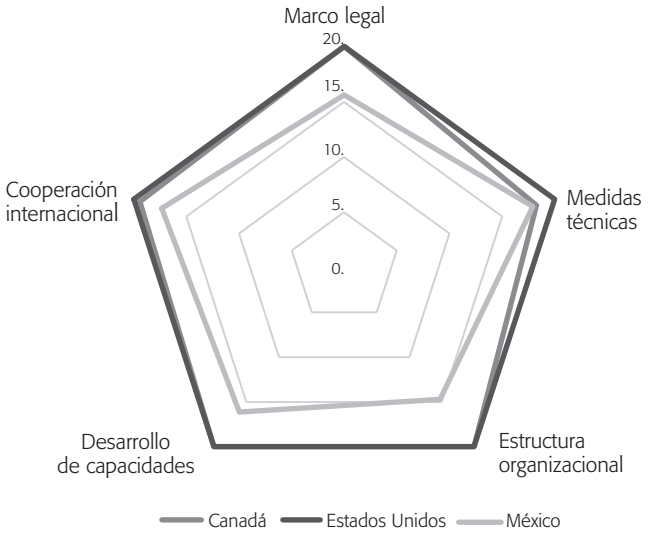
En el marco de las cinco dimensiones de evaluación del GCI, México presenta claros rezagos respecto de Estados Unidos y Canadá. Por ejemplo, Estados Unidos alcanza una calificación de 20/20 puntos en todas, con lo cual se lo considera potencia del ciberespacio. Por su parte, Canadá obtiene la máxima ponderación en las dimensiones de marco legal (20/20), estructura organizacional (20/20) y desarrollo de capacidades (20/20), mientras que en medidas técnicas su desempeño es de 18.2/20 puntos y en cooperación internacional, de 19.4/20 puntos. Por último, México alcanza 15.6/20 puntos en marco legal, 17.9/20 en medidas técnicas, 14.7/20 en estructura organizacional, 16.13/20 en desarrollo de capacidades y 17.3/20 en cooperación internacional, por lo cual muestra un claro rezago respecto de sus socios. Eso implica que tiene un menor nivel de compromiso con documentos como la Agenda sobre Ciberseguridad Global, de la ITU (2004), creada en 2004, que tiene como fin promover el compromiso con la cooperación y el multilateralismo para la gobernanza global del ciberespacio.

Gráfica 3
PROGRESIÓN DE LOS PAÍSES DE AMÉRICA DEL NORTE
SEGÚN EL GCI (2014-2021)



Fuente: ITU (2021a, 2021b, 2019, 2017, 2014).

Gráfica 4
COMPARATIVO DE NACIONES DE AMÉRICA DEL NORTE
EN CUANTO A CAPACIDADES CIBERNÉTICAS SEGÚN EL GCI (2021)

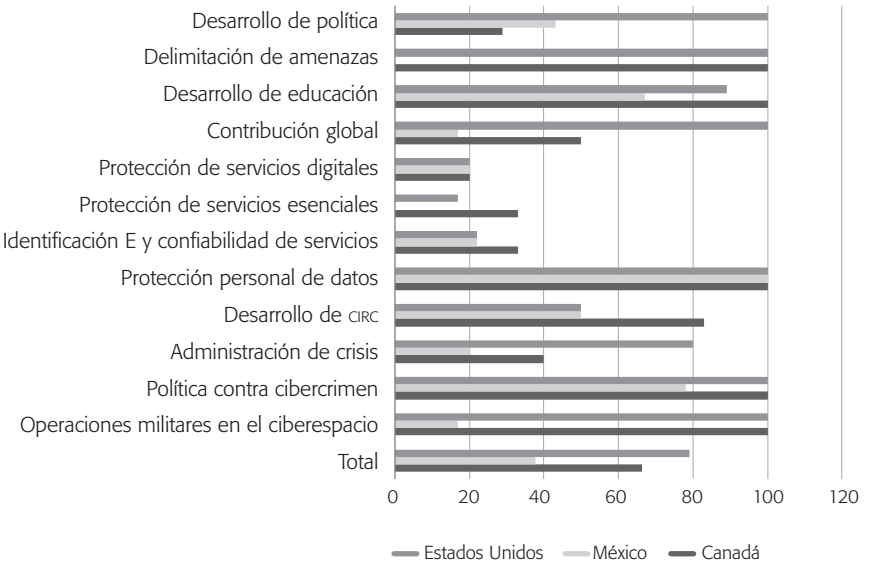


Fuente: GCI (2021a).

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

En lo tocante al NCSI, México presenta fuertes rezagos frente a Estados Unidos y Canadá en diez de doce dimensiones. Sólo está al parejo en los indicadores de política de protección de datos y de protección de servicios digitales; sin embargo, en la calificación global Estados Unidos tiene 79/100 puntos, Canadá, 66.2/100, y México, 37.7/100.

Gráfica 5
COMPARATIVO DE LOS PAÍSES DE AMÉRICA DEL NORTE
SEGÚN LOS INDICADORES DEL NCSI (2023)



Fuente: EGA (2023).

El NCSI también resultó útil para identificar en qué dimensiones el conjunto de países presenta simetrías y asimetrías. Por esta razón, se crearon cuatro categorías de análisis para cada uno de los doce indicadores: simetrías entre Estados Unidos, Canadá y México; simetrías entre Estados Unidos y Canadá, y rezago de México; liderazgo de Estados Unidos y liderazgo de Canadá (véase el cuadro 1).

Cuadro 1
CATEGORÍAS SOBRE EL DESARROLLO DE CAPACIDADES CIBERNÉTICAS DE AMÉRICA DEL NORTE

Categoría	Indicadores	Ponderaciones		
		EU	Canadá	México
I. Simetría entre Estados Unidos, Canadá y México	Protección personal de datos	100	100	100
	Protección de servicios digitales	20	20	20
II. Simetría Estados Unidos-Canada y rezago de México	Operaciones militares en el ciberespacio	100	100	17
	Política contra cibercrimen	100	100	78
	Delimitación de amenazas	100	100	0
III. Liderazgo de Estados Unidos	Administración de crisis	80	40	20
	Protección de servicios esenciales	17	33	0
	Contribución global	100	50	17
	Desarrollo de política	100	29	43
IV. Liderazgo de Canadá	Desarrollo de CIRC	50	83	50
	Identificación E y confiabilidad de servicios	22	33	22
	Desarrollo en educación	89	100	67

Fuente: Elaboración propia con base en EGA (2023).

Métricas cercanas al paradigma realista

Como se mencionó, en América del Norte existen dos naciones líderes globales en ciberseguridad. En el caso de Estados Unidos, es también la principal potencia económica y militar y esto se refleja en el dominio del ciberespacio como componente de su poderío, por lo que no es sorpresivo que métricas como el NCPI y el CCNP muestren que posee capacidades para cumplir con su interés nacional y aun para ejercer coerción en contra de los que considera sus adversarios, como China, Rusia o Irán (IISS, 2021).

Por su parte, el NCPI no considera a Canadá una de las cinco principales potencias del ciberespacio, pero sí una de segundo nivel o de alcance regional, aunado a que es la onceava potencia económica del mundo. Según datos del Banco Mundial (BM), esta condición le permite ocupar posiciones privilegiadas en organismos internacionales como el propio BM, el G7 y el G20 (Gobierno de Canadá, 2024). En el ámbito regional, cuenta con mejor prestigio que Estados Unidos y esto se refleja en sus iniciativas de cooperación en el continente en organismos como la OEA. También, a pesar

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

de que sus fuerzas armadas no figuran entre los diez ejércitos más poderosos del mundo, se asume que posee capacidades militares moderadas, lo que le ha valido ser miembro de la Organización del Tratado del Atlántico Norte (OTAN). Asimismo, Estados Unidos lo ve como un aliado estratégico en el marco del Norad (North American Aerospace Defense Command) y el Northcom (United States Northern Command), vinculados con el campo de la ciberseguridad (IISS, 2021).

Un aspecto que subraya el rezago de México es que tanto el NCPI, como el CCNP, no lo incluyen en sus respectivas mediciones, lo que refleja que no tiene una política nacional bien estructurada en ciberseguridad y tampoco la considera un campo de importancia para proyectar su interés nacional. Esta condición la comparte con el resto de América Latina, con excepción de Brasil, único incluido en las dos métricas citadas (Voo *et al*., 2022, 2020; IISS, 2023, 2021). Esto representa un problema, pues no se puede comparar a México con sus vecinos del Norte desde una perspectiva realista, al no contar con esa información.

Volviendo al NCPI, en sus dos ediciones, Estados Unidos compartió la primera posición con China, Rusia y Reino Unido. En la de 2020, Canadá ocupó la octava; no obstante, para 2022 fue desplazado hasta el décimo tercer sitio, siendo sustituido por Vietnam. A pesar de esto, se lo sigue considerando un país con capacidades cibernéticas efectivas (Voo *et al*., 2022).

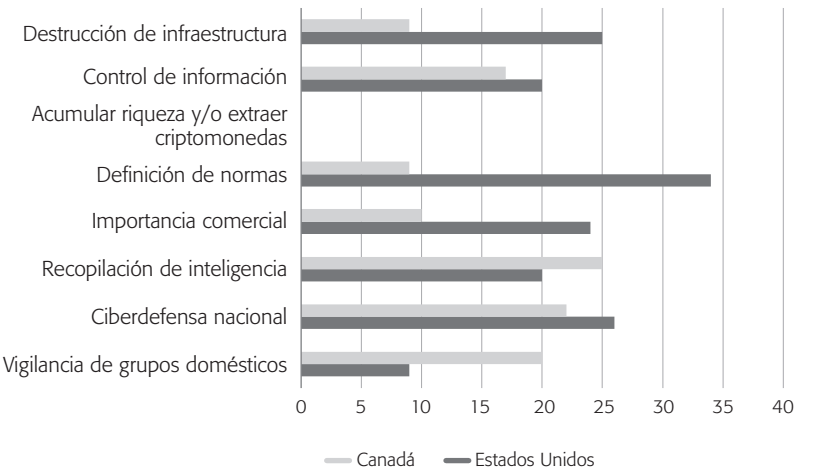
Cuadro 2
RANKING DE LOS 10 PAÍSES CON EL CIBERPODER MÁS COMPLETO SEGÚN EL NCPI 2020-2022

Ranking	2020	2022
1	Estados Unidos	Estados Unidos
2	China	China
3	Reino Unido	Rusia
4	Rusia	Reino Unido
5	Países Bajos	Australia
6	Francia	Países Bajos
7	Alemania	Corea del Norte
8	Canadá	Vietnam
9	Japón	Francia
10	Australia	Irán

Fuente: Voo *et al.* (2021; 2023).

Al comparar a nuestros socios, se encuentra que Estados Unidos supera a Canadá en cinco dimensiones: fortalecimiento y mejora de la ciberdefensa nacional (26 puntos contra 22); creciente competencia comercial cibernética y tecnológica nacional (24 *vs.* 10); definición de normas técnicas y normas cibernéticas internacionales (34 *vs.* 9); control y manipulación del entorno de información (20 *vs.* 17) y destrucción o desactivación de la infraestructura y las capacidades de un adversario (25 *vs.* 9); no obstante, Canadá lidera en vigilancia y seguimiento de grupos nacionales (25 *vs.* 9) y recopilación de información de inteligencia en el extranjero, para fines de seguridad nacional (25 *vs.* 20). Por último, ambos tienen una ponderación de 0 en lo tocante a acumular riqueza y/o extraer criptomonedas.

Gráfica 6
COMPARATIVO ENTRE ESTADOS UNIDOS Y CANADÁ EN EL NCPI 2022



Fuente: Voo *et al.* (2022).

El CCNP arroja información del papel de Estados Unidos como potencia global en ciberseguridad al presentar los indicadores de estrategia, gobernanza, comando y control, capacidades cibernéticas, poder nacional, empoderamiento cibernético y dependencia. Por ejemplo, detalla que, desde mediados de los noventa del siglo XX, el país ha buscado liderar en el quinto dominio y que es el único con una presencia global significativa tanto en el uso civil como militar del ciberespacio, mientras percibe amenazas serias de parte de China y Rusia, lo que lo lleva a un enfoque sólido y urgente para mejorar sus capacidades cibernéticas (IISS, 2021).

También, cuenta con estrategias nacionales bien desarrolladas para la defensa y seguridad en el ciberespacio, centrándose en la defensa del territorio y en conflictos

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

de baja y alta intensidad (guerras). Por esto, lidera la promoción de la gobernanza multisectorial en el ciberespacio, involucrando a diversas entidades como la comunidad de inteligencia, las fuerzas armadas y el sector privado en su política nacional. Esto ha consolidado capacidades de ciberinteligencia complejas y extensas, encabezadas por agencias como la Agencia de Seguridad Nacional (National Security Agency, NSA), la Agencia Central de Inteligencia (Central Intelligence Agency, CIA) y la Oficina Federal de Investigaciones (Federal Bureau of Investigation, FBI). A la par que colabora ampliamente con empresas del sector privado, universidades y socios internacionales, en especial a través de la alianza Five Eyes (Fvey) (Pfluke, 2019).

El CCNP indica también que el país es el más poderoso en términos de tecnologías de la información y comunicación (TIC) y en economía digital global, con una participación significativa en plataformas digitales globales, inversión de capital de riesgo y gastos en investigación y desarrollo. Respecto a su resiliencia frente a ciberataques, se informa que ha defendido su infraestructura crítica de información desde los años noventa, reconociendo la dificultad de dicha tarea; no obstante, se acepta que ha sido objeto de vulneraciones exitosas, como la operación rusa de ciberespionaje a la empresa SolarWinds (Willett, 2021), por lo que el gobierno está involucrado en detectar y neutralizar amenazas en colaboración con el sector privado.

Asimismo, en 2003 Estados Unidos lideró una iniciativa en el G8 que dio como resultado la adopción de once principios para proteger la infraestructura crítica, demostrando así su compromiso con la cooperación internacional (Sussmann, 2017). Esto promovió la adopción de normas voluntarias para la ciberseguridad en 2015, no obstante las crecientes tensiones con China y Rusia.

A pesar del enfoque cooperativo, el país también cuenta con capacidad para ejecutar medidas cibernéticas contra sus adversarios y un ejemplo se registró en 2008, con la operación Stuxnet en la central nuclear de Natanz, en Irán. También, desde 2015, realiza acciones cibernéticas para neutralizar al Estado islámico (ISIS) y la Agencia de Investigación de Internet de Rusia (François y Lin, 2021; Temple-Raston, 2019).

Respecto a Canadá, el CCNP indica que para la ciberseguridad sigue un enfoque multiactoral, integral y maduro, de partes interesadas, donde la sociedad se encuentra alineada con el gobierno (incluidos el Establecimiento de Seguridad de las Comunicaciones [Communications Security Establishment, CSE] y el Servicio de Inteligencia Canadiense [Canadian Security Intelligence Service, CSIS]) y su política exterior, todo ello respaldado por regulaciones adecuadas. Esto se beneficia del hecho de que el país tiene un sector tecnológico robusto, especialmente en áreas como la inteligencia artificial (IA) y la tecnología digital, siendo Toronto un centro importante (IISS, 2021). Para esto, entre los documentos clave centrados en la ciberseguridad hay estrategias diseñadas en los años 2010 y 2018.

Respecto a sus capacidades cibernéticas ofensivas, en 2019, el país estableció una fuerza cibernética en las fuerzas armadas; sin embargo, las operaciones de ese tipo requieren aprobación gubernamental caso por caso, de manera consistente con el uso de otros activos militares. Respecto a su compromiso global, Canadá participa en foros sobre la temática, buscando dar forma al entorno internacional de ciberseguridad, como en el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, y ha contribuido a crear capacidad de ciberseguridad a nivel global desde la Organización de Estados Americanos (OEA), con lo que reafirma su carácter de líder regional en el ciberespacio (IISS, 2021).

Análisis de política nacional de Norteamérica

La revisión del NCSI identificó cuatro dimensiones de análisis que permiten establecer las diferencias que explican el rezago de México en capacidades cibernéticas. De esta forma, el estudio de la política nacional de ciberseguridad de los tres países se dividió en dos partes: la política de protección de datos y los indicadores de desarrollo de la política nacional, la protección de servicios esenciales y los lineamientos contra el cibercrimen.

Simetría entre Estados Unidos, Canadá y México

Para comparar la política de protección de datos de los tres países se utilizaron los subindicadores de protección de datos del NCSI. Consultando fuentes abiertas y gubernamentales se revisaron las legislaciones e identificaron las instituciones encargadas de estas tareas (véase el cuadro 3). Se encontró que Estados Unidos ha adoptado una perspectiva descentralizada en su política de protección de datos. Las múltiples leyes federales y estatales abordan aspectos específicos de la privacidad y seguridad de aquéllos, reflejando la preferencia estadounidense por la autonomía individual y el acotamiento de la intervención gubernamental, posición cercana al paradigma liberal de las relaciones internacionales (Boyne, 2018).

Es importante señalar que no cuenta con una ley de privacidad de datos integral a nivel federal, pero su política se conecta indirectamente con varios instrumentos internacionales. Aunque no está vinculado con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, su relación comercial con ésta lo ha llevado a cumplir ciertos compromisos, como la iniciativa del Escudo de Privacidad UE-EE. UU. (EU-U.S. Privacy Shield), acuerdo bilateral para facilitar la transferencia de datos

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

personales, aunque fue invalidado en 2020 (Charlsey, 2022). Estados Unidos también ha participado en discusiones sobre normas internacionales de privacidad, como lo muestra su presencia en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC).

Cuadro 3
COMPARACIÓN DE POLÍTICA NACIONAL
DE PROTECCIÓN DE DATOS PERSONALES EN LOS TRES PAÍSES

Subindicador	Estados Unidos	México	Canadá
Ley de protección de datos	**Ley principal:** Privacy Act of 1974 **Leyes complementarias:** Driver's Privacy Protection Act (DPPA) Children's afine Privacy Protection Act (COPPA) Video Privacy Protection Act (VPPA) Cable CommunicatIons Policy Act (COPA) Gramm-Leach-Billey Act (GLBA) Fair Credit Reporting Act (FCRA) Health Insurance Portability and Accountability Act (HIFAA) Telephone Consumer Protection Act (TOPA) Family Educational Rights and Privacy Act (FERPA)	**Ley principal:** Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO) **Ley complementaria:** Ley federal de protección de datos personales en posesión de los particulares (LFPDPPP)	**Ley principal:** Personal Information Protection and Electronic Documents Act (PIPEDA) **Leyes complementarias:** Health Information Protection Act (HIPA) Personal Information Protection Act (PIPA) - Columbia Británica Privacy Act (Loi sur la protection des renseignements personneis)- Quebec Personal Information Protection Act (PIPA) - Quebec
Instituciones encargadas de la protección de datos	Federal Trade Commission (FTC) Department of Health and Human Services (HHS) Office of Information and Privacy	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)	Office of the Privacy Commissioner of Canada (OPC)

Fuente: Elaboración propia.

La Ley de Protección de Información Personal y Documentos Electrónicos (*Personal Information Protection and Electronic Documents Act*, PIPEDA) de Canadá refleja una postura más centralista. Esto puede interpretarse como un intento de ejercer

mayor control sobre sus políticas de datos, reduciendo su dependencia de estándares externos. La PIPEDA, aplicada tanto al sector público como al privado, representa un compromiso con la construcción de una identidad digital nacional; no obstante, la existencia de leyes provinciales adicionales señala la necesidad de equilibrar la búsqueda de cohesión nacional con el respeto a la autonomía regional (Swartz, 2007).

A pesar del enfoque centralizado, esta política se relaciona con instrumentos internacionales: Canadá es signataria del Convenio 108 del Consejo de Europa (1981), que establece principios para la protección de datos a nivel global (Kuner, 2018). Además, como miembro de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sigue estas directrices sobre protección de la privacidad y transmisión transfronteriza de datos. También se adhirió al GDPR para la transferencia de datos con la UE, demostrando su compromiso con los estándares internacionales.

México, por su parte, adoptó un enfoque dual al apegarse a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y, si bien participa en foros internacionales, como la ICDPPC, mostrando así su interés y colaboración en la definición de estándares globales (Mendoza Enríquez, 2018), sus compromisos no alcanzan a constituir acuerdos en materia bilateral o multilateral como sí ocurre con Estados Unidos y Canadá y organismos como la Unión Europea. De hecho, tampoco cuenta con un mecanismo de cooperación con sus socios de Norteamérica en protección de datos, lo que denota que, a pesar de estar en equilibrio con sus socios en esta dimensión, tampoco tiene una política internacional activa.

Simetría o liderazgo de Estados Unidos y Canadá frente a rezago de México

Para analizar este rezago, se tomaron tres indicadores de NCSI: el desarrollo de una política nacional de ciberseguridad, la protección de servicios esenciales y la existencia de una política contra el ciberdelito. En consecuencia, se procedió a buscar el cumplimiento de todo ello en fuentes abiertas, gubernamentales e institucionales de los tres países, y el resultado se presenta en el cuadro 4.

En cuanto al indicador de desarrollo de una política nacional destaca la trayectoria de Estados Unidos como pionero en la región, ya que su política de ciberseguridad se remonta a principios de la década de los años 2000 (Roesener *et al*., 2014). Por ejemplo, durante el mandato del presidente Barack Obama (2009-2017) se promulgó la Ley Nacional de Protección de la Ciberseguridad (*National Cybersecurity Protection Act*, 2014) y se crearon el Plan Nacional de Acción de Ciberseguridad (Cybersecurity

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

National Action Plan, CNAP, 2016) y posteriormente el Departamento de Defensa en Ciberestrategia (Department of Defense Cyber Strategy, DOD), demostrándose el compromiso nacional con este aspecto de la seguridad.

Durante su gobierno, Donald Trump (2017-2021) se centró en áreas como las redes 5G, dando lugar a la Estrategia Nacional de Seguridad para la 5G (National Strategy to Secure 5G of the United States of America, 2020) (Gagnon y Rapin, 2021), asunto al que Joe Biden dio continuidad con la creación de la Estrategia Nacional de Ciberseguridad (National Cybersecurity Strategy, 2023), consolidando un enfoque de largo plazo. En resumen, el país ha liderado la formulación de políticas de ciberseguridad con un enfoque integral, pues la fundación de la Agencia de Seguridad Cibernética y de la Infraestructura (Cybersecurity and Infrastructure Security Agency, CISA) y de la Oficina de Ciberespacio y Política Digital (Bureau of Cyberspace and Digital Policy, CDP) demuestra un compromiso sólido que evoluciona a lo largo de las administraciones y refleja una adaptación continua a las cambiantes amenazas digitales.

Canadá adopta una postura proactiva desde 2009 con el Plan de Acción 2010-2015 para la Estrategia de Seguridad Cibernética de Canadá (Action Plan 2010-2015 for Canada's Cyber Security Strategy), que al actualizarse en 2018 recibe el nombre de Estrategia Nacional de Ciberseguridad (National Cyber Security Strategy, NCSS), y se consolida con el Plan Nacional de Acción en Ciberseguridad (National Cyber Security Action Plan 2019-2024), que coordina la implementación de políticas, teniendo como eje gubernamental el Centro Canadiense de Ciberseguridad (Canadian Centre for Cyber Security o Cyber Centre, CCCS).

México incursiona en políticas de ciberseguridad en 2017 con la publicación de la Estrategia Nacional de Ciberseguridad (Aguilar Antonio, 2019; Aguirre Quezada, 2022); sin embargo, nunca llegó a implementarse (Aguilar Antonio, 2020b). La falta de una entidad claramente responsable y con facultades de coordinación a nivel nacional plantea interrogantes sobre la efectividad de las políticas mexicanas en ciberseguridad.

Respecto a la política de protección de servicios esenciales, la de Estados Unidos tiene sus raíces en el gobierno de Obama, con la emisión de la Directiva 21 de la Política Presidencial (Policy Directive. Critical Infrastructure Security and Resilience, PPD-21), en 2013 (Lewis, 2019), que estableció la política y directrices federales para fortalecer y proteger las infraestructuras esenciales del país contra amenazas cibernéticas y físicas. Asimismo, durante los gobiernos de Trump y Biden, se han emitido órdenes ejecutivas y directivas adicionales, destacando la atención continua a la ciberseguridad de las infraestructuras esenciales.

La CISA, establecida por la Ley de Ciberseguridad y de Seguridad de la Infraestructura (*Cybersecurity and Infrastructure Security Agency Act*, 2018), desempeña un papel fundamental en la gestión de riesgos y la protección de infraestructuras

esenciales, y es importante mencionar que su clasificación de las infraestructuras de Estados Unidos en dieciséis sectores,[2] es una de las más completas a nivel mundial (Humphreys, 2019).

Por su parte, Canadá inició su política de protección de infraestructuras esenciales en 2009 con el diseño de la Estrategia Nacional para la Infraestructura Crítica (National Strategy for Critical Infrastructure), que se ha fortalecido con documentos adicionales y la colaboración activa entre gobiernos y operadores a través de iniciativas como el Plan de Acción del Foro Nacional Intersectorial para Infraestructuras Críticas (National Cross Sector Forum Action Plan for Critical Infrastructure), el cual no cuenta con legislación específica para la gestión de riesgos cibernéticos por parte de los operadores, y el Departamento de Seguridad Pública de Canadá (Public Safety Canada, PSC), que se reconoce como la autoridad competente en ciberseguridad y seguridad de la información, y ha identificado diez sectores clave de infraestructura esencial (Gobierno de Canadá, 2023).[3]

En México, los primeros pasos en protección de las infraestructuras críticas se remontan a la Ley de Seguridad Nacional de 2006; sin embargo, no está claramente establecida su conexión específica con la ciberseguridad. Documentos como la "Guía de Ciberseguridad para Instalaciones Públicas de México" y el "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos" han contribuido a la toma de conciencia en la materia (Gobierno de México, 2023; 2018). Sobre este último documento, resalta que la Guardia Nacional, con base en el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST), identifica dieciséis sectores de infraestructuras esenciales, los mismos que reconoce la CISA, en Estados Unidos; no obstante, la falta de énfasis en ciberseguridad en el Programa Nacional de Infraestructura de la Calidad 2023 muestra áreas por mejorar, y esto se refleja en la falta de una autoridad competente para proteger las mencionadas infraestructuras, como consecuencia de la carencia de legislación específica para la gestión de riesgos cibernéticos y de supervisión de los operadores de servicios esenciales.

En cuanto a la política contra ciberdelitos, el análisis destaca que Estados Unidos cuenta con un marco legal extenso que ha evolucionado desde la Ley de Fraude y Abuso Informático (*Computer Fraud and Abuse Act*, CFAA) de 1986, hasta instrumentos

[2] Me refiero a los siguientes sectores: energía; agua y aguas residuales; tecnologías de la información y de las comunicaciones (TIC); instalaciones de fabricación; transporte; servicios de emergencia; salud pública; alimentación y agricultura; servicios financieros; gobierno; instalaciones nucleares; defensa industrial base; comercio; comunicaciones; agencias de seguridad nacional y funciones esenciales de fabricación, cada uno de los cuales juega un papel crucial en la sociedad y la economía.

[3] Dichos sectores son energía y servicios públicos; finanzas; alimentación; transporte; gobierno; tecnologías de la información y de la comunicación; salud; agua; seguridad, y manufactura.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

más recientes como la Ley de Intercambio de Información sobre Ciberseguridad (*Cybersecurity Information Sharing Act*), de 2015. Asimismo, posee agencias y grupos de trabajo que hacen efectiva su política, como la Fuerza Nacional de Tarea Conjunta de Investigación Cibernética (National Cyber Investigative Joint Task Force, NCIJTF) y el Grupo de Trabajo de Informática Forense (Cyber Forensics Working Group, CFWG).

El éxito del marco legal e institucional puede observarse en documentos como el "Report of The Attorney General's Cyber Digital Task Force" (U. S. Department of Justice –USDOJ–, 2018). En él se documentan múltiples casos de combate de delitos cibernéticos por parte de instituciones como el FBI, la CIA y la Fiscalía Federal. En particular, comparte casos de éxito como la neutralización de redes *bots* en casos representativos como VPNFilter, Kelihos, Avalanche y Corefood, que involucraban robo de datos, lo que derivó en pérdidas millonarias para gobiernos, empresas y usuarios. También, se resalta la capacidad de combate a mercados criminales en línea que operan en la *dark web*, como AlphaBay, Hansa, Silk Road y Darkode, casos en los que los instrumentos de cooperación internacional de Estados Unidos ayudaron a la captura y procesamiento de delincuentes (USDOJ, 2018).

En Canadá, las principales regulaciones son la Ley de Protección de los Canadienses contra los Delitos en Línea (*Protecting Canadians from Online Crime Act*) y la mencionada PIPEDA; mientras que las agencias y unidades a cargo son la Real Policía Montada (Royal Canadian Mounted Police, RCMP) y su unidad de criminalística digital, los Servicios de Investigación Técnica (Technical Investigation Services, TIS).

De forma semejante a Estados Unidos, Canadá publica reportes de acceso público en los que se evidencia el éxito de sus operaciones cibernéticas, tal es el caso del "Royal Canadian Mounted Police 2022-23. Departmental Results Report" (RCMP, 2023), que expone el desmantelamiento de la infraestructura de HIVE, un grupo experto en secuestro de datos (*ransomware*), con más de mil quinientas víctimas en más de ochenta países, y que además administraba el portal ílicito Canadian HeadQuarters, en la *dark web*, pero con presencia internacional.

Por su parte, México ha establecido tipificaciones para delitos informáticos en su Código Penal Federal, abordando temas como acceso ilegal, intercepción de datos, daños a sistemas informáticos, fraude informático, pornografía infantil en línea, hostigamiento cibernético, robo de identidad, etcétera, y sus principales agencias son la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Fiscalía General de la República (FGR) y la Dirección General Científica de la Guardia Nacional, que es responsable de la criminalística digital. También, destaca la Dirección General de Asuntos Policiales Internacionales e Interpol de la FGR, que es el punto de contacto para el ciberdelito internacional.

Cuadro 4
COMPARATIVO DE POLÍTICAS CONTRA CIBERDELITO, DE CIBERSEGURIDAD Y PROTECCIÓN DE SERVICIOS ESENCIALES

Desarrollo de Política Nacional de Ciberseguridad			
Subindicador	**Estados Unidos**	**México**	**Canadá**
Unidad de Políticas de Seguridad Cibernética	Bureau of Cyberspace and Digital Policy del US Deparment of State Cybersecurity and Infrastructure Security Agency (CISA) que forma parte de la estructura del US Deparment of Homeland Security	El país no cumple con el subindicador	Public Safety Canada Canadian Centre for Cyber Security
Coordinación de Políticas de Ciberseguridad	Office of the Coordinator for Cyber Issues Cybersecurity and Infrastructure Security Agency (CISA)	El país no cumple con el subindicador	El país no cumple con el subindicador
Estrategia de seguridad cibernética	Cybersecurity Enhancement Act (2014) National Cybersecurity Protection Act of (2014) Department of Defense Cyber Strategy (2018) National Cyber Strategy (2018) US Department of Homeland Security Cybersecurity Strategy (2018) Department of State International Cyberspace Policy Strategy (2020 National Strategy to Secure 5G of the United States of America (2020) National Cybersecurity Strategy (2023) National Cyber Workforce and Education Strategy (2023) CISA Cybersecurity Strategic Plan 2024-2026 (2023)	Estrategia Nacional de Ciberseguridad (2017)	Action Plan 2010-2015 for Canada's Cyber Security Strategy National Cyber Security Strategy (2018)
Plan para implementar la estrategia de ciberseguridad	Cybersecurity National Action Plan (2016) Cybersecurity and Infrastructure Security Agency: Strategic Intent (2019) National Cybersecurity Strategy Implementation Plan (2023)	El país no cumple con el subindicador	

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Cuadro 4
COMPARATIVO DE POLÍTICAS CONTRA CIBERDELITO, DE CIBERSEGURIDAD Y PROTECCIÓN DE SERVICIOS ESENCIALES
(continuación)

Protección de servicios esenciales			
Subindicador	**Estados Unidos**	**México**	**Canadá**
Se identifican operadores de servicios esenciales	**Administración de Barack Obama** Policy Directive-Critical Infrastructure Security and Resilience **Administración de Donald Trump** Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Cybersecurity and Infrastructure Security Agency Act of 2018 **Administración de Joe Biden** Proclamation on Critical Infrastructure Security and Resilience Month National Cybersecurity Strategy	Guía de Ciberseguridad para Instalaciones Públicas de México (2018) Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos (2023)	National Strategy for Critical Infrastructure Fundamentals of Cyber Security for Canada's CI Community Cross Sector Forum Action Plan for Critical Infrastructure 2018-2020 y 2020-2022
Requisitos de ciberseguridad para operadores de servicios esenciales	Cybersecurity and Infrastructure Security Agency Act of 2018	El país no cumple con el subindicador	Fundamentals of Cyber Security for Canada's CI Community Cross Sector Forum Action Plan for Critical Infrastructure 2018-2020 y 2020-2022
Autoridad de control competente	Cybersecurity and Infrastructure Security Agency (CISA)	El país no cumple con el subindicador	Department of Public Safety Canada
Regula el seguimiento de las medidas de seguridad	El país no cumple con el subindicador	El país no cumple con el subindicador	El país no cumple con el subindicador

Cuadro 4
COMPARATIVO DE POLÍTICAS CONTRA CIBERDELITO, DE CIBERSEGURIDAD Y PROTECCIÓN DE SERVICIOS ESENCIALES
(continuación)

Política contra el cibercrimen			
Subindicador	**Estados Unidos**	**México**	**Canadá**
Los ciberdelitos están tipificados	Computer Fraud and Abuse Act (CFAA) Communications Privacy Act (ECPA) Controlling the Assault of Non-Solicited Pornography And Marketing (Act CAN-SPAM) Critical Infrastructure Protection and Resilience Cybersecurity Act (CIPRA) Cybersecurity Information Sharing Act (CISA)	Art. 210 Ter, Código Penal Federal Art. 211 bis 1, Código Penal Federal Art. 212 bis 1, Código Penal Federal Art. 223 Bis, Código Penal Federal Art. 224 Bis, Código Penal Federal Art. 259 Ter, Código Penal Federal	Personal Information Protection and Electronic Documents Act (PIPEDA) Protecting Canadians from Online Crime Act
Unidad de ciberdelincuencia	National Cyber Investigative Joint Task Force (NCIJTF)	Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Fiscalía General de la República (FGR)	Royal Canadian Mounted Police, Integrated Technological Crime Units (ITCUs)
Unidad de criminalística digital	Cyber Forensics Working Group (CFWG)	Dirección General Científica de la Guardia Nacional (GN)	Royal Canadian Mounted Police, Technical Investigation
Punto de contacto 24/7 para cibercrimen internacional	Computer Crime and Intellectual Property Section (CCIPS) del U.S. Department of Justice	Unidad de Interpol de la Fiscalía General de la República (FGR)	Royal Canadian Mounted Police, National Operations Centre (NOC)

Fuente: Elaboración propia.

Un aspecto central que parece consolidar la política contra el ciberdelito de Canadá y Estados Unidos es su adhesión a instrumentos internacionales, como los antes

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

mencionados. En el caso del FiveEyes (Cinco Ojos), aunque es un grupo y no un tratado formal, los afiliados colaboran estrechamente en asuntos de inteligencia y seguridad cibernética, compartiendo información y recursos para abordar amenazas a nivel global. Estados Unidos es signatario del Tratado de Asistencia Legal Mutua (Mutual Legal Assistance Treaty, MLAT) a través del cual tiene acuerdos con varios países para cuestiones que incluyen la cooperación en investigaciones relacionadas con delitos cibernéticos. Tratados como éstos permiten compartir información y pruebas legalmente vinculantes. En este sentido, es importante mencionar que México no está adscrito a ningún mecanismo de colaboración internacional de esta naturaleza.

Conclusiones

La presente investigación partió de las siguientes hipótesis: en primer lugar, que Estados Unidos y Canadá, al ser el primero una potencia global, y la segunda, regional, poseen un perfil de naciones con una política exterior activa de impacto regional e internacional en ciberseguridad. En segundo término, que la trayectoria histórica individual de más de dos décadas de ambos países explica el nivel de consolidación de sus políticas nacionales e internacionales en ciberseguridad, lo que constituye una ventaja con respecto a México.

Puede concluirse que ambas hipótesis se verificaron a través del análisis de las mencionadas políticas, destacando que en éstas tanto Estados Unidos como Canadá están en capacidad de recurrir a múltiples mecanismos, foros o acciones internacionales para lograr sus objetivos en seguridad, además de que para la comprensión de la temática en sus diferentes dimensiones, así como para el diseño de sus políticas, pueden acudir a paradigmas tan antagónicos como el liberalismo y el realismo.

En este sentido, destaco la utilidad de los índices internacionales, con independencia de su cercanía a determinado paradigma teórico, ya que, desde la visión realista o liberal, Canadá y Estados Unidos cuentan con acciones, instituciones o políticas que permiten fortalecer y llevar a cabo una política exterior activa en materia de ciberseguridad. En ese sentido, al revisar las políticas nacionales a la luz del NCSI, se identificó cómo en el caso de ciertas subdimensiones de una política de ciberseguridad, como la protección de datos, el combate al ciberdelito o la protección de infraestructuras, ambos países se sirven de instrumentos internacionales que refuerzan sus capacidades cibernéticas en cada asunto.

Por último, es importante destacar que la trayectoria de las políticas de ciberseguridad de los socios de México es de más de veinte años, tiempo en el cual se han llevado a cabo múltiples acciones gubernamentales, políticas de estado y convenios

nacionales e internacionales para fortalecer su ciberseguridad. En contraste, nuestra Estrategia Nacional de Ciberseguridad sólo tiene siete años, periodo en el cual no se ha materializado en la construcción y, por tanto, tampoco en la implementación de una política de ciberseguridad, lo que constituye un rezago y hace prever fuerte disparidades dadas las asimetrías en la materia frente al estatus de líderes globales y regionales de nuestros socios del T-MEC, lo cual resultará problemático tanto en el ámbito del intercambio económico, como en las otras dimensiones holísticas que implica la ciberseguridad.

Fuentes

Aguilar Antonio, Juan Manuel

2021 "Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior", *Estudios Internacionales*, vol. 53, no. 198, enero-abril, pp. 169-197, DOI: http://dx.doi.org/10.5354/0719-3769.2021.57067

2020a "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas", *Revista de Estudios en Seguridad Internacional*, vol. 6, no. 2, pp. 17-43, DOI: http://dx.doi.org/10.18847/1.12.2

2020b "Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional", *Revista Legislativa de Estudios Sociales y de Opinión P*ública, vol. 13, no. 29, pp. 83-120.

2019 "Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las 'Estrategias Nacionales de Ciberseguridad'", *URVIO. Revista Latinoamericana de Estudios de Seguridad*, no. 25, pp. 24-40, DOI: https://doi.org/10.17141/urvio.25.2019.4007

Aguirre Quezada, Juan Pablo

2022 *Ciberseguridad, desafío para México y trabajo legislativo*, cuaderno de investigación no. 87, marzo, Instituto Belisario Dominguez, en <https://bibliodigitalibd.senado.gob.mx/handle/123456789/5551?show=full>.

Barnett, Michael y Martha Finnemore

2004 "The Power of Liberal International Organizations", en Michael Barnett y Raymond Duvall, eds., *Power in Global Governance*, Londres, Cambridge University Press, pp. 163-171.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Boyne, Shawn
2018 "Data protection in the United States", *The American Journal of Comparative Law*, vol. 66, supl. 1, pp. 299-343, doi: https://doi.org/10.1093/ajcl/avy016

Charlsey, Kelly
2022 "Data Privacy Regulations in the United States, China, and the European Union", tesis de Contaduría, Universidad del Sur de Georgia, en <https://digitalcommons.geor>, <giasouthern.edu/honors-theses/756/>.

Colino, César
2009 "Método comparativo", *Diccionario crítico de ciencias sociales. Terminología científico-social*, Madrid, Plaza y Valdés.

Consejo de Europa
2001 "Convenio sobre la Ciberdelincuencia", Budapest, 23 de noviembre, serie de tratados europeos no. 185, en <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.
1981 "Convenio para la Proteccion de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal", Estrasburgo, 28 de enero, serie de tratados europeos no. 108, en <https://rm.coe.int/16806c1abd>.

E-Governance Academy (ega)
2023 "National Cyber Security Index", en <https://ega.ee/project/national-cyber-security-index/>, consultada el 15 de enero de 2024.

Finnemore, Martha
1993 "International Organizations as Teachers of Norms: The United Nations Educational, Scientific, and Cutural Organization and Science Policy", *International Organization*, vol. 47, no. 4, pp. 565-597.

François, Camille y Herb Lin
2021 "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot", *Journal Of Cyber Policy*, vol. 6, no. 1, pp. 9-30.

Gagnon, Frédérick y Alexis Rapin
2021 "Cybersecurity in America: The US National Security Apparatus and Cyber Conflict Management", Sebastien-Yves Laurent, ed., *Conflicts, Crimes and*

Regulations in Cyberspace, vol. 2, diciembre, pp. 43-62, doi: https://doi.org/10.1002/9781119885092.ch2

Gobierno de Canadá

2024 "Canada and the World Bank", en <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/multilateral-multilateraux/world_bank-banque_mondiale.aspx?lang=eng>, consultada el 15 de enero de 2024.

2023 "National Strategy for Critical Infrastructure", Public Safety Canada, en <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>, consultada el 15 de enero de 2024.

Gobierno de México

2023 "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos", en <https://www.gob.mx/gncertmx/articulos/protocolo-283239>, consultada el 15 de enero de 2024.

2018 "Guía de ciberseguridad para instalaciones públicas de México", WikiGuías, 29 de noviembre, <https://www.gob.mx/wikiguias/articulos/guia-de-ciberseguridad-para-instalaciones-publicas?idiom=es>, consultada el 15 de enero de 2024.

s. a. "Tratado entre México, Estados Unidos y Canadá", en <https://www.gob.mx/t-mec>, consultada el 15 de enero de 2024.

Humphreys, Brian E.

2019 "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress", informe R45809, 8 de julio, Congressional Research Service, en <https://crsreports.congress.gov/product/pdf/R/R45809>.

International Institute for Strategic Studies (iiss)

2023 "Cyber Capabilities and National Power Volume 2", septiembre, en <https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/>, consultada el 15 de enero de 2024.

2021 "Cyber Capabilities and National Power: A Net Assesment", junio, en <https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power>, consultada el 15 de enero de 2024.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Intersog
2023 "A Global View of Cyber Security", 3 de octubre, en <https://intersog.com/blog/global-view-of-cyber-security/>.

Keohane, Robert
2012 "Twenty Years of Institutional Liberalism", *International Relations*, vol. 26, no. 2, pp. 125-138.

Kuner, Christopher
2018 "International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15 (EU-Canada PNR) of the Court of Justice of the EU", *Common Market Law Review*, vol. 55, no. 3, 10 de agosto, pp. 857-882.

Lewis, James
2011 "Confidence-building and International Agreement in Cybersecurity", *Disarmament Forum*, vol. 4, pp. 51-59, en <https://citizenlab.ca/cybernorms2012/Lewis2011.pdf>.

Lewis, Ted
2019 *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Hoboken, N.J., John Wiley & Sons.

Marín, Jefferson
2005 "Las teorías de la guerra justa. Implicaciones y limitaciones", *Guillermo de Ockham*, vol. 3, no. 2, DOI: 10.21500/22563202.478

Mendoza Enríquez, Olivio
2018 "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *IUS*, vol. 12, no. 41, pp. 267-291.

Moravcsik, Andrew
1992 "Liberalism and International Relations Theory", ensayo no. 92-6, Centro de Estudios Europeos, Universidad de Harvard, en <https://www.princeton.edu/~amoravcs/library/liberalism_working.pdf>.

Mordor Intelligence
2024 "Cyber Warfare Market Size & Share Analysis-Growth Trends & Forecasts (2024- 2029), en <https://www.mordorintelligence.com/industry-reports/cyber-warfare-market>, consultada el 15 de enero de 2024.

Nye Jr., Joseph
2011 "Cyber Power", *The Future of Power*, Nueva York, Public Affairs.
2004 "When Hard Power Undermines Soft Power", *New Persp. Q.*, vol. 21, no. 13.

Pfluke, Corey
2019 "A History of the Five Eyes Alliance: Possibility For Reform And Additions", *Comparative Strategy*, vol. 38. no. 4, pp. 302-315, doi: https://doi.org/10.1080/01495933.2019.1633186

Roesener, August, Carl Bottolfson y Gerry Fernandez
2014 "Policy for US Cybersecurity", *Air & Space Power Journal*, vol. 28, no. 6, pp. 38-54.

Royal Canadian Mounted Police (rcmp)
2023 "Royal Canadian Mounted Police 2022-23. Departmental Results Report", en <https://rcmp.ca/sites/default/files/doc/2022-2023-departmental-results-report.pdf>, consultada el 15 de enero de 2024.

Schmitt, Michael
2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press.

Shackelford, Scott
2009 "Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks", *Journal of Internet Law*, 10 de febrero.

Sürek, Çağri
2020 "An Analysis of the August War: A Constructivist Perspective", tesis de maestría, Middle East Technical University.

Sussmann, Michael
2017 "The Critical Challenges from International High Tech and Computer Related Crime at the Millennium", en Indira Carr, ed., *Computer Crime*, Londres, Routledge, pp. 379-418.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)

Swartz, Nikki
2007 "Canada Reviews PIPEDA", *Information Management*, vol. 41, no. 2, p. 8.

Sylvester, Christine
2012 "War Experiences/War Practices/War Theory", *Millennium*, vol. 40, no. 3, pp. 483-503, DOI: https://doi.org/10.1177/03058298124422

Temple-Raston, Dina
2019 "How the US hacked ISIS", National Public Radio (NPR), 26 de septiembre, en <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.

Tonon, Graciela
2011 "La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral", *Kairos: Revista de Temas Sociales*, no. 27, pp. 167-179.

Unión Internacional de Telecomunicaciones (ITU)
2021a "Global Cybersecurity Index", en <https://www.itu.int/en/ITU-D/Cybersecurity/ Pages/global-cybersecurity-index.aspx>, consultada el 15 de enero de 2024.
2021b "Measuring Digital Development. Facts and Figures", en <https://img.lalr.co/cms/2021/12/10163813/Facts-and-figures-2021.pdf>, consultada el 15 de enero de 2024.
2019 "Global Cybersecurity Index", en <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>, consultada el 15 de enero de 2024.
2017 "Global Cybersecurity Index", en <https://www.itu.int/pub/D-STR-GCI.01-2017>, consultada el 15 de enero de 2024.
2014 "Global Cybersecurity Index", en <https://www.itu.int/pub/D-STR-SECU-2015>, consultada el 15 de enero de 2024.
2004 "La Agenda sobre Ciberseguridad Global", en <https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html#:~:text=La%20Agenda%20sobre%20Ciberseguridad%20Global%20(GCA)%20de%20la%20UIT%2C,la%20sociedad%20de%20la%20informaci%C3%B3n>, consultada el 14 de enero de 2024.

U. S. Department of Justice (USDOJ)
2018 "Report of the Attorney General's Cyber Digital Task Force", 2 de julio, en <https://www.justice.gov/archives/ag/page/file/1076696/download>, consultada el 15 de enero de 2024.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre,
Daniel Cassidy y Anina Schwarzenbach
2020 "National Cyber Power Index 2020", septiembre, Belfer Center for Science and International Affairs, Harvard Kennedy School, en <https://www.belfercenter.org/publication/national-cyber-power-index-2020>.

Voo, Julia, Irfan Hemani y Daniel Cassidy
2022 "National Cyber Power Index 2022", septiembre, Belfer Center for Science and International Affairs, Harvard Kennedy School, en <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.

Wendt, Alexander
2004 "The State as Person in International Theory", *Review of International Studies*, vol. 30, no. 2, pp. 289-316.
1999 *Social Theory of International Politics*, Cambridge, Cambridge University Press.

Willett, Marcus
2021 "Lessons of the SolarWinds Hack", *Survival Online*, 31 de marzo.

 (DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663)