RAZÓN CRÍTICA Núm. 18 (2025)
https://doi.org/10.21789/22561498.2110 ARTÍCULO DE INVESTIGACIÓN

EL CIBERESPACIO COMO ESCENARIO DE CONFLICTO EN EL SIGLO XXI. ¿HACIA LA MILITARIZACIÓN DE LA CIBERSEGURIDAD?

CYBERSPACE AS A SCENARIO OF CONFLICT IN THE 21ST CENTURY. TOWARDS THE MILITARIZATION OF CYBERSECURITY?

O CIBERESPAÇO COMO CENÁRIO DE CONFLITO NO SÉCULO 21: RUMO À MILITARIZAÇÃO DA SEGURANÇA CIBERNÉTICA?

Noradilda Calderón Lara
Maestra en Estudios en Relaciones Internacionales, Universidad Nacional Autónoma de México, México
noradilda@politicas.unam.mx | https://orcid.org/0009-0009-7923-0354

Fecha de recepción: 15 de julio de 2024
Fecha de aceptación: 21 de octubre de 2024
Disponible en línea: 1 de enero de 2025

Sugerencia de citación: Calderón Lara, N. (2025). El ciberespacio como escenario de conflicto en el siglo XXI. ¿hacia la militarización de la ciberseguridad? *Razón Crítica, 18*, 1- 21. https://doi.org/10.21789/25007807.2110

Resumen

Esta investigación ofrece un panorama general respecto a los esfuerzos de la comunidad internacional a favor de la ciberseguridad por medio del desarrollo de capacidades cibernéticas. La participación del sector privado es crucial, sin embargo, a través del Estado el sector militar posee infraestructura cibernética cada vez más especializada, lo cual dota a las fuerzas armadas de nuevas tecnologías para su uso en las distintas facultades que tienen, incluyendo los escenarios de conflicto, generando varias interrogantes en torno a la militarización del ciberespacio. Por su parte, la alianza entre la Unión Europea y la OTAN se perfila como líder en el desarrollo de cibercapacidades; mientras que países como México aún no cuentan con las herramientas suficientes para hacer frente a los nuevos embates a la seguridad internacional en el siglo XXI.

Palabras clave: ciberespacio; ciberseguridad; tecnología; ciencias sociales.

Abstract

This research provides an overview of the international community's efforts to promote cybersecurity through the development of cyber capabilities. Although the participation of the private sector is crucial, the state, through its military forces, has increasingly specialized cyber infrastructure. Such infrastructure provides the armed forces with new technologies that can be used in their various capacities, including in conflict scenarios. This situation raises several questions about the militarization of cyberspace. The alliance between

the European Union and NATO is emerging as a leader in the development of cyber capabilities, while countries such as Mexico still do not have sufficient tools to face the new attacks on international security in the 21st century.

Keywords: Cyberspace; Cybersecurity; Technology; Social sciences.

Resumo

Esta pesquisa apresenta uma visão geral dos esforços da comunidade internacional para promover a segurança cibernética por meio do desenvolvimento de capacidades cibernéticas. O envolvimento do setor privado é crucial, no entanto, por meio do Estado, o setor militar possui uma infraestrutura cibernética cada vez mais especializada, que equipa as forças armadas com novas tecnologias para uso em suas diversas capacidades, incluindo cenários de conflito, levantando uma série de questões sobre a militarização do ciberespaço. Por sua vez, a aliança entre a União Europeia e a Otan está emergindo como líder no desenvolvimento de capacidades cibernéticas, enquanto países como o México ainda não têm ferramentas suficientes para enfrentar os novos desafios à segurança internacional no século 21.

Palavras-chave: espaço cibernético; segurança cibernética; tecnología; ciências sociais.

Introducción

El objetivo de este artículo es analizar la dinámica que se desarrolla en el ciberespacio en torno al conflicto, reconociéndolo como un dominio en el que convergen tecnología y diversos actores, tales como los Estados, las fuerzas armadas, organizaciones internacionales, empresas transnacionales y la población en general. Asimismo, se plantea la pregunta que forma parte del título de esta investigación: ¿hacia la militarización de la ciberseguridad?, a la que se busca dar respuesta a través del análisis de la creación de capacidades en el ciberespacio de actores que lideran el desarrollo e innovación en materia de ciberseguridad, así como de instrumentos internacionales a favor de la seguridad en el ciberespacio, incluyendo los mecanismos de operatividad, mando y control delegados a la disciplina castrense. La hipótesis parte de que el desarrollo de capacidades de índole militar llevadas al ciberespacio trae consigo una dinámica militarista que requiere de nuevas pautas y control en torno a la carrera cibernética, la cual podría generar efectos contraproducentes para las naciones que se encuentran en desventaja tecnológica, ocasionando patrones de dependencia y subordinación ante los retos, desafíos y amenazas que atentan contra la paz y seguridad internacional en el siglo XXI.

Planteamiento del problema de investigación

El ciberespacio es el único dominio producto de la acción humana; tierra, aire, mar y espacio existen sin intervención del ser humano, por lo que este espacio artificial facilita las relaciones entre individuos y naciones, aumentando la velocidad en el flujo de información en la búsqueda por potenciar las comunicaciones. El uso de las tecnologías parala información y comunicación (TIC) es cada vez más frecuente, incluso en los sitios más remotos del globo, puesto que tienen la capacidad de trascender las barreras de distancia y tiempo. Si bien las fronteras se están diluyendo, en la otra cara de la moneda se encuentran aquellas naciones con

menor desarrollo tecnológico, las cuales se encuentran en una situación de desventaja tecnológica respecto de los países con mayor avance en el área, puesto que aquellos que no cuentan con los recursos suficientes dependen de la tecnología de otras naciones, así como su ciberespacio también, de manera que "entre más periférica y subyugada sea su posición en la realidad material —por añadidura— lo mismo será en la realidad digital o virtual" (Arrollo, 2021, 12m20s).

En su informe anual, Data Reportal señala que 5,3 mil millones de personas en el mundo usan Internet, lo que representa más del 60 % de la población mundial (Kemp, 2024), es decir, la interconexión representa un factor elemental para la sociedad, incrementando asíla dependencia tecnológica y la digitalización de forma casi obligatoria en todo el mundo. En consecuencia, los delitos han transitado también al espacio digital, por lo cual, sumado a que la pandemia derivada del coronavirus SARS-CoV-2 puso en relieve la necesidad de proveer de seguridad al ciberespacio, los ciberdelincuentes aprovecharon esta coyuntura beneficiándose de los vacíos legales y las vulnerabilidades tecnológicas, así como del desconocimiento de protocolos para actuar ante los ciberataques, de manera que se ha extendido el espionaje, la destrucción, los delitos y el robo de secretos militares e industriales (Caro, 2012).

Por su parte, los datos del Índice Global de Ciberseguridad[1] (Global Cybersecurity Index) de la Unión Internacional de Telecomunicación (UIT) señalan que las pérdidas económicas por la ciberdelincuencia se estiman en un billón de dólares en 2020 y en 2021 aumentó de manera exorbitante a la cantidad de 6 billones de dólares (UIT, 2021); mientrasque el Foro Económico Mundial (2023) señala que para 2025 podrían alcanzar los 10,5 billones de dólares, lo que representa un gran desafío sobre todo para aquellos países en los que la brecha digital es cada vez mayor. De manera que las actividades de los ciberdelincuentes socavan la seguridad y generan un entorno digital de desconfianza, de ahí la importancia de desarrollar marcos legales suficientemente sólidos para enfrentarse a las amenazas, que brinden protección a quienes usan y se siguen sumando a la red de redes. Dicha certidumbre va ligada a la consolidación de instituciones con responsabilidades bien definidas y personal especializado que cuente con la infraestructura adecuada.

Aunado a lo anterior, la excesiva uniformidad y monopolización de las herramientas digitales disponibles (redes sociales, programas, servidores, incluso marcas de equipo tecnológico, entre otras) genera que las ventajas de conectividad estén al alcance de una gran parte de la población, no obstante, las desventajas también se vuelven parte del colectivo. Otra de las dificultades se refiere a los conflictos derivados de lo complejo que resulta la atribución de este, lo que genera dificultades para capturar a los atacantes debido a la falta de certidumbre legal o voluntad de los Gobiernos de los que podría provenir el ciberataque, puesto que los ataques no son perpetrados solamente por usuarios o grupos organizados de forma aislada, sino que en varios casos existe la sospecha de que los atacantes están aliados con Gobiernos que los proveen de información y recursos económicos.

[1] El Índice de Ciberseguridad Global (GCI) es una iniciativa de la Unión Internacional de Telecomunicaciones(UIT), la agencia especializada de las Naciones Unidas para las TIC.

Ejemplo de lo anterior es el caso de los ciberataques a Estonia en 2007,[2] pues, aunqueno fue comprobado, se presume que pudo contar con la participación del Gobierno ruso debido a las circunstancias que rodearon el evento. Por otro lado, los ciberataques a Georgiaen 2008[3] son considerados un precedente, ya que fue el primer conflicto armado en el que se utilizaron operaciones militares tradicionales y operaciones cibernéticas. Entre los ciberataques utilizados se encuentran ataques DDoS (de denegación de servicio), ataques de inyección y ataques de *malware*, mismos que se fueron especializando de uno a otro evento,generando una dinámica de caos e incertidumbre en las redes vulneradas.

Ningún sistema está exento de sufrir ciberataques como el robo de datos u información confidencial, pérdida o modificación de información, redireccionamiento de datos a páginas fraudulentas, interceptación de datos y correos, entre otros. Asimismo, las principales motivaciones y finalidades de los ataques cibernéticos son variadas, las cuales pueden ser inteligencia, espionaje industrial, propiedad intelectual, motivos políticos, extremismos, razones económicas, etc. De ahí que los antivirus o programas que ofrecen seguridad en el ciberespacio son cada vez más necesarios y especializados dependiendo de la infraestructura que requiera seguridad.

Para el caso de la ciberseguridad en el marco de la seguridad nacional, los requerimientos van más allá de los antivirus o programas de protección, puesto que es necesaria una sinergia del Estado con sus fuerzas armadas, la iniciativa privada, otros Estados, organizaciones internacionales y la población. Así, la dinámica internacional en el ciberespacio da cuenta de la paulatina inclusión de fuerzas militares en ejercicios en función del desarrollo de capacidades militares para la protección de redes, tecnología, infraestructura crítica y sistemas, reconociendo al ciberespacio como un nuevo campo de interés y, por consiguiente, de conflicto, un espacio que es necesario resguardar activamente tomando en cuenta las necesidades actuales.

[2] En abril de 2007 el Gobierno de Estonia decidió hacer excavaciones para buscar cuerpos de soldados caídos tras la Segunda Guerra Mundial y trasladarlos al cementerio de Tallin. Para realizarlo fue necesaria la movilización de una estatua conocida como el *Soldado de bronce*, la cual para la comunidad rusa representaba un símbolo libertador, sin embargo, para la comunidad estonia era símbolo opresor, por lo que tras la decisión del Gobierno la sociedad se polarizó, generando una ola de manifestaciones en la madrugada del 21 de abril de 2007. Al día siguiente los enfrentamientos continuaron e iniciaron los ciberataques luego de una advertenciaexpresa en la que fueron blanco sitios web de Estonia, en especial del Gobierno, Ministerio de Defensa y de los principales partidos políticos del país, todo ello enmarcado en un ambiente de tensión luego de la adhesión de Estonia en 2004 a la OTAN.

[3] En el marco del apoyo a las regiones separatistas de Osetia del Sur y Abjasia, en agosto de 2008 las fuerzas armadas de ambos bandos se enfrentaron, desencadenando una guerra en la región. Durante el desarrollo del conflicto se emplearon ataques militares convencionales y operaciones cibernéticas, por lo que es considerada como la primera ocasión en la que intervinieron fuerzas híbridas en un conflicto armado.

Las facultades de las fuerzas armadas se suscriben al ámbito de la seguridad nacional, operan con rigor y mando militar, por lo que cederle atribuciones en materia de ciberseguridad requiere de una amplia revisión en la que se garantice la privacidad, libertadde expresión y respeto a los derechos humanos. En ese sentido, derivado de las característicasdel ciberespacio, generar espacios de diálogo sobre las necesidades del sector privado, público, académico y social es requisito fundamental para la creación de instrumentos integrales, adaptables y eficaces sobre el uso de tecnologías y su aplicación en el ámbito cibernético.

Manuel Castells, en su obra *La era de la información*, llamaba la revolución de las tecnologías de la información y las comunicaciones desde comienzos del siglo XXI, evento que nos sitúa en un paradigma, toda vez que se caracteriza por ser integrador, complejo e interconectado. Hablamos de tecnologías que actúan sobre la información con capacidad de penetrar la vida cotidiana de las personas y transformarse con una creciente convergencia en un sistema hiperconectado que permite la aparición de una nueva estructura social.

La ciberseguridad y su integración en la agenda internacional

Luego del ataque a la central nuclear iraní por medio del virus Stuxnet en 2010,[4] quedó de manifiesto que las infraestructuras críticas[5] (el suministro de agua, electricidad, servicios bancarios, las redes a favor de la seguridad y defensa, entre otros) no solamente son susceptibles a ciberataques, sino que estas vulnerabilidades representan amenazas a la paz y seguridad internacionales. Por lo anterior, resulta menester contar con una red de protección profunda y sobre una lógica de cooperación multilateral que prevenga y responda de forma eficaz, ya que dichos ciberataques podrían causar daños a un país entero con una duración indeterminada, entendiendo por daños: cuestiones técnicas y pérdidas económicas, además de elementos cualitativos, tales como la confianza de la población y la resiliencia de un Estado receptor del ataque.

El ciberespacio es escenario de nuevas amenazas y ningún tipo de organización está excluida, lo que es altamente reconocido por Estados y organizaciones. Al respecto, el secretario general de la Organización de los Estados Americanos (OEA) en 2016 señaló que el tamaño del país o la cantidad de recursos asignados no son impedimento para que sean blanco de incidentes en el ciberespacio, expresó que "ningún país, grande o pequeño, está inmune a los ataques cibernéticos, que provienen de actores estatales y no estatales en un paisaje tecnológico en constante evolución" (Banco Interamericano de Desarrollo, 2016, p. 29). De modo que los problemas en torno a la ciberseguridad requieren, además de recursos materiales, contar con una red de cooperación transnacional que favorezca el mantenimiento de la seguridad en ciberespacio.

[4] Entre 2010 el virus Stuxnet se apoderó del sistema que controlaba las centrifugadoras de la planta nuclear en Natanz, Irán. Las investigaciones apuntan a que fue transferido por medio de una memoria USB y se logró replicar a otras máquinas de una forma muy sofisticada, ya que incluso logró anular los interruptores de apagadode emergencia, tomando el control de aproximadamente 1000 máquinas encargadas de la producción de materiales nucleares. Aún no se ha atribuido a nadie dicho ataque.

[5] Por infraestructuras críticas nos referimos al conjunto de recursos, servicios, tecnologías de la información yredes que en caso de sufrir un ataque causaría gran impacto en la seguridad tanto física como económica de los ciudadanos o en el buen funcionamiento de una nación.

En este sentido, la cooperación que se necesita para lograr que la ciberseguridad esté garantizada requiere de una amplia colaboración en diversos temas, además de que la necesidad de compartir información, la comunicación entre instituciones, Gobiernos y empresas es esencial. Por consiguiente, el compromiso y la voluntad política son elementos que van de la mano de la celebración de acuerdos o la creación de órganos encargados de garantizar la seguridad en el ciberespacio. Sin embargo, dicha cooperación se vuelve compleja cuando se habla de la soberanía nacional de las entidades involucradas en el ciberespacio, que no conoce de fronteras, lo que para algunas naciones puede verse como una debilidad, de modo que complica la atribución a los responsables de los ataques.

La transversalidad de los efectos de los ciberataques hace necesario impulsar que el sector público y privado y la población fortalezcan sus conocimientos respecto a cómo actuar ante dichos eventos, ya que el desconocimiento es uno de los factores que genera ventajas en relación con los efectos de las amenazas. Países como Irán, Israel, China, Rusia, Reino Unido o Estados Unidos poseen capacidades porque han invertido y promovidola agenda de ciberseguridad civil y militar (Calderín et al., 2016), lo cual los posiciona como referentes en la materia, pero también genera nuevos conflictos por la falta de un organismo internacional en el que confluyan miembros de distintas regiones para impulsar la cooperación necesaria y la certidumbre en el ciberespacio.

La creación de los distintos comandos cibernéticos en el mundo da cuenta de la incidencia que tiene el ciberespacio en las esferas políticas y militares. Los cuerpos cibernéticos de índole privada si bien tienen participación en el quehacer de las instituciones,distan del rigor gubernamental suscrito a leyes nacionales e internacionales. De modo que lacreación del cibercomando (USCYBERCOM, por sus siglas en inglés) en 2010 dio pauta a la concentración de facultades cibernéticas a favor de la seguridad de los Estados Unidos,mismo que

> Integra y lleva a cabo operaciones en el ciberespacio, guerra electromagnética y operaciones de información, lo que garantiza llevar a cabo acciones en todos los dominios y asegurar la libertad de acción con sus aliados en y a través del dominio cibernético y la dimensión de la información, negándoles lo mismo a nuestros adversarios. (US Army Cyber Command, 2022, párr. 1)

El control de las operaciones cibernéticas estratégicas se extiende no solo a Estados Unidos, sino también a Corea del Sur, Estonia, Colombia, Reino Unido, Turquía, España, Países Bajos, Rusia, China y Ecuador, por lo que el sector militar si bien resguarda la seguridad nacional en el ámbito cibernético, también requiere de recopilación de información para obtener ventajas estratégicas frente al enemigo. De modo que, al igual que las fuerzas tradicionales, el brazo cibernético es crucial para el devenir de los conflictos en el siglo XXI.

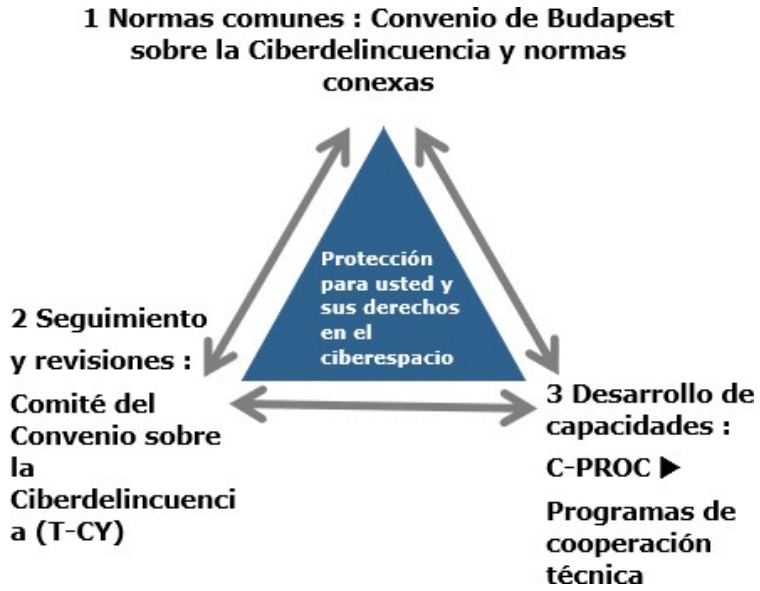
No cabe duda de lo importante que es desarrollar estrategias cibernéticas que respondan a las amenazas en el ciberespacio y que, entre otros elementos, incluyan la cooperación a través del intercambio de información de vulnerabilidades, alertas, amenazas y

ataques. Empero, el debate sobre los mandos militares y civiles requiere de especial atención para determinar los límites y alcances de las facultades del ejército frente a la sociedad civil. La mejora de las capacidades de contrainteligencia, la seguridad de productosy tecnologías, la concientización de la ciudadanía y la capacitación de servidores públicos enciberseguridad son factores que pueden proveer de certeza y confianza hacia el entorno cibernético.

Uno de los tratados internacionales más importantes en relación con el combate a la ciberdelincuencia es el auspiciado por el Consejo Europeo: el Convenio de Budapest sobre la ciberdelincuencia,[6] el cual fue firmado en noviembre de 2001, entró en vigor en 2004 y actualmente cuenta con dos protocolos adicionales: el primero sobre xenofobia y racismo y el segundo sobre pruebas electrónicas. La relevancia de este tratado reside en su carácter vinculante en materia penal, al tiempo que prevé tres ejes, como lo muestra la figura 1.

> (i) La criminalización de la conducta, que va desde el acceso ilícito, ataquesa la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil; (ii) herramientas de derecho procesal para hacer más efectiva la investigación relacionada conciberdelitos y la obtención de evidencias electrónicas; y (iii) una cooperación internacional más ágil y eficiente. (Council of Europe, 2023, párr. 2)

Figura 1. Ejes para la protección en el marco del Convenio de Budapest



Nota. Tomado de Council of Europe (2023).

[6] Para febrero de 2024 69 Estados forman parte del convenio: países europeos, además de Argentina, Australia,Brasil, Camerún, Canadá, Chile, Colombia, Costa Rica, Estados Unidos de América, Filipinas, Ghana, Israel, Japón, Mauricio, Marruecos, Nigeria, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga; 2 países firmantes: Irlanda y Sudáfrica, con 22 países invitados a adherirse Benín, Burkina Faso, Costade Marfil, Ecuador, Corea, Fiyi, Granada, Guatemala, Kazajstán, Kiribati, México, Mozambique Nueva Zelanda, Níger, Ruanda, Santo Tomé y Príncipe, Sierra Leona, Timor Oriental, Trinidad y Tobago, Túnez, Uruguay y Vanatu.

En este orden de ideas, el Convenio de Budapest sirve como una hoja de ruta internacional para sus miembros e incluso para aquellos que no lo son. El establecimiento de normas comunes, seguimiento y revisiones, así como el desarrollo de capacidades son los ejes sobre los que se sustenta el Convenio, por lo que la constitución de un marco normativo internacional que contribuya en la definición y delimitación de los conceptos relativos a los delitos cibernéticos y a los criterios jurídicos para su ejecución y aplicación es uno de los esfuerzos más sobresalientes en materia de ciberseguridad, ya que uno de los problemas al abordar temas de índole cibernética es la ambigüedad de conceptos en torno a la materia, así como la atribución de facultades a las autoridades e instituciones.

Además de la cooperación en delitos que contengan evidencia electrónica, también se crea la posibilidad de compartir experiencias a través del diálogo al ser parte del comité del Convenio sobre ciberdelincuencia (T-CY), el cual busca evaluar e interpretar la aplicación de las normas, así como ser parte de las negociaciones en torno a protocolos y creación de futuros instrumentos que favorezcan la evolución del Convenio de Budapest. De este modo, la firma y ratificación representa un gran avance para la comunidad internacional, puesto que genera mayor certidumbre a la hora de sancionar los ciberdelitos.

Por su parte, el 12 de noviembre de 2018, en el marco del Foro de la Paz de París, se pronunció el Llamamiento de París para la confianza y seguridad en el ciberespacio, que cuenta con la participación de más de 1200 participantes, incluidos 80 Estados (París Call, s. f.). Una de las características principales es que el Llamamiento no incluye solamente aEstados, sino que se apoya también en empresas y asociaciones profesionales y organizaciones de la sociedad civil, de modo que permite la aproximación desde múltiples enfoques al tiempo que reconoce la relevancia y responsabilidad de diversos actores, pues, como Celestino del Arenal (1989) señala, “en términos generales, se puede decir que desde el siglo XVII hasta la fecha relativamente reciente un único paradigma ha dominado absolutamente en el campo del estudio de las relaciones internacionales” (p. 154),refiriéndose a la visión estatocéntrica predominante en el quehacer internacional y la forma de abordar los temas emergentes.

El Llamamiento cuenta con 9 principios sobre los que centra sus esfuerzos, los cuales, aunque no se tratan de un acuerdo vinculante, ponen sobre la mesa una diversidad de temas que sin duda seguirán siendo parte de las preocupaciones concernientes al ciberespacio y, por lo tanto, a la ciberseguridad. Los 9 principios del Llamamiento son:

1. Proteger a las personas y la infraestructura crítica de prácticas cibernéticas maliciosas.
2. Proteger la accesibilidad e integridad de Internet.
3. Defender los procesos electorales a través de la cooperación.
4. Defender la propiedad intelectual.
5. Prevenir la proliferación de *software* y programas maliciosos.
6. Incrementar la seguridad del ciclo de vida de procesos, productos y servicios digitales.
7. Promover la higiene cibernética para todos los actores.

8. Prevenir ciberdelitos de actores no estatales y privados.
9. Fortalecimiento de normas internacionales para generar confianza en el ciberespacio (París Call, s. f.).

Asimismo, desde su unión en 2019, las principales empresas sobre las que el Llamamiento de París se sostiene son Microsoft, Kaspersky, Siemens, Google, Facebook y Huawei (France Diplomacy, 2021), lo cual da cuenta de que la ciberseguridad requiere de esfuerzos que no descansan exclusivamente en Estados y sus instituciones u organizaciones internacionales, puesto que la sinergia con la iniciativa privada, tomando en cuenta a la sociedad y la academia, es necesaria para generar un entorno cibernético seguro, en el que la convergencia de múltiples perspectivas sumen a las iniciativas y regulaciones en el ciberespacio, delimitando la participación de los actores para evitar la concentración de facultadas en un solo ente.

La Organización del Tratado del Atlántico Norte y la Unión Europea: líderes en la carrera cibernética

El ciberataque contra Estonia en 2007 es considerado uno de los primeros en su tipo por el nivel de profundidad de los daños causados. Estos eventos no hicieron más que fortalecer los proyectos encaminados hacia la regulación, prevención y respuesta a las actividades que se realizan en el ciberespacio. En este contexto, tanto la Organización del Tratado del Atlántico Norte (OTAN) como la Unión Europea (UE) han impulsado programas/estrategias de ciberseguridad y ciberdefensa con la finalidad de hacer frente a estas amenazas. La cooperación OTAN-UE en ciberseguridad es uno de los ejes más importantes de estos esfuerzos frente a los retos de la ciberseguridad tanto para el desarrollode capacidades de los países miembros y de ambos actores como para contribuir a la seguridad internacional en su conjunto.

Debido al impacto que tuvieron los ciberataques en países europeos y por la importancia que representan para los miembros de ambas organizaciones, la OTAN y la UE se propusieron desempeñar un papel de liderazgo en la materia. Como consecuencia, esta relación es pionera en el desarrollo de cibercapacidades, ya que cuentan con órganos especializados para ello.

Uno de los ejemplos más claros sobre la importancia de la ciberseguridad para la UE se encuentra en la creación de la Agencia Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) en 2004 y su respectivo reglamento sobre la ciberseguridad en 2019 (ENISA, 2024), que le da certidumbre y fortaleza a la agencia. Además, se creó el Reglamento General de Protección de Datos (GDRP, por sus siglas en inglés), el cual entró en vigor el 24 de mayo de 2016 y se aplica desde el 25 de mayo de 2018 (Comisión Europea, s. f.), el cual se encarga de la protección de las personas físicas a través del tratamiento de datos personales y la libre circulación de estos.

En cuanto a la OTAN, en 2010 desarrolló un concepto estratégico en el que se incluyó el tema de la ciberdefensa, considerando a los ciberataques entre las probables amenazas a la seguridad, lo que trajo, por consiguiente, la creación de Centros de Excelencia (CoEs) con la finalidad de evitar duplicidad de funciones o gastos. Por su parte, el llamado Equipo de Reacción Rápida, creado en 2011, busca ofrecer asistencia en caso de ciberataques en menos de 24 horas pasado el incidente cibernético. Además, en 2012 se creó el Centro Principal de la Alianza Responsable de la Ciberdefensa (NCIRC, por sus siglas en inglés), el equipo de respuesta a incidentes de seguridad informática. La agencia es la responsable de proveer de capacidades para la protección de las redes de la OTAN. Aunado a lo anterior, en la Cumbre de Varsovia de 2016 la Organización reconoció al ciberespacio como un dominio estratégico en el que las naciones son capaces de defenderse, así como aire, tierra y mar (OTAN, 2024).

Asimismo, en junio de 2022, en el marco del conflicto entre Rusia y Ucrania, la OTAN adoptó un concepto estratégico que reconoce la importancia del ciberespacio como dominio propenso a amenazas que requieren ampliar el espectro de operaciones de la alianza, de modo que se fortaleció la premisa sobre la posibilidad de invocar el artículo 5° sobre defensa colectiva del Tratado de Washington frente a un ciberataque. Todo ello da cuenta de las capacidades que la alianza ha desarrollado y del alto nivel de ciberseguridad que se está fijando para los Estados que se encuentran en proceso de formación de estrategias nacionales de ciberseguridad.

Además de los esfuerzos ya mencionados, los Estados miembros desarrollan a nivel nacional estrategias de ciberseguridad que incluyen en sus capacidades a las FAS (Fuerzas armadas). Este es el caso de países aliados de la OTAN que han conformado mandos únicos de ciberdefensa a sus procesos de planeación (Espona, 2018) de la mano del Estado y la alianza. Al respecto, Francisco Javier Roca, contralmirante, segundo comandante del mando conjunto del ciberespacio, señala con respecto a España:

> Fuimos pioneros a nivel mundial en 2013 con la creación de este mando. Nuestra misión es defender la redes y sistemas del Ministerio de Defensa: redes IT y sistemas OT. Todo ello para asegurar la libertad de acción de lasFuerzas Armadas y mantener sus capacidades. En el ciberespacio, la colaboración es fundamental; solos no vamos a ningún lado y por eso colaboramos mucho con el CCN, los cuerpos y fuerzas de seguridad del estado, y el INCIBE. También tenemos convenios bilaterales muchos países,alianzas con la OTAN en la parte militar, etc. En España, dentro de la parteprivada, con Foro Nacional de Ciberseguridad. El grupo de trabajo que lideramos es el fomento de la industria de defensa en la parte de ciberseguridad. (Rodríguez, 2021, párr. 4)

Así, todos los actores están en constante capacitación para enfrentarse a nuevos escenarios de conflicto, centrándose no solo en los mecanismos técnicos, sino también en marcos regulatorios, tales como:

> La Estrategia de Ciberseguridad, el Reglamento General de Protección de Datos Personales, el Real Decreto-Ley de Seguridad de las Redes y los Sistemas de información, el Esquema Nacional de Seguridad, la normativa sobre protección de infraestructuras críticas y la normativa de seguridad

> privada. Todas ellas con un factor común: establecer un conjunto de criterios o medidas de seguridad a aplicar. (Rodríguez, 2021, párr. 8)

De este modo, podemos señalar que la OTAN, en conjunto con los Ministerios de Defensa de los países miembros, están tomando medidas para fortalecer su ciberseguridad, sumando cada vez más capacidades a las fuerzas armadas, lo cual es un ejemplo de cómo las fuerzas de seguridad nacionales están incorporándose al ciberespacio a través del desarrollode cibercapacidades, lo que da cuenta de que las perspectivas en torno a la ciberseguridad incluyen conceptos de estrategia militar (Del Río, 2021), generando así nuevos espacios de acción para la disciplina castrense.

Esta situación, similar a lo que sucede con la normatividad emergente en el Convenio de Budapest, puede ser parteaguas para que otras naciones incorporen a sus FAS en estrategias de ciberseguridad nacionales, lo que sin duda abre el debate en cuanto a las labores de inteligencia, contrainteligencia y espionaje ligado a actores vinculados con Gobiernos que se sirven de la anarquía del ciberespacio para vulnerarlo a favor de sus intereses.

En este sentido, las tecnologías de la información hacen posible la comunicación de las FAS, pero también representan un elemento necesario para:

> Apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera (…) En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico. (Del Río, 2021, p. 250)

De manera que la sinergia de fuerzas de seguridad nacionales con las TIC es esencialpara las operaciones militares, siendo estas últimas un recurso estratégico que podríadeterminar su éxito o fracaso. La OTAN y la UE son un frente consolidado en varios temas relativos a la seguridad y con el paso de los años se han fortalecido, madurando con la experiencia compartida en los ámbitos políticos, económicos, militares, ecológicos, sociales, académicos, entre otros. En 2016 firmaron un Acuerdo Técnico de Colaboración a través del equipo de capacidad de respuesta de incidentes informáticos (NCIRC) y el equipo de respuesta ante incidentes de la Unión Europea (CERT-EU) con el objetivo de intercambiarinformación y fomentar buenas prácticas en la materia. Por ello, la sinergia de los paísesmiembros de ambas organizaciones genera avances cada vez más funcionales, eficaces y organizados.

De acuerdo con un informe de 2023 realizado por el Stockholm International Peace Research Institute (SIPRI), “el gasto militar de los miembros de la OTAN alcanzó los 1341 millones de dólares” (Tian et al., 2024, p. 8), representando un 55 % del total del gasto militar mundial. Todos los miembros de la alianza atlántica —excepto Grecia, Italia y Rumania— aumentaron su gasto militar, lo que se traduce en adquisición de equipo militar, tales como aviones de combate, sistemas de defensa aérea, además de la ayuda militar a Ucrania, por lo que el aumento en el gasto militar de la OTAN permite a los países miembros desarrollar capacidades ofensivas cibernéticas, fortaleciendo y dotando a los mandos militares de

infraestructura cada vez más especializada. Sin embargo, la priorización del gasto en ciberdefensa intensifica los riesgos de su uso indiscriminado en conflictos armados, lo que trae consigo el desarrollo de nuevas vulnerabilidades y amenazas en el entorno digital.

Los esfuerzos de la OTAN y la UE se encaminan hacia la búsqueda de una respuesta rápida y eficaz para la protección del ciberespacio mediante acciones como la capacitación de personal pararesponder ante los ataques, la creación de organismos especializados en ciberseguridad y el impulso de acuerdos de cooperación entre las entidades públicas y gubernamentales, favoreciendo así la cooperación a favor de la ciberseguridad y el resguardo de sus redes informáticas, desarrollando constantemente no solo capacidades estratégicas, sino marcos legales que favorezcan su aplicación. En este sentido, el establecer principios comunes de actuación, líneas de acción y, por consiguiente, la creación de estructuras de decisión y coordinación y canales adecuados para los flujos de información necesarios para coordinar la prevención y respuesta, así como la identificación de los actores y responsabilidades en la ciberseguridad, crearán un escenario con mayor ventaja ante ataques cibernéticos.

La capacidad de adaptación que ha desarrollado la OTAN y la UE frente a los nuevos desafíos que enfrenta la comunidad internacional es, sin duda, una de las mayores fortalezas de la alianza, lo cual la perfila como líder en el desarrollo de cibercapacidades a favor de la ciberseguridad. La UE, además de ser el proyecto de integración más grande de la escena internacional, es un referente en cuanto a cooperación internacional, puesto que su presencia está en todo el mundo en diversas áreas; por su parte, la OTAN es una organización especializada en materia de seguridad y defensa, de manera que en conjunto forman una alianza que abarca varios ámbitos de acción que le dan más fuerza. Sin embargo, a pesar dela relevancia del tema de ciberseguridad en la relación, aún quedan tareas pendientes, debidoa la multiplicidad de áreas que abarca el tema, tales como las capacidades civiles, económicas, políticas, militares y tecnológicas que son determinantes en el ciberespacio, de manera que la evoluciónde la alianza OTAN-UE seguirá en el radar para analizar el estatus de la ciberseguridad en el mundo.

Métricas internacionales de políticas de ciberseguridad: ¿cuál es la posición de México en materia de ciberseguridad?

Contar con métricas que evalúen el papel de los Estados hacia la creación de políticasde ciberseguridad es relevante, ya que ofrecen un panorama general sobre las capacidades de reacción que tiene una nación ante un ciberataque, con proyecciones con referencia al costo político y social que un evento adverso en el ciberespacio podría causar. De igual forma, al evaluar diferentes rubros ofrecen a las naciones la oportunidad de centrar sus esfuerzos en aquellas áreas más débiles o vulnerables, generando así un desarrollo uniforme para que la convergencia de todos los elementos tenga una mayor efectividad en la práctica.

Derivado de lo anterior, uno de los instrumentos creados para medir en términos cuantitativos y cualitativos la importancia y el grado de compromiso que tienen los Estados con relación a la ciberseguridad es el Índice de Ciberseguridad (Global Cybersecurity Index, GCI), el

cual, basado en 5 pilares de la Agenda Global de Ciberseguridad (AGCS), mide el desarrollode las políticas de seguridad nacional:

1. **Estructuras institucionales:** se refiere a la coordinación intergubernamental, ligado a la rendición de cuentas y a la adecuada designación de responsabilidades, así como el establecimiento de políticas e instituciones sobre ciberdelito, vigilancia, alerta y respuesta ante ataques en el ciberespacio.
2. **Cooperación internacional:** destaca la necesidad de establecer un entorno de diálogoregional e internacional con base en acuerdos bilaterales y multilaterales tomando encuenta instituciones públicas y privadas.
3. **Medidas legales:** se refieren al marco legislativo en el que se identifican las actividades ilícitas ligadas al ciberespacio, así como los mecanismos de cumplimiento y procedimientos de enjuiciamiento y sanciones a dichos ilícitos, de modo que sea aplicable y compatible con la comunidad internacional.
4. **Medidas técnicas y de procedimiento:** es importante la creación de mecanismos y estrategias eficaces que puedan dar respuesta a los incidentes, tales como los equipos de respuesta a incidentes informáticos (CIRT) o los equipos de respuesta a emergencias informáticas (CERT), bajo el paraguas gubernamental o incluso a travésde la contratación de un tercero.
5. **Creación de capacidades:** estas se realizan en torno a metas y objetivos que favorezcan el máximo aprovechamiento de la red, así como contribuir a minimizar los riesgos cibernéticos y el cumplimiento de los puntos anteriores.

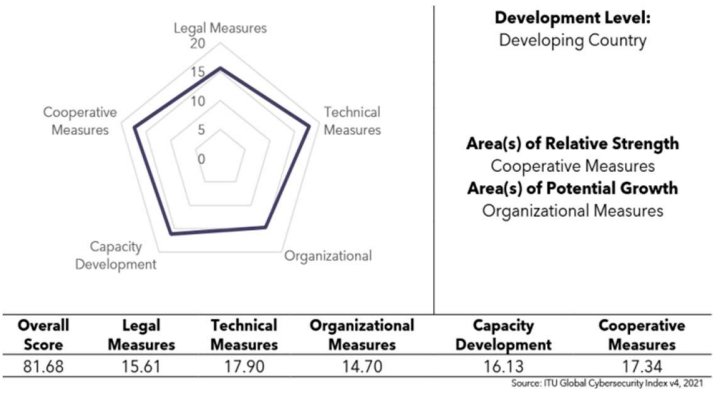
Por otro lado, dicho índice ubica globalmente a México en el sitio 52 con una puntuación de 81,68 en una tabla con 182 Estados que dieron respuesta a un cuestionario auspiciado por la institución, lo cual representa una mejora de 11 puntos respecto a 2018. Asimismo, a nivel regional México ocupa el puesto 4 por debajo de Brasil, Canadá y Estados Unidos (ITU, 2021). Dorren Bogdan-Martin, directora de la Oficina de Desarrollode Telecomunicaciones, señaló que:

> El Índice de este año muestra que muchos países emitieron nuevas legislaciones y regulaciones en torno a la ciberseguridad para reforzar áreas como privacidad, acceso no-autorizado y protección en línea. También enfatiza la necesidad de establecer estrategias y mecanismos para construirnuevas capacidades y ayudar a gobiernos y negocios a prepararse mejor para mitigar los crecientes ciber-riesgos. (Holloway, 2021, párr. 4)

Por lo tanto, este crecimiento representa para México un gran avance, en el cual cada vez se le da más peso a la ciberseguridad en el ámbito legislativo.

La figura 2 muestra la evaluación de la misma institución que muestra el perfil de México con base en los 5 pilares del GCI para obtener el puntaje general, en el cual la creación de estructuras institucionales se perfila como el área más débil con potencial de crecimiento y mejora; por su parte, la cooperación internacional es uno de los puntos más consolidados.

Figura 2. México y su evaluación según el Global Cybersecurity Index



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.68	15.61	17.90	14.70	16.13	17.34

Source: ITU Global Cybersecurity Index v4, 2021

Nota. Tomado de Unión Internacional de Telecomunicaciones (2021).

Por otro lado, el Índice Nacional de Seguridad Cibernética (National Cyber Security Index) de la e-Governance Academy es un índice global que se encarga de medir y evaluar la forma en que los países se enfrentan y previenen "amenazas cibernéticas y gestionar los incidentes cibernéticos. El NCSI también es una base de datos con materiales de evidencia disponibles públicamente y una herramienta para el desarrollo de capacidades de seguridad cibernética nacional" (Cybil, 2021, párr. 1). Para realizar su evaluación toma en cuenta 12 indicadores basados en información pública, estudiando a 160 países en función de la seguridad cibernética, la ciberseguridad como línea de base y la gestión de incidente y crisis. Los indicadores son:

1. Políticas de ciberseguridad.
2. Contribución global a la ciberseguridad.
3. Educación y desarrollo profesional.
4. Investigación y desarrollo en ciberseguridad.
5. Ciberseguridad de la infraestructura crítica.
6. Ciberseguridad de los habilitadores digitales.
7. Análisis de las amenazas cibernéticas y concientización sobre la ciberseguridad.
8. Protección de datos personales.
9. Respuesta a incidentes cibernéticos.
10. Gestión de crisis cibernéticas.
11. Lucha contra el ciberdelito.
12. Ciberdefensa militar.

Ahora bien, este índice ubica globalmente a México en la posición 42 con un promedio de 38,33 (NCSI, 2024) sobre Kiribati y por debajo de Botsuana. La diferencia metodológica con relación al GCI con el NCSI se centra en que el primero contempla 5 lineamientos de una índole que tiende a elementos cualitativos, mientras que el segundo se centra en variables más específicas también de naturaleza cualitativa, pero que dependiendo del grado de desarrollo

pueden dar valores cuantitativos como la información y análisis de amenazas cibernéticas, la protección de datos personales y operaciones cibernéticas militares. La figura 3 indica la evaluación por indicador en el caso mexicano.

Figura 3. Porcentajes de la evaluación de México según el NCSI.

Nota. Tomado de (NCSI, 2024).

De izquierda a derecha, los valores por indicador para México son: 20 %, 67 %, 60 %, 0 %, 50 %, 17 %, 25 %, 100 %, 57 %, 22 %, 38 % y 33 %. ¿Qué se puede concluir de estos valores? Dos indicadores tienen una valoración de 0 % (información y análisis de amenazas cibernéticas y protección de servicios esenciales), mientras que la protección de datos personales nos muestra un porcentaje de 100 %, lo cual podría representar la serie de proyectos realizados a favor de la protección de datos, consecuencia de la publicación de los datos del padrón electoral del Instituto Nacional Electoral (INE), que ocurrió por sexta ocasión para 2021. Esta disparidad entre indicadores da cuenta de que los esfuerzos mexicanos a favor de la ciberseguridad aún se encuentran en una etapa de desarrollo, puesto que, a pesar de la incorporación de elementos políticos, educativos, económicos e incluso militares, no se ha logrado un desarrollo uniforme en todas las áreas. Sin embargo, el hecho de que haya indicadores con 0 % no significa que haya nulos esfuerzos en la materia, sino que existe la posibilidad de que la información disponible no esté organizada de manera adecuada, que no existan instituciones que recaben esos datos o que se mantenga a resguardo por motivos de interés nacional.

Por otro lado, para ilustrar la importancia de la ciberseguridad en México cabe destacar el eco que tiene el tema de la ciberseguridad debido a las propuestas vertidas en el 2020 por legisladores mexicanos: el diputado federal de Morena, Javier Salinas Narváez, realizó una iniciativa de ley con la que busca la reforma del artículo 73 de la Constitución, en el que la ciberseguridad involucraría a instituciones de defensa y seguridad nacional; por su parte, Miguel Ángel Mancera, senador del Partido Revolucionario Democrático (PRD), presentó una iniciativa para la creación de la Ley General de Ciberseguridad; por último, la propuesta de la diputada morenista Eugenia Hernández, la cual busca la reforma de la Ley de Seguridad Nacional con la incorporación de conceptos relativos a la ciberdelincuencia en el rubro de amenazas a la seguridad nacional (Ramírez, 2021). Si bien dichas propuestas no se han materializado, podemos dar cuenta de que la ciberseguridad en México genera nuevos espacios

de discusión no solo a nivel técnico, sino también dentro de las instituciones responsables de establecer el marco legislativo en torno a la materia.

En abril de 2023 el diputado del Partido Verde Ecologista de México (PVEM), Javier López Casarín, presentó una iniciativa de ley de ciberseguridad que busca facultar a la Sedena y a la Semar en monitoreo del ciberespacio. La iniciativa ha sido señalada por poner en riesgo la privacidad de instituciones y la sociedad civil, principalmente activistas, periodistas y defensores de derechos humanos, ya que no expresa controles legislativos o judiciales que contemplen límites y responsabilidades en materia de vigilancia digital. Al centralizar las capacidades en los mandos militares y la carencia de mecanismos efectivos de coordinación y cooperación entre los distintos niveles de gobierno, la iniciativa podría derivar en problemas de operatividad y la violación de derechos humanos.

La iniciativa de ley de la senadora Alejandra Lagunes Soto Ruíz del PVEM, presentada en agosto de 2024, aborda el tema de los delitos cibernéticos, la protección a infraestructura crítica y la confianza digital. La iniciativa tiene una estructura que incluye no solo la legislación en la materia, sino también la capacitación y la participación de instituciones a favor de los derechos humanos. Sin embargo, entre sus principales debilidades se encuentra que su implementación tiene requerimientos técnicos y presupuestales, además de riesgos en la supervisión de las atribuciones a las autoridades en el tema de vigilancia digital y recopilación de datos.

En síntesis, con los datos del GCI y el NCSI y la exposición de algunos eventos en torno a la ciberseguridad en México, es evidente que si bien los esfuerzos en la materia se están desarrollando al tiempo que el tema cobra mayor fuerza en los distintos niveles de gobierno,la realidad es que el país aún está lejos de contar con una estrategia nacional de ciberseguridad que responda a las necesidades actuales.

Uno de los temas sobre la mesa es la necesidad de la firma del Convenio de Budapest, puesto que la nación tiene una invitación para adherirse desde hace diez años, sin embargo, ha existido falta de voluntad política con relación al desarrollo de procesos que hagan posible la armonización de dicho tratado con la legislación vigente. Sumado a ello, las iniciativas sobre la ley de ciberseguridad no cuentan con los elementos necesarios para enfrentarse a las amenazas que atentan contra el Estado y sus instituciones, las empresas y a la población, por lo que es uno de los temas que siguen pendientes, que concierne no solo a la clase política, sino a la sociedad en general y a la academia, generar espacios de diálogo que se sumen a los esfuerzos internacionales en favor de la ciberseguridad.

La pandemia por el coronavirus SARS-CoV-2 incrementó la brecha digital de por sí existente en el país, por lo que la acelerada inserción en la digitalidad generó nuevos debates relativos a la capacidad de resiliencia y adaptación ante los embates emergentes y constantes a los que nos enfrentamos. Por otro lado, esta característica no es propia de México, ya que, de manera general en América Latina, la cultura de la ciberseguridad a nivel local, federal y regional aún se encuentra en desarrollo, empero los avances a nivel internacional en la materia, así como la acelerada carrera cibernética, dan cuenta de que se necesita contar con

instrumentos nacionales e internacionales para enfrentar los nuevos desafíos y amenazas en el ciberespacio.

Consideraciones finales

La carrera cibernética avanza a pasos agigantados y la innovación es creciente y constante a pesar de que los Estados y las organizaciones internacionales tienen un proceso asimétrico para enfrentar los ataques a la seguridad internacional; aun así, estos esfuerzos por contrarrestar las amenazas y ataques están en constante desarrollo y evolución. La agenda de ciberseguridad comenzó a tener eco relevante en los diferentes países donde los ataques perpetrados comenzaron a diversificarse en cuanto a la frecuencia, objetivos y especialización. Así, surgió la necesidad de sumar esfuerzos de manera concreta y conjunta, por lo que la población, las instituciones públicas y privadas y los Gobiernos mismos comenzaron a demandar mayor seguridad en el ciberespacio.

La comunidad internacional está cada vez más inmersa en el mundo del Internet y porlo tanto es más dependiente de los servicios que ofrecen los gigantes tecnológicos, lo cual incrementa la vulnerabilidad de la información que se resguarda en las computadoras y plataformas gubernamentales o de la iniciativa privada. Aunado a lo anterior, las interacciones entre Gobiernos y organizaciones internacionales son cada vez más frecuentesa través de plataformas en línea a las que se suman de manera acelerada una multiplicidad denuevos actores que generan por consiguiente nuevas demandas, pero también nuevas amenazas frente a las vulnerabilidades en el espacio cibernético. Derivado de lo anterior, losciberdelincuentes pueden servirse de dichas vulnerabilidades, lo que genera una diversidad de desafíos que se abonan a la ciberseguridad.

No cabe duda de la importancia que la UE y la OTAN le han dado al tema en cuestión, pues desde hace años cuentan con capacidades técnicas, tecnológicas, jurídicas y militares en el ámbito de la ciberseguridad a nivel nacional y regional, lo que además tiene múltiples proyectos y alianzas internacionales que posicionan a esta unión como líder en la carrera cibernética. A pesar de que los países europeos han sido blanco de ataques en su ciberespacio, han logrado desarrollar resiliencia y capacidades efectivas para evitar la vulneración de sus redes, sistemas e infraestructuras. La tradición que guarda cada una de las organizaciones hace que en conjunto sea una alianza con características que se complementan y fortalecen en materia de ciberseguridad.

Para el caso de América Latina, el informe de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo (2020) señala que la región dista mucho de estar preparada ante los incidentes en el ciberespacio, puesto que, según afirma, 7 de los 32 países contaban con un plan de protección a infraestructuras críticas, en 22 países hay poca capacidad para investigar los delitos del ciberespacio y solo 12 cuentan con una Estrategia Nacional de Ciberseguridad; con relación al mismo informe pero de 2016 hubo un incremento, ya que para ese año solo 5 países contaban con dicha estrategia. En este sentido, la región cuenta con importantes desafíos, por lo que es importante generar instrumentos de

cooperación internacional para enfrentar las amenazas y retos que trajo consigo la cuarta revolución, puesto que la falta de capacidades nacionales en materia jurídica, técnica, tecnológica, económica y militar ponen en desventaja a la región, empero, una sinergia de esfuerzos colaborativos podría fortalecerla e integrarla en temas coyunturales en torno a la seguridad internacional en el siglo XXI.

Para el caso de México, es importante reconocer que los índices internacionales son alentadores, puesto que a pesar de su posición en la región, nuestro país cuenta con varios avances en materia de ciberseguridad. Así como México no se alinea con las capacidades de países que lideran la carrera cibernética, no es idóneo realizar una comparación de ese nivel, puesto que las características de la nación respecto de los miembros de la OTAN o la UE son sumamente distintas y obedecen a contextos dispares que nos ponen en una situación de desventaja. No obstante, es necesario abrir espacios de diálogo y debate en torno a la forma como las autoridades mexicanas están llevando el tema de la seguridad en el ciberespacio, debido a que una de las consecuencias que trajo la pandemia para toda la comunidad internacional, incluido por supuesto México, es que se requieren crear normas, estrategias y sinergias a favor de la ciberseguridad, puesto que no contar con estas nos pone en una situación de gran desventaja y vulnerabilidad ante los ciberataques.

Ahora bien, luego del panorama expuesto en párrafos anteriores, frente a la pregunta planteada en el objetivo de esta investigación (¿hacia la militarización de la ciberseguridad?)la respuesta es que si bien existe una amplia participación del sector militar en temas competentes a la ciberseguridad, no estamos ante una militarización ni del espacio cibernético ni de los temas relacionados con la misma, puesto que las capacidades, los tratados y los acuerdos en la materia no dan cuenta de que la comunidad internacional esté dejando exclusivamente en manos de las FAS los temas concernientes a la operatividad, mando, control y desarrollo de cibercapacidades. La injerencia de las fuerzas de seguridad nacionales y regionales para enfrentar las crecientes amenazas en el ciberespacio se complementa con la amplia y creciente participación de actores privados —como empresas de tecnología, organizaciones no gubernamentales y la academia— que se están sumando a los esfuerzos internacionales para fortalecer las acciones que buscan generar espacios de confianza y seguridad en relación con las nuevas dinámicas que trajo consigo la cada vez más frecuente necesidad de estar en línea y en constante interacción con las TIC.

En 2013 Richard Clarke afirmó: “hay dos tipos de empresas estadounidenses, aquellas que han sido hackeadas, y aquellas que no saben que han sido hackeadas” (HomelandSecurityMgmt, 2014), una sentencia que en la actualidad invita a todos los actores de la comunidad internacional a sumar esfuerzos para contemplar a la ciberseguridad como parte la seguridad nacional e internacional, puesto que, como ya se hizo mención, ningún Estado, empresa, infraestructura, organización o individuo está exento de sufrir algún incidente cibernético, lo cual, dependiendo de su origen y propósito, podría traer graves consecuencias e incluso irreparables.

La constitución de un ciberespacio seguro necesita de un enfoque colaborativo nacional e internacional que trascienda las atribuciones a las fuerzas armadas, ya que de fortalecer al

aparato militar, también se requieren marcos normativos robustos y mecanismosde cooperación interinstitucional. Una de las claves radica en la creación de capacidades deprevención, detección y respuesta frente a las amenazas cibernéticas sin caer en la militarización del ciberespacio, fortaleciendo y direccionando los esfuerzos hacia la innovación para erradicar la brecha digital, la vigilancia digital con fines políticos y económicos y la recopilación de datos desde el desconocimiento de la población usuaria delciberespacio.

Las tecnologías son cada vez más poderosas, no obstante, ante la gran cantidad de información que transita a diario en el ciberespacio y la creciente cantidad de ciberdelincuentes que se sirven de herramientas cada vez menos complejas, nos colocan en una situación de vulnerabilidad y desventajas que de no atenderse, podrían generar nuevas problemáticas de índole internacional por el alcance e impacto que tiene hoy en día la tecnología. Ante las nuevas necesidades y problemáticas que genera el desarrollo de las TIC, podemos decir que la ciberseguridad es hoy por hoy un tema en el que no solo deben trabajar los Estados, empresas u organizaciones, sino que se debe generar una cultura de seguridad en torno al uso de redes, tecnologías, plataformas en línea, entre otros; es una tarea pendiente de la que somos responsables.

Referencias

Arrollo, B. R. (2021, 12 de noviembre). ¿La geocultura de la digitalización? [Episodio de pódcast]. En *Bróker Internacional*. Spotify. https://open.spotify.com/episode/00x902J1YfhHL99ImzZqio?si=06c43ecdf9924e6b

Banco Interamericano de Desarrollo. (2016). *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?* https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Calderín, J. y Jiménez M. (2016). *Estados Unidos, Rusia o China presentan ventajas para el cibercrimen*. Observatorio Internacional de Estudios de Terrorismo. https://observatorioterrorismo.com/entrevistas/estados-unidos-rusia-o-china-presentan-ventajas-para-el-cibercrimen/

Caro Bejarano, J. M. (2012). *Ciberdefensa equipos de respuesta inmediata de la OTAN*. Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/servlet/articulo?codigo=7453877

Comisión Europea. (s. f.). *La protección de datos en la UE*. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu

Council of Europe. (2023, 19 de abril). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios*. https://rm.coe.int/cyber-buda-benefits-19april2023-es/1680aafa3f

Cybil. (2021). *National Cyber Security Index* [Índice Nacional de Seguridad Cibernética]. https://cybilportal.org/publications/national-cyber-security-index-ncsi/

Del Arenal, C. (1989). La teoría de las relaciones internacionales hoy: debates y paradigmas. *Estudios Internacionales*, *22*(86), 153-182. http://www.jstor.org/stable/41391301

Del Río Durán, J. J. (2021). La ciberseguridad en el ámbito militar. *Cuadernos de estrategia*, (149), 215-256. https://dialnet.unirioja.es/descarga/articulo/3837348.pdf

Espona, J. R. (2018). Guerra híbrida y capacidades estratégicas de la OTAN: aportaciones de Lituania, Letonia y Estonia. *Bie3: boletín IEEE*, (10), 654-665. https://dialnet.unirioja.es/servlet/articulo?codigo=6555531

European Union Agency for Cybersecurity. (2024). *Acerca de la ENISA-Agencia de la Unión Europea para la Ciberseguridad*. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_es

Ministère de l'Europe et des Affaires étrangères. (2021). *Paris call for trust and security in cyberspace* [Llamado de París para la confianza y seguridad en el ciberespacio]. https://www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace

Holloway, C. (2021). *México sube 11 lugares en el Índice Global de Ciberseguridad: Es cuarto en América*. https://www.itmastersmag.com/noticias-analisis/mexico-sube-11-lugares-en-el-indice-global-de-ciberseguridad-es-cuarto-en-america/

HomelandSecurityMgmt. (2014, 06 de febrero). *Richard Clarke at AIAA Aviation 2013: What the Cyber Security Experience Can Mean for Aviation* [Richard Clarke en AAIA Aviation 2013: ¿Qué significa la experiencia de seguridad cibernética en la aviación?] [video]. YouTube. https://www.youtube.com/watch?v=mXCzVQRcMuM

Kemp, S. (2024). *Digital 2024: Global overview report* [Digital 2024: Informe general global]. Data Reportal. https://datareportal.com/reports/digital-2024-global-overview-report

Ministerio de defensa del Reino de España. (2010). Ciberseguridad: retos y amenazas a la seguridad nacional en el ciberespacio. *Cuadernos de estrategia*, (149). https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Organización de los Estados Americanos y Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://observatoriociberseguridad.org/#/final-report

Organización del Tratado de Atlántico Norte. (2024). *Centres of Excellence* [Centros de Excelencia]. https://www.nato.int/cps/en/natohq/topics_68372.htm

National Ciber Security Index. (2024). *México*. https://ncsi.ega.ee/country/mx/

Paris Call. (s. f.). *The supporters* [Los partidarios]. https://pariscall.international/en/supporters

Ramírez, R. (2020, 21 de septiembre). Morena busca militarizar la ciberseguridad. *El Sol de México*. https://www.elsoldemexico.com.mx/mexico/politica/morena-busca-militarizar-la-ciberseguridad-delitos-internet-castigo-javier-salinas-sedena-5785013.html

Rodríguez, S. (2021). *Ciberseguridad Nacional en MTS: análisis de los principales indicadores*. https://cybersecuritynews.es/ciberseguridad-nacional-en-mts-analisis-de-los-principales-indicadores/

Tian, N., Da Silva, D. L., Liang, X. y Scarazzato, L. (2024). *Trends in world military expenditure, 2023* [Tendencias del gasto militar mundial, 2023]. https://doi.org/10.55163/BQGA2180

Unión Internacional de Telecomunicaciones. (2021). *Global Cybersecurity Index 2020* [Índice Global de Ciberseguridad]. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

US Army Cyber Command. (2022). *Army Ciber Command*. https://www.army.mil/armycyber#org-about

World Economic Forum. (2023). *Por qué necesitamos normas mundiales contra la ciberdelincuencia*. https://es.weforum.org/stories/2023/01/por-que-necesitamos-normas-mundiales-contra-la-ciberdelincuencia/#:~:text=Los%20seguros%20cibern%C3%A9ticos%20no%20splo,que%20fomente%20la%20resiliencia%20cibern%C3%A9tica.