Año 2024, Vol. 21, Nº 1, pp. 38 - 51.
DOI: https://doi.org/10.35628/resup.v16i2.125

Anotaciones sobre los desafíos de la cooperación internacional en ciberdefensa

Annotations about the challenges of the international cooperation in cyber defence

Recibido: 01 de Abril del 2024 | Aceptado: 03 de Mayo del 2024

Carmen Christina Guerra Huayllasco
https://orcid.org/0009-0002-7217-2138

Licenciada en Administración de Negocios Globales por la Universidad Ricardo Palma. Magíster en Diplomacia y Relaciones Internacionales por la Academia Diplomática del Perú. Tercera Secretaria del Servicio Diplomático de la República. Actualmente se desempeña en la Dirección de Relaciones Educativas y del Deporte de la Dirección General para Asuntos Culturales del Ministerio de Relaciones Exteriores. Es egresada del Curso de Dirección Estratégica para la Defensa y Administración de Crisis (CEDEYAC) – de la Escuela Superior de Guerra Naval
Email:cguerrah@rree.gob.pe

Resumen: Se conoce que la globalización oferta grandes oportunidades para el desarrollo de los Estados, pero trae consigo también diversos riesgos significativos que vulneran la soberanía de los países, siendo uno de ellos los ciberataques. Estos pueden afectar a la seguridad nacional trasgrediendo infraestructura crítica en los ámbitos de economía, salud, orden público e incluso política. Visto de esa manera, los ataques cibernéticos tienen la facilidad de afectar, sin ser detectados rápidamente, a los servicios públicos de un país, a sus telecomunicaciones, al transporte, a entidades financieras, entre otros, los cuales son activos críticos para toda nación. En ese sentido, la cooperación internacional en materia de ciberdefensa es cada vez más necesaria, pues permitiría que se afronte este problema, en particular, con mayor solvencia. No obstante, se presentan diversos desafíos a la cooperación en este ámbito, como las diferencias de desarrollo tecnológico de los Estados, la falta de confianza por tratarse de un tema que involucra la soberanía o la falta de legislación uniforme, especialmente en la región latinoamericana. Cabe precisar que la Marina de Guerra del Perú viene desarrollando esfuerzos para fortalecer la ciberdefensa en el Perú, junto a las demás instituciones

armadas, las cuales pueden contar también con las herramientas que ofrece la diplomacia peruana, específicamente en la cooperación internacional, logrando acercamientos con bloques de defensa, organismos internacionales, así como con otros países.

Palabras clave: Ciberdefensa, cooperación internacional, desafíos, diplomacia, ciberseguridad.

Abstract: *It is known that globalization offers great opportunities for the development of States, but it also brings with it various significant risks that violate the sovereignty of countries, being one of them cyber-attacks. These can affect national security by violating critical infrastructure in the areas of economy, health, public order and even politics. Viewed in this way, cyber-attacks can affect, without being quickly detected, a country's public services, its telecommunications, transportation, financial entities, among others, which are critical assets for every nation. In this sense, international cooperation in cyber defense is increasingly necessary, as it would allow this problem to be faced with greater solvency. However, there are various challenges for the cooperation in this area, such as the differences in technological development of the States, the lack of trust due it is an issue that involves sovereignty or the lack of uniform legislation, especially in the Latin American region. It should be noted that the Peruvian Navy has been developing efforts to strengthen cyber defence in Peru, together with the other armed forces, who can also count with the tools offered by Peruvian diplomacy, specifically in international cooperation, achieving rapprochements with defense blocs, international organizations, as well as with other countries.*

Keywords: *Cyber defense, international cooperation, challenges, diplomacy, cybersecurity.*

1. INTRODUCCIÓN

La cooperación internacional en materia de ciberdefensa resulta ser un desafío complejo, tanto a nivel global como a nivel regional. La cooperación internacional puede definirse como una acción conjunta a fin de apoyar y contribuir con el desarrollo económico y social de un país; pero también para lograr objetivos específicos como la ciberdefensa, utilizando herramientas como la transferencia de tecnologías, conocimiento, experiencias o recursos. Teniendo ello en cuenta, el desafío de la cooperación internacional en ciberdefensa se basa en los diversos

factores que constituyen un obstáculo para la sinergia de los esfuerzos realizados entre los países en este ámbito.

Uno de estos factores son las diferencias ideológicas y políticas, pues cada país posee prioridades y enfoques en materia de ciberdefensa únicos, que van acorde a sus intereses nacionales. Por lo tanto, resulta un tanto difícil establecer un acuerdo con respecto a políticas y procedimientos comunes. Otro de los factores son las discrepancias en los niveles de desarrollo de los países, lo cual puede ser medido en la cantidad de recursos y capacidades en ciberdefensa con los que cuenta, y que eventualmente podría afectar a una cooperación efectiva entre países con niveles distintos de desarrollo. Aunado a ello, los problemas de confianza pueden ser también un factor que genere un desafío para la cooperación en materia de ciberdefensa. Como se conoce, los países actúan en base a sus intereses nacionales, lo que significa que no poseen aliados sino socios estratégicos; en ese sentido, la desconfianza se puede reflejar en el no intercambio de información o en las oportunidades que se pueden perder por no trabajar con países que consideren hostiles.

No obstante, lo que queda claro para todos los países es que en esta era de la cuarta revolución industrial, con una acelerada generación de elementos como tecnologías, inteligencia artificial, el Internet de las Cosas , computación cuántica, etc., estas pueden generar una importante amenaza para los Estados, si es que llegan a utilizarse con el propósito de atentar contra la seguridad nacional. Tal es el caso de ataques cibernéticos dirigidos a servicios críticos, robo de información confidencial, manipulación de infraestructuras críticas, entre otros. Es por ello que la cooperación internacional en ciberdefensa resulta esencial para la seguridad nacional y es necesario identificar los desafíos a los que se enfrentan en esta materia, a fin de realizar los esfuerzos conducentes a mejorar la eficacia de la cooperación internacional en este ámbito.

En consecuencia, el objetivo de este artículo es realizar un breve análisis de la situación actual de la cooperación internacional en ciberdefensa a nivel mundial y a nivel regional, así como sobre los desafíos a los que se enfrentan, teniendo en cuenta el contexto geopolítico y realidades nacionales, aterrizando específicamente en la región latinoamericana. Además, busca identificar de qué

[1] Según Pérez, et al. (2019) en su publicación para el Banco Interamericano de Desarrollo (BID), el "Internet de las Cosas" es una nueva faceta del internet, en el que las conexiones y el intercambio de datos en la red se realizan con objetos o cosas físicas, permitiendo así que los datos puedan ser capturados, transmitidos y tratados de modo tal que los procesos de toma de decisiones sean más agiles y automáticos. Un ejemplo de ello son los sensores de humedad colocados en tierras de cultivo, los cuales permiten activar sistemas de irrigación si el suelo se encuentra seco excesivamente.

manera la diplomacia puede contribuir a desarrollar confianza y cooperación entre países latinoamericanos en materia de ciberdefensa, a fin de mejorar la capacidad de respuesta frente a cualquier ataque cibernético, y hallar así las oportunidades en las que la diplomacia peruana puede desarrollarse de manera conjunta con las Fuerzas Armadas del Perú, principalmente con la Marina de Guerra.

2. COOPERACIÓN INTERNACIONAL A NIVEL MUNDIAL EN MATERIA DE CIBERDEFENSA

En este siglo XXI, en el marco de la globalización, uno de los elementos más destacables que la conforman es la revolución de las comunicaciones, la misma que implica la necesidad de prestar más atención a la seguridad de las interacciones humanas en el ciberespacio. Ello, debido a que los ciberataques son una principal amenaza para los países en este mundo globalizado.

En esa línea, la tradicional seguridad ha podido adaptarse, a lo largo del tiempo, a los nuevos aspectos que rigen el sistema internacional; en este caso en particular; actualmente los Estados, los bloques regionales, así como las organizaciones internacionales se preocupan por resguardar, legislar y combatir las diversas amenazas que surgen en el ciberespacio, estableciendo así estrategias de ciberdefensa o ciberseguridad (Castro y Monteverde, 2018).

Un claro ejemplo de ello es el trabajo que viene realizando la Organización del Tratado del Atlántico Norte (OTAN), incluyendo el tema como parte de la agenda de sus cumbres, tal es el caso de la Cumbre de Riga de 2006. Cabe precisar que la OTAN creó un concepto de ciberdefensa y en base a ello ha elaborado ya una política y ha establecido, dentro de su estructura global, una estructura de gestión de la ciberdefensa. Aunado a ello, se observan cada vez más esfuerzos de la OTAN en el ámbito de la ciberdefensa, como es el caso de la Cumbre de Lisboa, en la que se diseñó una hoja de ruta en la materia (Caro,2011).

Por otro lado, como caso práctico, se aprecia que la guerra entre Rusia y Ucrania ha servido como un caldo de cultivo para la aparición de múltiples niveles de amenazas, como los continuos ciberataques que afectan a la economía y seguridad. Es por esa razón que la cooperación, con socios estratégicos en materia de ciberdefensa, se ha convertido en una necesidad para todos los Estados y que evidentemente, como cualquier otro tema que involucre soberanía, la cooperación internacional en este ámbito enfrenta diversos desafíos.

2.1 Organizaciones internacionales y convenios versados en ciberdefensa y ciberseguridad

Como expresión de la cooperación internacional en materia de ciberdefensa y ciberseguridad, los Estados han creado organizaciones internacionales, siendo algunas de ellas la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), la misma que tiene como misión velar por un alto nivel común de ciberseguridad en la Unión Europea (Agencia de la Unión Europea para la Ciberseguridad, s.f.); la Organización para la Seguridad y la Cooperación en Europa (OSCE), una de las organizaciones más grandes del mundo, conformada por 57 Estados de Europa, Asia Central y América del Norte (Organización para la Seguridad y la Cooperación en Europa, s.f.); y la ya mencionada OTAN. En el marco de esta última, por ejemplo, se implementó el Centro de Excelencia de Ciberdefensa Cooperativa, en Tallin, capital de Estonia, el cual es considerado en la actualidad un referente en ciberdefensa a nivel mundial. Además, la OTAN promulgó en el 2008 la Política de Ciberdefensa, a fin de fortalecer las capacidades de la Alianza para salvaguardar sus sistemas de información y comunicaciones y poder hacer frente a ciberataques (Castillo, 2021). De otro lado, otro de los organismos internacionales pionero en la ciberdefensa es la Organización de los Estados Americanos (OEA), cuyo Comité Interamericano contra el Terrorismo (CICTE) se encarga del desarrollo de capacidades de ciberseguridad de sus Estados miembros.

Asimismo, los Estados han suscrito diversos acuerdos de cooperación en la materia en cuestión, siendo algunos de ellos el Convenio sobre Delitos Cibernéticos del Consejo de Europa de 2001, el Acuerdo sobre Cooperación en la Lucha contra los Delitos Relacionados con la Informática de la Comunidad de Estados Independientes de 2001, el Convenio Árabe sobre la Lucha contra los Delitos Relacionados con la Tecnología de la Información de la Liga de Estados Árabes de 2010, el Convenio de la Unión Africana sobre Seguridad Cibernética y Protección de los Datos Personales de 2014 (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2019), el Convenio sobre la Ciberdelincuencia de la Convención del Cibercrimen de Budapest, cuyo objetivo es establecer herramientas legales a fin de combatir delitos cometidos en contra de sistemas o medios informáticos. Cabe mencionar que dicha convención ha sido ratificada por más de 50 naciones (Mosquera-Chere, 2021), incluyendo el Perú, Chile, Argentina, Brasil, Colombia, Costa Rica, Paraguay y República Dominicana.

2.2 Lineamientos de los principales países que otorgan cooperación en ciberdefensa

Como ya se ha mencionado en la sección anterior, los países de las diferentes regiones geopolíticas buscan cooperar con otros países de su misma región o a nivel mundial para hacer frente a las amenazas cibernéticas. La OTAN, por ejemplo, ha orientado su cooperación en el ámbito en ciberdefensa a las siguientes acciones: coordinación y asesoramiento en ciberdefensa, asistencia a las Naciones, investigación y formación, y cooperación con los socios.

Asimismo, resaltan otros grupos de discusión que son un referente en la materia a nivel internacional, perteneciendo ellos a diferentes regiones. Estos son el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN), y la Organización De Estados Americanos (OEA) (Castro y Monteverde, 2018).

Con respecto al GEG, de acuerdo a lo señalado en el Informe de la Primera Comisión de la Asamblea General – Desarme y Seguridad Internacional, se decide enfocar los esfuerzos en los siguientes temas: (a) amenazas existentes y emergentes; (b) cómo el derecho internacional se aplica al uso de las TIC; (c) normas, reglas y principios del comportamiento responsable de los Estados; (d) medidas para la construcción de confianza; y (e) construcción de capacidades (Organización de las Naciones Unidas, 2020, p.12).

Por otro lado, algunos países desarrollados han establecido diversos mecanismos que fortalecen sus legislaciones internas sobre ciberdefensa y ciberseguridad. Tal es el caso de Alemania, que ha lanzado su Estrategia de Seguridad Cibernética, ha creado su Centro Nacional de Ciberdefensa, y en el 2011 ha publicado su Plan Nacional para la Protección de Infraestructuras de Información (NPIIP). España, por su lado, en el mismo año creó un Centro y un Plan Nacional de Protección de las Infraestructuras Críticas. De igual manera, Francia en el mismo año creó una Agencia de Seguridad para las Redes e Información (ANSSI), y promulgó una Estrategia de Defensa y Seguridad de los Sistemas de Información (Vargas, et al., 2017).

Por lo tanto, todas estas acciones son un indicador de hacia dónde dirigen los países sus esfuerzos, a fin de proteger sus principales activos críticos que pueden ser afectados por ciberataques.

3. COOPERACIÓN INTERNACIONAL A NIVEL REGIONAL EN EL ÁMBITO DE LA CIBERDEFENSA

La cooperación internacional en la región latinoamericana sobre ciberdefensa se realiza principalmente en el marco de la OEA. En esa línea, la Asamblea General de la OEA, llevada a cabo en el 2004, aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, encargando a la Secretaría Técnica del CICTE (Comité Interamericano contra el Terrorismo) brindar atención a los asuntos de ciberseguridad. Con relación al programa de seguridad cibernética de la referida organización internacional, se debe resaltar que toma en consideración las particularidades de las amenazas cibernéticas de cada Estado miembro, así como sus capacidades nacionales para hacerles frente. De igual manera, promueve la participación directa tanto de los gobiernos como del sector privado y la sociedad civil en la formulación de las políticas de ciberseguridad (Castro y Monteverde, 2018).

3.1 Comparación de la legislación del Perú y sus países vecinos sobre ciberdefensa

En el presente apartado se presenta un cuadro que refleja brevemente la legislación sobre ciberdefensa y ciberseguridad, tanto del Perú como de sus países vecinos, Bolivia, Brasil, Chile, Colombia y Ecuador.

Cabe mencionar que el cuadro N°1 sólo muestra leyes, políticas y estrategias, con el objetivo de brindar una rápida identificación de qué tan preparado está el Perú en materia de ciberdefensa o ciberseguridad frente a los demás países fronterizos.

CUADRO 1
Legislación sobre ciberdefensa y ciberseguridad del Perú y sus países vecinos

Perú	• Ley N.º 30171 - Ley de Delitos Informáticos (2014) • Política Nacional de Ciberseguridad (2017) • Decreto Supremo N°012-2017-DE - Política de Seguridad y Defensa Nacional delEstado Peruano (2017) • Decreto Legislativo N°1412 - Ley de Gobierno Digital (2018) • Ley N°30999 - Ley de Ciberdefensa (2019)
Bolivia	• Ley N.º 30171 - Ley de Delitos Informáticos (2014)
Brasil	• Normativa N°3. 389/MD - Política Cibernética de Defensa (2012) • Estrategia de Seguridad de la Información y Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal (2015-2018) • Decreto N°9.637/2018 - Política Nacional de la Seguridad de la Información (2018) • Decreto Nº10.222 – Estrategia Nacional de Seguridad Cibernética (2020)
Chile	• Política Nacional de Ciberdefensa (2017) • Decreto N°164 - Política Nacional de Ciberseguridad (2023) • Plan Nacional de Ciberseguridad para el periodo 2023-2028 • Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (2024)
Colombia	• Ley 1273 de 2009 – Por medio de la cual se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” • Lineamientos de Política para Ciberseguridad y Ciberdefensa (Conpes 3701 de 2011) • Política Nacional de Seguridad Digital (Conpes 3854 de 2016) • Política de Defensa y Seguridad - PDS (2019) • Lineamientos Generales para Fortalecer la Gobernanza de la Seguridad Digital, la Identificación de Infraestructuras Críticas Cibernéticas y Servicios Esenciales, la Gestión de Riesgos y la Respuesta a Incidentes de Seguridad Digital (Decreto 338 de 2022)
Ecuador	• Acuerdo Ministerial N°006-2021 - Política Nacional de Ciberseguridad (2021) • Plan Específico de Defensa 2019-2030 • Plan Específico de Seguridad Pública y Ciudadana 2019-2030 • Política y Estrategia Nacional de Ciberseguridad (2022-2025)

Nota. Elaboración propia.

Cabe mencionar que, de la revisión de las legislaciones, hay ciertas similitudes entre estas, como el hecho de que establecen principios básicos de la ciberseguridad (protección integral, confidencialidad, integridad y disponibilidad), así como crean entes rectores responsables de coordinar políticas y medidas de ciberdefensa. Asimismo, los cinco países con sus legislaciones exigen que las empresas reporten incidentes cibernéticos a las autoridades correspondientes y obligan a los operadores de infraestructura crítica implementar medidas de ciberseguridad.

4. PRINCIPALES DESAFÍOS EN LA COOPERACIÓN INTERNACIONAL SOBRE CIBERDEFENSA

La cooperación internacional en esta materia se enfrenta a diferentes desafíos, tal como lo demuestra el análisis comparativo de las estrategias nacionales de diferentes países europeos en el campo de la ciberseguridad, realizado por Organización para la Cooperación y el Desarrollo Económicos (OCDE). Los países analizados fueron Australia, Canadá, Finlandia, Francia, Alemania, Japón, Países Bajos, España, Estados Unidos y Reino Unido. Dicho estudio reveló uno de los primeros desafíos a los que se enfrenta la cooperación internacional en esta materia: la diferencia del concepto de ciberseguridad que mantienen los países analizados. No obstante, se encontraron algunas similitudes como, por ejemplo, abordar la ciberseguridad de forma integral (UNODC, 2019).

Además, otro de los principales desafíos es que todos los Estados poseen no solo diferentes capacidades, las mismas que incluyen presupuesto, activo e infraestructura, sino también una gestión política distinta. Por lo tanto, estas diferencias ocasionan que, si bien los Estados se adaptan -de un modo u otro- a los modelos propuestos, estos esfuerzos se queden como meramente referencias, que pueden ser poco aplicables (Vargas, et al., 2017). Ello, debido a que la ciberdefensa es compleja y está en constante evolución; por lo tanto, los Estados pueden encontrarse en escenarios difíciles al momento de coordinar sus esfuerzos en ciberdefensa, dadas las diferencias en las tecnologías con las que cuentan y la legislación en la materia.

Otro desafío en la cooperación internacional en ciberdefensa se da a nivel político, es decir, los Estados pueden estar reacios a desarrollar actividades en conjunto por la falta de confianza con otros Estados, o debido a que su política exterior y de defensa están orientadas a diferentes objetivos, dificultando así la cooperación. Además, esa falta de confianza puede traducirse también en el temor de comprometer su soberanía o sus intereses nacionales.

5. CONTRIBUCIÓN DE LA DIPLOMACIA EN LA COOPERACIÓN INTERNACIONAL EN CIBERDEFENSA

Teniendo en cuenta los principales desafíos antes expuestos, esta sección busca identificar de qué manera la diplomacia puede contribuir a desarrollar confianza y cooperación en materia de ciberdefensa, en este caso en particular, entre países latinoamericanos, a fin de mejorar la capacidad de respuesta frente a cualquier ataque cibernético, y hallar así las oportunidades en las que la diplomacia peruana puede desarrollarse de manera conjunta con las Fuerzas Armadas del Perú, principalmente con la Marina de Guerra.

Cabe precisar que, según indica Vega (2023), el multilateralismo cibernético en la región de Latinoamérica resulta en un complejo entramado de mecanismos de cooperación sobrepuestos, así como enfoques que no logran una sinergia, debido principalmente a la integración política propia de esta región. En tal sentido, la diplomacia en este ámbito también posee diversos enfoques, ya que responde a la política exterior de cada Estado latinoamericano.

5.1. Esfuerzos realizados por la Marina de Guerra del Perú y la diplomacia peruana en pos de fortalecer la ciberdefensa del Perú

La Marina de Guerra del Perú (MGP) creó en el 2018 su Comandancia de Ciberdefensa (COMCIBERDEF), una comandancia operacional dedicada exclusivamente a realizar operaciones en el ciberespacio, siendo la primera de las tres Fuerzas Armadas de nuestro país en desarrollar dicho mecanismo. Cabe destacar que dicha Comandancia tiene como misión garantizar los intereses nacionales en materia de ciberdefensa, y busca ser un referente en la región (Rossi, 2021).

En esa línea, la MGP a fin de fortalecer sus capacidades, ha establecido acercamientos con diversos países, como Estados Unidos, Brasil, Colombia, México, Alemania, España y Corea del Sur, enviando a oficiales navales peruanos a cursar pasantías, estudios de especialización y maestrías desde el 2017 (Rossi, 2021), lo cual se da gracias a la cooperación internacional establecida con sus pares en los referidos países.

Por otro lado, una muestra de los esfuerzos que realiza nuestra Marina de Guerra en pos de la ciberdefensa fue su rol principal, junto a la empresa Telefónica, en el monitoreo y protección de la infraestructura de los Juegos Panamericanos Lima 2019, siendo este el primer escenario en el que se desarrolló la primera operación de ciberdefensa nacional (Rossi, 2021), mejorando así las capacidades

de ciberdefensa de nuestro país para enfrentar los ciberataques que puedan surgir en los Juegos Panamericanos Lima 2027.

Otras experiencias ganadas en este ámbito, son las Operaciones de Ciberdefensa en el proceso de las Elecciones Congresales del 2020 y las Operaciones de Ciberdefensa para el proceso de vacunación contra la COVID-19 entre 2020 y 2021; este último contó también con la participación de cibercomandos de la Fuerza Aérea del Perú (FAP) y del Ejército del Perú (EP), y de la Dirección Nacional de Inteligencia (DINI) (Rossi, 2021).

Es necesario resaltar que, junto a la Comandancia de Ciberdefensa de la Marina de Guerra, las otras dos ramas de las Fuerzas Armadas contribuyen con el fortalecimiento de la ciberdefensa del Perú y ejecutan operaciones de ciberdefensa en y mediante el ciberespacio. Estos son la Dependencia de Ciberdefensa y Telemática del Ejército y el Comando Espacial y Ciberespacial de la Fuerza Aérea del Perú (COMEC). Asimismo, el Comando Conjunto de las Fuerzas Armadas activó el Comando Operacional de Ciberdefensa (COCID), establecido en el marco de la Ley N°30999, Ley de Ciberdefensa, del 2019, el mismo que establece el marco normativo en materia de ciberdefensa en el Estado Peruano.

La diplomacia peruana, por su parte, contribuye también con el fortalecimiento de la ciberseguridad, enmarcando sus acciones en una de sus competencias que es la cooperación internacional. En ese sentido, por ejemplo, permite la articulación internacional del Perú con grandes bloques como la OTAN, pues los vínculos actuales se basan en la participación peruana en el programa de integridad, en cursos de formación, en diálogos sobre ciberdefensa y en la pertenencia al sistema de interoperabilidad (Jiménez, 2022).

Además, es preciso destacar que la cooperación cibernética en Latinoamérica se caracteriza por ser multilateral, ya que la mayor cantidad de esfuerzos que realizan los países de esta región, se desarrollan en el marco de foros internacionales preexistentes como la OEA, CELAC, MERCOSUR o Alianza del Pacífico. Asimismo, se caracteriza por desarrollarse a diferentes niveles, dado que coexisten (i) iniciativas entrelazadas a nivel panregional, es decir incluyendo a América del Norte, con (ii) pronunciamientos de la región de Latinoamérica y el Caribe, así como con (iii) programas subregionales de Sudamérica y Centroamérica (Vega, 2023).

Teniendo ello en cuenta, la diplomacia peruana puede contribuir en espacios multilaterales, gestionando oportunidades para potenciar la postura del Perú en materia de ciberdefensa, orientándose no solo a la búsqueda de buenas prácticas que se logren obtener de los países de la región, sino también ofreciendo las

capacidades que nuestro país pueda ir desarrollando, buscando así posicionar al Perú como un referente en ciberdefensa a nivel regional.

Por ejemplo, una de las actividades que se realizaron durante la Presidencia Pro-Tempore del Perú 2018-2019 de la Alianza del Pacífico, fue el "Taller de ciberseguridad en el sistema financiero y el mercado de capitales de la Alianza del Pacífico". Dicho evento, llevado a cabo en Lima, tuvo como finalidad abordar diversos temas relacionados a las ciberamenazas que afectan a los países miembros del citado mecanismo de integración regional, específicamente a sus sistemas financieros y sus mercados de capitales (Alianza del Pacífico, s.f.).

De otro lado, el Ministerio de Relaciones Exteriores del Perú, a través de su diplomacia ejercida mediante sus misiones en el exterior, resulta ser un factor fundamental para la cooperación internacional en materia de ciberdefensa, ya que nuestras misiones diplomáticas pueden contribuir a estrechar lazos con otros países -en un marco bilateral-, ello considerando que de lo señalado en párrafos precedentes, se infiere que la cooperación bilateral en ciberdefensa es aún incipiente en la región latinoamericana. Claro está que las acciones para sentar las bases de la confianza con los países de la región, así como buscar las oportunidades que permitan fortalecer las capacidades del Perú en ciberdefensa, estarían alineadas a la política exterior peruana y a los intereses nacionales.

Finalmente, la diplomacia es una herramienta útil para la cooperación bilateral en ciberdefensa, ya que mediante esta se pueden construir oportunidades para la suscripción de acuerdos bilaterales que tengan como finalidad compartir buenas prácticas, realizar ejercicios conjuntos con la Marina de Guerra -y con las demás Fuerzas Armadas- de cada país de la región, o cooperar con los países fronterizos compartiendo información importante para contraatacar a ciber ataques transfronterizos.

6. CONCLUSIONES

Hoy en día el ciberespacio se ha convertido en un escenario que agiliza la interacción de la humanidad, pero también propicia ciertas actividades que pueden llegar a vulnerar la soberanía de los Estados, afectando a sus activos críticos, generando desestabilidad con una gran rapidez y con la particularidad de que los ciberataques sean difícilmente rastreables de inmediato. En ese sentido, la ciberdefensa es un tema importante en la agenda internacional, estrechamente vinculada a la seguridad nacional y política exterior de los Estados.

Por lo tanto, dado que ese riesgo -si es que puede denominarse como ciberriesgo- no conoce los límites geográficos, la cooperación internacional en ciberdefensa

resulta de gran interés para los países, ya que puede contribuir al fortalecimiento de sus capacidades para defender su soberanía en el ciberespacio, tal como sucede en el dominio marítimo, aéreo y terrestre, reconociendo así al ciberespacio un dominio más de las operaciones militares.

No obstante, la cooperación internacional en esa materia enfrenta diversos desafíos, siendo algunos de ellos las diferencias de desarrollo tecnológico de los Estados, la falta de confianza por tratarse de un tema que involucra la soberanía o la falta de legislación uniforme, de manera particular, en la región latinoamericana.

En tal sentido, en el caso del Perú, se debería continuar con los esfuerzos que realiza la Marina de Guerra del Perú, así como las demás ramas de las Fuerzas Armadas, para fortalecer las capacidades en ciberdefensa mediante la cooperación internacional, específicamente en capacitaciones, pasantías y similares. Asimismo, estos importantes esfuerzos pueden ser reforzados con el significativo rol que desempeña la diplomacia en la cooperación internacional en materia de ciberdefensa. Así, el Perú puede estrechar su acercamiento a diferentes bloques de defensa como la OTAN, robustecer su participación en espacios multilaterales como en la Primera Comisión de las Naciones Unidas, en la OEA o en la Alianza del Pacífico, así como promover la cooperación bilateral con los países de la región, para lo cual se puede contar con las herramientas que ofrece la diplomacia peruana.

Referencias

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (s.f.). Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/about-enisa/about/es

Alianza del Pacífico. (s.f.). Consejo de Ministros de Finanzas de la Alianza del Pacífico: Taller de ciberseguridad en el sistema financiero y el mercado de capitales de la Alianza del Pacífico. https://alianzapacifico.net/consejo-de-ministros-de-finanzas-de-la-alianza-del-pacifico-taller-de-ciberseguridad-en-el-sistema-financiero-y-el-mercado-de-capitales-de-la-alianza-del-pacifico-2/

Castillo, E. (2021). Política Sectorial de Ciberdefensa: una necesidad impostergable. Centro de Estudios Estratégicos del Ejército del Perú. https://ceeep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/

Castro, H y Monteverde, A. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. Espacios, 39(39), p.31.

Caro, M. (2011). Documento informativo del IEEE 09/2011 Nuevo concepto de ciberdefensa de la OTAN. Instituto Español de Estudios Estratégicos [IEEE]. https://www.ieee.es/publicaciones-new/documentos-informativos/2011/DIEEEI09_2011ConceptoCiberdefensaOTAN.html

Jiménez, C. (2022). El acercamiento del Perú a la Organización del Tratado del Atlántico Norte como socio global. Lima. Academia Diplomática del Perú.

Mosquera-Chere, S. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. Polo del Conocimiento, 6(3),1251-1273.

Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC] (2019). Cooperación internacional en asuntos de seguridad cibernética. https://www.unodc.org/e4j/es/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

Organización de las Naciones Unidas (2019). Informe de la Primera Comisión: Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Asamblea General de las Naciones Unidas. https://undocs.org/es/A/75/394

Organización para la Seguridad y la Cooperación en Europa. (s.f.). Quiénes somos - Organización para la Seguridad y la Cooperación en Europa. https://www.osce.org/es/who-we-are

Pérez R., et al. (2019). IoT en ALC 2019: Tomando el pulso al Internet de las Cosas en América Latina y el Caribe. Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0001968

Rossi, G. (2021). La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbrida. Lima. Academia Diplomática del Perú.

Vargas, R., et al. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. Revista Latinoamericana de Estudios de Seguridad (20), 31-45, http://dx.doi.org/10.17141/urvio.20.2017.2571

Vega, J. (2023). Ciberdiplomacia en América Latina: niveles, enfoques y velocidades. Real Instituto Elcano (38), https://www.realinstitutoelcano.org/analisis/ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades/