ACADEMIA DIPLOMÁTICA DEL PERÚ JAVIER PÉREZ DE CUÉLLAR

MAESTRÍA EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TESIS PARA OBTENER EL GRADO DE MAESTRO EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TEMA DE TESIS

"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 híbridas"

PRESENTADO POR:
Giancarlo Rossi Lévano

ASESORES:

Asesor temático: Consejero Carlos Alberto Ríos Segura
Asesor metodológico: Dra. Milagros Aurora Revilla Izquierdo

Lima, 8 de noviembre de 2021

Nadie puede tener razón si es contra el Perú.

Andrés Avelino Cáceres

Resumen

Desde finales del siglo XX, el mundo se encuentra cada vez más interconectado e interdependiente debido a los avances de la Cuarta Revolución Industrial, caracterizada por la convergencia disruptiva de tecnologías digitales, físicas y biológicas. Estos avances traen consigo nuevas formas de amenazas a la seguridad y defensa de los Estados, lo cual ya se ha manifestado con guerras y ataques cibernéticos provenientes de actores estatales y no estatales que han llegado a neutralizar capacidades defensivas, digitales y económicas de los mismos.

Por ello, la ciberseguridad y la ciberdefensa son necesarios, en tanto sirven para proteger y responder ante ataques cibernéticos dirigidos hacia la infraestructura crítica, las redes y los sistemas informáticos y digitales de entidades gubernamentales, militares y del sector privado, garantizando así, dentro de sus capacidades, la seguridad y la defensa de la Nación. En ese sentido, diversos países, organizaciones y organismos internacionales han desarrollado marcos normativos, capacidades, agendas e instituciones orientadas a la ciberseguridad, la ciberdefensa y la atención a amenazas híbridas.

El Perú reconoce a las amenazas cibernéticas en su Política de Seguridad y Defensa Nacional (PSDN) y ha desarrollado un marco normativo inicial que sirve de base para orientar a la ciberseguridad y la ciberdefensa en el país. No obstante, no existe aún una entidad, estrategia o doctrina que oriente de manera integrada los esfuerzos del Estado en dichos temas, y no existen capacidades operativas avanzadas que pudiesen garantizar una situación óptima al respecto. El Ministerio de Relaciones Exteriores (MRE) tiene la responsabilidad y la oportunidad de elaborar una estrategia de política exterior orientada a fortalecer las capacidades en la materia, mediante el relacionamiento estratégico con actores internacionales que permitan la capacitación de especialistas y militares peruanos, la transferencia tecnológica y el desarrollo conjunto de tecnologías.

Palabras clave: Perú, Seguridad, Defensa, Ciberseguridad, Ciberdefensa, Ciberguerra, Amenazas híbridas

Abstract

Since the end of the 20th century, the world has become increasingly interconnected and interdependent due to the advances of the Fourth Industrial Revolution, characterized by the disruptive convergence of digital, physical and biological technologies. These advances bring with them new forms of threats to the security and defense of States, which have already manifested itself with cyber wars and attacks from state and non-state actors that have come to neutralize their defensive, digital and economic capacities.

For this reason, cybersecurity and cyber defense are necessary, as they serve to protect and respond to cyber-attacks directed at critical infrastructure, networks, and computer and digital systems of government, military and private sector entities, thus guaranteeing, within their capabilities, the security and defense of the Nation. In this sense, various countries, organizations and international bodies have developed regulatory frameworks, capacities, agendas and institutions oriented to cybersecurity, cyber defense and attention to hybrid threats.

Peru recognizes cyber threats in its National Security and Defense Policy (PSDN) and has developed an initial regulatory framework that serves as the basis to guide cybersecurity and cyber defense in the country. However, there is not yet an entity, strategy or doctrine that guides the State's efforts in such matters in an integrated manner, and there are no advanced operational capacities that could guarantee an optimal situation in this regard. The Ministry of Foreign Relations (MRE) has the responsibility and the opportunity to develop a foreign policy strategy aimed at strengthening capacities in the matter, through strategic relationships with international actors that allow training for Peruvian specialists and military personnel, technology transfer and the joint development of technologies.

Key words: Peru, Security, Defense, Cybersecurity, Cyber defense, Cyberwar, Hybrid threats

Lista de abreviaturas

ACN	Activos Críticos Nacionales
AELC	Asociación Europea de Libre Cambio
AFIN	Asociación para el Fomento de la Infraestructura Nacional
ASBANC	Asociación de Bancos del Perú
BID	Banco Interamericano de Desarrollo
C2	Comando y Control
CAL	Colegio de Abogados de Lima
CCDCOE	Centro de Excelencia de Ciberdefensa Cooperativa
CCFFAA	Comando Conjunto de las Fuerzas Armadas
CCL	Cámara de Comercio de Lima
CE2020	Cyber Europe 2020
CERT	Equipo de Respuesta ante Emergencias Informáticas
CERT-EU	Equipo de Respuesta ante Emergencia Informáticas de la Unión Europa
CI	Contrainteligencia
CIA	Agencia Central de Inteligencia
CICTE	Comité Interamericano contra el Terrorismo
CIP	Colegio de Ingenieros del Perú
CISO	Director de Seguridad de la Información
CITELE	Comando de Ciberdefensa y Telemática
CNSD	Centro Nacional de Seguridad Digital
COCID	Comando Operacional de Ciberdefensa
COIN	Consejo Nacional de Inteligencia
COMCIBERDEF	Comandancia de Ciberdefensa
CONFIEP	Confederación Nacional de Instituciones Empresariales Privadas
CSIRT	Equipo de Respuesta ante Incidencias de Seguridad Informática
CyCon	Conferencia Internacional sobre Ciberconflicto
DGM	Dirección General para Asuntos Multilaterales y Globales

DIH	Derecho Internacional Humanitario
DINI	Dirección Nacional de Inteligencia
Directiva NIS	Directiva (EU) 2016/1148 sobre seguridad de redes y sistemas de información
DIVINDAT	División de Investigación de Delitos de Alta Tecnología
DoS	Denegación de servicio
DSD	Dirección de Seguridad y Defensa
EE.UU.	Estados Unidos de América
EMA	Agencia Europea de Medicamentos
ENI	Escuela Nacional de Inteligencia
ENISA	Agencia de la Unión Europea para la Ciberseguridad
EP	Ejército del Perú
FAP	Fuerza Aérea del Perú
FBI	Oficina Federal de Investigaciones
FF.AA.	Fuerzas Armadas del Perú
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSB	Servicio Federal de Seguridad
GGE	Grupo de Expertos Gubernamentales
GROCE	Grupo de Operaciones en el Ciberespacio
GRU	Directorio Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia
Hybrid CoE	Centro Europeo de Excelencia para la lucha contra las Amenazas Híbridas
I+D	Investigación y desarrollo
IA	Inteligencia artificial
IC	Infraestructura crítica
IP	Protocolo de Internet
JCU	Unidad Cibernética Conjunta
KGB	Comité para la Seguridad del Estado
MGP	Marina de Guerra del Perú
MINDEF	Ministerio de Defensa

MINEDU	Ministerio de Educación
MININTER	Ministerio del Interior
MINJUS	Ministerio de Justicia y Derechos Humanos
MP	Ministerio Público
MRE	Ministerio de Relaciones Exteriores
NAP	Network Access Point Peru
NSA	Agencia de Seguridad Nacional de los EE.UU.
NSS	Estrategia de Seguridad Nacional
OEA	Organización de los Estados Americanos
OEWG	Grupo de Trabajo de Composición Abierta
OEWG-CTI	Grupo de Composición Abierta sobre Desarrollos en el Campo de las Tecnologías de la Información y Comunicaciones en el Contexto de la Seguridad Internacional
OLCT	Oficina de las Naciones Unidas de Lucha Contra el Terrorismo
ONU	Organización de las Naciones Unidas
OTAN	Organización del Tratado del Atlántico Norte
PCM	Presidencia del Consejo de Ministros
PCSD	Política Común de Seguridad y Defensa de la Unión Europea
Pe-CERT	Sistema de Coordinación de Emergencias en Redes Teleinformáticas
PERUCÁMARAS	Cámara Nacional de Comercio, Producción, Turismo y Servicios
PESCO	Cooperación Estructurada Permanente
PESEM	Plan Estratégico Sectorial Multianual
PJ	Poder Judicial
PNP	Policía Nacional del Perú
PSDN	Política de Seguridad y Defensa Nacional
PYMES	Pequeñas y medianas empresas
RCP	Red Científica Peruana
ROF	Reglamento de Organización y Funciones

SBS	Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones
SEGDI	Secretaría de Gobierno y Transformación Digital
SGSI	Sistema de Gestión de la Seguridad de la Información
SICOMRE	Sistema de Comunicaciones del MRE
SIDENA	Sistema de Defensa Nacional
SIGINT	Inteligencia de señales
SINA	Sistema de Inteligencia Nacional
SNI	Sociedad Nacional de Industrias
SouthCom	Comando Sur de los EE.UU.
SUNAT	Superintendencia Nacional de Aduanas y de Administración Tributaria
SVR	Servicio de Inteligencia Exterior
TIC	Tecnología de la información y las comunicaciones
UE	Unión Europea
URSS	Unión de Repúblicas Socialistas Soviéticas
USCC	Cibercomando de Estados Unidos
VANT	Vehículo Aéreo No Tripulado
VRAEM	Valle de los Ríos Apurímac, Ene y Mantaro

Índice

Índice de tablas

Introducción

Desde finales del siglo XX, el mundo se encuentra cada vez más interconectado e interdependiente debido a los avances de la Cuarta Revolución Industrial, caracterizada por la convergencia disruptiva de tecnologías digitales, físicas y biológicas que hace necesario que los Estados y la sociedad global busquen nuevos mecanismos o acuerdos internacionales para atender la gobernanza global. Estos avances propios de la Cuarta Revolución Industrial traen consigo nuevas formas de amenazas a la seguridad y defensa de los Estados, lo cual ya se ha manifestado con guerras cibernéticas entre Estados y ataques que han neutralizado capacidades defensivas, digitales y económicas de los mismos.

En este contexto, es necesario que el Perú pueda estar en la capacidad de defenderse y responder ante las amenazas en el dominio cibernético y de poder aplicar estas mismas capacidades en favor de sus intereses, en concordancia con el Objetivo Estratégico 1 del Plan Estratégico Sectorial Multianual (PESEM) del Ministerio de Relaciones Exteriores (MRE): Posicionar al Perú como potencia regional.

La Política de Seguridad y Defensa Nacional (PSDN) del Estado Peruano identifica las amenazas que podrían afectar negativamente sus intereses estratégicos o su propia existencia. Entre ellas, las amenazas que provienen del campo cibernético han cobrado mayor relevancia debido a los avances tecnológicos de la Cuarta Revolución Industrial. Asimismo, la Ley de Ciberdefensa (Ley N° 30999), establece el marco normativo en materia de ciberdefensa del Estado Peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa.

En cuanto a los actores encargados de la ciberseguridad y ciberdefensa del país, la Presidencia del Consejo de Ministros (PCM) cuenta con el Centro Nacional de Seguridad Digital (CNSD), encargada de la ciberseguridad y seguridad digital en la Administración Pública; la Policía Nacional del Perú (PNP) cuenta con la División de

Investigación de Delitos de Alta Tecnología (DIVINDAT), encargada de combatir la ciberdelincuencia; las Fuerzas Armadas (FF.AA.), bajo la dirección del Comando Operacional de Ciberdefensa (COCID) del Comando Conjunto de las Fuerzas Armadas (CCFFAA), cuentan con cibercomandos encargados de la ciberdefensa; y la Dirección Nacional de Inteligencia (DINI) se encarga de la ciberinteligencia.

Sin embargo, no existe una entidad, estrategia o doctrina que sea compartida por las entidades competentes del Estado Peruano en la materia. A la fecha, la ciberseguridad y la ciberdefensa son trabajados independientemente en áreas específicas bajo entes articuladores propios, pero sin mayores capacidades de interoperabilidad. En ese sentido, no está establecido con claridad cuál es el rol del MRE, el cual tampoco cuenta con una estrategia de política exterior que, en la actual era de la Cuarta Revolución Industrial, oriente la consolidación y la mejora continua de las capacidades en ciberseguridad, ciberdefensa y amenazas híbridas.

Asimismo, el Estado Peruano no cuenta con la infraestructura física ni digital que sustente una capacidad efectiva en ciberdefensa, ni con el personal capacitado suficiente para poder sustentar equipos de ciberdefensa de manera permanente. No obstante, el MRE pareciese ser un actor fundamental que puede lograr mayor capacitación del personal civil y militar peruano, ya que puede concretar posibles alianzas y acuerdos que permitan que entes del Estado Peruano, como el CNSD, las FF.AA. y la DINI, puedan entrenar y capacitarse junto a Estados y organizaciones líderes en el mundo en materia de ciberseguridad y ciberdefensa.

Tomando en cuenta lo anterior, la presente tesis aborda la siguiente pregunta: ¿La capacidad actual de estas instituciones puede garantizar la ciberseguridad y ciberdefensa del Perú? Como hipótesis se plantea que, a pesar de los diferentes esfuerzos de diversas instituciones del Estado, persiste el problema de la falta de un liderazgo claro en materia de ciberseguridad y ciberdefensa, lo cual conlleva a problemas en la capacidad para hacer frente a amenazas que se manifiesten en y a través del ciberespacio, incluyendo a las amenazas híbridas. Para hacer frente a los efectos que genera este problema, sobre todo referido a las capacidades, se propone

que el MRE puede desarrollar una estrategia de política exterior que acerque al Perú a actores internacionales que sean pioneros en la materia y que sean considerados aliados o con los que se compartan similares intereses de seguridad y defensa, con el objetivo de asegurar alianzas o convenios que involucren la capacitación y el entrenamiento de las entidades peruanas competentes; así como abrir posibilidades a la transferencia tecnológica o el desarrollo conjunto de nuevas tecnologías.

Siguiendo un método deductivo, analítico, cualitativo y comparado, el esquema de trabajo de la tesis se divide en tres capítulos. El primer capítulo tiene como objetivo presentar el marco teórico y conceptual de la Seguridad y Defensa en el marco de la teoría de las Relaciones Internacionales, en el que se aborda la conceptualización de los tipos de amenazas a las que se enfrentan los Estados, incluyendo aquellas existentes en el ciberespacio y las amenazas híbridas; y se presentan ejemplos en los que Estados se han visto involucrados en casos de ciberguerra o ciberataques.

El segundo capítulo presenta un análisis de la situación en la que se encuentran las organizaciones y los organismos internacionales y regionales más avanzados en materia de ciberseguridad, ciberdefensa y amenazas híbridas; y se abordan los sus avances, agendas, capacidades e instituciones encargados de dichos temas. Específicamente, se analiza a la Organización de las Naciones Unidas (ONU), la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE) y la Organización de los Estados Americanos (OEA). Asimismo, se analiza la situación de los Estados Unidos de América (EE.UU.), la Federación Rusa y la República Popular de China por ser potencias mundiales que resaltan por sus capacidades militares y cibernéticas.

Finalmente, el tercer capítulo tiene como objetivo realizar un análisis y balance de la situación actual del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas, considerando todos los elementos relevantes desde el marco jurídico existente sobre la materia, los actores principales dedicados a dichos temas, sus avances y sus vulnerabilidades. Tomando en cuenta lo desarrollado en los dos capítulos que le preceden, se concluye con una presentación de los elementos que se

deben considerar para formular una propuesta de estrategia de política exterior que apunte al fortalecimiento de las capacidades del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas.

En cuanto a la bibliografía, la presente tesis hace referencia a trabajos académicos de Seguridad Internacional; artículos y publicaciones actualizadas sobre ciberseguridad, ciberdefensa y amenazas híbridas; resoluciones, documentos de trabajo y publicaciones oficiales de los organismos internacionales abordados; noticias de actualidad sobre incidentes cibernéticos; reportes estadísticos sobre la situación de ciberseguridad del Perú; normas oficiales del Estado Peruano; e información recibida en entrevistas a especialistas y militares encargados de la ciberseguridad y la ciberdefensa en diferentes instituciones del Estado y del sector privado.

Capítulo I: Marco teórico y conceptual

La conceptualización de los asuntos de seguridad internacional y de las amenazas a las que se enfrentan los Estados ha sido una de permanente evolución, en tanto la aparición de nuevos actores, tendencias y tecnologías en el sistema internacional a lo largo de la historia ha traído consigo cambios en la forma en que se relacionan los Estados entre ellos y con otros actores. En ese sentido, para lograr una comprensión integral de las amenazas vigentes en la actualidad y de aquellas que afectan al Perú, se requiere conceptualizar a los diversos tipos de amenazas y sus implicaciones.

Para ello, se dividirá este capítulo en dos subcapítulos. El primer subcapítulo abordará los conceptos centrales en la Seguridad y Defensa, así como las amenazas convencionales y no convencionales que tradicionalmente han formado parte de la producción académica hasta ahora vigente en dicha materia. El segundo subcapítulo introducirá a las nuevas amenazas surgidas particularmente en la era de la Cuarta Revolución Industrial, en las que cobran especial relevancia las amenazas propias del ciberespacio y las amenazas híbridas, las cuales traen nuevos retos para los Estados en el campo de la Seguridad y Defensa.

1. La Seguridad y la Defensa

En la literatura acerca de la Seguridad y la Defensa en las Relaciones Internacionales, también entendida como los estudios de Seguridad Internacional, se conceptualiza a la seguridad como aquella situación que implica la ausencia de amenazas[1] para un Estado. Esta situación de seguridad puede ser absoluta, en tanto no exista ninguna amenaza; o se puede tener diferentes niveles de seguridad, en tanto un Estado se encuentra más o menos protegido de las distintas amenazas[2]. Lógicamente, se puede entender que la situación de seguridad no es únicamente aquella que implica la

[1] Robinson, P., 2008, p. 1.
[2] *Ibid*, p.1.

ausencia de amenazas, sino que también se entiende como aquellas situaciones en las que un Estado se encuentra en condiciones de enfrentarlas exitosamente.

La Defensa, por otro lado, se entiende como la herramienta que utiliza un Estado para alcanzar esta situación de seguridad. Esto implica que el Estado, a través de la Defensa, aborda directamente las diversas amenazas a las que se encuentra enfrentado, y, por lo tanto, supone la posibilidad de conflicto[3]. Así, la Defensa se aplica en cuatro grandes campos: el militar, el económico, el político y el psicosocial; y en cinco dominios: el terrestre, el marítimo, el aéreo, el espacial y el ciberespacial. La Defensa en la actualidad es, por lo tanto, multidimensional. En ese sentido, las Fuerzas Armadas no pueden ser ni son las únicas instituciones comprometidas en la defensa nacional[4].

Entonces, en tanto el objetivo de la defensa nacional es la Seguridad Nacional, a través de ella se adopta un conjunto de previsiones y acciones que tienden a fortalecer las capacidades del Estado o el Poder Nacional con el fin de evitar, eliminar o paliar vulnerabilidades para poder enfrentar con éxito amenazas y agresiones de origen interno y externo[5].

Las amenazas, por su lado, son acciones o situaciones internas y externas que atentan en contra de los intereses, la independencia, la integridad territorial o la soberanía de un Estado[6]. Por lo tanto, implican la existencia de un actor humano con la intención de ejecutar una acción perjudicial al Estado, y que además cuente con la capacidad para ello[7]. Si alguno de esos elementos no existiese, no se le puede considerar una amenaza. El análisis de una amenaza, entonces, se realiza tomando en consideración las capacidades y las intenciones del actor humano o enemigo en cuestión.

[3] Valeiano-Ferrer, G., 2013, p.26.
[4] *Ibid*, p.26.
[5] *Ibid*, p. 26.
[6] *Ibid*, p. 51.
[7] *Ibid*, p. 51.

Las capacidades son más fáciles de conocer, ya que tradicionalmente se traducen en cantidad de armamento y en capacidad destructiva, ya sea a través del mismo armamento o a través del uso de tecnologías disruptivas u otros medios que afecten las capacidades de un Estado. Por otro lado, las intenciones son menos tangibles y usualmente están sujetas a consideraciones subjetivas[8]. En respuesta a ello, los Estados consiguen información acerca de las intenciones del enemigo a través de la inteligencia estratégica, que involucra acciones de espionaje e infiltración de sistemas digitales.

En la actualidad existe una variedad de amenazas que provienen de diversos actores y con distintos efectos. Estas se suelen agrupar en dos grandes categorías: las amenazas convencionales y las amenazas no convencionales.

1.1. Amenazas convencionales

Las amenazas convencionales se entienden como aquellas acciones o comportamientos por parte de un Estado que atentan o buscan atentar contra la soberanía, la integridad o la independencia de otro Estado. Usualmente se asocia al uso del poder militar por parte de un Estado para ejercer poder sobre el otro en torno a un fin político o económico, lo cual generalmente se traduce en una guerra o conflagración armada abierta.

De hecho, el término "convencional" en el concepto de "amenazas convencionales" viene del término "armas convencionales"[9], que hace referencia a los típicos arsenales que poseen los Estados para expresar su poder militar en los tres ambientes tradicionales de tierra, mar y aire. Así, la máxima expresión del poder convencional de un Estado en la historia ha sido la capacidad de destrucción nuclear por parte de las

[8] *Ibid*, p. 52.
[9] Fatić, A., 2002, p. 93.

dos superpotencias de la Guerra Fría[10]: los Estados Unidos de América (EE.UU.) y la Unión de Repúblicas Socialistas Soviéticas (URSS).

Tomando en consideración la naturaleza esencialmente estatal de las amenazas convencionales, la forma de responder ante ellas también es estatal. Ante la posibilidad de una guerra o de conflicto con otro Estado, un Estado aplica las dos técnicas propias de la "seguridad convencional": la diplomacia y la disuasión mediante una fuerza armada superior[11] o capaz de infligir tanto daño en el otro Estado que éste prefiere no arriesgarse a un enfrentamiento armado.

Cabe resaltar dos características inherentes del concepto de amenazas convencionales. En primer lugar, una amenaza convencional no proviene únicamente del uso del poder militar por parte de un Estado contra otro, sino que también involucra la posibilidad creíble de su uso. Segundo, la expresión de esta amenaza convencional, que viene a ser el poder militar, se da en un entorno físico o geográfico específico[12], por lo tanto, es de carácter destructivo y claramente visible[13].

Un ejemplo clásico que ilustra lo anterior es la Organización del Tratado del Atlántico Norte (OTAN), actor en las Relaciones Internacionales que nació como un bloque militar para hacer frente a ciertas amenazas convencionales. Durante la Guerra Fría, la OTAN se concibió como una alianza que atendería a conflictos globales y regionales que surjan a causa de rivalidades entre Estados que, a su vez, podrían escalar y convertirse en guerras interestatales[14]. Evidentemente, la principal preocupación de la OTAN era una posible agresión militar por parte de la URSS, especialmente en Europa.

[10] *Ibid*, p. 93.
[11] *Ibid*, p, 93
[12] *Ibid*, p. 94.
[13] *Ibid*, p. 96.
[14] *Ibid*, p. 94.

Así, la amenaza convencional que significaba la URSS implicaba la atención a un espacio geográfico específico. Entonces, la respuesta ante esta amenaza requería, necesariamente, del posicionamiento estratégico de fuerzas militares en ciertos lugares, para asegurar una defensa física del territorio amenazado[15]. Esta concentración selectiva de fuerzas de combate conlleva otros esfuerzos como el logístico o el de planeamiento estratégico militar. En suma, la amenaza convencional tiene una implicación geoestratégica, en tanto lo que está en juego es un territorio, y por lo tanto, la soberanía, la integridad o la existencia misma de un Estado.

1.2. Amenazas no convencionales

Las amenazas no convencionales son aquellas que provienen de actores no estatales o las que se manifiestan en el conflicto entre Estados y fuerzas irregulares[16]. Con el proceso de globalización de fines del siglo XX e inicios del siglo XXI, la cantidad de actores en el sistema internacional incrementó exponencialmente. De igual manera, la cantidad de actores con la capacidad de afectar los intereses de los Estados también aumentó.

Así, son amenazas no convencionales el terrorismo; el narcotráfico; los grupos ideológicamente fundamentalistas y extremistas; el tráfico de armas, materiales y sustancias peligrosas o potencialmente peligrosas; el crimen organizado; el tráfico de personas; la extracción ilegal de recursos naturales; el desarrollo y transferencia ilegal de tecnologías sensibles de uso dual; la degradación de los sistemas ecológicos y del medio ambiente, entre otros[17].

Si bien no todas estas amenazas comprometen objetivamente la integridad territorial y la soberanía de los Estados como sí lo hacen las amenazas convencionales, las

[15] *Ibid*. p. 94.
[16] Valeiano-Ferrer, G., 2013, p.57.
[17] *Ibid*, p.53.

amenazas no convencionales sí afectan el normal funcionamiento de las instituciones de los Estados y el desarrollo económico y social de sus sociedades, vulnerando los derechos y la calidad de vida de las personas[18]. Esto se entiende como la inclusión del aspecto de seguridad humana a los conceptos de seguridad y sus amenazas, en tanto ahora existe una creciente preocupación por proteger al ser humano y las esferas que influyen en su vida como la política, la económica, la jurídica, la social y la medioambiental.

Un primer acercamiento de los Estados frente a las amenazas no convencionales se basa en el uso de fuerzas de seguridad interna convencionales, como las fuerzas policiales o, según el caso, guardias nacionales, para intervenir físicamente. Cuando se estima que la gravedad de la amenaza no convencional incrementa a niveles que no pueden ser controladas por las fuerzas de seguridad interna, usualmente se opta por desplegar a fuerzas militares convencionales para hacer frente a ella. Ejemplo de ello es el uso de fuerzas militares para hacer frente al crimen transnacional organizado, al narcotráfico o al terrorismo transnacional.

La respuesta estatal frente a las amenazas no convencionales puede ser muy variada y distinta a la que hace frente a las amenazas convencionales. Sin embargo, al tratarse de amenazas que no provienen de actores estatales con capacidades militares convencionales, no resulta del todo lógico emprender acciones militares de la misma índole para neutralizar al adversario, ya que usualmente las amenazas no convencionales son de carácter transfronterizo o pueden encontrarse dentro de un solo Estado. Entonces, la respuesta estatal ante una amenaza no convencional dependerá de la naturaleza misma de esta amenaza, y no siempre incluirá o requerirá acciones militares.

Entonces, las respuestas estatales ante las amenazas no convencionales se pueden enmarcar dentro del concepto de '*soft' security*. Este concepto hace referencia a la

[18] *Ibid*, p. 53.

seguridad relacionada a amenazas que no se caracterizan por ser elementos propios de las relaciones interestatales[19], es decir, que no pertenece al campo de las amenazas convencionales. Así, el '*soft' security* responde a amenazas que son primordialmente internas o transfronterizos[20]. Por ejemplo, amenazas no convencionales conocidas por su carácter transfronterizo son el terrorismo internacional, el narcotráfico, el tráfico de armas, el tráfico de personas y la degradación del medio ambiente.

Estas amenazas, evidentemente, requieren en el campo de las Relaciones Internacionales una respuesta conjunta por parte de los Estados afectados, ya que uno solo por su cuenta no podrá controlarlas. No obstante, cada una de estas amenazas se puede manifestar de manera distinta en cada Estado, y puede requerir respuestas variadas dependiendo del contexto específico, lo cual hace complicado determinar si una amenaza no convencional es esencialmente externa o interna.

Por otro lado, mientras que para las amenazas convencionales la respuesta estatal suponía una centrada en la acción militar, que consiste en la aplicación o movilización de la fuerza en un espacio geográfico y momento determinados, asegurar un estado de '*soft' security* requiere que el Estado lleve a cabo una gestión efectiva de su sociedad en el aspecto de prevención de conflictos acompañada de la realización y ejecución de políticas públicas que aborden temas que usualmente no están considerados en el concepto tradicional de seguridad[21].

Esto se debe a que las amenazas no convencionales suelen extenderse en el espacio físico y expandirse con el tiempo[22], entremezclándose con las dinámicas políticas, económicas y sociales de una sociedad, lo cual las hace totalmente diferentes a un clásico área de operaciones militar.

[19] Fatić, A., 2002, p. 95.
[20] *Ibid*, p. 95.
[21] *Ibid*, p. 95.
[22] *Ibid*, p. 96.

Mientras que el concepto tradicional de seguridad se reduce a buscar la protección del Estado de amenazas a su integridad, soberanía y existencia, el '*soft' security* amplía el concepto de seguridad para incluir los aspectos de la seguridad humana mencionados anteriormente. Esta inclusión de aspectos de seguridad humana en el '*soft' security* no pone en desmedro la importancia de las fuerzas de seguridad internas o policiales ni la de servicios especializados de seguridad y agencias de inteligencia; las cuales usualmente están mejor equipadas y preparadas para atender una variedad de amenazas internas y transfronterizas que las Fuerzas Armadas[23].

Las amenazas no convencionales, entonces, representan un conjunto de amenazas totalmente distintas a las convencionales, ya que difieren en actores, espacio geográfico, tiempo y naturaleza. Así, la respuesta de los Estados frente a los desafíos que trae consigo la lucha contra las amenazas no convencionales ha requerido de una ampliación del concepto de seguridad para que aborde elementos de la seguridad humana, lo cual hace que la seguridad nacional deje de lado la concepción tradicional de seguridad reforzada por el poder militar en favor de un concepto de seguridad multidimensional.

1.3. Amenazas híbridas

Las amenazas híbridas son aquellas que provienen de un actor estatal, un actor no estatal o la combinación de ambos; y los instrumentos de poder que se utilizan pueden ser militares, políticos, económicos, sociales, de infraestructura o informacionales, incluyendo el dominio cognitivo[24]. Así, estos actores buscan afectar con estos instrumentos de poder a aquellos pertenecientes al Estado objetivo[25].

[23] *Ibid*, p. 95.
[24] *Ibid*, p. 3.
[25] *Ibid*, p. 3.

El uso de este tipo de instrumentos de poder para afectar diferentes dimensiones del poder estatal se entiende como guerra híbrida, que viene a ser el uso sincronizado de múltiples instrumentos de poder con el objetivo de afectar vulnerabilidades específicas dentro del espectro de funciones de la sociedad para generar efectos sinérgicos perjudiciales para el afectado[26].

La agresión en la guerra híbrida es escalable en términos verticales y horizontales, y se aplica hasta que se consiga el objetivo deseado al mismo tiempo que evita o complica una respuesta decisiva del adversario. La escalada vertical de la agresión hace referencia a su intensidad al afectar a alguno de los instrumentos de poder (militar, político, económico, civil o informacional); mientras que la escalada horizontal implica una sincronización en la agresión, atacando simultáneamente estos mismos instrumentos de poder[27].

La guerra híbrida tiene el potencial de crear efectos desestabilizadores en el sistema internacional[28]. Los Estados pueden utilizar una combinación de medidas militares y no militares para desestabilizar a otros Estados, generando en ellos efectos similares a las de una guerra, posiblemente disrumpiendo infraestructura crítica (IC) o estableciendo las condiciones para que una futura agresión convencional sea más efectiva[29]. Se trata de una amenaza seria y hostil, y que representa un nuevo reto para los Estados.

Un análisis de las tendencias en el poder, la interdependencia y la tecnología actuales, permite entender que existe una variedad de razones para suponer que habrá un incremento en el uso de la guerra híbrida en el futuro. En primer lugar, el equilibrio cambiante y la difusión de poder en el sistema internacional significará que más Estados estarán más motivados a retar el *status quo*.

[26] Multinational Capability Development Campaign [MCDC], 2019, p. 3.
[27] *Ibid*, pp. 13-15.
[28] *Ibid*, p. 16.
[29] *Ibid*, p. 17.

En segundo lugar, la creciente interdependencia entre actores en el sistema internacional hará que sean cada vez más vulnerables y en una mayor cantidad de formas. En tercer lugar, el desarrollo tecnológico propio de la Cuarta Revolución Industrial traerá consigo la posibilidad de que cada vez más actores tengan los medios efectivos e inmediatos para influenciar y amenazar a otros actores.

Así, estas tendencias están convergiendo de tal modo que actores revisionistas del sistema internacional tendrán las oportunidades de beneficiarse mientras neutralizan el poder político o militar convencional de otros actores. Se trataría de un futuro en el que la competencia y el conflicto entre Estados se intensificarán mediante la guerra híbrida.

En los niveles global y regional, poderes emergentes o actores insatisfechos con el *statu quo* buscarán competir en las áreas en las que podrían conseguir una ventaja relativa. Ya que los poderes mundiales y regionales ya establecidos sustentan parte de su poder en la superioridad militar, quienes busquen retarlos emplearán, consecuentemente, técnicas de la guerra híbrida que combinen una amplia variedad de medios no militares a través de un amplio rango de actores estatales y no estatales para afectar funciones sociales del Estado adversario en diversas formas[30].

Asimismo, los actores revisionistas utilizarían la guerra híbrida no sólo como un medio para burlar el poder convencional del adversario, sino como un fin en sí mismo para subvertir y degradar reglas y normas establecidas por los poderes actuales[31]. Evidentemente, los Estados que no se encuentren en la capacidad de defenderse o de actuar en favor de sus intereses tomando en consideración los retos y oportunidades inherentes de la guerra híbrida se verán en una clara posición de desventaja frente a los que sí lo estén.

[30] *Ibid*, p. 18.
[31] *Ibid*, p. 18.

La respuesta de los Estados frente a las amenazas híbridas, una vez que estas son identificadas, variará dependiendo del actor, del contexto, de la intensidad de la amenaza, de la voluntad política y de la capacidad para neutralizar la amenaza. En ese sentido, las políticas a llevar a cabo podrán basarse en simplemente absorber los ataques, en disuadir la agresión, o en tomar medidas de represalia con el fin de disrumpir y prevenir futuros ataques. La elección de la política a seguir deberá seguir objetivos estratégicos, los cuales serían establecidos al inicio de una campaña contra la guerra o amenaza híbrida[32].

Estos objetivos estratégicos se mantendrían constantemente revisados en un ambiente estratégico dinámico. En general, los Estados persiguen tres objetivos estratégicos en sus estrategias contra amenazas o guerra híbrida:

1. Mantener la capacidad gubernamental de actuar de manera independiente, lo cual incluye garantizar el funcionamiento básico del gobierno y de la sociedad a través de medidas como la disuasión por negación de las acciones del adversario. El cumplimiento de este objetivo estratégico es una condición previa para lograr cualquier otro objetivo[33].
2. Disuadir al adversario de cometer una agresión híbrida. Esto requiere ir más allá de generar resiliencia, ya que implica imponer costos sobre el agresor mediante la disuasión por castigo o represalia. Asimismo, la capacidad de disuasión del defensor debería ser restablecida en caso de que falle.
3. Interrumpir o prevenir que el adversario realice futuras agresiones híbridas, mediante medidas que degraden la capacidad del adversario para actuar. Este es el objetivo estratégico más ambicioso, y también considerado necesario porque es improbable que un agresor híbrido cambie su comportamiento a menos que se le ataque directamente o afecte sus capacidades. Evidentemente, este objetivo también tiene un valor disuasivo en sí mismo[34].

[32] *Ibid*, p. 19.
[33] *Ibid*, p. 19.
[34] *Ibid*, p. 20.

Adicionalmente, estos objetivos estratégicos deben seguir principios generales. En primer lugar, el nivel de establecimiento de metas debe establecerse al nivel nacional y multinacional[35], ya que la respuesta estratégica ante amenazas híbridas podrá nutrirse de la experiencia o inteligencia que puedan proporcionar Estados aliados, o se podrá contar con su apoyo directo. Esto responde a que las amenazas híbridas son, por su naturaleza, transnacionales y multidimensionales.

En segundo lugar, se deberá velar por el reforzamiento del orden internacional basado en reglas, por lo que los Estados deberían evitar tomar acciones tácticas que degraden las reglas y normas que estabilicen el ambiente estratégico[36]. Evidentemente, en contraposición con este principio, los Estados que no se vean favorecidos por el sistema internacional basado en reglas serán los más propensos a realizar ataques híbridos en desmedro de este.

En tercer lugar, debe tomarse en consideración que nunca se encontrará una fórmula perfecta para contrarrestar a la guerra híbrida, ya que actores hostiles motivados seguirán buscando formas alternativas y más peligrosas de dañar a sus adversarios. Cabe resaltar que toda agresión híbrida tiene un carácter *ad hoc* o "hecho a la medida", ya que para cada ataque se utilizan los mejores medios disponibles para el objetivo específico que busca alcanzar. En ese sentido, sería muy improbable ver el uso de la misma estrategia en diferentes agresiones híbridas. De igual manera, puede entenderse que las amenazas híbridas no dejarán de existir, ya que siempre existirán actores que sean adversarios a los intereses de los Estados, incluyendo otros Estados.

En cuarto lugar, debe asumirse que el factor sorpresa es inevitable en las amenazas híbridas, por lo que, al establecer objetivos estratégicos, los Estados deben prepararse para escenarios disruptivos y para adaptarse e innovar frente a ellos y frente a adversarios que siempre buscarán estar un paso más adelante. Los ataques híbridos rara vez siguen una plantilla, así que los objetivos y las estrategias frente a ellos deben

[35] *Ibid*, p. 20.
[36] *Ibid*, p. 20.

ser constantemente revisados y actualizados[37]. No puede asumirse, entonces, que el establecimiento de objetivos estratégicos para hacer frente a las amenazas híbridas puede llegar a un estado definitivo o estático.

En suma, las estrategias que emplean los Estados frente a la guerra híbrida se diseñan e implementan basándose en tres componentes generales: la detección de la amenaza híbrida, que involucra un análisis distinto al de amenazas convencionales; la disuasión de los agresores híbridos; y la respuesta ante un ataque híbrido[38]. Estos tres elementos son similares a los que se aplican en las estrategias de defensa, aunque incluyen muchos más aspectos que los tradicionalmente militares.

La detección de amenazas híbridas, por su lado, trae consigo desafíos propios que las tradicionales actividades de inteligencia no pueden abordar. En general, las actividades de inteligencia detectan y reportan acerca de sucesos que pueden significar intenciones o acciones hostiles por parte de un tercer actor, a través de métodos basados en indicadores, en las que se identifican indicadores clave que representen la base de actividades y operaciones "normales" del adversario frente a los que no lo son. Así, se provee alertas tempranas de actividades indeseadas a analistas de inteligencia y tomadores de decisiones. [39]

Dentro de las amenazas híbridas se encuentra la ciberguerra, en tanto los Estados, a veces coludidos con actores no estatales para llevar a cabo operaciones cibernéticas con el fin de vulnerar sistemas defensivos, bancarios, gubernamentales y sociales; influenciar en la opinión pública de otro Estado; o robar propiedad intelectual y paralizar empresas e infraestructuras críticas enteras. El ciberespacio se ha convertido en un campo de batalla activo, sobre todo con los constantes avances tecnológicos de la Cuarta Revolución Industrial.

[37] *Ibid*, pp. 20-21.
[38] *Ibid*, p. 23.
[39] *Ibid*, p. 25.

2. Amenazas en la era de la Cuarta Revolución Industrial

Desde finales del siglo XX, el mundo se encuentra cada vez más interconectado e interdependiente debido a los avances de la Cuarta Revolución Industrial, caracterizada por la convergencia disruptiva de tecnologías digitales, físicas y biológicas que hace necesario que los Estados y la sociedad global busquen nuevos mecanismos o acuerdos internacionales para atender la gobernanza global. Los avances tecnológicos propios de la Cuarta Revolución Industrial traen consigo nuevas formas de amenazas a la seguridad y defensa de los Estados, en tanto se pueden ver vulneradas sus capacidades defensivas, digitales, económicas y sociales.

Ejemplos de la disrupción que trae consigo la Cuarta Revolución Industrial será el establecimiento de tecnologías 5G, y a futuro, la creación de computadoras cuánticas que incrementarán exponencialmente la velocidad de las comunicaciones y del funcionamiento de sistemas digitales e informáticos como la inteligencia artificial (IA), con nuevas posibilidades para su uso en armamento tecnológicamente avanzado, *software* malicioso inteligente, entre otros. De igual manera, a futuro los desarrollos en bioingeniería y nanotecnología permitirán conectar partes del cuerpo humano con órganos artificiales que se comunicarán entre sí, permitiendo ser monitoreados internamente o externamente por otros sistemas o dispositivos. Todos estos sistemas o dispositivos tendrán la posibilidad de ser vulnerados.

Si bien el desarrollo y uso de tecnologías disruptivas ya está considerada como una amenaza no convencional, las amenazas en el campo cíber requieren de un tratamiento especial debido a la característica intrínseca de que se manifiestan en el dominio cibernético, a diferencia del dominio físico en el que se desenvuelven las amenazas convencionales y el resto de amenazas no convencionales.

En este dominio, los Estados protegen sus intereses frente a actores estatales y no estatales, y puede llevarse a cabo múltiples formas de conflicto en ella, con posibles efectos sobre el dominio físico. Para entender cómo es que los intereses de seguridad

y defensa de los Estados pueden verse afectados en el campo cíber, es necesario abordar conceptualmente cada uno y sus implicancias.

2.1. Ciberseguridad y ciberdefensa

El internet, las redes de telecomunicaciones, las computadoras, el uso de las redes sociales, y la interacción entre personas y máquinas en el ciberespacio ha llevado a la modificación de los tradicionales conceptos de seguridad y defensa. Como se verá más adelante, esto tiene efectos en las relaciones internacionales, en tanto la ciberseguridad y la ciberdefensa han evolucionado de ser temas netamente técnicos, para convertirse en una capacidad estratégica clave de los Estados y de su conducción dentro de los diversos niveles de decisión a nivel regional e internacional[40].

En adelante se detallan las características de la ciberseguridad y la ciberdefensa, el tipo de amenazas a las que se enfrentan, el tipo de actores que las perpetran, sus efectos y la forma en que los Estados responden ante ellas.

2.1.1. Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas críticos e información sensible de ataques digitales. También se le conoce como seguridad de tecnologías de la información. En ese sentido, las medidas de ciberseguridad están diseñadas a combatir amenazas contra sistemas interconectadas y *software*[41].

En el año 2020, el costo promedio para los Estados por robo de información a nivel mundial fue de US$ 3.86 millones por cada Estado, incluyendo los costos de descubrimiento y respuesta a los ciberataques, el costo por tener los sistemas

[40] Vargas, R., Recalde, L., y Reyes, R., 2017, p. 35.
[41] International Business Machines Corporation [IBM], s/f.

desconectados y las rentas perdidas, y los costos por los daños a la reputación de las empresas o marcas a largo plazo[42].

Los cibercriminales suelen tener como blanco la información personal de los clientes o usuarios de empresas o entidades públicas, como sus nombres, direcciones de hogar y centro de trabajo, números de identificación nacional, información de tarjetas de crédito, entre otros; para luego vender esa información en mercados digitales clandestinos[43], usualmente en espacios digitales como la *Deep Web*.

Una forma de prevenir o responder asertivamente ante ciberataques implica estrategias que combinen el uso de tecnologías cuyo desarrollo y uso se encuentra en uso en el marco de la Cuarta Revolución Industrial, como la analítica avanzada, la IA y el *machine learning*[44]. Estas tecnologías se deberían aplicar transversalmente en los diversos dominios o capas de ciberseguridad, que buscan ejercer protección frente a ataques que intenten vulnerar y acceder, cambiar o destruir información; robar dinero o disrumpir las operaciones de una empresa[45] o entidad gubernamental.

El primer dominio o capa de ciberseguridad es el de la IC, entiéndase como los sistemas de computadores, redes y otros que sustentan la seguridad nacional, la salud económica o la seguridad pública[46]. Este dominio corresponde esencialmente al Estado, y tiene implicancias que se cruzan con el aspecto de la ciberdefensa, como se verá más adelante. La segunda capa es la seguridad de redes, en la que se busca proteger a una red de computador de intrusos, ya sea a través de conexiones físicas o inalámbricas, entre ellas, la conexión Wi-Fi[47].

[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*
[45] *Ibid.*
[46] *Ibid.*
[47] *Ibid.*

Una tercera capa es la de la seguridad de aplicaciones o *software*, que incluye la protección de la data que contiene, la forma es que es gestionada, la seguridad de acceso, entre otros aspectos. La cuarta capa es la seguridad en la nube, que incluye la encriptación de la data en la nube y que garantice la privacidad de la información de los usuarios. La quinta capa es la seguridad de la información, que implica medidas de protección de data, reguladas por la legislación correspondiente de cada país, que garantiza que ésta no sea accedida sin autorización, expuesta o robada[48].

Otro aspecto importante en la ciberseguridad es la educación y capacitación sobre el tema[49]. Es necesario que se concientice acerca de las amenazas cibernéticas a las que se enfrentan empresas y entidades gubernamentales, especialmente si manejan información sensible o si utilizan sistemas de comunicación que son esenciales para la seguridad nacional.

También se debe considerar la creación de planes ante posibles ataques y disrupciones de redes a causa de ataques cibernéticos u otras causas como desastres naturales o fallas en los sistemas energéticos[50], para que las operaciones de la entidad no se vean paralizadas y que la empresa, el Estado o los usuarios y ciudadanos no se vean afectados. Esto es de suma importancia para aquellas entidades esenciales para el funcionamiento del Estado y su seguridad, como aeropuertos, edificios gubernamentales y bases militares; así como aquellas que otorgan servicios básicos a la población como hospitales y centros energéticos.

Un problema es que algunos gobiernos y empresas deciden no reconocer el haber sido víctimas de ciberataques por diversos motivos, lo cual ocasiona que esta información no sea compartida y que otras entidades no se puedan preparar, lo ocasiona que sigan siendo vulnerables a ataques. Asimismo, entidades gubernamentales y empresas suelen resistirse a invertir en una ciberseguridad completa y efectiva, bajo la falsa idea

[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*

de que es más rentable pagar por los efectos de un ataque que prevenirlo en primer lugar[51].

La ciberseguridad es un aspecto cada vez más importante para el correcto funcionamiento de las empresas, los gobiernos y las sociedades en general. Sin embargo, junto a los avances tecnológicos de la Cuarta Revolución Industrial se incrementa el número y la forma de amenazas en el ciberespacio. Una de esas amenazas es la que provienen de otros Estados, o de Estados coludidos con actores no estatales para vulnerar alguna capacidad de un tercer Estado. Al tratarse de intereses y capacidades estatales en juego, el concepto de ciberseguridad evoluciona al concepto de ciberdefensa.

Por ello, es importante la cooperación y la coordinación entre los actores estatales y las entidades del sector privado para poder lograr óptimos niveles de ciberseguridad, sobre todo considerando el desarrollo de nuevas tecnologías que tendrán efectos disruptivos en la sociedad. La ciberseguridad resulta ser un aspecto transversal a la seguridad en todas las dimensiones de la vida humana, y será imposible asegurarla sin la acción coordinada entre Estados, y entre ellos con el sector privado.

Por otro lado, en el aspecto operativo, las entidades encargadas de responder ante las amenazas en el ciberespacio son los Equipos de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT, por sus siglas en inglés), también conocidos como Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), que cada Estado puede poseer. Estos equipos de especialistas informáticos, que pueden variar en su denominación o nombre, están encargados del desarrollo de medidas de prevención y respuesta ante incidencias cibernéticas en los sistemas de información de sus respectivos países. Cabe resaltar que hay países que poseen una gran cantidad de CSIRTs, como España y Alemania, que poseen 59 y 47 equipos, respectivamente[52;]

[51] Flournoy, M. y Sulmeyer, P., 2018, p.44.
[52] Agencia de la Unión Europea para la Ciberseguridad [ENISA], 2021b.

frente a países que poseen solo uno o ninguno, como es el caso de la gran mayoría en el mundo.

2.1.2. Ciberdefensa

Desde el inicio de su existencia, el ciberespacio ha sido reconocido como una nueva arena de competencia entre los Estados[53]: el quinto dominio de la guerra, luego de los dominios de la tierra, del mar, del aire y del espacio exterior. Además, en este dominio están en juego cuestiones políticas y geopolíticas de interés de los Estados[54], incluyendo una intensa competencia económica y guerras informacionales[55].

En ese sentido, los Estados están desarrollando con creciente interés capacidades defensivas y ofensivas cibernéticas que les permitan defender y perseguir sus intereses en este dominio. El uso de estas capacidades defensivas y ofensivas cibernéticas es lo que se denomina ciberguerra, que en esencia se entiende como el conflicto en el ciberespacio. La ciberdefensa, por otro lado, es el concepto que corresponde al conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas que tienen como fin asegurar el uso propio del ciberespacio y negárselo al enemigo[56].

Entonces, la ciberdefensa se puede entender como la capacidad el Estado para cumplir con aquellas responsabilidades que le permiten prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte sus capacidades e intereses[57]. Dentro del dominio cíber existen activos críticos para los Estados, como masivas cantidades de información sensible y de sistemas de comunicación digital de uso civil, gubernamental y militar.

[53] Flournoy, M. y Sulmeyer, P., 2018, p.40.
[54] Riordan, S., 2019.
[55] Flournoy, M. y Sulmeyer, P., 2018, p.46.
[56] Cárdenas, W., 2015, p. 1.
[57] *Ibid.*, p. 1.

Asimismo, el ciberespacio es hoy en día la base del comercio mundial y de la comunicación[58]. Por eso, una disrupción en estos sistemas a través de un ataque digital masivo podría vulnerar y neutralizar la IC de un país sin que se dispare ni una sola bala[59], y las consecuencias serían catastróficas, desde ciudades enteras sin energía o la pérdida total de bases de datos esenciales para un país, hasta toda la capacidad defensiva de un Estado neutralizado, dejándolo indefenso contra cualquier ataque convencional posterior.

Entonces, se puede entender que la soberanía de los Estados está presente en el ciberespacio, y esto trae consigo una mayor responsabilidad por parte de estos para proteger a sus comunidades, empresas y gobiernos de amenazas digitales[60].

Las ciber-operaciones son negables y escalables, y sirven tanto para tiempos de guerra y paz[61]. En la actualidad, docenas de Fuerzas Armadas han establecido o están estableciendo ciber-comandos y están incorporando a las ciber-operaciones dentro de sus doctrinas oficiales[62]. De hecho, cada vez más hay Estados que están "armando" al Internet o utilizándolo como arma, como se ejemplificará más adelante. No obstante, por la naturaleza encubierta de estas operaciones, muy pocas de ellas han sido registradas[63], lo cual dificulta a su vez la posibilidad de determinar a los responsables detrás de un ataque cibernético.

Evidentemente, los Estados también llevan a cabo ciber-operaciones en apoyo a sus fuerzas militares convencionales. Esta es una preocupación cada vez más creciente para países con Fuerzas Armadas tecnológicamente avanzadas, ya que una mayor digitalización de sus arsenales y sistemas defensivos trae consigo un mayor riesgo de que estos puedan ser vulnerados. Por ejemplo, las Fuerzas Armadas de EE.UU. son

[58] Flournoy, M. y Sulmeyer, P., 2018. p 40.
[59] *Ibid*, p. 40.
[60] *Ibid*, p. 40.
[61] *Ibid*, p. 40.
[62] *Ibid*, p. 42.
[63] *Ibid*, p. 40.

tan dependientes del ciberespacio que un ataque en su Comando y Control (C2), sus cadenas de suministros o sus redes de comunicaciones podría afectar su habilidad de proyectar poder en ultramar dejando a sus fuerzas desconectadas y vulnerables[64].

En tanto cada vez más se modernicen las Fuerzas Armadas en el mundo, cada vez más cobrará mayor importancia la ciberdefensa en el aspecto convencional de la defensa. Este crecimiento en relevancia será exponencial, ya que el desarrollo de una tecnología militar trae consigo el desarrollo posterior de una tecnología que lo neutralice, y así sucesivamente.

Por ejemplo, en la reciente guerra del Alto Karabaj entre Armenia y Azerbaiyán (2020), fue evidente la superioridad táctica y tecnológica de los Vehículos Aéreos No Tripulados (VANT) o drones sobre los tanques convencionales en tierra. Ahora se están desarrollando tecnologías que neutralicen los VANT de manera digital o a través de pulsos electromagnéticos, los cuales en un futuro podrían ser equipados en vehículos terrestres.

Por otro lado, la ciberguerra también representa una amenaza híbrida, en tanto los agresores son Estados, actores no estatales o una combinación de ambos. Asimismo, las operaciones cibernéticas que apuntan a afectar a un tercer Estado tienen como objetivo, además de vulnerar sus capacidades defensivas convencionales, vulnerar y disrumpir sus sistemas políticos, económicos, sociales, de infraestructura, informacionales y cognitivos. Estas son características propias de la guerra híbrida o de las amenazas híbridas, explicadas anteriormente.

La población civil será probablemente la que sufra mayor daño colateral cuando haya ataques cibernéticos a sus gobiernos. Por ejemplo, un ciberataque que introduzca un *malware* a una red eléctrica estadounidense para dejar sin energía eléctrica a alguna de sus bases militares podría extenderse más allá de los objetivos tácticos del ataque y

[64] *Ibid*, p. 42.

afectar a la población civil circundante, teniendo como efecto que se vean afectados hospitales, sistemas de calefacción o cadenas básicas de suministros de bienes esenciales.

De hecho, un caso similar ocurrió en el 2017, en el que un *malware* fue introducido a través de un *software* de preparación de impuestos de Ucrania, presumiblemente por Rusia, con el fin de vulnerar empresas ucranianas. Este ciberataque terminó afectando también a otras empresas occidentales. Una de ellas, el conglomerado naviero danés Maersk, reportó que el ataque le costó entre US$ 200 y US$ 300 millones[65].

Un aspecto de la ciberdefensa que aún no ha sido regulado es la responsabilidad de los Estados en el uso del ciberespacio como dominio de la guerra. Así como existe el Derecho Internacional Humanitario (DIH) para la guerra actual en todas sus formas físicas, se debate si el ciberespacio también debería ser regulado en el mismo sentido, o si las normas y principios del DIH deberían extender su alcance al campo del ciberespacio.

Estas posturas se sustentan en el hecho de que la ciberguerra involucra un enfrentamiento entre Estados con posibles efectos colaterales sobre la población civil, como la guerra convencional. No obstante, a pesar de que el DIH prohíbe que los civiles sean blancos militares en el campo de batalla, algunos Estados ya lo hacen en el ciberespacio. Ejemplo de ello fue un ciberataque masivo de nacionalistas rusos hacia Estonia que dejó desconectada a la población de ese país en el 2007, o un ataque perpetrado por Corea del Norte hacia bancos surcoreanos y sus clientes en el 2013[66].

Si bien hasta la fecha no se ha producido evidencia de que alguien haya resultado muerto como causa directa de un ciberataque, es posible que esto cambie a medida que, en el marco de la Cuarta Revolución Industrial, cada vez más aspectos de la vida cotidiana de las personas se tornen digital e interconectado.

---

[65] *Ibid*, p. 43.
[66] Flournoy, M. y Sulmeyer, P., 2018, p. 43.

Por ejemplo, los vehículos particulares se encuentran cada vez más conectados a redes WiFi y Bluetooth, y el Internet de las Cosas penetra cada vez más en los espacios privados de los hogares. En el futuro, ya se estará hablando del "Internet de las Personas", en tanto será posible que el organismo humano reciba implantes digitalmente interconectados. Cada uno de estos dispositivos son, o serán, objetivos potenciales para los ataques cibernéticos[67], y sus efectos, cada vez más devastadores.

Ante esta preocupación, algunos Estados han empezado a desarrollar tecnologías de redes de información separadas del actual Internet. No obstante, ya se ha demostrado que es posible "saltar" de una red digital a otra mediante resonancia acústica o frecuencias de radio, por lo que ni siquiera un desarrollo tecnológico de ese tipo lo hace invulnerable a ataques externos[68].

2.2. Infraestructura crítica

La infraestructura crítica (IC) de un Estado, también conocida como activos críticos nacionales (ACN), puede ser objetivo de un ataque cibernético por el inmenso valor que representa. La protección de estos resulta crucial debido a que la IC sustenta las capacidades nacionales de un Estado, los cuales a su vez otorgan a su población de los servicios y recursos necesarios para su subsistencia. Debido a sus efectos, la afectación a la IC de un país sería de igual modo una afectación a su soberanía e independencia, a su estabilidad política, económica y social, y a sus intereses; con posibles efectos catastróficos para la población civil, en tanto tendría efectos que debiliten la seguridad, la economía nacional, la salud pública, o una combinación de estos[69].

Ejemplos de IC son aeropuertos y puertos, por su importancia para la economía, el traslado de personas, bienes y materiales, incluyendo su posible uso militar; centros de

[67] *Ibid*, p. 43.
[68] *Ibid*, p. 43.
[69] Cybersecurity & Infrastructure Security Agency [CISA], s/f.

energía como centrales hidroeléctricas o redes eléctricas, que suministran de energía eléctrica a ciudades, bases militares, empresas y entidades gubernamentales; rutas estratégicas como puentes, túneles y carreteras que no tienen reemplazo, las cuales son necesarias para la movilización de personas, bienes, materiales y tropas; centros de servidores, sobre todo las que contienen información, bases de datos y sistemas de entidades gubernamentales, de las Fuerzas Armadas, de los servicios de inteligencia, de bancos, entre otros.

También se considera IC a instalaciones y sistemas que abastecen centros industriales y comerciales; fábricas que tienen un potencial uso estratégico; la industria militar; los servicios de emergencia; los sistemas financieros; las cadenas de logística del sector de alimentos y agricultura; los hospitales y otros centros de salud; los reactores nucleares e instalaciones de materiales químicos, biológicos y radiológicos; represas y sistemas de desagüe y salubridad; entre otros[70]. Su destrucción o afectación tendría claros efectos sobre las capacidades nacionales de un Estado, ya sea neutralizando sus capacidades defensivas tradicionales o militares, o generando dentro de él situación de inestabilidad social.

El ataque a la IC de un Estado puede ser de tres tipos: de naturaleza física, de naturaleza cibernética o de naturaleza cibernética que dependa de la infiltración física de un agente externo. Claro está, no toda la IC tiene elementos cibernéticos o digitales, por lo que aquella IC que sea netamente física solo se vería amenazada por el tipo de ataque físico. El primer tipo de ataque, de naturaleza física, requiere de la destrucción parcial o total o el bloqueo en el funcionamiento de las instalaciones, sistemas cruciales o fuentes de abastecimiento de la IC. Este ataque se logra mediante la infiltración de agentes externos o el uso de operadores internos que lleven a cabo acciones de sabotaje que neutralicen efectivamente una IC.

[70] *Idem*.

Debido a su naturaleza, la respuesta estatal ante este tipo de ataque es también de naturaleza física, ya que la protección del IC para estos casos requerirá de seguridad interna y externa, ya sea proveniente de una entidad privada o estatal, instalaciones difíciles de penetrar y capacidades en inteligencia que permitan detectar estas infiltraciones antes de tiempo. En este caso, el rol de la ciberdefensa sería la de apoyar a las actividades de inteligencia para detectar posibles infiltraciones o intenciones de infiltración por parte de agentes externos.

El segundo tipo de ataque a la IC es aquel de naturaleza netamente cibernética. Con el creciente uso de tecnologías digitales para administrar sistemas de la IC de un país, crecen también las posibilidades de que sean vulneradas por un atacante que no requiere llevar a cabo una acción física destructiva sobre ella. Debido al inmenso daño que podría suponer la neutralización de una IC en un país, sus capacidades de defensa cibernética deben estar a la altura de poder proteger a la IC.

La protección cibernética puede provenir tanto de una entidad privada, como la misma empresa que administra esa IC, o del Estado. Evidentemente, el hecho que lo gestione una entidad privada trae consigo riesgos en sí mismo, como la posibilidad de que esta entidad afloje sus capacidades de ciberseguridad en favor de un actor externo. Lo más favorable en estos casos es que un Estado sea autosuficiente en sus capacidades de ciberseguridad para la IC, aunque esto sigue siendo una meta lejana para varios países. Peor aún, a veces ni se toma en cuenta la importancia de proteger cibernéticamente una IC en un país.

El tercer tipo de ataque combina el aspecto físico y el aspecto cibernético anteriormente descritos. Este ataque consistiría en la infiltración física de algún agente externo o del control sobre algún operador interno en la IC para que inserte algún tipo de *software* en los sistemas cibernéticos que la componen. Una vez insertado el *software* malicioso, agentes cibernéticos del agresor podrán vulnerar los sistemas cibernéticos de la IC a distancia y causar el daño deseado. La protección ante este tipo

de ataques combina las formas de respuestas y prevención descritas para los tipos de ataque netamente físico y netamente cibernético.

De los tres tipos posibles de ataque a una IC, la más común en la actualidad y para el futuro vendría a ser la de naturaleza netamente cibernética, seguida por la que combina elementos físicos y cibernéticos. Esto se debe a que el uso de tecnologías disruptivas con la intención de vulnerar las capacidades de otro Estado está en crecimiento. Asimismo, el ataque físico a una IC se daría usualmente en casos de guerra, ya sea interestatal o asimétrica. No obstante, como se detallará en los casos de ciberguerra y ciberataque más adelante, los Estados no siempre atacan la IC de otros Estados únicamente en caso de guerra; lo hacen también en tiempos de paz.

Un riesgo en la protección de IC es la posible falta de voluntad de entidades privadas de proteger efectivamente la IC que gestionan. Guiados por la lógica de la rentabilidad económica, las empresas pueden evitar invertir en sistemas de seguridad física o digital si no va acorde a sus propios objetivos. A menos de que esté estipulado objetivamente en un contrato o acuerdo entre la empresa y el Estado o que sea obligatorio por ley, la empresa no tendría por qué aceptar el incremento de sus medidas de seguridad si el Estado se lo pidiese. Asimismo, si el Estado ofreciera ser quien invierta en seguridad física y cibernética para la IC que gestiona la empresa, la empresa podría no estar obligada a hacerlo.

Existe un escenario peor al descrito en el párrafo anterior. Puede haber empresas que gestionen IC y que sean de la nacionalidad de un Estado rival o cuyos puestos directivos pertenezcan a personas vinculados a actores estatales o no estatales que podrían suponer una amenaza para el Estado en el que se encuentra la IC. En estos casos, es labor de la inteligencia estratégica del Estado conocer los vínculos, y si es posible, las lealtades e intenciones de estas personas. El riesgo que suponen estas personas o empresas se sustenta en el hecho de que, en caso de conflicto, podrían recibir instrucciones de actores rivales para detener el funcionamiento de la IC o

reducir su efectividad, generando evidentes efectos adversos en el Estado en el que se encuentra.

De todos modos, un Estado debe proteger su IC de manera física y digital. En materia de protección física, las fuerzas de seguridad interna deberían mantener localizadas y protegidas permanentemente las instalaciones de una IC, dependiendo de su valor. La protección es progresiva, en tanto aumenta cuando haya reportes de inteligencia que indiquen la presencia de una amenaza física y activa a determinada IC

En caso de que la IC se encuentre ubicada en una zona que haya caído en una condición de desestabilización social, ya sean en el marco de protestas, saqueos o enfrentamientos entre civiles o grupos armados, el nivel de protección física debe incrementar considerablemente, incluyendo el posible uso de las Fuerzas Armadas para ello.

Las Fuerzas Armadas también serían desplegadas para defender la IC de un Estado cuando se encuentre en guerra, ya sea convencional o asimétrica. Dependiendo de la naturaleza de la amenaza y de la propia IC, la defensa de ella se compondría de elementos de tierra que puedan frenar o neutralizar cualquier intento de incursión terrestre destinado a atacar la IC; de elementos de defensa anti aérea, si es que la IC pudiese ser objeto de bombardeo o asalto aéreo; y de elementos de defensa marina, en caso de que la IC se encuentre en una zona costera o en ríos y mares, para evitar el ataque por parte de fuerzas marinas adversarias.

Entonces, la defensa convencional de una IC debe combinar los elementos terrestres, antiaéreos y marinos dependiendo a la naturaleza de la IC y de la amenaza bajo la que se encuentre. Sumado a este tipo de defensa física, es necesario que un Estado lo defienda de manera cibernética y digital en caso de que la IC tenga componentes de esta naturaleza. La protección en esta materia incluye todos los elementos de ciberseguridad, ciberdefensa y atención a amenazas híbridas descritas en la primera parte de este capítulo.

Cabe resaltar que mientras la defensa física de una IC es progresiva, en tanto se incrementan los elementos de seguridad y defensa de acuerdo a las amenazas detectadas para ella, la defensa cibernética es permanente y se debe mantener al máximo nivel posible, tanto en tiempos de guerra como de paz. De hecho, es difícil hacer una clara distinción de "tiempos de guerra" y "tiempos de paz" en el campo cíber, como se describió en el apartado de ciberdefensa. Por esta razón, debe suponerse que una IC está bajo la amenaza constante de poder ser atacada y vulnerada por medios cibernéticos y digitales.

En estos casos, el ciberataque no necesariamente buscaría la neutralización del funcionamiento de la IC, sino que podría tener como objetivo el robo de información protegida o confidencial, o simplemente tener conocimiento del funcionamiento de sistemas digitales militares, de inteligencia, de operación de una IC, entre otros. La protección de la IC en estos casos igual debe seguir los principios de ciberseguridad y ciberdefensa, ya que la adquisición por parte de un adversario de este tipo de información e inteligencia sensible le otorgaría una ventaja estratégica sobre el Estado vulnerado. Asimismo, esta información e inteligencia podría ser usada en contra del Estado vulnerado en caso de conflicto abierto o de guerra.

Por esta razón, también es importante en la labor de protección de IC la actividad de la contrainteligencia, que consiste en proveer intencionalmente de información falsa o engañosa al actor que lleve a cabo una infiltración de los sistemas de datos o de comunicaciones de la IC. De este modo, el atacante no obtendría ninguna ventaja estratégica al robar u obtener información de la IC. En todo caso, sería el propio Estado vulnerado el que adquiriría una ventaja estratégica sobre el atacante, ya que le habría suministrado información falsa o engañosa que podría llevar a que el atacante tome decisiones estratégicamente erróneas en base a ella.

La ciberseguridad y la ciberdefensa, entonces, son de suma importancia para la protección de la IC de los Estados. Con el creciente desarrollo y uso de tecnologías

disruptivas en la era actual Cuarta Revolución Industrial, la importancia de la ciberseguridad y ciberdefensa será aún mayor, considerando además que ya ha habido numerosos casos de ciberataques y de ciberguerra que involucraron o que afectaron Estados, su IC y sus capacidades nacionales.

2.3. Casos de ciberataques y de ciberguerra que involucren a Estados

Potencias mundiales como los Estados Unidos de América (EE.UU.), la Federación Rusa y la República Popular de China; y otros países como Corea del Norte e Irán han demostrado tener altos niveles de capacidad para ejercer operaciones cibernéticas en favor de sus intereses. De las operaciones conocidas, algunas resaltan por su impacto político, estratégico y mediático.

2.3.1. Casos de ciberguerra en apoyo a operaciones militares

EE.UU. ha realizado varias operaciones cibernéticas en apoyo a operaciones militares. Una de estas se llevó a cabo durante la campaña de bombardeos de la ex Yugoslavia por parte de la OTAN en 1999. Este ataque, perpetrado por una unidad cibernética del Pentágono, vulneró y obtuvo acceso a los sistemas de defensa antiaéreos de Serbia, configurándolos para que parezca que los aviones estadounidenses se aproximaban desde una dirección distinta a la real[71]. Esto permitió realizar bombardeos sin que los aviones de ataque fuesen detectados a tiempo suficiente como para que las defensas serbias se activen cuando era realmente necesario: antes del bombardeo.

Asimismo, autoridades estadounidenses han confirmado que el Pentágono ha realizado ciberataques en la actual lucha contra el Estado Islámico en Irak y Siria, obligando a los militantes yihadistas a abandonar sus posiciones[72], generando desorden y,

[71] *Ibid*, p. 42.
[72] *Ibid*, p. 42.

eventualmente, revelando sus posiciones a ataques por parte de las fuerzas de la coalición militar liderada por EE.UU.

Rusia también ha llevado a cabo ciber-operaciones en apoyo a operaciones militares convencionales. Durante la invasión rusa de Georgia en el 2008, Rusia empleó ataques de denegación de servicio (DoS, por sus siglas en inglés) para silenciar los medios televisivos georgianos momentos antes de incursiones blindadas con el objetivo de incrementar los niveles de pánico en la población[73]. Asimismo, Rusia estuvo detrás de la vulneración de la red eléctrica de Ucrania en el 2015 durante la actual Guerra del Donbás, dejando sin electricidad a cerca de 225,000 personas[74].

2.3.2. Casos de ciberataques en apoyo a otros objetivos

Una operación cibernética emblemática fue la del intento de influencia encubierta por parte de Rusia en las elecciones presidenciales de EE.UU. en el 2016. Esta operación consistió en la vulneración de cuentas de correo electrónico pertenecientes al Comité Demócrata Nacional y de uno de los asesores personales de la ex Secretaria de Estado y candidata presidencial Hillary Clinton, con el fin de recolectar inteligencia y de encontrar información que pudiese dañar su imagen[75]. Los *hackers* rusos compartieron esta información con WikiLeaks, portal en el que se publicaron los correos electrónicos.

Así, la candidata demócrata fue objeto de una cobertura negativa por parte de los medios de comunicación hasta el mismo día de las elecciones. Asimismo, empresas rusas vinculadas al Estado ruso realizaron una gran cantidad de compras de espacios publicitarios en redes sociales como Facebook y crearon un "ejército" de cuentas falsas en Twitter que apoyaron al candidato republicano Donald Trump. En suma, el Internet

[73] *Ibid*, p. 42.
[74] *Ibid*, p. 42.
[75] *Ibid*, p. 41.

les brindó a los servicios de seguridad e inteligencia de Rusia la posibilidad sin precedentes de influenciar con propaganda a millones de votantes estadounidenses[76].

Por otro lado, China ha realizado operaciones cibernéticas clandestinas con el objetivo de obtener beneficios económicos. Por al menos una década entera, este país ha robado propiedad intelectual de innumerables empresas extranjeras con el fin de tener la ventaja en negociaciones económicas o de compensar su falta de innovación doméstica. De acuerdo a un reporte del 2017 de la Comisión sobre Robo de Propiedad Intelectual Americana de EE.UU., al año las empresas estadounidenses pierden entre US$ 225 miles de millones y US$ 600 miles de millones, de los cuales gran parte puede ser atribuible a China[77].

Esta propiedad intelectual incluye avances tecnológicos en la industria militar, y es conocido que países como EE.UU. y otros miembros de la OTAN son víctimas de múltiples y constantes ataques cibernéticos por parte de China con el fin de robar información sobre sus últimos avances militares.

Corea del Norte también ha demostrado tener capacidades cibernéticas que ha podido explotar en favor de sus intereses. Un caso conocido ocurrió en el 2014 cuando agentes cibernéticos de Corea del Norte vulneraron la red de *Sony Pictures*: destruyeron sus servidores y revelaron información confidencial como represalia a que se mostrase una parodia ficticia sobre el asesinato del líder norcoreano Kim Jon Un en el programa *The Interview*[78]. Asimismo, en el 2016, agentes cibernéticos norcoreanos lograron retirar ilegalmente decenas de millones de dólares del banco central de Bangladesh[79]. Este es un conocido método norcoreano para poder sustentar financieramente a su Estado, debido a las sanciones económicas que mantiene, mediante el robo de dinero o la aplicación de las extorsiones informáticas o *ransomware*.

[76] *Ibid,* p. 41.
[77] *Ibid.,* p. 42.
[78] *Ibid,* pp. 41-42.
[79] *Ibid,* p. 42.

En conclusión, la ciberseguridad y la ciberdefensa tienen una importancia vital en la protección de la integridad, la soberanía y los intereses de un Estado. Ha quedado demostrado en los diversos casos de ciberataques y ciberguerra que el ciberespacio es, efectivamente, el quinto dominio de la guerra, y que en él los Estados manifiestan su poder sobre otros en favor de sus propios intereses. La inclusión del ciberespacio como nueva dimensión de competencia entre Estados ha traído consigo la evolución de los tradicionales conceptos de seguridad y defensa, en tanto representa también una arena en la que las amenazas híbridas y la combinación de esfuerzos privados y estatales pueden representar un peligro real para los Estados.

Ya que la actual Cuarta Revolución Industrial potenciará el desarrollo de nuevas tecnologías disruptivas, diversos Estados, bloques de Estados y organizaciones internacionales han desarrollado normativas y construido capacidades para poder regular las acciones de ciberguerra que los involucren, y para poder protegerse o llevar a cabo operaciones ofensivas en el ciberespacio, de acuerdo a sus intereses. Así, el segundo capítulo de la presente tesis realiza un análisis de los avances en ciberdefensa y en la atención de amenazas híbridas en el mundo, sobre todo acerca de los organismos internacionales y Estados que más avances han demostrado tener en dicha materia.

Capítulo II: Análisis de la situación de la ciberseguridad, ciberdefensa y amenazas híbridas en el escenario internacional

La ciberdefensa y la atención a las amenazas híbridas cobran cada vez mayor relevancia a medida que, en la era de la Cuarta Revolución Industrial, se crean nuevas tecnologías digitales, físicas y biológicas que convergen y generan efectos disruptivos sobre las sociedades y los sistemas digitales y físicos que las sustentan. En ese sentido, diferentes organizaciones y organismos internacionales, así como países individuales y sobre todo las grandes potencias, han desarrollado agendas, marcos normativos, capacidades propias y esquemas de cooperación en materia de ciberdefensa y amenazas híbridas.

En el presente capítulo se realiza un análisis de la situación en la que se encuentran los avances internacionales en materia de ciberseguridad, ciberdefensa y amenazas híbridas. Primero se desarrolla el Convenio de Budapest sobre Ciberdelincuencia del 2001, por ser el primer y único tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet. Segundo, se analiza a las organizaciones y los organismos internacionales y regionales más avanzados en materia de ciberseguridad, ciberdefensa y amenazas híbridas, específicamente la Organización de las Naciones Unidas (ONU), la OTAN, la Unión Europea (UE) y la Organización de los Estados Americanos (OEA). Tercero, se analiza la situación de los Estados Unidos de América (EE.UU.), la Federación Rusa y la República Popular de China por ser potencias mundiales que resaltan por sus capacidades militares y cibernéticas.

1. Convenio de Budapest contra la Ciberdelincuencia

Elaborado y aprobado por el Consejo de Europa en el 2001, el Convenio de Budapest contra la Ciberdelincuencia entró en vigor el 1 de julio de 2004. A la fecha, 64 Estados la han ratificado. Este Convenio es el primer y el único tratado internacional vigente que busca hacer frente a los delitos informáticos y en Internet, para lo cual apunta a la

armonización de la legislación al respecto entre sus países firmantes, así como una mayor cooperación entre ellas[80].

El contexto de la elaboración del Convenio es uno en el que incrementan los riesgos que emergen con el uso de las tecnologías digitales en un mundo cada vez más interconectado y dependiente de ellas. En ese sentido, el Convenio pone énfasis en la seguridad digital, es decir, la prevención de actos que afecten la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos. Asimismo, busca la penalización común de delitos como la piratería, el fraude informático, la falsificación informática, la pornografía infantil, la violación de la propiedad intelectual, el acceso ilícito, la interceptación ilícita y el abuso de los dispositivos[81].

En ese sentido, el Convenio tiene tres objetivos principales:

a) La armonización del derecho penal nacional en materia de infracciones y otras disposiciones conectadas al ámbito de los delitos informáticos.
b) Proporcionar las facultades necesarias en el derecho procesal penal interno para la investigación y enjuiciamiento de tales delitos, así como otros delitos cometidos por medio de un sistema informático o que se encuentren en formato electrónico.
c) El establecimiento de un régimen rápido y efectivo de cooperación internacional en la materia.

Una sección del Convenio sugiere diversas medidas normativas para que los Estados empoderen a sus autoridades competentes para que puedan llevar a cabo su tarea de actuar contra la ciberdelincuencia de manera más efectiva. Estas medidas incluyen facilitar legalmente la interceptación en tiempo real de comunicaciones e información en el ciberespacio, la búsqueda y la obtención de datos informáticos almacenados, entre otros. Para ello, en el Convenio se señala que los países firmantes deben adoptar las medidas necesarias para facilitar la aplicación de los medios técnicos necesarios

[80] Presidencia del Consejo de Ministros [PCM], 2019.
[81] *Ibid*.

para perseguir los delitos informáticos, así como para facilitar la cooperación entre las autoridades y entidades competentes en la materia[82].

En el tercer capítulo del Convenio, sobre la cooperación internacional, se indica que las partes ofrecerán entre sí asistencia mutua el máximo nivel posible para investigaciones criminales relacionados a sistemas y datos informáticos, incluyendo la colección de evidencia en forma electrónica de otros delitos. Entre las medidas enmarcadas en dicho capítulo, se incluye la posibilidad de que una parte pueda solicitarle a otra parte una acelerada obtención de comunicaciones o datos informáticos almacenados en el territorio de esta última, siempre y cuando estén relacionados a un delito informático[83].

Asimismo, el Convenio establece una red 24/7, en tanto cada parte debe establecer un punto de contacto que esté permanentemente disponible. Esto, con el fin de asegurar la asistencia inmediata para investigaciones criminales de delitos relaciones a sistemas y datos informáticos, o para recolectar evidencia en formas electrónicas de otros tipos de delitos. Estos puntos de contacto deberán estar facultados para responder a las comunicaciones de otros puntos de contacto de manera inmediata, facilitar asesoramiento técnico, preservar datos, recolectar evidencia, proveer información legal y ubicar sospechosos[84].

En el 2006 entró en vigor el primer protocolo adicional del Convenio: el Protocolo Adicional a la Convención sobre el delito cibernético. Mediante dicho protocolo, los estados que lo ratifiquen deben penalizar la difusión de propaganda, insultos y amenazas racistas y xenófobas a través de los sistemas informáticos. A la fecha, 29 Estados lo han ratificado.

[82] Consejo de Europa, 2001, pp. 9-11.
[83] *Ibid*, pp. 16-17.
[84] *Ibid*, p. 18.

Cabe resaltar que la mayoría de los Estados que han ratificado el Convenio son europeos y norteamericanos. Por otro lado, desde que entró en vigor, países como Brasil y la India se negaron a adoptarlo bajo el argumento de que no participaron en su elaboración. Rusia, por su parte, se ha opuesto firmemente al Convenio señalando que violaría su soberanía.

El Perú se adhirió al Convenio recién en el 2019 bajo el impulso de la Secretaría de Gobierno y Transformación Digital (SEGDI) de la Presidencia del Consejo de Ministros (PCM) con el interés de promover un ambiente de confianza digital para las empresas y los ciudadanos en el desarrollo de la economía digital nacional; así como para establecer consecuencias penales contra la pornografía infantil, la piratería y la violación de la propiedad intelectual[85]. En la región, los países que han ratificado el Convenio son Argentina, Chile, Colombia, Panamá y Paraguay.

2. Situación de la ciberseguridad, ciberdefensa y amenazas híbridas en organizaciones y organismos internacionales

Diversas organizaciones y organismos internacionales han desarrollado capacidades, agendas e instituciones orientadas a la ciberseguridad, la ciberdefensa y la atención a amenazas híbridas. Generalmente, se busca generar conjuntamente capacidades para los Estados miembros que componen dichas organizaciones para lograr una situación de seguridad colectiva frente a las amenazas propias de la ciberseguridad y la ciberdefensa, incluyendo las amenazas híbridas.

Algunas de estas organizaciones internacionales, sobre todo las enfocadas a la defensa colectiva como la OTAN, tienen además mecanismos de cooperación y generación de capacidades para el tema específico de las amenazas híbridas. Por otro lado, algunas organizaciones menos avanzadas en los temas a los que se ha hecho referencia se han limitado a establecer las bases para una agenda o un marco normativo general sobre el

[85] *Ibid*.

cual recién se empezaría a desarrollar capacidades conjuntas en ciberseguridad, ciberdefensa y amenazas híbridas.

2.1. Organización de las Naciones Unidas (ONU)

En la ONU, los temas de ciberseguridad, e indirectamente, los de amenazas híbridas relacionados a la ciberseguridad, son trabajados en la Oficina de las Naciones Unidas de Lucha Contra el Terrorismo (OLCT), creada en el 2017 mediante Resolución 71/291 de la Asamblea General de la ONU[86]. Su creación es parte de la implementación de la Estrategia Global de las Naciones Unidas en Lucha contra el Terrorismo, adoptada en el 2006 mediante Resolución 60/288 de la Asamblea General.

Dicha estrategia sirve de base para tomar medidas prácticas, tanto individual como colectivamente, para prevenir y combatir el terrorismo. Estas medidas incluyen un rango de posibilidades, desde el fortalecimiento de la propia capacidad estatal para hacer frente a amenazas terroristas, hasta generar mejor coordinación con las actividades de lucha contra el terrorismo del Sistema de las Naciones Unidas[87].

La estrategia y su Plan de Acción se sustentan en cuatro pilares:

1. Medidas para hacer frente a las condiciones que propician la propagación del terrorismo;
2. Medidas para prevenir y combatir el terrorismo;
3. Medidas destinadas a aumentar la capacidad de los Estados para prevenir el terrorismo y luchar contra él, y a fortalecer el papel del sistema de las Naciones Unidas a ese respecto;
4. Medidas para asegurar el respeto de los derechos humanos para todos y el imperio de la ley como base fundamental de la lucha contra el terrorismo[88].

[86] Organización de las Naciones Unidas [ONU], s/f.
[87] *Ibid.*
[88] *Ibid*

En base a dichos pilares, la OLCT tiene las siguientes cinco funciones principales:

1. Liderar los mandatos de lucha contra el terrorismo de la Asamblea General que se encomiendan al Secretario General desde las distintas entidades del sistema de las Naciones Unidas;
2. Reforzar la coordinación y la coherencia entre las entidades del Pacto Mundial de Coordinación de la Lucha Antiterrorista de las Naciones Unidas a fin de garantizar la aplicación equilibrada de los cuatro pilares de la Estrategia Global de las Naciones Unidas contra el Terrorismo;
3. Mejorar la prestación de asistencia de la Organización a los Estados Miembros para la creación de capacidad contra el terrorismo;
4. Aumentar la visibilidad y la promoción de las actividades de las Naciones Unidas contra el terrorismo, así como la movilización de recursos destinados a esas iniciativas;
5. Velar por que se dé la prioridad oportuna a la lucha contra el terrorismo en todo el sistema de las Naciones Unidas y por que la importante labor de prevención del extremismo violento se asiente firmemente en la Estrategia[89].

En ese sentido, la OLCT tiene un Programa de Ciberseguridad y Nuevas Tecnologías, cuyo objetivo es fortalecer las capacidades de los Estados Miembros y de organizaciones privadas en la prevención de ciberataques realizados por agentes terroristas contra infraestructuras críticas; así como mitigar los efectos de estos ataques y recuperar y restaurar los sistemas que sean el blanco de estos en caso de que ocurran[90]. Este objetivo busca enfrentar, entonces, la amenaza no convencional del terrorismo en el ciberespacio, que en la práctica puede tener efectos destructivos reales sobre la IC de un país, ya sea de carácter público o privado.

Asimismo, el programa de Ciberseguridad de la OLCT trabaja con los Estados Miembros y organizaciones privadas para generar conciencia acerca del uso indebido de la tecnología de la información y las comunicaciones (TIC), especialmente por parte

[89] *Ibid.*
[90] *Ibid.*

de actores terroristas. Este uso indebido se realiza principalmente en el internet y nuevas tecnologías digitales, con el objetivo de cometer acciones terroristas concretos o para realizar actividades asociados como la incitación, el reclutamiento, la financiación o la planificación para actos de terrorismo[91].

Siendo el internet y el ciberespacio una dimensión tan complicada de supervisar o controlar, los Estados Miembros han recalcado la importancia, en el marco de la ONU, de cooperar con las múltiples partes interesadas para hacer frente a la amenaza anteriormente descrita. En esta labor de cooperación, tienen un rol especial los mismos Estados Miembros; las organizaciones internacionales, regionales y subregionales; el sector privado y la sociedad civil[92].

Esta preocupación compartida y la voluntad de cooperación de los Estados Miembros de la ONU ha sido manifestada en la resolución 2341 (2017) del Consejo de Seguridad de las Naciones Unidas, que exhorta a los Estados Miembros a "establecer o reforzar las alianzas nacionales, regionales e internacionales con las partes interesadas, tanto públicas como privadas, según proceda, para intercambiar información y experiencias a fin de prevenir, proteger, mitigar e investigar los daños causados por atentados terroristas contra instalaciones de infraestructura vital, así como para responder a ellos y recuperarse de ellos, en particular mediante actividades conjuntas de capacitación, y la utilización o el establecimiento de redes de alerta de emergencia o de comunicación pertinentes"[93].

Es evidente que los atentados terroristas contra instalaciones o IC de los que se hace mención en dicha resolución pueden tener un aspecto netamente físico, en tanto los actores terroristas pueden emplear métodos violentos de destrucción física contra dicha IC de manera directa. Sin embargo, hoy en día los avances tecnológicos y la mayor interconectividad de los diversos sistemas digitales que sustentan el funcionamiento

[91] *Ibid.*
[92] *Ibid.*
[93] *Ibid.*

de dicha IC o que sustentan el funcionamiento de otros sistemas complementarios a la IC como transporte, seguridad, entre otros; hace igual de vulnerables a la IC ante atentados terroristas de naturaleza física como cibernética.

Asimismo, el acto terrorista implica otras acciones que se remontan hasta las etapas de planificación y reclutamiento, las cuales también se llevan a cabo en el ciberespacio. Por esta razón, prevenir un atentado contra IC, sin importar que vaya a ser de naturaleza física o cibernética, requiere necesariamente de neutralizar la posibilidad de reclutamiento y posiblemente, de planificación y coordinación terrorista en el ciberespacio.

Adicionalmente, la inteligencia y la contrainteligencia de un país debe poder tener la capacidad de monitorear y de ser posible, neutralizar las acciones de los agentes terroristas en el ciberespacio, o deben poder adquirir la inteligencia necesaria en el ciberespacio para neutralizar a los agentes terroristas por otros medios.

En atención a todo lo anterior, la OLCT cuenta con varias iniciativas. Entre ellas, tiene un proyecto sobre el uso de las redes sociales para reunir información de fuentes abiertas y pruebas digitales con el fin de combatir el terrorismo y el extremismo violento. Asimismo, brinda conocimientos especializados en foros internacionales acerca de los usos terroristas de sistemas aéreos no tripulados[94].

Este último punto cobra mayor importancia con hechos en los que grupos terroristas acceden a armamento tecnológicamente avanzado, como recientemente ha ocurrido en Afganistán que ha caído bajo control de los talibanes, quienes ahora poseen en su arsenal armamento, vehículos blindados y vehículos aéreos no tripulados que le pertenecían a las fuerzas estadounidenses anteriormente desplegadas en ese país. Este tipo de situaciones en los que grupos armados irregulares acceden a armamento avanzado podría replicarse en diversas situaciones de conflicto, por lo que se considera

[94] *Ibid.*

que la labor de la OLCT es oportuna al brindar conocimientos especializados al respecto.

2.2. Organización del Tratado del Atlántico Norte (OTAN)

La OTAN, por su naturaleza como bloque militar, se ha enfocado en generar capacidades conjuntas en materia de ciberdefensa para proteger a sus miembros de amenazas cibernéticas que puedan atentar contra su soberanía y seguridad nacional. En ese sentido, la OTAN prioriza el desarrollo de capacidades operacionales que sean efectivos en la guerra cibernética.

En el Comunicado de la Cumbre de la OTAN en Varsovia del año 2016, los jefes de Estado reconocieron que los países miembros se encuentran enfrentando retos y amenazas a la seguridad que incluyen a actores estatales y no estatales, amenazas por parte de fuerzas militares y terroristas, y de ataques cibernéticos e híbridos. Asimismo, reconocen que la ciberdefensa es ahora parte esencial de la defensa colectiva sobre la que se sostiene la alianza, y que el ciberespacio es un dominio en el que la OTAN debe defenderse efectivamente. En ese sentido, el comunicado también afirma que los miembros de la OTAN deben estar debidamente entrenados y equipados para este nuevo dominio de la guerra[95].

2.2.1. Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE)

La OTAN cuenta desde el 2008 con un Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE), un centro de ciberdefensa multinacional e interdisciplinario que realiza investigación, capacitación y ejercicios en cuatro áreas clave: tecnología, estrategia, operaciones y legislación[96]. A diferencia del Programa de Ciberseguridad y

[95] Organización del Tratado del Atlántico Norte [OTAN], 2017.
[96] Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN [CCDCOE], s/f.

Nuevas Tecnologías de la OLCT de la ONU, el CCDCOE tiene capacidades operativas debido a la propia naturaleza militar de la OTAN.

Cabe resaltar que el CCDCOE es financiado y cuenta con personal de sus Estados miembros, en tanto no es una unidad operacional que forma propiamente parte de la Estructura de Comando de la OTAN, aunque sí pertenece a la red de Centros de Excelencia acreditados por la OTAN[97].

Con sede en Estonia, el CCDCOE tiene además la visión de fomentar la cooperación con naciones que tengan principios y valores similares a los de la OTAN, incluyendo aliados y socios más allá de la Alianza. Así, naciones que no pertenecen a la OTAN pueden ser parte del trabajo que realiza el CCDCOE, incluso formar parte del Comité Directivo del mismo, órgano encargado de guiar, supervisar y tomar decisiones en materia de administración y operación del CCDCOE, incluyendo la implementación del presupuesto, planes de trabajo y de desarrollo y cronogramas de actividades anuales[98].

La presidencia del Comité Directivo del CCDCOE es asumida por el país anfitrión, Estonia. Los funcionarios, tanto a cargo de la dirección como asesores, jefes de área e investigadores en las ramas de Tecnología, Estrategia, Operaciones, Legislación, Educación y Entrenamiento, y Apoyo, son militares de alto rango y especialistas de los países asociados al CCDCOE[99].

Estonia es el país anfitrión del CCDCOE y principal impulsor del concepto de ciberdefensa en la OTAN debido a su experiencia con la ciberguerra que tuvo con Rusia en el 2007[100]. Dicha ciberguerra consistió en una serie de ciberataques coordinados que tuvieron como blanco páginas web de diversas organizaciones estonias, incluyendo su parlamento, bancos, ministerios, diarios y locutoras. La

[97] *Ibid.*
[98] *Ibid.*
[99] *Ibid.*
[100] *Ibid.*

naturaleza de los ataques, sobre todo aquellos que buscaron afectar a la población en general, fueron ataques DoS perpetrados por individuos o botnets, que vienen a ser conjuntos o redes de robots informáticos o bots que se ejecutan de manera autónoma y automática.

Hasta la fecha no se ha confirmado el origen exacto de los ciberataques, pero es mayormente aceptado que un ataque de tal magnitud y precisión habría requerido la cooperación del gobierno ruso con alguna organización privada con la infraestructura y capacidad tecnológica suficiente para llevarla a cabo, posiblemente una compañía de telecomunicaciones. En caso de que no se haya tratado de una compañía de telecomunicaciones, pudo haberse tratado de diferentes grupos que operaron botnets distribuidos para llevar a cabo el ataque.

Tampoco se ha confirmado si los ciberataques fueron directamente ordenados por Rusia o si solo fueron "permitidos" por ella. Lo que es incuestionable es que este ataque corresponde a lo que se ha definido anteriormente como una amenaza híbrida, en tanto un actor estatal, en conjunto o en coordinación con actores no estatales, lleva a cabo una agresión para afectar negativamente a otro Estado en diversas dimensiones, ya sea la económica, política, social, militar, entre otras.

Cabe resaltar que, en el año siguiente, el 2008, ciberataques similares se llevaron a cabo por parte de Rusia contra Georgia mientras que paralelamente fuerzas armadas rusas invadían dicho país, como se detalló en el capítulo anterior. Si bien Estonia no fue producto de una invasión militar durante el tiempo que fue afectado por ciberataques, es necesario mencionar que dicho país se encontraba en un contexto de disturbios sociales debido a acalorados debates en la opinión pública debido a la reubicación de tumbas y monumentos soviéticos. En un contexto como ese, el daño que un conjunto de ciberataques le puede hacer a un país se multiplica, ya que agudiza aún más la inestabilidad social, política y económica del momento.

Como se ha mencionado, la creación del CCDCOE en el 2008 fue un efecto directo de este gran ciberataque a Estonia, quien impulsó la necesidad de actualizar la doctrina de defensa colectiva de la OTAN para que incorpore a la ciberdefensa como aspecto permanente a considerar. Asimismo, entre los primeros y más resaltantes avances del CCDCOE se encuentra la redacción del Manual de Tallin sobre Derecho Internacional aplicable a la Ciberguerra, escrito y actualizado entre los años 2009 y 2012 y publicado recién en el año 2013[101].

2.2.2. El Manual de Tallin y la introducción del Derecho Internacional Humanitario en el ciberespacio

El Manual de Tallin, como producto insignia del CCDCOE, es, en síntesis, un estudio académico no vinculante acerca de cómo el Derecho Internacional Público, en particular el *Ius ad bellum* y el Derecho Internacional Humanitario pueden ser aplicados para los conflictos que se desarrollan en el ciberespacio, entendidos como ciberguerra. Este manual es el primer intento serio y comprensivo que han realizado Estados para poder regular de manera uniforme la actuación de los Estados en el ciberespacio en casos de conflicto entre ellos[102].

El Manual de Tallin fue actualizado en el 2017, cuya edición se conoce como Manual de Tallin 2.0. Este año, el 2021, se ha iniciado el Proyecto Manual de Tallin 3.0 en el que se revisarán los capítulos existentes y se explorará nuevos temas que son de importancia para los Estados, relacionados a la práctica de los Estados, el derecho internacional, las actividades de organizaciones internacionales, la investigación académica e iniciativas multi-actor que incluyen a gobiernos, industrias y sociedad civil. Todas las entidades y actores mencionados serán considerados en la elaboración del Manual de Tallin 3.0[103].

[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*

El Manual de Tallin 2.0 le agrega a la primera versión del manual temas que relacionan la aplicabilidad del derecho internacional en el ciberespacio más allá de tiempos de conflicto, es decir, en tiempos de paz en los que día a día los Estados también son víctimas o perpetradores de ciberataques. Asimismo, expande los conceptos de soberanía, responsabilidad estatal, derechos humanos y derechos del aire, del espacio y del mar.

A modo de resumen, el Manual de Tallin 2.0 desarrolla una gran variedad de temas relacionados a la actividad de los Estados en el ciberespacio y analiza cómo se puede aplicar el derecho internacional a estas. Los temas más resaltantes que aborda son el concepto de soberanía en el ciberespacio, incluyendo la dimensión interna y externa de esta, la violación de la soberanía y casos de inmunidad e inviolabilidad. Cabe resaltar que dicho manual aclara que, si bien los Estados no son soberanos en el internet, la infraestructura física sobre la cual existe el internet existe en espacios físicos que sí pertenece a la soberanía de los Estados[104].

Asimismo, el manual desarrolla extensivamente la aplicabilidad del principio de responsabilidad estatal frente al derecho internacional. Esta responsabilidad se analiza para casos en los que los Estados lleven a cabo acciones cibernéticas internacionalmente ilegales, y en caso de que estas acciones sean llevadas a cabo por órganos estatales, actores no estatales, o en conexión con operaciones cibernéticas llevadas a cabo por terceros Estados[105].

Otro tema tratado es el de las represalias o contramedidas que puede llevar a cabo un Estado en el ciberespacio, por lo que se desarrollan los conceptos y principios de limitaciones y proporcionalidad que son aplicados en la guerra física convencional entre Estados en la actualidad. En línea con esto, el manual también desarrolla el concepto de las obligaciones que tienen los Estados frente a actos internacionalmente

[104] Schmitt, M. N., 2017, p. i.
[105] *Ibid*, p. vi.

ilegales, lo cual incluye un análisis de los principios de cesación, garantías y reparaciones aplicables a este tipo de actos en el ciberespacio[106].

También se incluyen temas novedosos que no son regulados completamente por el derecho internacional en la actualidad. Entre estos temas están las ciberoperaciones de espionaje en tiempos de paz y la actuación de actores no estatales o irregulares en el ciberespacio. Asimismo, se desarrollan temas relacionados al derecho alrededor de los derechos humanos, sobre todo lo referido a las obligaciones que tienen los Estados en respetar y proteger los derechos humanos reconocidos internacionalmente.[107]

El manual incorpora elementos que también se relacionan directamente con el derecho diplomático y el derecho consular. Los temas al respecto abordados incluyen la inviolabilidad de lugares en los que se encuentre infraestructura ciber; el deber de proteger infraestructura cibernética; y la inviolabilidad de archivos, documentos y correspondencia electrónica[108].

Por otro lado, se desarrollan temas como la aplicación del derecho del mar en el ciberespacio, haciendo distinciones para ciberoperaciones llevadas a cabo en alta mar, en zonas económicas exclusivas, en mares territoriales, en zonas contiguas, en estrechos y ríos internacionales, y en mares de archipiélagos, ya sea en tiempos de paz como de guerra o conflicto armado. Asimismo, se analiza la situación especial que tienen los cables de conexión submarina como infraestructura importante para las ciberoperaciones[109], ya sea porque son necesarias para llevar a cabo algunas de ellas o porque pueden ser blanco de las mismas.

En ese sentido, se analiza también la aplicabilidad del derecho del aire y del espacio exterior al ciberespacio. Entre los temas de derecho del aire, se incluyen el control de aeronaves que llevan a cabo ciberoperaciones en espacio aéreo nacional de un Estado

[106] *Ibid*, p. vi.
[107] *Ibid*, pp. vi-vii.
[108] *Ibid*, p. vii.
[109] *Ibid*, p. vii.

y en espacio aéreo internacional. Asimismo, se analiza la situación de las operaciones cibernéticas que pueden poner en peligro la seguridad de la aviación civil, lo cual está relacionado en parte con otro tema abordado por el manual, el derecho de las telecomunicaciones internacionales y las posibilidades de interferencias dañinas en ellas a causa de las ciberoperaciones[110].

En otra parte del manual se desarrollan los conceptos de paz internacional y actividades de ciberseguridad relacionadas a ella. Estos conceptos involucran el análisis de temas como la resolución pacífica de disputas, la intervención de los Estados o de las Naciones Unidas en casos de conflicto, la prohibición del uso o de la amenaza del uso de la fuerza, el principio de legítima defensa y de defensa colectiva, el concepto de seguridad colectiva y operaciones de paz[111]. Todos estos temas pertenecen a la literatura actual sobre seguridad y defensa en las relaciones internacionales, y el Manual de Tallin hace un esfuerzo por incorporarlos en la dimensión del ciberespacio para poder regular efectivamente el uso del dominio ciber en caso de conflicto entre Estados.

Así, en otra sección del manual, con todo lo anteriormente descrito se desarrolla a profundidad el novedoso concepto de derecho del conflicto armado cibernético. Esta parte analiza la responsabilidad criminal de individuos, de comandantes y de superiores en caso de que se cometan crímenes de guerra en el ciberespacio[112].

También se desarrollan principios como la proporcionalidad, la prohibición de atacar civiles en caso de ciberguerra, el caso de ciberataques terroristas, la prohibición de atacar infraestructura civil y su diferencia con objetivos militares, y crímenes como generar sufrimiento innecesario, utilizar métodos de destrucción indiscriminada, crear y usar trampas y sistemas engañosos en el ciberespacio, generar hambruna y otros padecimientos mediante el ciberespacio, entre otros[113].

[110] *Ibid*, p. vii.
[111] *Ibid*, p. viii.
[112] *Ibid*, pp. viii-ix.
[113] *Ibid*, pp. ix-x.

El manual también incluye temas como la correcta diferenciación de blancos en casos de ciberguerra, el uso de advertencias, el uso inapropiado de indicadores o símbolos protectores, como emblemas de organizaciones humanitarias o de las Naciones Unidas; así como el uso inapropiado de indicadores o símbolos enemigos o neutrales. Por otro lado, se analiza la necesidad de proteger a niños y periodistas en caso de guerra[114].

Finalmente, el manual desarrolla temas como la necesidad de proteger instalaciones que contienen elementos o fuerzas peligrosas, como represas, diques, centrales nucleares y otros similares. También se incluye la necesidad de proteger otro tipo de infraestructura indispensable para la supervivencia de la población civil, la propiedad cultural y el medio ambiente. Por último, el manual analiza la situación de la asistencia humanitaria en el ciberespacio y su respeto, así como el respeto de personas protegidas en territorio ocupado, la protección de infraestructura cibernética neutral y la realización de ciberoperaciones en territorio neutral[115].

El lector podrá apreciar la aplicación de conceptos y principios ya utilizados en la actualidad para casos de guerra o conflicto armado entre Estados, especialmente en el Derecho Internacional Humanitario o derecho de la guerra, para los conflictos que se lleven a cabo en el ciberespacio que involucren la participación de Estados. Así, los análisis desarrollados en el Manual de Tallin presentan enfoques novedosos de la posibilidad de empezar a regular el ciberespacio mediante la aplicación de ciertas normas y principios del derecho internacional al actuar de los Estados en el ciberespacio.

Eventualmente, una aplicación obligatoria de estas propuestas implicaría innovaciones y cambios en el ordenamiento jurídico internacional vigente. Para ello sería necesario contar con la voluntad política necesaria por parte de los Estados para que se sometan

[114] *Ibid*, p. xi.
[115] *Ibid*, p. xi.

voluntariamente a este tipo de regulación, y la existencia de entidades como el CCDCOE significa un primer paso en juntar a un grupo de Estados que justamente apuntan hacia ese objetivo.

No obstante, si bien gran cantidad de países, sobre todo los europeos, han declarado estar a favor de la regulación del ciberespacio y de la aplicación del DIH en él, EE.UU. es un país miembro de la OTAN que está en contra de dicha regulación, ya que, como se verá más adelante, es un actor sumamente activo en usar el ciberespacio para fines políticos y militares. Por otro lado, existen países que buscan un punto intermedio, es decir, la regulación del ciberespacio pero sin que se le aplique el DIH.

Además del gran aporte que significa el Manual de Tallin para la regulación de la guerra en el ciberespacio, el CCDCOE también resalta por sus capacidades operativas y sus esfuerzos por mantener a sus miembros altamente capacitados y entrenados en materia de ciberseguridad y ciberdefensa. Desde el año 2009, el CCDCOE lleva a cabo anualmente la Conferencia Internacional sobre Ciberconflicto (CyCon), en los que se abordan los aspectos legales, tecnológicos y de investigación del conflicto en el ciberespacio. Hoy en día, CyCon se ha convertido en un gran evento académico del más alto nivel de construcción de comunidad para profesionales en ciberseguridad[116].

2.2.3. Ejercicio multinacional *Locked Shields*

Desde el año 2010 el CCDCOE organiza anualmente el ejercicio de ciberdefensa de "fuego-real" más grande y más complejo de todo el mundo. Este ejercicio, *Locked Shields*, simula la gran complejidad que significa un incidente cibernético masivo, lo cual pone a prueba las capacidades de prevención y respuesta de los Estados para defender sus sistemas informáticos civiles, empresariales y militares y sus

[116] CCDCOE, s/f.

infraestructuras críticas; en la toma de decisiones estratégicas y en la comunicación legal y mediática[117].

En la edición de *Locked Shields* del 2021, el ejercicio consistió en el enfrentamiento entre grupos, con más de 800 expertos en total. Los equipos de expertos asumieron el rol de Equipos de Reacción Rápida cibernética desplegados para asistir a un país ficticio en controlar un masivo incidente cibernético en tiempo real y todas sus implicaciones. Este ejercicio involucró cerca de 5,000 sistemas virtualizados que fueron objeto de más de 4,000 ataques. Los equipos debían ser efectivos en reportar incidentes, ejecutar decisiones estratégicas y resolver desafíos legales y mediáticos[118].

Evidentemente, *Locked Shields* busca mantener a sus participantes actualizados con lo último en tecnología, razón por la cual se centra en simular escenarios realistas con los últimos avances en tecnología, redes y métodos de ataque. Asimismo, el masivo ejercicio involucra sistemas ciber-físicos y elementos técnicos y estratégicos de manera combinada. Esto implica que los participantes deben poner a prueba toda su cadena de mando para resolver a gran escala el incidente cibernético[119].

Reflejando amenazas cibernéticas reales, el ejercicio aborda la protección de servicios vitales e IC fundamentales para el funcionamiento de las sociedades modernas. Esto incluye infraestructura crítica para la información, suministro de energía y agua, y sistemas de defensa nacional. En la edición del 2021, *Locked Shields* incluyó también por primera vez en la historia la simulación de sistemas de control de una misión de satélite en el espacio exterior necesario para proveer conciencia situacional en tiempo real para apoyar en la toma de decisiones militares[120].

El 2021 también ha sido la primera vez que el ejercicio *Locked Shields* se haya desarrollado en múltiples partes del mundo en tiempo real, ya que la pandemia por

[117] *Ibid.*
[118] *Ibid.*
[119] *Ibid.*
[120] *Ibid.*

COVID-19 ha dificultado la posibilidad de centralizar todo el ejercicio en un solo lugar[121]. No obstante, el éxito de la última edición del ejercicio ha demostrado su efectividad y capacidad para ser realmente el ejercicio de ciberdefensa mundial por excelencia.

Así, *Locked Shields* representa una oportunidad única para experimentar, entrenar y fortalecer la cooperación entre miembros del CCDCOE, la OTAN y naciones amigas. Es el único espacio actual en el que Estados pueden ponerse a prueba en escenarios reales y seguros contra adversarios altamente capacitados, tanto en el aspecto civil como el aspecto militar de lo que podría ser un masivo ataque cibernético[122].

Además, los equipos participantes salen capacitados y entrenados en temas como proteger sistemas especializados poco comunes y de los que no están necesariamente familiarizados; saber proveer reportes de situación bajo presión; detectar y mitigar ataques en ambientes tecnológicos grandes y complejos en tiempo real; tanto en sistemas civiles, empresariales y militares; y fortalecer el trabajo coordinado en sus propios equipos[123].

Finalmente, cabe resaltar que *Locked Shields* es organizado por el CCDCOE en cooperación con diversas entidades gubernamentales y privadas. Las entidades gubernamentales u oficiales que participaron en la organización de la edición del ejercicio en el 2021 fueron la Agencia de Comunicaciones e Información de la OTAN, el Ministerio de Defensa de Estonia, las Fuerzas Armadas de Estonia, la Unidad de Innovación en Defensa de los EE.UU., el Centro Europeo de Excelencia para la lucha contra las Amenazas Híbridas (Hybrid CoE), la Agencia de Defensa Europea, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) y el Centro de Excelencia en Modelaje y Simulación de la OTAN[124].

---

[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] *Ibid.*

Por otro lado, las organizaciones privadas que participaron fueron Siemens, Ericsson, TalTech, la Fundación CR14, Bittium, *Clarified Security*, *Arctic Security*, Cisco, *Stamus Networks*, SpaceIT, Sentinel, el *Financial Services Information Sharing and Analysis Center* (FS-ISAC), Microsoft, Atech, Avibras, *SUTD iTrust Singapore*, *Space ISAC*, STM, *VTT Technical Research Centre of Finland Ltd* y *PaloAlto networks*[125].

En conclusión, el CCDCOE representa una oportunidad única para países interesados en capacitar y entrenar a sus equipos de ciberseguridad y ciberdefensa nacional con los actores internacionales occidentales más avanzados en la materia. Además del entrenamiento a nivel operativo, el CCDCOE también es el primer y único espacio en el que los Estados impulsan la regulación del ciberespacio y los ciberataques, tanto en caso de conflicto como de paz; y para ello aglomera a expertos del más alto nivel en ciberseguridad y ciberdefensa, así como analistas y expertos de derecho internacional, militares y otros agentes estatales.

Un país que participe de las actividades y de las innovaciones del CCDCOE se verá sumamente beneficiado, y como valor agregado, se verá beneficiado también de poder conocer cuáles son los avances que tienen los países que ya forman parte del CCDCOE y cuáles son las temáticas en las que están interesados.

2.3. **Unión Europea (UE)**

Dentro de la UE existen agencias, redes y centros de excelencia especializados de carácter oficial o independientes que trabajan en temas de ciberseguridad y ciberdefensa con los objetivos generales de crear espacios de cooperación entre los países europeos y de mejorar las capacidades de los mismos en la materia. Estas instituciones vienen a ser la Agencia de la Unión Europea para la Ciberseguridad

[125] *Ibid.*

(ENISA), la Red de Equipos de Respuesta ante Incidencias de Seguridad Informática (CSIRTs), la propuesta de una Unidad Cibernética Conjunta (JCU) y *Hybrid CoE*.

2.3.1. Agencia de la Unión Europea para la Ciberseguridad (ENISA)

La UE considera que sus ciudadanos deben poder vivir una vida digital con seguridad. Por ello, resalta en sus avances en materia de ciberseguridad, considerando especialmente que su economía, democracia y sociedad dependen más que nunca de herramientas digitales o productos y servicios conectados que deben mantenerse seguras y viables para proteger la conectividad que estas mismas le ofrece[126].

En ese sentido, en el 2004 se creó la ENISA como agencia especializada en materia de ciberseguridad de la UE con la misión de velar por un alto nivel común de ciberseguridad en toda Europa. En la práctica, la ENISA contribuye a la política de seguridad cibernética de la UE mejorando la fiabilidad de los productos, servicios y procesos de las tecnologías de la información y comunicación mediante programas de certificación de la ciberseguridad y la cooperación con Estados miembros y organismos de la UE[127].

Así, la ENISA ayuda a los países de la UE prepararse para los futuros desafíos en materia de ciberseguridad. Para ello, se basa en el intercambio de conocimientos, la creación de capacidades y la sensibilización para fortalecer la confianza entre los miembros de la UE y generar mayor resiliencia en sus infraestructuras, con el fin último de proteger a la sociedad y a la ciudadanía europea de las amenazas digitales[128].

Evidentemente, el énfasis que tiene la ENISA es la ciberseguridad y no la ciberdefensa como es el caso del CCDCOE. La preocupación de la ENISA es la actividad de los

[126] Unión Europea [UE], 2021.
[127] ENISA, 2021a.
[128] *Ibid.*

ciberdelincuentes y la amenaza constante que supone para la seguridad interna de la UE y para la seguridad en línea de sus ciudadanos, cada vez más interconectados. Además, la actual pandemia por COVID-19 ha llevado a que más personas lleven a cabo sus actividades diarias en línea, lo cual ha tenido como efecto que la actividad de la ciberdelincuencia también incremente[129].

En el último documento de Panorama de Amenazas de ENISA, elaborado en octubre de 2020, se identificaron los principales ciberdelitos que afectan a la UE. En orden de importancia, estos son el *malware*; ataques basados en web; *phishing*; ataques a aplicaciones web; spam; DDoS; robo de identidad; filtración de datos; amenazas internas; *botnets*; manipulación, daño o robo físico; filtración de información; *ransomware*; ciberespionaje; y *cryptohacking*[130].

Asimismo, se consideran como retos en ciberseguridad, de manera general, la necesidad de reforzar la resiliencia; la compartición de información, análisis y respuesta conjunta; la seguridad de la cadena de suministro; el resurgimiento de la IA; la computación cuántica y criptográfica; la escasez de gente formada; la 'ciber-higiene'; la vulnerabilidad de las organizaciones más pequeñas como pequeñas y medianas empresas (PYMES); la comercialización de la investigación y el desarrollo (I+D); y el alineamiento de la investigación, el despliegue, las policías y la regulación[131].

Considerando las amenazas y los retos mencionados, la ENISA despliega una serie de actividades dispuestas en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo. De estas actividades, la principal es la capacitación a comunidades. De acuerdo a la ENISA, la ciberseguridad es una responsabilidad compartida, y es justamente esta institución la que juega un rol clave al estimular la cooperación activa entre las partes encargadas e interesadas en la ciberseguridad dentro de los Estados

[129] *Ibid.*
[130] Unión Europea [UE], 2021.
[131] *Ibid.*

miembros con las otras instituciones y agencias de la UE. Así, se busca generar sinergias y que se utilice de manera eficaz los conocimientos técnicos y los recursos limitados en materia de ciberseguridad[132].

En ese sentido, la ENISA también fomenta la inversión por parte de la UE en la creación de capacidades y talentos en materia de ciberseguridad en todos los niveles. Esto incluye crear capacidades y conocimientos desde el personal no especializado hasta el profesional altamente cualificado, ya que todos pueden ser objeto de amenazas cibernéticas. Asimismo, la inversión debe realizarse también para garantizar que las diferentes comunidades operativas cuenten con los medios y equipos tecnológicos y físicos adecuados para abordar estas amenazas cibernéticas[133].

Esto viene acompañado del fomento de la elaboración y ejecución de políticas en materia de ciberseguridad, ya que se considera que la ciberseguridad no debe estar limitada a una comunidad especializada de expertos técnicos, sino que debe estar integrada de manera transversal en todos los ámbitos de las políticas de la UE. Por esta razón, la ENISA vela por evitar la fragmentación de iniciativas y contar con un enfoque cohesivo y coherente que además tome en cuenta las características particulares de cada sector[134].

Asimismo, la ENISA realiza análisis de prospectiva en materia de nuevas tecnologías, las cuales suponen nuevas amenazas y oportunidades. Por ello, la ENISA fomenta que se mejore la resiliencia de la UE frente a las futuras amenazas para la ciberseguridad, como se ha mencionado anteriormente. Esto también implica que se lleve a cabo un continuo proceso de recojo, organización, resumen, análisis, comunicación y mantenimiento del conocimiento y de la información en materia de ciberseguridad con el fin de que se comparta y expanda dentro de la UE[135].

[132] ENISA, 2021a.
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*

Operativamente, la ENISA coopera y apoya a operaciones cibernéticas reales para que los Estados miembros y las instituciones de la UE puedan lograr respuestas más rápidas y coordinadas a todos los niveles: estratégico, operativo, técnico y comunicativo. Nuevamente, esto se basa en el principio que recoge la ENISA acerca de la necesidad de trabajar conjuntamente frente a las amenazas en el ciberespacio debido a la natural interdependencia transfronteriza entre los miembros de la UE y que "los ciberataques no conocen fronteras", por lo que pueden afectar negativamente a todas las capas de la sociedad, sobre todo si se trata de ciberataques masivos.[136]

En ese sentido, la ENISA trabaja conjuntamente con el Equipo de Respuesta ante Emergencia Informáticas de la Unión Europa (CERT-EU, por sus siglas en inglés)[137], encargada de la ciberseguridad de las principales instituciones de la UE como la Comisión Europea, la Secretaría General del Consejo, el Parlamento Europeo, el Comité de las Regiones, y el Comité Económico y Social[138]. Adicionalmente, la ENISA coordina con los CSIRT de cada Estado miembro de la UE, que, de igual manera, están encargadas del desarrollo de medidas de prevención y respuesta ante incidencias cibernéticas en los sistemas de información de sus países[139].

Por otro lado, la ENISA organiza los ejercicios paneuropeos *Cyber Europe*, que reúne a los sectores privado y público de los Estados miembros de la UE y de la Asociación Europea de Libre Cambio (AELC o EFTA, por sus siglas en inglés) en simulaciones a gran escala de incidentes cibernéticos que escalan hasta convertirse en ciber crisis. Estos ejercicios sirven para aprender a gestionar la continuidad de las empresas y la gestión de crisis en casos de incidentes cibernéticos técnicamente avanzados. Los escenarios se inspiran en eventos reales y son desarrollados por expertos europeos en ciberseguridad. *Cyber Europe* se lleva a cabo cada dos años desde el 2010, siendo la edición del 2018 la más reciente[140].

---

[136] *Ibid.*
[137] Oficina de Publicaciones de la Unión Europea, s/f.
[138] Equipo de Respuesta ante Emergencia Informáticas de la Unión Europa [CERT-EU], s/f.
[139] Oficina de Publicaciones de la Unión Europea, s/f.
[140] ENISA, 2021c.

Debido a la pandemia por COVID-19, *Cyber Europe 2020* (CE2020) tuvo que ser postergada. Esta edición se centrará en escenarios que giren alrededor de temas como la salud pública, e incluirán a gobiernos nacionales, sus CSIRTs, autoridades en ciberseguridad, ministerios de salud, organizaciones de salud como hospitales y clínicas, proveedores de servicio de salud electrónica (*eHealth*), y aseguradoras de salud. Los incidentes en el ejercicio irán incrementando a todos los niveles de crisis: desde local y organizacional hasta nacional y europeo[141], lo cual pondrá a prueba las capacidades de respuesta de las instituciones involucradas.

2.3.2. Red de Equipos de Respuesta ante Incidencias de Seguridad Informática (CSIRTs)

La UE cuenta con una Red de CSIRTs compuesta por los CSIRT acreditados por los Estados miembros de la organización y el CERT-EU. La Comisión Europea participa como observador en dicha red, mientras que la ENISA tiene la tarea de apoyar activamente en la cooperación de los CSIRT para proveer a la UE de la capacidad de coordinación en caso de un incidente cibernético. La Red de CSIRTs ofrece también un foro en el que los miembros pueden cooperar, intercambiar información y generar confianza entre ellos. Así, sus participantes podrán tener la capacidad de manejar incidentes transfronterizos y discutir cómo responderán de manera coordinada ante incidentes específicos[142].

Cabe mencionar que además de los CSIRTs nacionales y la Red de CSIRTs de la UE, existen grupos de CSIRTs de algunos países europeos que no necesariamente abarcan la totalidad de la Unión. Por ejemplo, los que enmarcan dentro de la Cooperación Estructurada Permanente (PESCO, por sus siglas en inglés)[143], que busca la

[141] ENISA, 2021d.
[142] CSIRTs Network, s/f.
[143] Cooperación Estructurada Permanente [PESCO], s/f.

integración estructural de las fuerzas armadas de la mayoría de los Estados miembros de acuerdo a la Política Común de Seguridad y Defensa de la Unión Europea (PCSD).

En cuanto a las Red de CSIRTs de la UE, los CSIRTs que la componen pertenecen tanto al sector público como privado de los Estados miembros y provienen del sector gubernamental, militar, financiero, policial, energético, entre otros. Asimismo, operan protegiendo los sistemas de servicios esenciales como transporte aéreo, marítimo y terrestre, salud, agua y suministro y distribución de agua, infraestructuras digitales, petróleo, gas, mercado financiero, entre otros[144].

Esta red de CSIRTs existe desde que se adoptó la Directiva (EU) 2016/1148 sobre seguridad de redes y sistemas de información (*NIS Directive*, por sus siglas en inglés) en el año 2016, que representa la primera norma en ciberseguridad que abarca a toda la UE. Esta directiva tiene como objetivo asegurar un alto nivel común de seguridad en las redes y los sistemas de información dentro de la UE, mediante el incremento de las capacidades de ciberseguridad a nivel nacional, la cooperación, la gestión de riesgos dentro de la UE y la obligación de los operadores de servicios esenciales y proveedores de servicios digitales de reportar incidentes que los afecten[145].

Específicamente, el artículo 12 de la directiva establece que la Red de CSIRTs tiene el deber de contribuir al desarrollo de la confianza entre Estados miembros y de promover una rápida y efectiva cooperación operacional"[146]. Asimismo, la directiva busca mejorar la preparación de los Estados miembros al requerirles que estén debidamente equipados con, por ejemplo, un CSIRT y una autoridad competente que supervise la aplicación de la propia directiva[147].

Adicionalmente, la directiva incentiva la cooperación entre los Estados miembros de la UE al crear, mediante su artículo 11, un Grupo de Cooperación NIS, que tiene como

[144] CSIRTs Network, s/f.
[145] *Ibid.*
[146] *Ibid.*
[147] Comisión Europea, s/f.

objetivo apoyar y facilitar la cooperación estratégica y el intercambio de información entre los miembros. Este Grupo de Cooperación provee de lineamientos estratégicos a la Red de CSIRTs, y éste, a su vez, sirve como apoyo operacional del Grupo de Cooperación. Asimismo, el Grupo de Cooperación NIS trabaja de cerca con la Red de Cooperación Europea para Elecciones de la Comisión Europea[148].

Dicha Red de Cooperación Europea para Elecciones fue creada con el objetivo de proteger las elecciones al Parlamento Europeo del 2019, y hoy en día, junto al Grupo de Cooperación NIS[149], trabajan para hacer frente a amenazas a procesos electorales de la UE, en temas como protección de datos, ciberseguridad, transparencia y sensibilización[150]. También ayuda a diseminar información y alertas relevantes, como parte del Plan de Acción Europeo para la Democracia que busca hacer frente a amenazas presentes especialmente en tiempos electorales como el extremismo, la interferencia externa, la manipulación de información y amenazas contra periodistas[151].

Por otro lado, el Grupo de Cooperación NIS publica una serie de documentos en forma de compendios, lineamientos, reportes y documentos de referencia acerca de medidas de seguridad que adoptan operadores de servicios esenciales, la identificación de estos operadores, tecnologías para las elecciones, reportes anuales de incidentes, la ciberseguridad en redes 5G, entre otros[152].

Todo esto se enmarca dentro de otro objetivo de la Directiva NIS: Promover y consolidar una cultura de seguridad a través de todos los sectores que son vitales para la economía y la sociedad que depende fuertemente de las TIC, tales como el energético, el de transportes, el de agua, la banca, las infraestructuras del mercado financiero, la salud y la infraestructura digital.

[148] *Ibid.*
[149] *Ibid.*
[150] Comisión Europea, 2021a.
[151] Comisión Europea, 2020a.
[152] Comisión Europea, 2021c.

De este modo, las entidades privadas identificadas por los Estados miembros como operadores de servicios esenciales en los sectores mencionados tienen la obligación de adaptar sus medidas de seguridad a los lineamientos de la directiva, e informar a las autoridades nacionales en caso de que se presenten incidentes serios. Esto último implica que servicios específicos como proveedores clave de servicios digitales, como motores de búsqueda, servicios de computación en la nube y mercados virtuales se adapten a los requerimientos de seguridad establecidos en la directiva[153].

Para facilitar la implementación de la Directiva NIS a lo largo y ancho de la UE, la Comisión Europea emitió una Comunicación oficial (COM/2017/0476) conocida como la "Caja de herramientas NIS". Este documento provee de información práctica a los Estados miembros acerca de la misma Directiva NIS, presentando las mejores prácticas de la implementación de la misma en otros Estados miembros, con explicaciones detalladas e interpretaciones para clarificar cómo es que la directiva debe funcionar en la práctica[154].

Por otro lado, el artículo 23 de la misma Directiva NIS indica que la Comisión Europea debe revisar periódicamente su funcionamiento. Esto responde al objetivo de política de hacer que Europa esté lista para desenvolverse en esta era digital en línea con los objetivos de seguridad de la Unión. En ese sentido en el 2020 se llevó a cabo un proceso de consulta y revisión para evaluar el impacto de la directiva. Como resultado, se presentó una propuesta legislativa en diciembre de 2020: la NIS2[155].

En general, la NIS2 busca actualizar a la actual Directiva NIS, enmendando algunas de sus fallas y volviéndola más apta para cambios que vendrán en el futuro. Asimismo, expande su ámbito de aplicación al incluir a medianas y grandes empresas como sectores que deben seguir los lineamientos de la directiva, así como también le otorga

[153] Comisión Europea, s/f.
[154] *Ibid.*
[155] *Ibid.*

mayor flexibilidad a los Estados miembros de identificar entidades pequeñas con perfiles de riesgo alto[156].

La propuesta también elimina la distinción entre operadores de servicios esenciales y los proveedores de servicios digitales[157], ya que dicha división carece de sentido al tomar en cuenta que hay servicios digitales que son, justamente, esenciales. Asimismo, la propuesta fortalece los requerimientos de seguridad para las empresas al imponer un método de gestión de riesgos con una lista de elementos básicos de seguridad que deben ser aplicadas, incluyendo precisiones más específicas para el reporte de incidentes, el contenido de los reportes y cronogramas[158].

Asimismo, la Comisión propuso que se incluya la seguridad de las cadenas de suministros, sobre todo para lo referido a información clave y tecnologías de comunicación. En ese sentido, los Estados miembros de la UE, en cooperación con la Comisión Europea y ENISA, llevarían a cabo evaluaciones de riesgo de cadenas de suministros críticos. La propuesta también incluye medidas de supervisión más estrictas para autoridades nacionales, y fortalece el rol del Grupo de Cooperación en el diseño de políticas estratégicas de decisión sobre tecnologías emergentes y nuevas tendencias, buscando que se incremente la cooperación entre autoridades de los Estados miembros y el compartir de información[159].

La aprobación de la propuesta NIS2 sigue pendiente por parte del Parlamento Europeo. Una vez adoptada, los Estados miembros de la UE tendrían dieciocho meses para aplicarla efectivamente[160].

[156] Comisión Europea, 2020b.
[157] *Ibid.*
[158] *Ibid.*
[159] *Ibid.*
[160] *Ibid.*

2.3.3. Unidad Cibernética Conjunta (JCU)

La creciente cantidad de ataques cibernéticos que han afectado a los Estados miembros de la UE ha llevado a que la Comisión Europea proponga recientemente la creación de una Unidad Cibernética Conjunta (JCU, por sus siglas en inglés)[161]. Los ciberataques que han afectado a la UE han variado desde ataques a instituciones oficiales y privadas hasta casos de espionaje a altas autoridades nacionales.

Entre los más resaltantes, en el presente año la Agencia Europea de Medicamentos (EMA, por sus siglas en inglés) fue atacada por cibercriminales que manipularon información de vacunas contra la COVID-19[162]; se reportaron campañas de ciberespionaje a autoridades nacionales como el ministro del interior de Bélgica y docenas de políticos de Polonia; y fueron atacadas con *ransomware* hospitales en Irlanda y Francia[163].

Operativamente, la mayoría de los Estados miembros deben responder individualmente a los ataques en sus países, y sus capacidades varían bastante de uno a otro[164]. En ese sentido, la JCU, en coordinación con la ENISA, trabajará para ayudar a comunidades de ciberdefensa militar, diplomática, de seguridad interna y civil para prevenir, disuadir y responder a ciberataques. De este modo, la JCU se beneficiará de contar con la experiencia de todos los actores relevantes en el campo de la ciberseguridad, y todos los involucrados estarán en la capacidad de actuar rápidamente contra amenazas cibernéticas y de movilizar recursos para apoyarse mutuamente[165].

Las acciones clave de la JCU incluirán crear una plataforma física alrededor de la sede de la ENISA y oficinas adyacentes de CERT-EU en Bruselas, establecer una plataforma virtual compuesta de herramientas para compartir información de forma

[161] Politico, 2021b.
[162] Politico, 2021a.
[163] Politico, 2021b.
[164] *Ibid.*
[165] Comisión Europea, 2021b.

rápida y segura, elaborar un plan de respuesta para crisis e incidentes de ciberseguridad para la UE, producir reportes de situación sobre la ciberseguridad de la UE que incluyan información e inteligencia acerca de amenazas e incidentes, y establecer y movilizar a los CSIRTs[166].

Asimismo, la JCU buscará llegar a memorandos de entendimiento para la cooperación y la asistencia mutua entre sus miembros, llegar a acuerdos de cooperación operacional con empresas del sector privado y proveedores y usuarios de servicios y soluciones de ciberseguridad, conformar un inventario de las capacidades operacionales y técnicas de la UE, definir sinergias estructuradas con capacidades avanzadas de detección, y establecer un plan multianual para coordinar ejercicios y organizar entrenamientos conjuntos[167].

Se espera que la JCU esté operativa entre los años 2022 y 2023. Esta iniciativa es pionera a nivel internacional al buscar dotar a una organización supranacional como la UE de capacidades operacionales conjuntas en materia de ciberseguridad. Así, el JCU vendría a ser la contraparte de ciberseguridad del CCDCOE, que está más enfocado a la ciberdefensa por provenir de la OTAN. De este modo, el CCDCOE de la OTAN y la planificada JCU de la UE le proveerían a Europa de dos entidades con plenas capacidades operacionales para defender al continente de ataques cibernéticos en materia de seguridad y defensa.

En ese sentido, Europa, mediante las entidades mencionadas de la OTAN y de la UE, sería el continente más avanzado en materia de ciberseguridad y ciberdefensa conjunta. Los esfuerzos de los países europeos por ser la vanguardia en el desarrollo de capacidades y tecnologías en dichas materias no se detienen ahí, ya que también existen centros de excelencia dedicados a la ciberseguridad y a las amenazas híbridas.

[166] *Ibid.*
[167] *Ibid.*

2.3.4. Centro Europeo de Excelencia para la Lucha contras las Amenazas Híbridas (*Hybrid CoE*)

Con sede en Helsinki, el *Hybrid CoE* fue fundada en el 2017 por 16 países de la UE y OTAN. Hoy en día está conformada por treinta Estados y tiene como objetivos generales concientizar acerca de las amenazas híbridas, compartir experiencias y mejores prácticas, facilitar el establecimiento de redes y ser líder en la discusión europea acerca de las amenazas híbridas.

El *Hybrid CoE* es independiente en su funcionamiento, en tanto no es parte de la estructura de la UE ni de la OTAN. Finlandia, como país sede, paga la mitad de su presupuesto, y la otra mitad es pagada por los Estados miembros del centro de excelencia. De este modo, no depende de otros países u organizaciones.

Este centro de excelencia trabaja bajo el principio de que es necesario el trabajo conjunto para hacer frente a las amenazas híbridas, ya que, si un país es objeto de un ataque o amenaza híbrida, lo más probable es que sea direccionado también a otro país. Cabe resaltar que su enfoque está en la zona del Euro-Atlántico, aunque el mismo centro de excelencia ha manifestado que este enfoque puede ser expandido para incluir a países de otras regiones y que no pertenezcan a la UE ni la OTAN. No obstante, por el momento países como el Perú pueden cooperar con el *Hybrid CoE*, pero no ser parte integral de ella. Aun así, el Perú es el primer país de América Latina que ha tenido contacto oficial con el centro de excelencia.

Cabe resaltar que este centro de excelencia es una organización que trabaja en el nivel estratégico. No tiene la capacidad operativa de reaccionar a ataques cibernéticos, lo cual tampoco es su objetivo. El *Hybrid CoE* se dedica a la investigación y el análisis del escenario internacional actual para identificar los controladores del entorno de amenazas. Hay cuatro controladores o factores generales. En primer lugar, el retorno de la competencia de los grandes poderes mundiales, que crea nuevas posibilidades de

conflicto entre grandes potencias y sus aliados en todos los campos del poder, incluyendo el económico, político, militar, y cibernético.

El segundo controlador viene a ser lo que el *Hybrid CoE* denomina la democratización de la guerra, ya que, si bien los ciberataques más sofisticados provienen de Estados poderosos, hoy en día otros Estados y actores no estatales pueden representar amenazas híbridas. En tercer lugar, el rol de las nuevas tecnologías, cuyo desarrollo y uso masivo generan nuevos espacios posibles en los que puedan tener efectos las amenazas híbridas.

Finalmente, el cuarto controlador sería la COVID-19, que ha obligado a la humanidad a interconectarse más y a trasladar sus actividades al ciberespacio, que evidentemente no está exento de amenazas cibernéticas e híbridas, y ha sido a raíz de la pandemia que se han incrementado notablemente los esfuerzos de desestabilización en Europa.

En este nuevo ambiente, las amenazas híbridas se manifiestan como una combinación de las ya conocidas amenazas a la seguridad de los Estados y sus poblaciones. Así, el *Hybrid CoE* conceptualiza a las amenazas híbridas como acciones coordinadas y deliberadas que atacan vulnerabilidades sistémicas de Estados e instituciones a través de una amplia variedad de medios. Estas actividades explotan las capacidades de detección y atribución, así como las fronteras entre guerra y paz, lo interno y lo externo, lo militar y lo civil, y lo público y lo privado.

De este modo, el objetivo de las amenazas híbridas es influenciar en la toma de decisiones para favorecer los intereses estratégicos del agente híbrido mientras que daña o minimiza las capacidades de la víctima. Los medios para esto incluyen ciberataques, desinformación, medios militares, atentados contra infraestructura, manipular el derecho internacional en favor de intereses particulares, entre otros. Así, las amenazas híbridas también pueden generar inestabilidad social dentro de un país, creando un problema o agudizando uno que ya existe en la esfera doméstica del mismo.

Por ejemplo, el *Hybrid CoE* identifica como principales actores híbridos a Rusia y a China, seguidos por países más pequeños como Irán.

Ante esto, el centro de excelencia busca generar resiliencia y capacidad de disuasión en las sociedades de sus miembros, y lo busca hacer mediante aproximaciones comprensivas e integradas a los problemas, procesos democráticos y estructurados, y multilateralización. Así, busca consolidar la preparación, las capacidades, la legislación y la comunicación necesaria para dichos objetivos. También se busca preparar a la ciudadanía para que puedan hacer frente, en tanto sus capacidades les permitan, a las amenazas híbridas en caso de que se enfrenten a ellas. Según el centro de excelencia, esto tomaría por lo menos cerca de 10 a 20 años, mediante educación y la generación de un fuerte sentimiento de ciudadanía.

En la actualidad, el *Hybrid CoE* se encuentra en la fase de realización de investigaciones y reportes y de concientización en autoridades políticas de los Estados miembros. Para lo que resta del año 2021, se tiene planificado publicar reportes de análisis completos sobre la disuasión de amenazas híbridas; futuras tecnologías; estudios regionales como el Ártico, Europa del Norte y Europa del Sur; actores no estatales que sirven a otros Estados; la salvaguardia de procesos democráticos; la aviación y el espacio exterior; y resiliencia legal. Estos productos estarán disponibles mediante listas de suscripción y boletines informativos.

2.4. Organización de los Estados Americanos (OEA)

La OEA no posee el nivel de desarrollo en materia de ciberseguridad, ciberdefensa y amenazas híbridas similar ni cercano a la de las instituciones europeas descritas anteriormente. No obstante, la OEA cuenta con una Declaración sobre Seguridad en las Américas del año 2003 que sirve como marco normativo para futuros esfuerzos en materia de ciberseguridad; y el Comité Interamericano contra el Terrorismo (CICTE) de la OEA cuenta con un Programa de Ciberseguridad que tiene como objetivo el

fortalecimiento de la capacidad técnica y el desarrollo de políticas de ciberseguridad en las Américas[168].

También se han realizado estudios conjuntos con otras entidades como el Banco Interamericano de Desarrollo (BID) que evalúan la situación de la ciberseguridad en la región.

2.4.1. Declaración sobre Seguridad en las Américas

Aprobada en el marco de la Conferencia Especial sobre Seguridad realizada en Ciudad de México el año 2003, la Declaración sobre Seguridad en las Américas amplía el concepto tradicional de amenaza tradicional a la seguridad de los Estados y presenta una nueva concepción de la seguridad en el hemisferio, de alcance multidimensional y que incluye a las amenazas no convencionales[169].

En el artículo 4 de la declaración, se hace referencia a las "nuevas amenazas, preocupaciones y otros desafíos" a la seguridad hemisférica como problemas intersectoriales que requieren respuestas diversas por parte de las distintas organizaciones nacionales, incluyendo asociaciones entre los gobiernos, el sector privado y la sociedad civil. Entre dichas amenazas se encuentran las amenazas no convencionales o asimétricas descritas en el primer capítulo de la presente tesis, incluyendo a las amenazas a la seguridad cibernética[170].

En ese sentido, en el artículo 23 de la declaración se hace mención al compromiso de formar en los países del hemisferio las capacidades para prevenir, sancionar y eliminar el terrorismo. Para ello, la declaración propone fortalecer el CICTE y la cooperación bilateral, subregional y hemisférica a través del intercambio de información, asistencia

[168] Organización de los Estados Americanos [OEA], 2021.
[169] Organización de los Estados Americanos [OEA], 2003, p. 2.
[170] *Ibid*, p. 4.

mutua y el impedimento a la circulación internacional de terroristas. Asimismo, mediante la declaración los países de la OEA se comprometen a identificar y combatir las amenazas terroristas emergentes, tales como las amenazas a la seguridad cibernética, el terrorismo biológico y amenazas a la IC[171].

Específicamente sobre el tema de ciberseguridad, el artículo 29 menciona que se desarrollará una cultura de seguridad cibernética en las Américas mediante la adopción de medidas de prevención eficaces para prevenir, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, y para luchar contra las amenazas cibernéticas y la delincuencia cibernética. Esto se lograría mediante la tipificación de los ataques contra el espacio cibernético, la protección de IC, y el aseguramiento de las redes de sus sistemas; dentro de una estrategia integral sobre seguridad cibernética[172].

La Declaración sobre Seguridad en las Américas, entonces, representa el primer paso a nivel normativo para que se lleven a cabo esfuerzos hemisféricos para hacer frente a las amenazas a la ciberseguridad de los países de la OEA, al identificarlas precisamente como nuevas amenazas a la seguridad y la IC de los Estados americanos

2.4.2. Comité Interamericano contra el Terrorismo (CICTE)

El CICTE cuenta con un Programa de Ciberseguridad que lidera la provisión de iniciativas de investigación, el fortalecimiento de la capacidad técnica y el desarrollo de políticas de ciberseguridad en la OEA. En ese sentido el programa trabaja en base a tres ejes: el desarrollo de políticas; el desarrollo de capacidades, que incluye capacitación y la realización de ejercicios cibernéticos; y la investigación y divulgación.[173].

[171] *Ibid*, p. 9.
[172] *Ibid*, pp. 9-10.
[173] OEA, 2021.

En primer lugar, el desarrollo de políticas está enfocado a ayudar a los Estados miembros de la OEA a desarrollar estrategias nacionales y regionales de ciberseguridad que involucren a todas las partes relevantes que estén interesadas y que se ajusten a la realidad legislativa, cultural, económica y estructural de cada país. Asimismo, el programa apoya el desarrollo de medidas de fomento de la confianza en el ciberespacio[174].

En segundo lugar, la creación de capacidades del programa busca establecer y desarrollar las capacidades de los CSIRTs existentes en la región, y brindar asistencia técnica personalizada y oportunidades de ejercicio para fortalecer las instituciones y organizaciones nacionales y regionales. En tercer lugar, la investigación y divulgación se centra en el desarrollo de documentos técnicos, conjuntos de herramientas e informes basados en investigaciones que sirvan para guiar a los responsables de políticas o tomadores de decisiones, a los CSIRTs, a los operadores de infraestructura, a las organizaciones privadas y la sociedad civil[175].

De esta manera, el Programa de Ciberseguridad busca cumplir con los siguientes objetivos:

a) Apoyar a los Estados miembros de la OEA en el desarrollo de capacidades técnicas y políticas para efectivamente prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
b) Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
c) Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet[176].

[174] *Ibid.*
[175] *Ibid.*
[176] *Ibid.*

Este programa ha tenido resultados favorables para la ciberseguridad en el hemisferio. De acuerdo a datos de la propia OEA, se ha entrenado a más de 20,000 ciudadanos y funcionarios del sector público y privado, se ha apoyado en la elaboración de 11 Estrategias Nacionales de Ciberseguridad, se ha llevado a cabo 14 ejercicios cibernéticos en la región (8 nacionales y 6 internacionales), y se ha apoyado para que la cantidad de CSIRTs nacionales aumente de 4 a 21[177].

Asimismo, el Programa de Ciberseguridad cuenta con una red de CSIRTs conocida como *CSIRT Americas*, una iniciativa que une a los CSIRTs del hemisferio bajo cuatro objetivos compartidos: la promoción de la colaboración y la integración de los CSIRTs; compartir información sobre ciberataques, patrones de amenazas y análisis sobre herramientas de respuesta ante incidentes para los CSIRTs; la promoción de la creación de más CSIRTs y el apoyo a los que han sido recientemente establecidos; y el diseño de proyectos técnicos que apuntan a mejorar los servicios ofrecidos por los CSIRTs existentes[178].

Esta red de CSIRTs está conformada por CSIRTs nacionales, de defensa, policiales y de gobierno pertenecientes a todos los países de la OEA[179].

Adicionalmente, el CICTE celebra reuniones anuales con el fin de fomentar el diálogo y promover el intercambio de experiencias y prácticas tendientes a prevenir y contrarrestar el terrorismo en el hemisferio, incluyendo amenazas cibernéticas. La más reciente reunión se llevó a cabo en septiembre de 2020 de manera virtual, en la que se aprobó un plan de trabajo para el periodo 2020-2021 que incluye lineamientos para diferentes programas, incluyendo el de ciberseguridad[180].

Lo novedoso del plan de trabajo 2020-2021 es la inclusión de temas como la capacitación a jóvenes y mujeres en ciberseguridad a través de programas específicos

[177] *Ibid*.
[178] CSIRT Americas, 2016.
[179] *Ibid.*
[180] Comité Interamericano contra el Terrorismo [CICTE], 2020.

que buscan promover mayor diversidad y empleabilidad en la industria de la ciberseguridad; y el apoyo al desarrollo y fortalecimiento de capacidades de los Estados miembros en materia de ciberdiplomacia a través de la realización de seminarios, conferencias y talleres, y actividades de intercambio de experiencias en ciberdiplomacia, ciberseguridad y ciberespacio[181].

Finalmente, el CICTE publica constantemente trabajos de análisis y reportes sobre la situación de la ciberseguridad en la región, y organiza eventos y talleres virtuales orientados al público en general de los países de la OEA para capacitarlos y concientizarlos en materia de ciberseguridad, infraestructuras críticas y temas relacionados.

3. Situación de la ciberseguridad, ciberdefensa y amenazas híbridas en potencias cibernéticas mundiales

Las grandes potencias mundiales como Estados Unidos (EE.UU.), Rusia y China cuentan con avanzadas capacidades para llevar a cabo la ciberguerra en función de sus intereses. Estos países llevan a cabo constantes operaciones cibernéticas ofensivas y defensivas que, dependiendo de la naturaleza y el objetivo de éstas, pueden considerarse dentro del espectro de amenazas híbridas desarrolladas en el primer capítulo, ya que no sólo buscan afectar las capacidades militares convencionales de su rival, sino también influir en la toma de decisiones de alto nivel o en la opinión pública, infiltrarse y espiar sobre el adversario, sabotear sistemas esenciales de su sociedad civil, generar desorden social y político, entre otros objetivos.

Conscientes de este nuevo tipo de enfrentamiento y competencia entre Estados en lo que viene a ser el quinto dominio de la guerra, y diluyendo cada vez más la ya delgada línea en lo que se define como tiempos de conflicto o tiempos de paz, estos países han creado unidades operacionales dedicadas exclusivamente a la guerra o defensa en el

[181] *Ibid.*

ciberespacio, o utilizan actores no estatales con capacidades cibernéticas que puedan cumplir con sus intereses en dicho dominio.

3.1. Estados Unidos de América (EE.UU.)

El Cibercomando de Estados Unidos (USCYBERCOM o USCC, por sus siglas en inglés) es el comando de combate dentro del Departamento de Defensa de los Estados Unidos encargado de la ciberdefensa del país. Creado en el 2009, tiene como misión velar por los intereses de EE.UU. o sus aliados mediante el uso de técnicas informáticas o cibernéticas. Esto incluye la protección de sistemas informáticos, acciones de respuesta rápida frente a ataques e incidentes cibernéticos, y la ejecución de ataques y operaciones cibernéticas para defender sus intereses.

Esta entidad trabaja de cerca con la Agencia de Seguridad Nacional de los EE.UU. (NSA, por sus siglas en inglés), institución que ha solido compartir el mismo director general con el USCC desde su fundación. Este trabajo conjunto se debe a que la naturaleza del USCC le permite proveer de gran cantidad de información y data a la NSA para que sea procesada en sus actividades de inteligencia, lo cual viene a ser el objetivo mismo de la NSA, especialmente la referida a la inteligencia de señales (SIGINT, por sus siglas en inglés).

El USCC menciona explícitamente que tiene como misión planear, coordinar, integrar, sincronizar y conducir actividades para dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios y asegurar la libertad de acciones a los EE.UU. y sus aliados en aquel dominio e impedir lo mismo a sus adversarios.

Así, se puede evidenciar que existe un claro entendimiento en el USCC de que las operaciones cibernéticas pueden servir de apoyo a otras operaciones y acciones, no necesariamente de índole militar, para el cumplimiento de otros objetivos. Esto, de acuerdo a la conceptualización realizada anteriormente acerca de las amenazas híbridas, convertiría a los EE.UU. en un actor estatal capaz de llevar a cabo ataques híbridos. Evidentemente, también es un actor consciente de la existencia de amenazas híbridas que se pueden manifestar en el dominio del ciberespacio, lo cual refleja que es un Estado con capacidades suficientes para atacar y defenderse de amenazas cibernéticas e híbridas.

De hecho, la Estrategia de Seguridad Nacional (NSS, por sus siglas en inglés) del 2017 hace mención al hecho de que "la línea divisoria entre la guerra y la paz es borrosa".[182] Una sección de dicha estrategia, titulada "Preservar la Paz mediante la Fuerza", describe implícitamente a las amenazas híbridas, al referirse a las acciones de la "zona gris del conflicto" como métodos utilizados por los Estados que integran medios económicos, militares y, especialmente, informacionales, para cumplir con sus objetivos, lo cual configura esencialmente una amenaza contra los EE.UU. cuando se trata de Estados adversarios, y que además buscan imposibilitar una respuesta militar convencional por parte de EE.UU. para poder defenderse[183].

Incluso se hace referencia a que los Estados pueden aprovecharse del derecho internacional, abusando de ambigüedades legales, imponiendo normas o violándolas para beneficio propio, creando un ambiente legalmente asimétrico en el que estos Estados se ven beneficiados frente a los Estados que sí cumplen el derecho internacional, aunque no sea a su favor[184].

Es necesario recalcar que el USCC no es el único órgano dedicado a la ciberguerra en EE.UU. Mientras que el USCC tiene un énfasis militar y está compuesta por fuerzas

[182] Sari, A. y Lauva, A., 2018.
[183] *Ibid.*
[184] *Ibid.*

cibernéticas del Ejército, de la Armada, de la Fuerza Aérea y del Cuerpo de Marines de los Estados Unidos; existen dieciocho agencias de inteligencia que también cuentan con brazos operacionales dedicados a operaciones de ciberseguridad. Asimismo, algunas de estas agencias, como la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), cuentan con capacidades operacionales ofensivas propias.

Así, la existencia de una gran variedad de agencias de inteligencia y entidades de defensa con capacidades en ciberseguridad, con diversos objetivos y formas de actuar, aunque todos apuntando a defender los intereses de los EE.UU., sumado a la existencia de estrategias de seguridad nacionales que comprenden la realidad de las amenazas híbridas y de las posibles amenazas en el ciberespacio, convierte a este país en uno de los más avanzados en ciberseguridad, ciberdefensa y amenazas híbridas; siendo capaz de llevar a cabo un gran espectro de operaciones de índole ofensiva y defensiva en los tres aspectos.

En la práctica es reconocida la capacidad de los EE.UU. en dicha materia, ya que es uno de los pocos países capaces de llevar a cabo ciberataques, guerra psicológica, operaciones de inteligencia, sabotaje, espionaje, destrucción de objetivos específicos y ciberoperaciones de apoyo a operaciones militares convencionales; todas a gran escala y sustentadas con medios tecnológicos sofisticados.

3.2. Federación Rusa

No existe gran cantidad de información disponible en fuentes abiertas acerca de la forma en que se organizan las entidades rusas encargadas de llevar a cabo ciberoperaciones ofensivas y defensivas. No obstante, la gran cantidad de ciberataques provenientes de Rusia y los objetivos que presumiblemente han tenido, han permitido demostrar que sí existe una estrategia rusa para su accionar en el ciberespacio. Un aspecto importante a considerar es que Rusia usualmente se reúsa a cooperar en investigaciones policiales relacionados al cibercrimen y que se opone iniciativas

internacionales que buscan penalizar la ciberdelincuencia como el Convenio de Budapest.

En cuanto a su modo de operar en el ciberespacio, se diferencia del accionar de otras potencias como EE.UU. y China que se caracterizan por llevar a cabo acciones encubiertas y quirúrgicas con fines de espionaje, ya que los ciberataques rusos han sido notorios por su gran visibilidad. Ejemplo de ello fue el ataque masivo a infraestructura cibernética de Estonia en el 2007. Esto, de acuerdo a algunos autores, se ha debido a que el liderazgo detrás de dichas operaciones estaba en manos del Servicio Federal de Seguridad (FSB, por sus siglas en inglés) y luego por el Directorio Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (conocido como GRU, por sus siglas anteriores en ruso), en tanto ambas provienen de agencias como el Comité para la Seguridad del Estado (KGB, por sus siglas en ruso) y el GRU soviético, reconocidas por llevar a cabo operaciones agresivas y de alto riesgo operacional.[185]

En cambio, recientemente se ha visto un incremento en la actividad del Servicio de Inteligencia Exterior (SVR, por sus siglas en ruso), lo cual supondría que las operaciones cibernéticas se orienten más a ser operaciones de largo plazo enfocadas en el espionaje y el recojo de inteligencia. Por ejemplo, la infiltración a la infraestructura digital de la empresa SolarWinds que gestiona sistemas computacionales que pertenecen a diversos departamentos del gobierno de los EE.UU.[186] por parte de agentes cibernéticos rusos fue detectado recién a finales del 2020, cuando la infiltración había empezado en realidad nueves meses antes de ser descubierta[187].

Cabe resaltar que mantener operaciones cibernéticas encubiertas requiere una mayor sofisticación técnica para evitar las crecientes herramientas de detección de intrusos y

[185] Wolff, J., 2021.
[186] Constantin, L., 2020.
[187] Wolff, J., 2021

de monitoreo de redes. Entonces, además de representar un cambio de estrategia general para las operaciones cibernéticas ofensivas por parte de Rusia, habría un incremento en las capacidades técnicas y tecnológicas de Rusia para llevar a cabo este tipo de ciberoperaciones. En términos prácticos, Rusia estaría dejando de lado técnicas como el *phishing* tradicional y los ataques DoS en favor de tácticas de intrusión como el robo de credenciales, y la infiltración en cadenas de suministros y plataformas proveedoras de servicios críticos[188].

Esto también supone que Rusia está desarrollando su propio *malware* en vez de únicamente usar herramientas y programas adquiridas del mercado negro cibernético. Este *malware* personalizado también ha resultado demostrar una implementación avanzada de técnicas criptográficas y protecciones anti análisis que les permiten escudarse de ser detectados por software antivirus. Aun así, Rusia no ha dejado de utilizar completamente malware adquirido o elaborado por grupos menores de ciberdelincuentes[189].

Asimismo, las ciberoperaciones más recientes de Rusia se han caracterizado por basarse en la infiltración de terceros en vez de atacar directamente a sus víctimas. Estas intrusiones a través de terceros hacen que el ataque sea más difícil de detectar porque usualmente se llevan a cabo a través de fuentes confiables como el mismo servicio de seguridad cibernética de la compañía, el proveedor de servicios de correos electrónicos o las redes basadas en la nube que sostienen aquellos servicios. Esto permite también atacar a más víctimas de manera simultánea, a través de la infiltración de una sola compañía[190].

Si bien las tácticas, técnicas y la sofisticación de las ciberoperaciones rusas han evolucionado, muchos de los ataques provenientes de Rusia se basan en infraestructura compartida y familias de *malware* que sugieren que este país depende de un limitado

[188] *Ibid*.
[189] *Ibid*.
[190] *Ibid*.

círculo de proveedores y desarrolladores de *software*. La evolución de tácticas no ha ido acompañada de una evolución al mismo nivel de las infraestructuras digitales que sustentan las ciberoperaciones, razón por la cual no son tan resilientes a ser detectados y en muchas ocasiones se logra atribuir la responsabilidad de varios ataques a Rusia[191].

De este modo, en el marco de la conceptualización de las amenazas híbridas, todo lo mencionado permite confirmar que Rusia es un actor híbrido por excelencia, sobre todo considerando que su gobierno permite o impulsa a organizaciones cibercriminales dentro de su territorio a que lancen ataques destructivos al exterior. Estos ataques cibernéticos siempre apuntan a cumplir objetivos que favorecen a Rusia en diversas materias como la política, económica, social, milita, informacional o de opinión pública. Así, Rusia es un país que ha sabido actuar en el ciberespacio conforme a sus intereses.

Un ejemplo conocido de guerra híbrida liderada por Rusia fue el conjunto de operaciones que este país llevó a cabo en Crimea en el 2014, en el que se combinó el uso de métodos no convencionales como actividades subversivas y ciberataques en conjunto con una invasión de fuerzas militares convencionales[192].

3.3. República Popular de China

Similar al caso de Rusia, no existe gran cantidad de información de fuente abierta que detalle la forma en que se organizan los actores encargados de llevar a cabo ciberoperaciones en China, aunque sí es posible determinar un *modus operandi* de acuerdo a los ciberataques descubiertos que este país ha llevado a cabo.

La estrategia china para el dominio ciber se centra en la guerra de la información, la cual está a cargo de las fuerzas armadas de dicho país. Como se menciona en el Papel

[191] *Ibid*.
[192] Yu, Y., 2018.

Blanco de la Defensa China del 2008, la guerra informacional incluye el uso de armamento y fuerzas basadas en la información, incluyendo sistemas de gestión de escenarios de batalla, capacidades de ataque quirúrgico y C2 asistido por la tecnología. Este tipo de guerra está enmarcado en el largo proceso de modernización de las Fuerzas Armadas de China que busca transformar a la doctrina militar china en una ciber-céntrica.

La estrategia de la guerra de la información de china se basa en lo que ellos denominan "estratagemas". Estas estratagemas tienen como objetivo darle a China la capacidad de desarrollar y mantener superioridad en la información, para así compensar sus deficiencias en el armamento basado en tecnologías que ésta posee. Asimismo, buscan crear errores cognitivos en el adversario e influenciar en los contenidos, los procesos y la dirección de su pensamiento. En ese sentido, China lleva a cabo operaciones en el ciberespacio para lograr superioridad en el campo de la información mediante reconocimiento, espionaje, ataques e intrusiones en redes y robo o alteración de data.

Esta doctrina se enmarca dentro del concepto chino de "Guerra Irrestricta", que combina elementos de operaciones de la información, operaciones cibernéticas, guerra irregular, conflictos en el aspecto normativo, y relaciones internacionales; tanto en tiempos de paz como de conflicto. Una de las entidades a cargo de la guerra cibernética y electrónica de China, por lo que se conoce, es la Unidad 61398 del Ejército Popular de Liberación, con sede en Shanghái; aunque el gobierno chino haya negado consistentemente que dicha unidad haya estado involucrada en ataques cibernéticos. Aun así, en 2013 China admitió que tiene unidades secretas de ciberguerra tanto en el brazo militar como civil del gobierno.

La estrategia china para la guerra cibernética se basa en conseguir ventajas competitivas frente a otros países, especialmente potencias rivales como los EE.UU. En el 2009, China fue la principal sospechosa de haber robado gran cantidad de información del diseño de jet de combate F-35 estadounidense de los sistemas de su creador, Lockheed Martin. En consecuencia, en el año 2014 China produjo el jet J-31

como rival para el F-35, con capacidades similares. Este tipo de casos de robo de información ha sido recurrente, sobre todo cuando se ha tratado de sistemas de armamento avanzados que no posee China en el momento.

Por otro lado, cabe mencionar que, en el aspecto de la ciberdefensa, China emplea sus recursos informáticos y legales para la censura y la supervisión interna mediante un programa conocido como el "Escudo Dorado", también conocido como "el Gran Firewall de China". Además, este país promueve activamente la idea de la soberanía cibernética, buscando crear fronteras en el ciberespacio basado en el principio de integridad territorial. De este modo, China busca justificar su accionar de control y vulneración de derechos individuales en el ciberespacio al insistir en que ese control se ejerce dentro de su "ciberespacio soberano".

De igual modo, la gran cantidad de productos tecnológicos y software provenientes de China le ha posibilitado obtener incontables cantidades de data sobre personas y organizaciones que existen fuera de China[193]. Esta fue una de las razones por las que, en países occidentales, especialmente EE.UU., hubo preocupación acerca de la instalación de la empresa Huawei en sus territorios.

Así, China, al igual que EE.UU. y Rusia, es una potencia que de acuerdo a la conceptualización de las amenazas en la presente era de la Cuarta Revolución Industrial, es un actor híbrido. China utiliza sus capacidades ofensivas cibernéticas en favor de sus intereses en el ciberespacio y en campos como la información, la opinión pública y el desarrollo tecnológico para conseguir ventajas comparativas.

Cabe resaltar que Rusia y China vienen realizando una profundización en sus relaciones militares, lo cual incluye intercambios de sistemas sofisticados de defensa, ventas de armamento y cada vez más maniobras conjuntas de sus fuerzas armadas.

[193] *Ibid.*

Asimismo, tienen prácticas cada vez más similares en el uso del espacio y el ciberespacio[194].

En conclusión, EE.UU., Rusia y China, como potencias mundiales, se han adaptado al quinto dominio de la guerra, el ciberespacio, desarrollando capacidades defensivas y ofensivas que les permiten perseguir sus intereses dentro de un escenario en el que la línea divisoria entre la paz y el conflicto es casi inexistente. El análisis de estos tres casos permite tener un entendimiento general de cómo es que los Estados poderosos utilizan sus capacidades cibernéticas en la ciberseguridad, la ciberdefensa y como actores que también representan amenazas híbridas.

El presente capítulo ha mostrado la forma en que los Estados trabajan conjuntamente en favor de ambientes más seguros en materia de ciberseguridad, ciberdefensa y amenazas híbridas; así como la forma en que potencias mundiales utilizan sus capacidades cibernéticas de manera unilateral para el cumplimiento de sus propios intereses estratégicos. El análisis general realizado permitirá entender en qué situación se encuentra el Perú en comparación con los actores analizados, con el fin de proponer los elementos de una estrategia que fortalezca sus capacidades para poder estar debidamente preparado para desenvolverse adecuadamente en el ciberespacio.

[194] Piqué, J., 2021.

Capítulo III: Situación de la ciberseguridad, ciberdefensa y amenazas híbridas en el Perú

El Perú no cuenta con capacidades cibernéticas cercanas a las de los actores mencionados, ni de organizaciones como la UE y la OTAN, ni de potencias como EE.UU., Rusia y China. Esto parece ser una tendencia en toda la región de América Latina, en tanto es una región periférica al considerar que los principales conflictos cibernéticos se llevan a cabo entre países occidentales que giran dentro de las esferas de influencia de la OTAN y sus aliados en Norteamérica, Europa y Asia, y países aliados de Estados que EE.UU. denomina como potencias revisionistas, como Rusia, China, Irán y Corea del Norte.

Si bien América Latina, y, por ende, el Perú no se encuentran en el centro de la competencia mundial cibernética, es una necesidad permanente poder contar con capacidades en ciberseguridad, ciberdefensa y de amenazas híbridas para poder contrarrestar cualquier ataque que pueda afectar al Estado, a sus intereses y a su población. Esta importancia se sustenta también en el hecho de que la tendencia hacia una creciente interconectividad de la sociedad peruana y de sus sistemas gubernamentales, civiles, empresariales y militares en la presente era de la Cuarta Revolución Industrial implicaría una mayor situación de vulnerabilidad ante ataques o intrusiones cibernéticas e híbridas.

Asimismo, sólo en el ámbito de la ciberseguridad, el Perú es el país que mayor número de ataques de *spyware* ha sufrido en Latinoamérica, y en todo el mundo ocupa la posición 39 de países más atacados en el dominio cíber. En general, los ciberdelincuentes apuntan principalmente a atacar servicios financieros, consultorías, servicios de telecomunicaciones, manufacturas o proveedores de seguros.

Una situación resaltante y reciente de vulneración a la ciberseguridad en el Perú se dio durante los Juegos Panamericanos del 2019 en Lima. Durante los días en los que se llevó a cabo el masivo evento, entre el 26 de julio y el 11 de agosto, se reportaron más

de 4 millones de incidentes cibernéticos, equivalentes a cerca de más de 400,000 incidentes por día. De estos, por lo menos 170,000 de los incidentes diarios estuvieron ligados a infraestructura relacionada a los Juegos Panamericanos. Esto equivale a aproximadamente 7,000 ataques por hora, 118 ataques por minuto y 2 ataques por segundo. La mayoría de los ataques tenían como objetivos acceder a información económica de todo tipo de personas que se encontraban asistiendo o trabajando para los Juegos Panamericanos.

Pese a esto, no existe aún una Ley de Ciberseguridad en vigor en el Perú[195]. Sí existe, sin embargo, una Ley de Ciberdefensa que establece de manera general un marco normativo que regula las operaciones militares en el dominio cíber.

En cuanto al sector Relaciones Exteriores, como se evidencia en el Objetivo Estratégico 1 del Plan Estratégico Sectorial Multianual (PESEM) 2015-2021 del MRE, el Perú apunta a posicionarse como una potencia regional. Esto implica el desarrollo de capacidades cibernéticas y de poder híbrido que le permita al país proyectar su poder tanto dentro como fuera de sus fronteras en favor de sus intereses, incluyendo el uso de capacidades cibernéticas e híbridas ofensivas contra potenciales adversarios. Para ello se requiere necesariamente del desarrollo de infraestructuras digitales complejas, al igual que la formación de personal especializado, que pueda sustentar este nuevo tipo de poder para el Perú.

En ese sentido, el presente capítulo realiza un análisis y balance de la situación actual del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas, considerando todos los elementos relevantes desde el marco jurídico existente sobre la materia, los actores principales dedicados a dichos temas, y sus avances. Finalmente, tomando en cuenta lo desarrollado en los dos capítulos anteriores, se concluye con una presentación de los elementos que se deben considerar para formular una propuesta de

[195] Benedet, M., 2020.

estrategia de política exterior que apunte al fortalecimiento de las capacidades del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas

1. Marco jurídico

El Perú ha puesto en marcha desde el año 2017 una Política Nacional de Ciberseguridad que ha dado como resultado algunos avances con leyes que establecen un marco normativo inicial para futuros esfuerzos en materia de ciberseguridad y ciberdefensa, como la Ley de Gobierno Digital (Decreto Legislativo N° 1412) del 2018 que delega competencia en materia de seguridad digital. No obstante, no existe aún en el país una estrategia ni una doctrina en ciberseguridad y ciberdefensa, que orienten de manera integrada los esfuerzos del Estado peruano en dichos temas.

Asimismo, no existe en vigor una ley que sea propiamente de ciberseguridad. Hasta la fecha, su creación se encuentra en proceso. El 2019 se aprobó el dictamen del proyecto de Ley de Ciberseguridad (Proyecto de Ley No. 4237 y 4352), que buscaría establecer el marco normativo en materia de seguridad digital en el Perú[196]. Dicho marco normativo sería aplicable al sector público, al sector privado, a la academia y a la sociedad civil; y buscaría establecer los siguientes principios rectores: Colaboración multidisciplinaria multisectorial e interinstitucional, respeto a los derechos humanos, enfoque basado en gestión de riesgos, y comunicación de incidentes[197].

El cuarto principio mencionado, sobre la comunicación de incidentes, busca establecer la obligación de notificar incidentes que impliquen violación de datos personales al personal responsable en la entidad pública[198]. Esto reconoce la importancia de contar con CISO en las entidades, y de que esta información sea compartida, para, eventualmente, poder realizar un análisis de la situación, las vulnerabilidades más

[196] Gestión, 2020.
[197] Niubox, 2019.
[198] *Ibid.*

explotadas, los tipos de ataque, entre otros; lo que, a su vez, permitirá desarrollar estrategias de prevención y respuesta más eficientes.

El proyecto de ley buscaría crear también un Comité de Ciberseguridad del Estado Peruano adscrito a la PCM, y que funcione bajo dirección de la SEGDI. Este comité estaría conformado por representantes del sector privado, de la academia, de la comunidad técnica nacional de internet y del sector gubernamental[199].

Sus funciones consistirían en reformular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de gestión de respuestas incidentes de seguridad digital en el sector privado, fomentar la cultura de ciberseguridad en el país, y coadyuvar al fomento de currículos de educación superior en materia de ciberseguridad. Asimismo, dicho comité establecería los lineamientos para el establecimiento de CSIRTs en el sector privado, la academia, la sociedad civil y la comunidad técnica nacional, fomentando el desarrollo de instrumentos de cooperación público-privado en materia de ciberseguridad[200].

Por otro lado, tampoco existe una política nacional de ciberdefensa que complemente a la Política Nacional de Ciberseguridad existente y que brinde lineamientos generales para el Estado peruano y sus instancias en materia de ciberdefensa. A continuación, se presentan las leyes, normas y políticas nacionales referidas a la ciberseguridad y la ciberdefensa en orden cronológico de su adopción.

1.1. Ley de Delitos Informáticos

En el 2013 se renovó la Ley de Delitos Informáticos (Ley N.º 30096), que complementa y cubre de cierta forma el vacío normativo que existía hasta el momento sobre algunos de los ciberataques más comunes, como la vulneración de sistemas y

[199] *Ibid.*
[200] *Ibid.*

datos informáticos. Esta norma fue perfeccionada posteriormente en el año 2014, bajo la Ley N.º 30171[201], que amplía el Código Penal para incluir a los delitos informáticos y las penas para los infractores[202].

La Ley de Delitos Informáticos realiza una tipificación de los delitos que pueden ser cometidos en el ciberespacio, a fin de poder facilitar su identificación y codificación en aras de garantizar la lucha eficaz contra la ciberdelincuencia. En general, esta ley tipifica y detalla delitos contra datos y sistemas informáticos como el acceso ilícito, atentados a la integridad de datos informáticos, y atentados a la integridad de sistemas informáticos; y delitos informáticos contra la indemnidad y libertad sexuales como proposiciones a niños y adolescentes con fines sexuales por medios tecnológicos[203].

Asimismo, incluye delitos informáticos contra la intimidad y el secreto de las comunicaciones como el tráfico ilegal de datos, y la interceptación de datos informáticos; delitos informáticos contra el patrimonio como el fraude informático; delitos informáticos contra la fe pública como la suplantación de identidad; y delitos como el abuso de mecanismos y dispositivos informáticos para cometer otros delitos[204].

Por otro lado, la Ley incorpora la figura del agente encubierto en delitos informáticos. Bajo autorización de un fiscal, la Policía Nacional del Perú (PNP) puede desplegar agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en dicha Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación[205].

Adicionalmente, la Ley establece las bases para la coordinación interinstitucional entre la PNP, el Ministerio Público (MP), el Poder Judicial (PJ), el Equipo de respuesta ante

[201] Gestión, 2020.
[202] Benedet, M., 2020.
[203] Congreso de la República del Perú, 2013, pp. 1-4.
[204] *Ibid*, pp. 3-6.
[205] *Ibid*, p. 7.

incidentes de seguridad digital del Perú (Pe-CERT) o el CNSD, la SEGDI y los Organismos Especializados de las FF.AA. En esta relación, la PNP centraliza la información referida a delitos informáticos, aporta en la elaboración de programas y acciones para la adecuada persecución de éstos, y desarrolla programas de protección y seguridad al respecto[206].

Además, la Ley establece líneas de acción a ser seguidas para garantizar su cumplimiento, aunque a la fecha éstas no tengan resultados visibles. Por un lado, con el objetivo de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades relacionadas para dar efectividad a la Ley, los actores anteriormente mencionados y los operadores del sector privado involucrados en la lucha contra delitos informáticos deben establecer protocolos de cooperación operativa[207].

Por otro lado, la Ley indica que las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal, especialmente de la PNP, el MP y el PJ, en el tratamiento de los delitos previstos en la presente Ley. Además, la SEGDI, en coordinación con las instituciones del sector público, deberían promover permanentemente el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

Cabe mencionar que también existe desde el 2011 una Ley de Protección de Datos Personales (Ley N.° 29733), que busca crear un ámbito de protección sobre la disposición y uso de bases de datos tanto públicas como privadas por terceros[208].

[206] *Ibid*, p. 8.
[207] *Ibid*, p. 9.
[208] Gestión, 2020.

1.2. Política de Seguridad y Defensa Nacional (PSDN) del Estado Peruano

En el 2017 se aprobó la más reciente Política de Seguridad y Defensa Nacional del Estado Peruano mediante Decreto Supremo N°012-2017-DE. Formulada sobre la base de la adecuación del concepto de seguridad nacional, los objetivos nacionales y el fortalecimiento del Sistema de Defensa Nacional, busca garantizar el orden interno contribuyendo al normal funcionamiento de la institucionalidad del Estado con el fin de alcanzar niveles de desarrollo sostenible en beneficio de la seguridad humana. Así, contiene objetivos y lineamientos que sirven para orientar y articular la actuación de todos los actores involucrados en las actividades de Seguridad y Defensa Nacional[209].

Esta Política basa su fundamentación en la necesidad de actualizar la conceptualización de las amenazas y riesgos al Perú debido a la evolución internacional y nacional de diversas dinámicas que pueden tener efectos sobre la seguridad y defensa del Estado. De este modo, identifica como principales amenazas a la seguridad del país al terrorismo y el tráfico ilícito de drogas presentes en la zona del Valle de los Ríos Apurímac, Ene y Mantaro (VRAEM), por un lado; y a la inseguridad ciudadana ocasionada por la delincuencia común y el crimen organizado, por otro lado[210].

En general, se considera que los problemas que requieren ser atendidos, que por su magnitud afectan a los objetivos de la Seguridad Nacional del Perú, son, entre otros, la inseguridad ciudadana, el tráfico ilícito de drogas, el terrorismo, el crimen organizado, el tráfico de armas, la deficiente calidad de los servicios de justicia, la corrupción, la inadecuada gestión del Estado, los conflictos sociales, las actividades de la minería informal y la minería ilegal, la contaminación ambiental, la vulnerabilidad ante desastres, los escasos niveles de desarrollo tecnológico y la pobreza[211].

---

[209] Decreto Supremo N.° 012-2017-DE. Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional. (22 de diciembre de 2017), p. 25.
[210] *Ibid*, pp. 12-13.
[211] *Ibid*, p. 15.

Estos son problemas que, de acuerdo a la metodología utilizada en la Política para la elaboración del diagnóstico de la situación de la seguridad y la defensa en el Perú, son abordados con mayor importancia por sobre otros problemas presentes en la gran variedad de fenómenos sociales, políticos, económicos, diplomáticos, tecnológicos, ambientales y militares que amenazan al Estado y a la población[212].

El diagnóstico que se realiza aborda todas las capacidades del Estado peruano relacionadas a la Seguridad y Defensa del país, y analiza su relación, situación y aporte en la materia. Estas capacidades vienen a ser:

- Capacidad militar de las Fuerzas Armadas (FF.AA.)
- Protección de la Amazonía, la presencia en la Antártida y el combate a la minería ilegal
- Capacidad para la lucha contra el terrorismo
- Capacidad para combatir el tráfico ilícito de drogas y delitos conexos
- Capacidad para combatir la corrupción
- Capacidad para efectivizar la modernización de la gestión pública
- Cultura de Seguridad Nacional en el país
- Capacidad para enfrentar la inseguridad ciudadana
- Identidad nacional en los ciudadanos
- Capacidad de gestión de riesgo de desastres
- Competitividad de la economía peruana
- Inversión en ciencia y tecnología
- Infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad
- Capacidad para atender el abastecimiento energético
- Capacidad para desacelerar el deterioro del ambiente
- Capacidad para el desarrollo de tecnologías
- Capacidad para la gestión del territorio

[212] *Ibid*, p. 13.

- Capacidad para combatir la pobreza y desigualdad social
- Capacidad para el manejo de los conflictos sociales[213]

Así, la Política busca ser socializada entre las entidades oficiales para que sirva de referencia con el fin de que, de manera transversal, todos los niveles de gobierno adapten sus instrumentos políticos y de planeamiento estratégico en lo que se refiere a los temas que amenazan a la Seguridad Nacional, previamente mencionados[214].

De las capacidades diagnosticadas, es de especial relevancia para la presente investigación la infraestructura para enfrentar ataques a los sistemas de información que incluye a la ciberseguridad como componente principal. En aquel apartado de la Política de Seguridad y Defensa Nacional del Estado Peruano, se reconoce explícitamente que la protección del ciberespacio y su infraestructura es un asunto de Seguridad Nacional.[215]

Este reconocimiento se debe a que las tecnologías de la información están cada vez más integradas a la operación de la infraestructura física, incluida la IC, razón por la cual existe un mayor peligro de que se pueda dañar o interrumpir su funcionamiento, lo cual a su vez pondría en peligro a la economía y a la vida cotidiana de millones de peruanos[216].

Asimismo, el diagnóstico anuncia los problemas existentes en la materia, los cuales vienen a ser la falta de esfuerzos unificados, la falta de reconocimiento de este asunto como problema público, la carencia de tecnologías de última generación y la ausencia de un ente rector especializado. Estos problemas debilitan la capacidad de defensa sincronizada a nivel público-privado y agravan aún más esta precaria situación, a pesar

[213] *Ibid*, pp. 15-25.
[214] *Ibid*, p. 14.
[215] *Ibid*, p. 14.
[216] *Ibid*, p. 21.

de los esfuerzos realizados desde la SEGDI y el Sistema de Coordinación de Emergencias en Redes Teleinformáticas (Pe-CERT) o CNSD de la PCM[217].

El diagnóstico identifica también las fuentes de amenaza al ciberespacio y su infraestructura al señalar que son susceptibles a una amplia gama de riesgos físicos y cibernéticos, detrás de los cuales podría haber una serie de actores que aprovecharán las vulnerabilidades anteriormente mencionadas para robar información; interrumpir, poner en peligro o destruir la capacidad de prestar servicios en el país; o acceder a información reservada de diversas entidades públicas, poniendo en peligro la gobernabilidad del Estado. Adicionalmente, se señala que la protección del ciberespacio es particularmente difícil debido a la capacidad que pueden tener estos actores de actuar desde cualquier parte del mundo[218].

Finalmente, el diagnóstico en materia de ciberseguridad señala que, al haberse alcanzado un elevado nivel de informatización en el país, se impulsará la creación de un Sistema Nacional de Ciberseguridad con la participación del sector privado y la sociedad en su conjunto para promover la formación de especialistas para la defensa del ciberespacio[219].

En ese sentido, también se fortalecerán las misiones constitucionales de las FF.AA. y la PNP para incrementar sus capacidades militares y policiales, respectivamente, y paralelamente, sus recursos humanos, con el objetivo de garantizar la paz internacional relacionado al Estado peruano y el orden interno; a través de la integración de sistemas relacionados con la seguridad para disuadir, enfrentar y eliminar eficazmente a organizaciones terroristas y de narcotraficantes[220].

Como se verá en adelante, los objetivos y lineamientos de la Política de Seguridad y Defensa Nacional buscarán corregir los problemas diagnosticados y orientar las

[217] *Ibid*, p. 21.
[218] *Ibid*, p. 21.
[219] *Ibid*, p. 21.
[220] *Ibid*, p. 21.

acciones para asegurar una situación óptima de Seguridad y Defensa para el Perú. Bajo el enfoque de seguridad multidimensional, la Política presenta tres objetivos y veintinueve lineamientos orientados a alcanzar dichos objetivos, y que están relacionados a un sector determinado que los ejecutarán según sus políticas, planes, programas y proyectos, considerando además sus capacidades administrativas y presupuestales[221].

El primer objetivo, "Garantizar la soberanía, la independencia, la integridad territorial y la protección de los intereses nacionales", está relacionado al conjunto de previsiones y acciones que el Estado genera y ejecuta con ese fin. Sus lineamientos, de manera resumida, son las siguientes:

1. Fomentar la participación activa, articulada e integral de los poderes del Estado en todos los niveles para garantizar la Seguridad Nacional.
2. Controlar y proteger el territorio de la República.
3. Alcanzar el nivel de capacidades militares necesarias para el cumplimiento de los roles constitucionales de las FF.AA. impulsando su modernización.
4. Participar activamente en organismos internacionales competentes en temas de seguridad global, hemisférica y regional para promover el principio de la solución pacífica de controversias entre los Estados, el respeto a los principios de derecho internacional y las medidas de confianza mutua, así como proteger y proyectar los intereses nacionales en organismos y mecanismos de cooperación bilaterales y multilaterales.
5. Fortalecer el Sistema de Inteligencia Nacional (SINA) impulsando su especialización y el empleo de tecnología avanzada que permita mejorar su desempeño frente a las amenazas externas a la Seguridad Nacional.
6. Promover el fortalecimiento de los valores de identidad y compromiso con la Nación de las comunidades peruanas en el exterior.

[221] *Ibid*, p. 26.

7. Proteger los ACN contra todo tipo de amenazas, así como los sistemas de información, de las amenazas que, desde el ciberespacio, atenten contra la Seguridad y Defensa Nacional.
8. Promover la educación en Seguridad y Defensa Nacional en todas las etapas y niveles del Sistema Educativo, contribuyendo a la afirmación de una cultura de paz y seguridad.
9. Fortalecer la identidad nacional, promoviendo el reconocimiento, el respeto y la valoración de la historia del Perú, sus héroes, su cultura y sus tradiciones[222].

El segundo objetivo, "Garantizar el orden interno contribuyendo al normal funcionamiento de la institucionalidad política y jurídica del Estado" cuenta son los siguientes lineamientos:

1. Fortalecer el Estado de Derecho, la paz social, la estabilidad interna, así como la promoción y la protección de los derechos humanos.
2. Impulsar mecanismos que permitan consolidar la gobernabilidad, la institucionalidad democrática y fomentar el equilibrio de poderes y la adecuada representatividad política.
3. Fortalecer los sistemas de seguridad ciudadana, de gestión de riesgos de desastres, de inteligencia nacional y otros que coadyuven a garantizar la Seguridad Nacional.
4. Fortalecer la lucha contra el terrorismo, el tráfico ilícito de drogas, el crimen organizado, la criminalidad y la delincuencia en todas sus modalidades, empleando los recursos tecnológicos, humanos y logísticos necesarios.
5. Fortalecer el SINA, impulsando su especialización y el empleo de herramientas y tecnología avanzada que permiten mejorar su desempeño frente a las amenazas internas a la Seguridad Nacional.
6. Alcanzar el nivel de capacidad policial que permita mayor eficiencia en el cumplimiento de los roles que la Constitución Política asigna a la PNP

[222] *Ibid*, p. 26.

impulsando su modernización e incluyendo su especialización técnica, profesional y el uso de tecnología avanzada

7. Promover la construcción de un sistema de integridad coordinado e integral en el país para luchar contra la pequeña, mediana y gran corrupción en todas sus modalidades.
8. Contribuir al fortalecimiento y modernización del Sistema de Administración de Justicia, para garantizar la seguridad jurídica y la celeridad en la resolución de los conflictos, y en las acciones contra las amenazas a la seguridad nacional.
9. Promover un proceso integral de reforma y adecuación de las normas vigentes del ordenamiento jurídico, referidas a las amenazas a la Seguridad Nacional, en particular el terrorismo, la ciberdelincuencia, el tráfico ilícito de drogas y delitos conexos, el tráfico ilícito de flora y fauna silvestre, la tala ilegal, la minería ilegal e informal, la trata de personas y el lavado de activos, entre otras.
10. Fortalecer y modernizar el Sistema Penitenciario, poniendo énfasis en la desarticulación de las organizaciones criminales al interior de los establecimientos penitenciarios y en la efectiva reinserción social de las personas que hayan cumplido sus sentencias.
11. Alcanzar el nivel de capacidad de la Autoridad Marítima, que permita mayor eficiencia en el cumplimiento de los mandatos legales para el control y vigilancia de las actividades acuáticas, impulsando su equipamiento con polivalencia de los medios navales, así como su especialización y tecnificación.
12. Impulsar el desarrollo de tecnologías de prevención, vigilancia y gestión de respuestas oportunas para el apoyo al mantenimiento del orden interno, la protección de la infraestructura crítica nacional y la gestión del riesgo de desastres tomando en cuenta la gestión de la continuidad operativa.
13. Fomentar la prevención y la adecuada gestión de conflictos sociales con un enfoque de diálogo y sostenibilidad, para fortalecer la gobernabilidad, fomentar las inversiones responsables y garantizar los derechos ciudadanos[223].

[223] *Ibid*, p. 26

El tercer objetivo, "Alcanzar niveles de desarrollo sostenible que contribuyan a garantizar la Seguridad Nacional", está relacionado al concepto de desarrollo humano, que viene a ser el proceso de creación, ampliación o incremento racional, sostenido y sustentable de las condiciones económicas, psicosociales, políticas, científicas, tecnológicas, ambientales y militares que permitan alcanzar crecientes niveles de bienestar general[224]. Sus lineamientos son los siguientes:

1. Reducir las brechas de desigualdad fomentando e impulsando un enfoque de seguridad humana en el que todas las personas tengan igualdad de oportunidades para desarrollarse, focalizando la intervención en áreas críticas, zonas vulnerables y de difícil acceso.
2. Promover el desarrollo de proyectos de energía renovable y limpia, a través de la exploración y explotación de fuentes alternativas de energía que aseguren el abastecimiento energético.
3. Promover el desarrollo en ciencia, tecnología e innovación, priorizando las tecnologías de la información y comunicación, la energía, la alimentación, la salud, el medio ambiente, la acuicultura, la agricultura, la industria de la Defensa, entre otras áreas estratégicas, con la participación de la comunidad académica y de las entidades especializadas públicas y privadas.
4. Promover el desarrollo de la infraestructura pública de utilidad estratégica, que contribuya a garantizar la Seguridad Nacional, con prioridad en el acceso universal al agua potable y al saneamiento.
5. Promover la participación integral de las entidades públicas y privadas en el desarrollo económico y social de las poblaciones aisladas y vulnerables, orientado a la erradicación de la pobreza extrema, con la participación de las FF.AA. y la Policía Nacional.
6. Asegurar la protección y la conservación del ambiente, la explotación sostenible de los recursos naturales, el desarrollo y la ocupación ordenada del territorio nacional, en especial de la Amazonía, con respeto a los usos

[224] *Ibid*, p. 25.

asignados, los ecosistemas, la diversidad y la identidad cultural de las comunidades.

7. Asegurar la investigación, el desarrollo y el uso de la tecnología aeroespacial, como recurso básico para el desarrollo socio-económico del país, cuyas aplicaciones redundan en el beneficio de todos los sectores del Estado, tales como: comunicación satelital para la extensa demografía y diversa geografía de nuestro territorio, prevención y atención de desastres naturales, estudio y protección de los recursos naturales, combate de ilícitos y para la Defensa y Seguridad Nacional[225].

De todos los lineamientos listados, los únicos que hacen referencia explícita al ciberespacio son el lineamiento 7 del primer Objetivo de Política, que hace referencia a la protección de los ACN; y el lineamiento 9 del segundo Objetivo de Política, que hace mención de un proceso de reforma de la normativa vigente para incluir amenazas a la Seguridad Nacional como la ciberdelincuencia. No obstante, una gran cantidad de lineamientos en los tres Objetivos de Política hace referencia a procesos de modernización de las entidades y sistemas del Estado, incluyendo la implementación de nuevas tecnologías y la interconexión entre éstas para asegurar un funcionamiento más eficiente del Sistema de Defensa Nacional (SIDENA).

La ciberseguridad y la ciberdefensa, son, entonces, aspectos transversales en los tres objetivos de la PSDN y sus respectivos lineamientos. Este es un resultado natural de la tendencia global a la mayor modernización y digitalización de los Estados, de la Seguridad y Defensa, y de la vida cotidiana en general. De este modo, la ciberseguridad y la ciberdefensa resultan ser aspectos de Seguridad y Defensa que cobran una relevancia única, en tanto son necesarias en todos los niveles, en todo el espectro temporal y en todos los sectores del Estado.

[225] *Ibid*, p. 27.

En la actualidad, no se puede prescindir de la ciberseguridad ni la ciberdefensa porque las amenazas de carácter cibernético son permanentes y pueden afectar ahora a cualquier componente del Estado o de la sociedad que tenga un elemento informático y digital. Reconociendo la importancia de este tema, la SEGDI publicó en el mismo año 2017 la Política Nacional de Ciberseguridad, que institucionaliza la percepción anterior de la necesidad de contar con un enfoque integral de la ciberseguridad y ciberdefensa en todo el Estado peruano y en la sociedad civil.

1.3. Política Nacional de Ciberseguridad

En el 2017, la SEGDI publicó la Política Nacional de Ciberseguridad, que tiene como objetivo general "proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información". Así, la Política se aplica a todas las entidades de la Administración Pública[226].

Si bien esta política aún no entra en vigencia, servirá de base para la implementación de propuestas legislativas y, en general, de normatividad relacionada con la seguridad de la información o la ciberseguridad. Asimismo, busca mantenerse siempre actualizada y promover la participación de las entidades del sector público y privado, así como representantes de la sociedad civil y la academia peruanas.

Por un lado, la Política establece conceptos como la Gestión de Riesgos en la información, que viene a ser el conjunto de actividades para dirigir y controlar una organización en lo que concierne al riesgo, entendiéndose esta como las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma; la probabilidad de que ocurran y su potencial impacto en la operación del Organismo. La Gestión de Riesgos, evidentemente, también incluye al Tratamiento de

[226] Secretaría de Gobierno Digital, 2017, p. 1.

Riesgos, es decir, el proceso de selección e implementación de medidas para modificar el riesgo[227].

Asimismo, la Política conceptualiza dos figuras que deben existir en las entidades del gobierno. Una de ellas es el Comité de Seguridad de la Información, que consiste en un Colegiado integrado por representantes de todas las áreas sustantivas de la entidad, destinado a garantizar el apoyo manifiesto de las autoridades competentes a las iniciativas de seguridad de la organización o entidad. La otra es la figura de un Responsable de Seguridad de la Información, que viene a ser una persona que cumpla la función de supervisar el cumplimiento de la Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad[228].

Por otro lado, la Política conceptualiza a los Incidentes de Seguridad como eventos adversos en un sistema o red de computadoras que puede comprometer la confidencialidad, la integridad o la disponibilidad de la información. Este incidente podría ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes. Adicionalmente, define a las amenazas como causas potenciales de incidentes no deseados que pueden ocasionar daños a un sistema u organización[229].

En cuanto al contenido sustantivo, la Política Nacional de Ciberseguridad cuenta con siete lineamientos de acción. El primer lineamiento es "Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el [dominio] de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio". Este lineamiento se sustenta en dos campos de acción transversales para el resto de la Política: la participación y la concientización[230].

[227] *Ibid*, p. 4.
[228] *Ibid*, p. 4.
[229] *Ibid*, p. 4.
[230] *Ibid*, p. 5.

En el aspecto de la participación, se considera necesario involucrar a todos los sectores y entidades del Estado con responsabilidad en el campo de la ciberseguridad y la ciberdefensa, con el fin de crear un ambiente participativo con representantes del sector privado, de la sociedad y de la academia, en el que cada quien aporte y actúe de acuerdo a propósitos comunes, estrategias concertadas y esfuerzos coordinados[231].

Por el lado de la concientización, se estima de vital importancia crear conciencia y sensibilizar a la población respecto de la importancia de la seguridad de la información o ciberseguridad; y fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques[232].

El segundo lineamiento es "Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública"[233]. Lo resaltante de este lineamiento es que plasma una secuencia general para generar y fortalecer las capacidades existentes en materia de seguridad cibernética a funcionarios y servidores públicos de todo el Estado, identificando los actores pertinentes para ello.

En ese sentido, primero se capacitaría a funcionarios y servidores que estén directamente involucrados en la atención y manejo de incidentes cibernéticos y gradualmente se extendería esta capacitación a las demás entidades del Estado. Entre los planes de capacitación, el Pe-CERT o CNSD, con el apoyo del CICTE de la OEA, entre otros, elaboraría un Plan de Capacitación para los demás funcionarios y servidores del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general[234].

---

[231] *Ibid*, p. 5.
[232] *Ibid*, p. 5.
[233] *Ibid*, p. 5.
[234] *Ibid*, p. 5.

De igual manera, el Ministerio del Interior (MININTER) velaría por la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa en las escuelas de formación y de capacitación de oficiales y suboficiales de la PNP[235]. Así, a largo plazo el Estado peruano contaría con una base completa de funcionarios y servidores públicos capacitados y concientizados en ciberseguridad y ciberdefensa, en cómo aplicarla en sus funciones diarias, y en cómo protegerse de o prevenir incidentes que pudiesen afectar su persona a las instituciones en las que trabajan, y, por ende, al país.

El tercer lineamiento consiste en "Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad". Como lo indica el nombre, busca que la sociedad civil tome conciencia sobre la ciberseguridad, identifique posibles vulnerabilidades o amenazas y tome acciones oportunas para su seguridad[236], volviéndose así un actor más en la ciberseguridad del país. Este Plan contaría también con una estrategia de difusión que incluya la organización de conferencias orientadas a instituciones educativas de todo nivel y foros que permitan intercambiar opiniones y experiencias entre entidades públicas y privadas, sociedad civil y academia, con el objetivo de compartir las mejores prácticas en ciberseguridad y ciberdefensa[237].

Estas acciones implicarían socializar la normatividad vigente en materia de ciberseguridad y ciberdefensa, sobre todo aquellas normas más relevantes para la sociedad civil y su quehacer diario, como la Ley N° 27933 de Protección de Datos Personales y la Ley N° 30096 de Delitos Informáticos, modificada por la Ley N° 30171[238]. De este modo, junto con el lineamiento número dos, se apunta a tener una sociedad que esté enteramente consciente de la importancia de la ciberseguridad y la ciberdefensa, y de su rol activo en su protección personal y del país en general.

[235] *Ibid*, p. 5.
[236] *Ibid*, p. 6.
[237] *Ibid*, p. 6.
[238] *Ibid*, p. 6.

El cuarto lineamiento de la Política Nacional de Ciberseguridad tiene una especial importancia para la política exterior del Perú. Este lineamiento consiste en "Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática". En ese sentido, por un lado, se busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos informáticos; así como para dar cumplimiento a los tratados internacionales sobre ciberseguridad y ciberdelincuencia[239].

Por otro lado, bajo este lineamiento se indica que las entidades responsables de la ciberseguridad y la ciberdefensa deben buscar y evaluar la participación del Perú en diferentes redes y mecanismos internacionales de cooperación como las mencionadas en el capítulo anterior de la presente tesis; las cuales prepararían al país para afrontar los crecientes desafíos del entorno internacional en materia de ciberseguridad. Esto debería realizarse en concordancia con compromisos asumidos internacionalmente como la adhesión del Perú al Convenio de Ciberdelincuencia de Budapest del 2001 y el Compromiso de la Cumbre Mundial sobre Sociedad de la Información asumido en Túnez en el 2005[240].

Los últimos tres lineamientos de la Política Nacional de Ciberseguridad tienen un carácter más general que las anteriores. El quinto lineamiento busca "Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencia en Redes Teleinformáticas de la Administración Pública y el sector privado". Para ello, se señala que es necesario que cada ministerio coordine con el Pe-CERT o CNSD de manera permanente y que sea prioritario ante cualquier amenaza que vulnere la seguridad de la Nación[241].

[239] *Ibid*, p. 6.
[240] *Ibid*, p. 6.
[241] *Ibid*, p. 7.

El sexto lineamiento es "Elaborar un Plan de Acción Nacional en Ciberseguridad", que debería realizarse de forma multisectorial y multidisciplinaria con representantes de las entidades del sector público, el sector privado, la sociedad civil y la academia[242]. La existencia de un plan como este es necesario ya que no existe en el Perú una doctrina en materia de ciberseguridad o ciberdefensa que articule integralmente a todos los sectores involucrados y que oriente la acción de éstas para la prevención, identificación y respuesta ante ataques cibernéticos.

Finalmente, el séptimo lineamiento propone "Crear el Comité Nacional de Ciberseguridad", que tendría entre sus funciones velar por el cumplimiento de las políticas y lineamientos que se establezcan en el país respecto a la ciberseguridad. Este Comité estaría conformado por la PCM, representada por la SEGDI, el PJ, la Dirección Nacional de Inteligencia (DINI), el Ministerio de Defensa (MINDEF), el MININTER, la PNP, la Asociación de Gobiernos Regionales, la Sociedad Nacional de Industrias (SNI), la Cámara de Comercio de Lima (CCL), la Cámara Nacional de Comercio, Producción, Turismo y Servicios (PERUCÁMARAS), el Colegio de Abogados de Lima (CAL), el Colegio de Ingenieros del Perú (CIP), el *Network Access Point Peru* (NAP), la Confederación Nacional de Instituciones Empresariales Privadas (CONFIEP), la Asociación de Bancos del Perú (ASBANC), la Asociación para el Fomento de la Infraestructura Nacional (AFIN), la Red Científica Peruana (RCP), y otros que puedan tener competencias al respecto[243].

La Política Nacional de Ciberseguridad, entonces, establece lineamientos generales a seguir para la futura elaboración de normas jurídicas y de acciones orientadas a fortalecer las capacidades en ciberseguridad y ciberdefensa en la sociedad peruana, tanto a nivel gubernamental como de sector privado y sociedad civil. Quedaría pendiente su implementación y que se lleven a cabo las acciones indicadas en ella; que se elabore el Plan de Acción Nacional en Ciberseguridad que articule y operativice los

[242] *Ibid*, p. 7.
[243] *Ibid*, p. 7.

esfuerzos de las entidades competentes en la materia; y que se crea el Comité Nacional de Ciberseguridad propuesto.

1.4. Ley de Gobierno Digital

En el 2018 se aprobó la Ley de Gobierno Digital (Decreto Legislativo N° 1412) con el objeto de establecer el marco de gobernanza del gobierno digital para la adecuada gestión de diversos aspecto relacionados a la regulación del ciberespacio, como la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno[244].

En lo que concierne al tema de seguridad digital, la Ley de Gobierno Digital aporta con la conceptualización de arquitectura digital. Esta se entiende como el conjunto de componentes, lineamientos y estándares que permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital[245].

Asimismo, se conceptualiza al Gobierno Digital como el "uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público"[246]. Siendo el Gobierno Digital el fin sustantivo de esta Ley, se incluye al necesario elemento de seguridad dentro de sus objetivos, los cuales se listan a continuación:

[244] Decreto Legislativo N° 1412, 13 de setiembre de 2018, p. 4.
[245] *Ibid*, p. 5.
[246] *Ibid*, p. 5.

1. Normar las actividades las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.
2. Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.
3. Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.
4. Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno[247].

La Ley establece como Ente Rector en materia de Gobierno Digital a la PCM, a través de la SEGDI. En ese sentido, tiene la función de dirigir, coordinar, supervisar y elaborar lineamientos en materia de Seguridad Digital, como lo establecen sus funciones y el capítulo sexto de la Ley[248].

La Seguridad Digital se define como:

> El estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas[249].

Así, se establece en la Ley el Marco de Seguridad Digital del Estado Peruano, que se constituye en el "conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad integridad, disponibilidad de la información en el entorno digital administrado por las

[247] *Ibid*, p. 5.
[248] *Ibid*, pp. 5-7.
[249] *Ibid*, p. 8.

entidades de la Administración Pública"[250]. En cuanto a su gestión, se faculta el liderazgo a diversas entidades del Estado en relación a los cuatro ámbitos que lo componen: el ámbito de la defensa, de la inteligencia, de la justicia, y el institucional[251].

En el ámbito de la defensa, el MINDEF es la entidad que dirige, supervisa y evalúa las normas en materia de ciberdefensa. En el ámbito de la inteligencia, la DINI emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital relacionadas a dicha actividad. En el ámbito de la justicia, el Ministerio de Justicia y Derechos Humanos (MINJUS), el MININTER, la PNP, el MP y el PJ dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia. En el ámbito institucional, son las propias entidades de la Administración Pública las que deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)[252].

De este modo, la Ley de Gobierno Digital de 2018 establece a la PCM, a través de la SEGDI, como el Ente Rector en materia de gobierno digital, que incluye a la seguridad digital y aspectos de ciberseguridad. Asimismo, reafirma el rol que tienen otros sectores en ámbitos especializados de la seguridad y defensa en el ciberespacio, entre ellos el del MINDEF en cuanto a la ciberdefensa, que sería regulado con mayor profundidad en la Ley de Ciberdefensa del 2019.

1.5. Ley de Ciberdefensa

Promulgada en el 2019, la Ley de Ciberdefensa (Ley N.° 30999) busca establecer un marco normativo en materia de ciberdefensa del Estado peruano a cargo de los órganos ejecutores del MINDEF, es decir, el Ejército, la Marina y la Fuerza Aérea; y el CCFFAA. De este modo, tiene como finalidad proteger y defender la soberanía

[250] *Ibid*, p, 8.
[251] *Ibid*, p. 8.
[252] *Ibid*, p. 8.

nacional, los intereses nacionales, los ACN y los sistemas de información digital de los órganos ejecutores mencionados de amenazas o ataques en y mediante el ciberespacio que atenten, finalmente, contra la seguridad nacional[253].

Esta Ley define a la ciberdefensa como "la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional". Asimismo, define a las capacidades de ciberdefensa como "el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias".[254]

Como se centra en las operaciones militares que se puedan llevar a cabo en el ciberespacio, las define como "el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa [...] contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional"[255]. Asimismo, detalla que los encargados de la planificación y ejecución de dichas operaciones son los órganos ejecutores del Ministerio de Defensa y el CCFFAA, conforme a las leyes que regulan su naturaleza jurídica, sus competencias y los tratados internacionales existentes[256].

Un aspecto resaltante de la ley es que determina que el uso de la fuerza por parte de las FF.AA. en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas sobre la legítima defensa, y por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables[257].

Respecto a la legítima defensa, la Ley señala que toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos

[253] Niubox, 2019.
[254] Congreso de la República del Perú, 2019, p.9.
[255] *Ibid*, p. 9.
[256] Niubox, 2019.
[257] Congreso de la República del Perú, 2019, p.9.

críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa, el cual está sujeto a los principios de legalidad, necesidad y oportunidad. De este modo, se genera la posibilidad de conducir una operación de respuesta mediante el ciberespacio[258].

La Ley también incluye un cambio en la protección de los ACN, en tanto le otorga al CCFFAA la responsabilidad de hacerse cargo de su ciberdefensa cuando la capacidad de protección por parte de sus operadores, del sector responsable de cada uno de ellos, o de la DINI sea sobrepasada. Esto, a fin de mantener las capacidades nacionales y evitar la perturbación en su correcto funcionamiento, lo cual podría afectar negativamente a la seguridad nacional[259].

La Ley también modifica la Ley de Gobierno Digital, estableciendo al MINDEF como el encargado del ámbito de Defensa del Marco de Seguridad Digital del Estado Peruano. Asimismo, reconoce la importancia de las entidades que gestionan lo que la Ley denomina como "recursos críticos de Internet", como nombres de dominio, números de Protocolo de Internet (IP, por sus siglas en inglés) y otros protocolos, en tanto su naturaleza las convierte en entidades vinculadas a la ciberdefensa, razón por la cual deben mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional[260].

Finalmente, la Ley le otorga a la PCM, en su calidad de ente rector en materia de seguridad digital, el importante y necesario mandato de coordinar con el MINDEF y el Ministerio de Educación (MINEDU) la pertinencia del desarrollo de currículos con contenidos especializados en materia de seguridad digital, que incluye la ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, tanto a nivel de pregrado como de postgrado. Para ello, la PCM debe establecer instrumentos de

[258] *Ibid*, p. 9.
[259] *Ibid*, p. 10.
[260] *Ibid*, p.10.

cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica[261].

En conclusión, la Ley de Ciberdefensa crea un mandato hasta entonces inexistente que sirve de base para regular las operaciones militares en el ciberespacio. Aunque sea, en principio, de naturaleza defensiva, su entrada en vigor ha sido necesaria ya que especifica a qué entidades del Estado les corresponde la labor de la ciberdefensa. Esto, a su vez, reconoce la importancia de la ciberdefensa para la seguridad y defensa nacionales, lo cual se traduce en el otorgamiento de funciones en la materia a los órganos ejecutores del MINDEF, y en la señalada importancia de educar a la población en el tema.

Quedaría pendiente, entonces, la reglamentación de la Ley por parte del MINDEF y el CCFFAA, así como el diseño de una política nacional de ciberdefensa por los mismos en conjunción con la PCM que pueda articular y servir de pivote para los esfuerzos de estas diferentes instituciones con otras entidades en materia de ciberdefensa.

2. Actores principales en ciberseguridad y ciberdefensa

El Perú existen diversos actores dedicados a la ciberseguridad y ciberdefensa, algunos dedicados a áreas mucho más específicas dentro del campo general de la seguridad o la defensa. De manera resumida, la entidad con capacidades operativas dedicadas a la ciberseguridad civil y de Administración Pública es el Centro Nacional de Seguridad Digital (CNSD) de la PCM; las encargadas de la ciberdefensa nacional son los cibercomandos de las tres armas de las FF.AA. bajo la dirección del COCID del Comando Conjunto de las Fuerzas Armadas (CCFFAA); la encargada de combatir la ciberdelincuencia es la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP; y la encargada de la ciberinteligencia es la DINI.

[261] *Ibid*, p. 10.

No obstante, como se verá más adelante, no existe una entidad o una doctrina que integre los esfuerzos conjuntos en ciberseguridad y ciberdefensa bajo estándares y tecnologías compartidas. Es decir, cada uno opera bajo sus propios lineamientos y doctrinas, pero sin mayor capacidad de posibilitar una óptima interoperabilidad entre ellas para cuando sea necesario combinarlas, sobre todo considerando que en la actualidad las amenazas en el ciberespacio son multidimensionales o híbridas y no se circunscriben a un único área de operaciones.

2.1. Centro Nacional de Seguridad Digital (CNSD)

Siendo la SEGDI el ente rector del Sistema Nacional de Transformación Digital, y, por lo tanto, de la seguridad digital y la ciberseguridad, el CNSD es la entidad encargada de la gestión, la dirección, la articulación y la supervisión de las actividades de operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital[262].

En ese sentido, tiene los siguientes objetivos:

- Promover la coordinación entre las entidades de la administración de redes informáticas de la Administración Pública Nacional, para la prevención, detección, manejo, recopilación de información y desarrollo de soluciones para los incidentes de seguridad.
- Coordinar, colaborar y proponer normas destinadas a incrementar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito de la Administración Pública Nacional.
- Asesorar técnicamente ante incidentes de seguridad en los sistemas informáticos que reporten los distintos organismos de la Administración Pública Nacional.

[262] Gob.pe, 2021a.

- Asesorar a los organismos de la Administración pública Nacional sobre las herramientas técnicas de protección y defensa de sus sistemas de información.
- Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas de la Administración Pública Nacional y facilitar el intercambio de información para afrontarlos. Al respecto, cabe resaltar que cuenta con medios de contacto para reportar incidentes de seguridad digital para tal fin.
- Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.
- Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas de la Administración Pública Nacional.
- Interactuar con coordinaciones de similar naturaleza.
- Promover el desarrollo de capacidades humanas y la adopción de estándares en materia de ciberseguridad.
- Proteger las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales frente a los ciberataques.
- Desarrollar y mantener actualizada las normas, leyes, políticas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad
- Garantizar la seguridad del ciberespacio frente a su uso ilícito o malicioso.[263]

El CNSD incorporó, a través del Decreto de Urgencia N° 007-2020 al Pe-CERT, que había sido creado en el 2009 con la resolución Ministerial 360-2009-PCM. En la práctica, el CNSD es la entidad encargada de liderar los esfuerzos para resolver, anticipar y enfrentar los ciberdesafíos, y coordinar la respuesta ante los ciberataques que afecten a la Administración Pública. Su objetivo principal, entonces, es la de proveer al país de seguridad en el entorno digital, es decir, mantener una óptima situación de ciberseguridad[264].

[263] Gob.pe, 2021c y 2021d.
[264] Gob.pe, 2021b.

La PCM, a través del CNSD, crea CSIRTs o grupos de trabajo con objetivos específicos en ciberseguridad. Uno de ellos es el foro de CSIRT electoral, que tiene reuniones semanales en las que se analiza, junto con las operadoras del sector privado y la DIVINDAT de la PNP, cómo se debe proteger las elecciones llevadas a cabo en el país, a qué aspectos deben estar atentos para detectar un ataque y qué rol tendrá cada entidad involucrada.

Operativamente, cuando se detecta un incidente cibernético que atente contra una entidad de la Administración Pública, el CNSD interviene para defender los sistemas vulnerados y repeler el ataque. Cuando se trata de un ataque cibernético a algún ACN, el operador del sector privado sería la primera línea de defensa, y en caso reporte y solicite el apoyo del CNSD, éste entraría, en coordinación con la DINI, a repeler el ataque. Cabe resaltar que además de la capacidad técnica que se requiere para este tipo de operaciones cibernéticas, es necesario contar con la experiencia que ofrecen los especialistas de dichas entidades o ACN, quienes son los mayores conocedores de sus procedimientos y funcionamiento internos.

Por ejemplo, si hubiese un ataque al Sistema de Comunicaciones del MRE (SICOMRE), los especialistas técnicos en ciberseguridad del CNSD requerirán de la orientación de los especialistas que conocen el proceso de funcionamiento del SICOMRE, que vendrían a ser los especialistas en informática del MRE e incluso algunos diplomáticos. Para ello, evidentemente, los especialistas y funcionarios del propio MRE deberán tener la capacidad de trabajar conjuntamente con el CNSD para hacer frente al ataque, lo cual también implica que tengan un mínimo nivel estandarizado de conocimiento sobre ciberseguridad.

No obstante, el CNSD se encuentra aún en implementación y cuenta con personal limitado. No cuenta con las capacidades de poder responder a varios y diversos incidentes cibernéticos graves que puedan ser simultáneos. Asimismo, no se encuentra en total capacidad de operar conjuntamente con las demás entidades dedicadas a la ciberseguridad y ciberdefensa. Por otro lado, la falta de concientización en la

Administración Pública acerca de la importancia de la ciberseguridad crea el problema de que muchas entidades del Estado no reporten incidentes cibernéticos y no compartan información sobre sus vulnerabilidades. La SEGDI está intentando capacitar personal y estandarizar los procesos de ciberseguridad en el Estado peruano, pero lo está haciendo lentamente.

2.2. Fuerzas Armadas del Perú (FF.AA.)

Las tres armas que componen las FF.AA., Ejército, Marina y Fuerza Aérea, cuentan con equipos de ciberdefensa o cibercomandos encargados de llevar a cabo acciones y operaciones preventivas y de respuesta en el ciberespacio, de acuerdo a sus funciones. El CCFFAA es el encargado de coordinar acciones conjuntas entre ellas, y por extensión, debería coordinar el trabajo en ciberdefensa de las tres armas mencionadas.

No obstante, aún no existe una coordinación real en estrategias ni operaciones de ciberdefensa, considerando que aún existen dificultades para coordinar estrategias operaciones conjuntas a nivel de fuerzas militares convencionales en teatros de operaciones que son físicos. Si bien cada arma de las FF.AA. trabaja bajo sus propias doctrinas para llevar a cabo operaciones en el ciberespacio, hace falta una doctrina unificada que oriente a las tres armas de manera unificada y que permita su interoperabilidad entre ellas y con otras entidades como la DINI y el CNSD.

2.2.1. Comando Operacional de Ciberdefensa (COCID)

La Ley de Ciberdefensa descrita anteriormente le provee a las FF.AA. y al CCFFAA un mandato que les brinda la responsabilidad de planificación y ejecución de operaciones militares en el ciberespacio de acuerdo al principio de la legítima defensa. Es decir, no se les provee, por lo menos en este marco normativo, de facultades ofensivas en el ciberespacio. Asimismo, el CCFFAA tiene la responsabilidad, bajo

mandato de la Ley de Ciberdefensa, de hacerse cargo de la ciberdefensa de los ACN cuando la capacidad de protección por parte de sus operadores, del sector responsable de cada uno de ellos, o de la DINI sea sobrepasada.

El brazo operacional del CCFFAA en materia de ciberdefensa es el Comando Operacional de Ciberdefensa (COCID), creado el 2019 con la misión de planear, organizar, dirigir y conducir Operaciones Conjuntas de Ciberdefensa con el fin de enfrentar amenazas a la seguridad y defensa nacional en y mediante el ciberespacio, asumiendo el C2 de ellas. Así, el COCID funciona como ente articulador entre los tres cibercomandos de las FF.AA. bajo la misión de defender y proteger la soberanía, los intereses, los recursos claves y los activos críticos nacionales para mantener las capacidades nacionales, frente a amenazas o ataque en y mediante el ciberespacio cuando afecten a la seguridad nacional[265].

Específicamente, las operaciones del COCID apuntan a defender, explotar y responder ante amenazas que afecten a la seguridad digital de las redes, los sistemas de información, las telecomunicaciones y los activos críticos de las fuerzas y medios de alto valor militar, de conformidad con la Ley de Ciberdefensa[266]. Cabe resaltar que los conceptos manejados en el CCFFAA acerca de ciberdefensa, incluyendo el de las amenazas híbridas, están basados en la conceptualización que hace la OTAN sobre los mismos temas[267]. Asimismo, el COCID pertenece a la iniciativa *CSIRT Americas* de la OEA[268].

Las capacidades con las que cuentan cada uno de los cibercomandos de las tres armas de las FF.AA. son esencialmente las mismas: 1) la defensa, que implica la protección de una red propia, de una IC o de su capacidad militar en general frente a una amenaza obvia; 2) la explotación o la disuasión, que incluye un sistema de alera temprana que

[265] Sosa, A. A., 2021.
[266] Gob.pe, 2020.
[267] Astudillo, C., 2021.
[268] Sosa, A. A., 2021.

permita identificar amenazas y adelantarse a ellas; y 3) la respuesta, que implica acciones ofensivas contra el adversario o contra la amenaza misma para neutralizarla.

2.2.2. Marina de Guerra del Perú (MGP)

La MGP es considerada la institución armada más avanzada en cuanto a ciberdefensa. Actualmente, es la única arma de las FF.AA. que cuenta con un CERT, aunque depende mucho de la colaboración estadounidense[269]. Asimismo, se encuentra construyendo un pabellón nuevo que será dedicado para este fin. Sus avances se explican por el apoyo y la coordinación constante que mantiene esta institución con los EE.UU.

La MGP ha sido la primera de las tres armas de las FF.AA. en establecer una comandancia operacional que se dedique exclusivamente a operaciones en el ciberespacio, habiendo creado su Comandancia de Ciberdefensa (COMCIBERDEF) en 2018[270], entidad que se encuentra al mismo nivel que las demás Comandancias Generales de la MGP[271]. Esta Comandancia tiene como misión garantizar los intereses nacionales en materia de ciberdefensa, y como visión ser un referente en la región.

Además, ha sido una de las primeras entidades en establecer un centro de procesamiento de datos o *data center* propio, y procura almacenar allí la mayor parte de su información. Adicionalmente, el *data center* le ha posibilitado establecer canales de comunicación y mecanismos adicionales de cooperación con otras entidades que también trabajan en ciberseguridad, como la empresa Telefónica.

Por otro lado, la MGP ha recibido asesoría y tiene nexos con varios países, especialmente EEUU, Brasil, Colombia, México, Alemania, España y Corea del Sur, a los que se ha enviado oficiales peruanos para que lleven a cabo pasantías, estudios

[269] Obando, E., 2021.
[270] Sosa, A. A., 2021.
[271] Del Carpio, L., 2021.

de especialización y estudios de maestría que les han permitido adquirir mejores capacidades en ciberdefensa desde el 2017. Además, esto sirve para que los oficiales peruanos informen de los avances alcanzados en aquellos países, y para ver qué experiencias se pueden replicar en el Perú. Cabe resaltar que estos oficiales deben tener una base de estudios en informática, electrónica o disciplinas afines; y no hay muchos en la MGP.

En cuanto a los entrenamientos y la formación en amenazas híbridas, la MGP, al igual que el resto de las FF.AA., cuenta con un Plan de Entrenamiento que se actualiza cada mes. No obstante, a resultado complicado llegar a realizar entrenamientos avanzados en ciberdefensa por razones coyunturales o presupuestales. Por otro lado, el concepto de amenazas híbridas sí se enseña de manera completa en la MGP.

La MGP y Telefónica tuvieron un rol central en monitorear y proteger la infraestructura de los Juegos Panamericanos del 2019 en Lima, considerado el escenario en la que se llevó a cabo la primera operación de ciberdefensa nacional. A este le seguirían 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[272], en la que también participaron los cibercomandos de la Fuerza Aérea del Perú (FAP) y del Ejército del Perú (EP), y la DINI.

2.2.3. Fuerza Aérea del Perú (FAP)

La FAP es considerada el arma en el segundo puesto en cuanto a capacidades y avances en ciberdefensa. En el 2019 creó e inauguró su primer *Data Center* y Centro de Amenazas Cibernéticas, y el 2020 se dispuso el funcionamiento del Grupo de

[272] Astudillo, C., 2021 y Sosa A. A., 2021.

Operaciones en el Ciberespacio (GROCE)[273], luego de haberse comprobado la utilidad del Departamento de Ciberdefensa, una unidad experimental establecida en el 2016[274].

Desde el año 2006, la FAP ya venía trabajando con el concepto de operaciones en el ciberespacio en su doctrina y documentos, que incluía capacidades de respuesta ofensivas como defensivas. En el 2014 se oficializaron estas operaciones, encargándoselas a la Dirección de Telemática y la Dirección de Inteligencia. Sin embargo, no existía un liderazgo claro sobre el tema de ciberdefensa, lo cual recién se logra cuando se crea el GROCE en el 2020.

El GROCE fue creado en un contexto en el que el tema de la ciberdefensa cobra mayor relevancia a nivel mundial. Su creación involucró el reclutamiento de los mejores talentos de la FAP en áreas de informática, inteligencia, legal, entre otras disciplinas. Eventualmente, se vela por la permanente capacitación de su personal, razón por la cual son enviados a estudiar a países como México, Colombia y EE.UU. para formarse en ciberdefensa[275]. No obstante, un problema detectado en la formación del personal es que se capacita a todos los oficiales por igual, sin tomar en cuenta sus perfiles especializados.

Por otro lado, el concepto de amenazas híbridas se enseña en todos los niveles y se utiliza desde la formación hasta el planeamiento estratégico. En cuanto a tecnología e infraestructura, la FAP cuenta desde el 2019 con un centro de monitoreo y un *data center* institucional de última generación. Así, la FAP busca mantener un estado de alerta y aptitud permanentes, considerando que la ciberdefensa es transversal a todos los aspectos de la defensa nacional[276].

[273] Sosa, A. A., 2021.
[274] García, A., 2021.
[275] *Ibid*.
[276] *Ibid.*

2.2.4. Ejército del Perú (EP)

El EP cuenta con el Comando de Ciberdefensa y Telemática (CITELE) desde el 2018[277]. Este cibercomando fue establecido en cooperación con Brasil, luego de que se desarrollara el talento humano necesario, producto de enviar a capacitar al extranjero, principalmente a países de Europa y Latinoamérica, a oficiales del ejército en materia de TIC, desde el 2003 que se adquirió una plataforma tecnológica que sirve para conectar a todos los cuarteles del ejército[278].

El personal que actualmente compone el CITELE proviene de los primeros puestos del curso de informática del EP. Por otro lado, los batallones del Ejército cuentan cada uno con una sección de ciberdefensa, con capacidades operaciones de combate. Internamente, el EP realiza juegos de guerra o simulaciones que involucran todos los retos informáticos que existen en situaciones reales. A través de estos juegos, bajo un espíritu de competencia, se logra capacitar y mantener preparado al personal[279].

El CITELE también busca concientizar acerca de la importancia de la ciberdefensa en la población civil, especialmente acerca de la ciberhigiene[280]. Esto responde al hecho de que la seguridad y al defensa nacional, como lo indica el Capítulo XII de la Constitución Política del Perú, es responsabilidad de todos los peruanos, sean personas naturales y jurídicas.

Los cibercomandos, entonces, se dedican a proteger las capacidades, los recursos y los sistemas de comunicación de su respectiva institución, sea EP, MGP y FAP. Como se ha visto, sí existe en cierta medida capacidades para llevar a cabo operaciones cibernéticas a gran escala para proteger capacidades, recursos y ACN en el marco de la realización de eventos o procesos nacionales importantes como elecciones, olimpiadas y acciones sanitarias. Para mejorar las capacidades del personal, el

[277] Sosa, A. A., 2021.
[278] Castillo, E., 2021.
[279] *Ibid*.
[280] *Ibid*.

CCFFAA procura su capacitación con la SEGDI, mediante el Programa de Especialización en Ciberseguridad y Ciberdefensa para el personal de las Fuerzas Armadas[281].

Habiéndose realizado aun pocas operaciones de este tipo, las capacidades de personal, tecnología y de acción conjunta siguen siendo trabajadas, y se espera desde el CCFFAA que el Perú pueda llegar a ser un referente en la región en materia de ciberseguridad y ciberdefensa. Asimismo, se quiere generar la idea de que los países de la región deben apoyarse mutuamente en materia de ciberdefensa cuando realicen actividades de gran escala que sean de interés compartido[282].

2.3. Policía Nacional del Perú (PNP)

La PNP cuenta desde el 2005 con la DIVINDAT, que se especializa en combatir delitos informáticos[283], especialmente los señalados en la Ley de Delitos Informáticos y la Ley de Seguridad Digital. Sus miembros están capacitados para llevar a cabo "patrullas virtuales"[284], recojo de evidencia e identificación de delincuentes informáticos[285].

De acuerdo a sus estadísticas, los delitos cibernéticos más cometidos en el Perú están referidos al fraude informático o el robo de dinero mediante diferentes modalidades. Entre las modalidades más comunes está la clonación de tarjetas o *skimming*, que consiste en copiar la banda magnética de una tarjeta financiera para luego transferir la información confidencial como el número y la claves a otra tarjeta en blanco, con el fin de realizar retiros asumiendo la identidad del titular real[286].

[281] Sosa, A. A., 2021..
[282] *Ibid*.
[283] Gestión, 2020.
[284] Benedet, M., 2020.
[285] Ministerio del Interior [MININTER], 20216.
[286] *Ibid*.

Otra modalidad común es el *pharming*, que consiste en el uso de páginas web falsas que suplantan a las originales, con el fin de apoderarse de información confidencial como usuarios y contraseñas de diversas aplicaciones web que luego se usarán en perjuicio del titular. Asimismo, el *phishing* es una modalidad común mediante la cual los delincuentes buscan acceder a información personal con el envío de correos falsos que solicitan siempre la actualización de información y credenciales personales. Evidentemente, estos ciberdelincuentes buscan conocer números de cuentas bancarias y claves de seguridad[287].

2.4. Dirección Nacional de Inteligencia (DINI)

La DINI es la agencia peruana de inteligencia estratégica con funciones con competencia en los frentes interno y externo del país, y preside el Consejo Nacional de Inteligencia (COIN), conformada por las agencias de inteligencias de las FF.AA., del CCFFAA, de la PNP y del MININTER; así como por el MRE, representado por el Director General de Asuntos Globales y Multilaterales.

En materia de ciberseguridad, la DINI cuenta con una Dirección de Contrainteligencia (CI) encargada, principalmente, de proteger a los ACN del Estado peruano, centrándose en detectar y prevenir amenazas a sus infraestructuras digitales y físicas. Estos ACN o IC está detallada en una lista de carácter secreto que es elaborada por la DINI con información suministrada por los diferentes sectores que componen el Estado peruano, e incluyen infraestructuras como represas, centrales hidroeléctricas, energéticas, aeropuertos, entre otros.

Cabe resaltar que gran cantidad de esta IC es gestionada por el sector privado, y que la ciberseguridad, entonces, depende de las empresas a su cargo. Si bien la DINI se mantiene en contacto con estos actores privados para concientizar acerca de la

[287] *Ibid.*

necesidad de contar con estrategias y capacidades de seguridad física y cibernética óptimas para proteger a la IC, la decisión final depende de las empresas, ya que la DINI no cuenta con el mandato legal de imponer decisiones sobre ellas. Esto es motivo de preocupación, ya que se genera la situación en la que ciertas empresas no mantienen suficientes capacidades de ciberseguridad, o de seguridad en general, para proteger efectivamente a la IC.

La experiencia de la DINI con el sector privado demuestra que existen problemas de confianza del segundo respecto del primero, lo cual ha dado como resultado casos en los que los operadores de los ACN no le permitían a la DINI a que los apoye en la atención a incidentes cibernéticos. Asimismo, es común que los operadores de ACN no reporten a la DINI cuando son atacados cibernéticamente.

De este modo, la IC en el Perú se encuentra un tanto vulnerable. Por un lado, al no estar todas protegidas en el dominio cíber, pueden ser blanco de ataques cibernéticos con mayor facilidad, y estos ataques pueden tener como consecuencia la disrupción de los servicios que provee la IC con potenciales efectos dañinos o hasta catastróficos sobre la situación de seguridad del Estado peruano o de su población en general.

Un problema adicional es que la lista de la IC o los ACN, que son establecidos por la DINI, no incluye a la banca ni al sistema financiero peruano. Este hecho es materia de debate en las comunidades peruanas de inteligencia y de ciberseguridad, puesto que su inclusión se considera necesaria en tanto una afectación grave a la banca y al sistema financiero traería consigo una fuerte disrupción en la economía nacional, con posibles consecuencias sociales debido al malestar y la incertidumbre que generaría la pérdida del capital que poseen las personas y las empresas en los bancos.

Por otro lado, la Dirección de CI en la DINI parece contar con un número limitado de especialistas en ciberseguridad. Por esta razón, incluso si la DINI se propusiera hacerse cargo de la ciberseguridad de toda la IC en el Perú, no tendría la capacidad ni los recursos humanos para ello. La mayor captación de profesionales en ciberseguridad y

la formación de los mismos, posiblemente mediante su Escuela Nacional de Inteligencia (ENI) es un tema pendiente en la DINI.

2.5. Ministerio de Relaciones Exteriores (MRE)

La Ley de Organización y Funciones del MRE (Ley N° 29357), en su artículo 6°, y su Reglamento de Organización y Funciones (ROF), en su artículo 3°, indican que está entre las funciones específicas del MRE participar en el Sistema de Seguridad y Defensa Nacional[288] establecido en el capítulo XII de la Constitución Política del Perú[289]. Se puede afirmar, entonces, que la Cancillería tiene una obligación en la seguridad y defensa del país, y por ello su participación en temas como la ciberseguridad y ciberdefensa es activa y se debe potenciar.

Internamente, la Dirección General para Asuntos Multilaterales (DGM) es el órgano de línea responsable de la promoción y defensa de los intereses y objetivos del Perú en el ámbito multilateral, incluyendo el tema de la seguridad internacional, la lucha contra el terrorismo y el control de drogas, en coordinación con los sectores competentes[290]. Asimismo, la DGM miembro del COIN y tiene una participación con capacidad de voz y voto al igual que el resto de sus miembros.

Adicionalmente, la Dirección de Seguridad y Defensa (DSD) de la DGM es la unidad orgánica responsable de la promoción y defensa de los intereses y objetivos del Perú a nivel multilateral en los asuntos de seguridad internacional y defensa, en coordinación con el Ministerio de Defensa y otros sectores competentes. Asimismo, es responsable de ejercer las funciones de la Oficina de Defensa Nacional del sector y aquellas funciones que le correspondan al Ministerio como parte integrante de la estructura del SINA[291]. Así, actualmente es la dirección del MRE encargada de los temas de

[288] Congreso de la República del Perú, 2009, p. 2 y Gob.pe, 2018, p. 2.
[289] Oficialía Mayor del Congreso, 2004, p. 32.
[290] Gob.pe, 2018, p. 36.
[291] *Ibid*, p. 38.

ciberseguridad, ciberdefensa y amenazas híbridas, al tratarse de asuntos de seguridad y defensa nacional.

Entre sus funciones específicas están identificar, analizar, coordinar, proponer y ejecutar las acciones de política exterior orientadas a promover y defender los intereses y objetivos del Perú en el ámbito multilateral ya sea regional, hemisférico o mundial; analizar el tratamiento multilateral a los asuntos de seguridad internacional, desarme, no proliferación y los demás temas que le sean encomendados; y formular y proponer la posición nacional en materia de seguridad y defensa en los foros multilaterales especializados, la elaboración de informes nacionales y la formulación de instrucciones para a la votación de las resoluciones en el ámbito de su competencia[292].

Asimismo, tiene como funciones promover el cumplimiento de los planes de acción, declaraciones y recomendaciones de las cumbres y conferencias internacionales vinculadas con los temas de la agenda de seguridad y defensa, de conformidad con el ordenamiento jurídico nacional; y coordinar con los sectores públicos y privados pertinentes a fin de articular la política exterior en materia de seguridad internacional y defensa[293].

En ese sentido, la DSD ha venido elaborando reportes situacionales e informes prospectivos en materia de ciberdefensa y amenazas híbridas. Además, reconociendo que es necesario fortalecer las capacidades de ciberdefensa de las FF.AA. y de su Comando Conjunto para poder garantizar el cumplimiento de los fines de la Ley de Ciberdefensa, viene desplegando esfuerzos a nivel bilateral y con bloques regionales con el fin de mejorar el intercambio de información y la identificación de oportunidades de cooperación en el ámbito de la ciberdefensa.

Como se indica desde la DSD, estos esfuerzos han incluido la instrucción a diversas misiones peruanas en el exterior para que promuevan la cooperación con fuerzas

[292] *Ibid*, p. 38.
[293] *Ibid*, p. 38-39.

armadas de países europeos en actividades de entrenamiento en ciberdefensa, el intercambio y la canalización de información que resulte relevante para fortalecer las capacidades, la infraestructura y el equipamiento de los comandos de ciberdefensa peruanos.

Asimismo, desde la DSD se considera importante el acercamiento con bloques regionales de integración como la UE y bloques de defensa como la OTAN para acceder a importantes centros dedicados a la ciberdefensa, como el CCDCOE y el *Hybrid CoE*, siendo este último reconocido por elaborar el único protocolo militar de ciberdefensa que apunta a ser aplicado universalmente, el Manual de Tallin.

En el ámbito multilateral, el Perú forma parte de importantes esfuerzos para regular el uso de las tecnologías de la información y comunicaciones en los ámbitos de la ciberdefensa y la lucha contra la criminalidad informática. Ejemplo de ello es la participación del Perú en dos grupos de trabajo la Comisión de Desarme de las Naciones Unidas - Primera Comisión sobre la Seguridad Internacional en el campo de las TICs: el Grupo de Expertos Gubernamentales (GGE) y el Grupo de Trabajo de Composición Abierta (OEWG).

En cuanto al GGE, su trabajo da como resultado recomendaciones para su adopción de los Estados miembros mediante resoluciones de la Asamblea General. Temáticamente, el GGE se enfoca en la identificación de amenazas existentes y emergentes; la aplicación del derecho internacional uso de las TICs; las normas, reglas y principios del comportamiento responsable de los Estados; las medidas para la construcción de confianza; y la construcción de capacidades.

Por otro lado, el Grupo de Composición Abierta sobre Desarrollos en el Campo de las Tecnologías de la Información y Comunicaciones en el Contexto de la Seguridad Internacional (OEWG-CTI), busca diseñar un marco en el ámbito de la seguridad internacional para las TICs, a la vez que se orienta a establecer entendimientos entre los Estados que permitan aplicar las recomendaciones de los GGE y ser un espacio en

el cual puedan participar la industria, la academia, la sociedad civil y otros actores privados.

Así, el Perú tiene la postura de considerar necesario contar con instrumentos legales internacionales para regular el ciberespacio en los términos del derecho internacional de los conflictos armados o DIH, y enfrentar a la ciberdelincuencia en sus múltiples facetas, de manera firme y acertada, sin perjuicio a la libertad de expresión y a la privacidad. En ese sentido, el Perú se encuentra adherido al Convenio sobre la Ciberdelincuencia o Convenio de Budapest, el cual constituye un marco para la cooperación internacional y el desarrollo de los esfuerzos nacionales para combatir la ciberdelincuencia. Finalmente, en orden con los principios que rigen la Política Exterior peruana, se considera que el desarrollo normativo internacional de dichos temas debe ser resultado de una negociación inclusiva, participativa y transparente entre los Estados Miembros de las Naciones Unidas.

3. Balance de la situación del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas

Existe una tendencia al aumento de las amenazas cibernéticas y de privacidad[294], y consecuentemente, una tendencia al aumento de que estas formen parte de amenazas híbridas que pueden afectar a varios sectores de la sociedad y del gobierno de manera simultánea, ya sea en el aspecto de la defensa, la economía, la infraestructura digital del Estado, los servicios esenciales, los bancos, las empresas, entre otros. Estas amenazas se han multiplicado durante la pandemia de la COVID-19, que ha forzado a Estados, empresas y a las sociedades en general a utilizar más intensivamente las tecnologías digitales.

De acuerdo al Reporte Ciberseguridad 2020 del BID y la OEA: “Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe”, el Perú aún no cuenta con una

[294] Gestión, 2020.

estrategia nacional de seguridad cibernética, sin embargo, como se ha mencionado anteriormente, sí ha puesto en marcha una recién naciente Política Nacional de Ciberseguridad y un marco jurídico ya desarrollado. Aun así, un análisis de la situación de preparación del Perú en materia de ciberseguridad y ciberdefensa, tanto a nivel del sector privado, del sector público y de los órganos encargados de la seguridad y defensa del país, muestra que aún hay aún mucho por mejorar.

En el aspecto civil de la ciberseguridad en el Perú, el sector privado es el que se encuentra más avanzado a comparación de las capacidades con las que cuentan las entidades de la Administración Pública. En un nivel superior se encuentran las entidades privadas de banca y finanzas, debido a la naturaleza misma de las actividades que desempeñan y a que se les exige el cumplimiento de normas en materia de ciberseguridad. En un segundo nivel se encuentran las empresas de tecnología que además funcionan alrededor del sector de banca y finanzas, como aquellas que se dedican a las telecomunicaciones y la informática en general.

Según el ESET Security Report 2020 de Latinoamérica, el 61% de las empresas peruanas encuestadas afirmó que cuenta con políticas de ciberseguridad; sin embargo, solo un 29% indicó que cuenta con un plan de respuesta y continuidad del negocio, y tan solo un 23% clasifica su información. Asimismo, resulta preocupante que las medidas más básicas de control no están implementadas en la totalidad de dichas empresas. La mayoría de estas organizaciones no cuenta con una solución de seguridad antivirus (78%), un *backup* de información (62%) o una solución de Firewall (62%). Se esperaría, por lo menos, que este tipo de medidas tan básicas estén presentes hoy en día en todas las empresas por su importancia y facilidad de adquisición.[295]

Este hecho se corresponde con la percepción casi generalizada en el sector privado peruano de que la ciberseguridad no es un aspecto importante a tomar en cuenta para sus empresas. La Encuesta Global de Seguridad de la Información 2019-2020 de EY

[295] *Ibid*.

señala que solo el 27% de empresas en el Perú incluye a la ciberseguridad desde la etapa de planificación en sus nuevas iniciativas empresariales; mientras que un 51% sostiene que la relación entre la ciberseguridad y sus líneas de negocio es inexistente o neutral[296].

Aun así, según la encuesta global de Gestión de Riesgos del Directorio de EY, el 48% de las empresas consultadas cree que los ataques cibernéticos y la violación de datos tendrán un impacto más que moderado en su negocio en los próximos doce meses. Por esta razón, sorprende que solo el 27% de empresas en el Perú realmente tomen en cuenta a la ciberseguridad en sus planes a futuro[297].

Al parecer, la razón de esta falta de consideración de la ciberseguridad como un elemento importante para las empresas, sería que la inversión en ella parecería no generarle rentabilidad o mayores beneficios al negocio. De este modo, las empresas peruanas, en general, tampoco innovan en sus sistemas de ciberseguridad. De acuerdo a Kris Lovejoy, Líder de Ciberseguridad Global de EY, "Cuando la función de ciberseguridad hable el idioma del negocio, dará el primer paso crítico para ser escuchada y entendida. Comenzará a demostrar valor porque podrá unir directamente los impulsores de negocios con lo que la ciberseguridad hace para habilitarlos, justificando sus gastos y efectividad. Esto mueve el debate de la reducción de riesgos a la innovación"[298].

Asimismo, la falta de educación y concientización de los trabajadores de una empresa, y de la sociedad en general, acerca de las amenazas informáticas y de la importancia de la ciberseguridad permite que los atacantes se aprovechen de su falta de alfabetización digital y vulneren su privacidad y la de la organización para la cual se trabaja. Además, la evidente falta de expertos en ciberseguridad u oficinas encargadas de la ciberseguridad en una empresa empeora su situación.

[296] *Ibid.*
[297] *Ibid.*
[298] *Ibid.*

Esto se evidencia en los resultados de la encuesta realizada por ESET, en la que solo un 31% de las empresas peruanas encuestadas dijo llevar a cabo actividades de concientización de manera periódica, mientras que un 49% lo realiza ocasionalmente, un 10% no las realiza y el 10% restante no lo hace actualmente, pero planea hacerlo próximamente[299].

La encuesta también evidencia que la existencia de un Oficial o Director de Seguridad de la Información (CISO, por sus siglas en inglés) en la empresa significa una reducción en los ataques de las que ésta es víctima. Así, la incidencia de los ataques con códigos maliciosos (*malware*), el método más utilizado por los ciberdelincuentes, se reduce del 34% al 29% en aquellas empresas que implementan capacitaciones de seguridad de forma periódica; y, sobre todo, en las que cuentan con un CISO. No obstante, la misma encuesta revela que un considerable 59% de las empresas peruanas no cuenta con un responsable de ciberseguridad que reporte al Directorio o que se encuentre a nivel de gerencia ejecutiva[300].

De este modo, el conjunto de estas faltas ha tenido como resultado que un 70% de las empresas encuestadas por EY afirmen que su empresa haya experimentado un incidente cibernético significativo entre el 2019 y 2020[301]. Entonces, la mayoría de las empresas en el Perú se encuentran vulnerables a las amenazas cibernéticas. Esto podría ser especialmente peligroso si se tratase de empresas que gestionan servicios importantes o esenciales para la población o entidades gubernamentales, ya que su afección podría tener efectos disruptivos sobre la situación de seguridad de la población y el Estado mismo. Cabe resaltar que estas tácticas de ciberdelincuencia las pueden realizar actores particulares como actores estatales, o ambos de manera asociada, lo cual configuraría una amenaza híbrida.

[299] *Ibid.*
[300] *Ibid.*
[301] *Ibid.*

Además, existe el problema bastante conocido por la DINI y el CCFFAA de que las entidades privadas operadoras de ACN como puertos, aeropuertos, gaseoductos, ejes energéticos, sistemas informáticos bancarios, sistemas satelitales, entre otros, no suelen reportar los incidentes cibernéticos que sufren. Es conocido también que niegan totalmente haber sido atacados cibernéticamente, incluso cuando el ataque ha sido detectado por la DINI o el CCFFAA[302]. Esto puede ser especialmente peligroso para la seguridad y defensa del Perú, ya que la neutralización de los ACN tendría graves efectos sobre la estabilidad social y económica internas, así como sobre las mismas capacidades militares y nacionales. Este es un problema pendiente por resolver, que implicará el trabajo en el fomento de la confianza entre los operadores privados de ACN, las FF.AA. y la DINI.

Por otro lado, el Estado peruano no cuenta con *data centers* propios, en tanto depende de servicios en la nube o de terceros. Esto genera una situación de vulnerabilidad en toda la información que de otra forma podría estar almacenada de manera segura en instalaciones que le pertenezcan al mismo Estado, ya que, al depender de servicios e infraestructura de terceros, éstos podrían acceder a dicha información, o peor, otorgarlo a otros. En ese sentido, se puede afirmar que el Perú no tiene internet soberano[303].

Por ejemplo, la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT) adquiere servicios informáticos en la nube a proveedores estadounidenses sin tomar en cuenta que estos puedan ser vigilados por EE.UU., sus agencias de inteligencia, o algún otro actor que vulnere aquellos servicios. Un caso ejemplar en este tema, en cambio, es el de Brasil, que además de contar con centros de procesamiento de datos propios, cuentan con sistemas satelitales propios, lo cual les permite asegurar que la información sensible del Estado brasileño no se filtre.

[302] Astudillo, C., 2021.
[303] Obando, E., 2021.

Se considera necesario que el Estado invierta en *data centers* locales potentes que puedan almacenar la información importante y sensible de las entidades gubernamentales y de seguridad y defensa del país. Además, estos *data centers* podrían aprovecharse para llevar a cabo ingeniería de datos y abrir así nuevas posibilidades de desarrollo tecnológico e informacional local.

La falta de *data centers* acarrea un problema en sí mismo, ya que, en tanto gran cantidad de información del Estado peruano está almacenado en el Internet, el corte repentino de este servicio, sea por causas de desastres naturales, conflictos armados o masivos ataques cibernéticos en las entidades que la proveen, implicará preocupantes pérdidas de información y grandes dificultades para acceder a ella. De acuerdo a especialistas en ciberseguridad, lo ideal es que los *data centers* sean establecidos en pares, siendo uno la copia en tiempo real del otro, para tener un soporte en caso de que el original se vea afectado, alterado, saboteado o destruido.

Adicionalmente, la dependencia del Estado en infraestructura digital externa genera otros riesgos. La conectividad del Perú se sostiene gracias al cable interoceánico de internet conectado con EE.UU. y manejado por el Comando Sur de los EE.UU. (SouthCom). Si este único cable fuese dañado estructuralmente y fuese incapaz de seguir funcionando, el Perú entero se quedaría sin internet[304]. Asimismo, naturalmente existe una vigilancia permanente de las comunicaciones que entran y salen del país por parte de quien gestiona el cable interoceánico, EE.UU.

Por otro lado, el Estado tiene cerca de cuarenta sistemas informáticos disímiles entre todas las entidades que lo componen, y los servidores que poseen son antiguos o casi obsoletos. Estos sistemas informáticos no están integrados y no se comunican entre sí. Esto genera preocupación ya que la falta de estandarización en los sistemas informáticos de las diferentes entidades de la Administración Pública dificulta el accionar del CNSD y el CCFFAA cuando deben intervenir ante un incidente

[304] *Ibid.*

cibernético grave, ya que las tecnologías y los sistemas que utilizan las entidades del Estado difieren entre sí. Así, ante un ataque cibernético masivo al Estado peruano, podría ser imposible proteger a todas sus entidades.

Asimismo, no existe en el Perú una preocupación ni concientización real y compartida entre los actores estratégicos como el sector privado y varias instituciones gubernamentales acerca de la importancia de la ciberseguridad y la ciberdefensa. Esto tiene como consecuencia que el Perú se encuentre en una situación vulnerable ante actores estatales y no estatales que pueden realizar una serie de acciones contra el país en el dominio cíber, o utilizarlos con otros fines, configurando así amenazas asimétricas al Estado peruano.

Lamentablemente, el mayor uso de las tecnologías de la información por parte del Estado y por parte de la población en general no ha traído consigo una mayor concientización ni uso de herramientas de ciberseguridad para su propia protección. Como bien menciona el informe de 2016 del Banco Interamericano de Desarrollo, "mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en Perú, la conciencia social es generalmente baja en lo que respecta a la seguridad cibernética"[305].

Efecto de esta falta de concientización en materia de ciberseguridad trae consigo problemas como la falta de colaboración, preparación y entrenamiento en el poco personal existente que se dedica o se está iniciando en la ciberseguridad. En la Administración Pública civil y el sector privado, no existe actualmente casi ninguna capacidad de entrenamiento que permita simular ataques cibernéticos reales que pongan a prueba las capacidades de colaboración y preparación operativa de las entidades públicas, los operadores de los ACN ni del propio CNSD.

[305] Benedet, M., 2020.

Esto también responde a la falta de un ente que organice estos entrenamientos y que asuma el liderazgo total e integral de incidentes cibernéticos que se lleven a cabo en más de un sector, es decir, de incidente que afecten a la vez a la ciberseguridad de las entidades de la Administración Pública, los ACN, y empresas privadas; así como la ciberdefensa nacional y, por ende, las capacidades de las FF.AA. En la actualidad, existe un ente rector o articular sectorial separado cada uno de sí en materia de ciberseguridad y ciberdefensa, así como para roles y áreas de operaciones específicos en seguridad digital, ciberdelincuencia y ciberinteligencia, como se muestra en la figura 1.

Tabla 1
Organización de las entidades del Estado peruano dedicadas a la ciberseguridad y ciberdefensa

Área específica	Capacidad nacional o institucional	Ente rector o articulador	Área de operaciones
Confianza digital	Interacciones digitales	PMC-SEGDI-CNSD SBS	Economía y Transformación Digital
Ciberseguridad	Capacidad tecnológica	PCM-SEGDI-CNSD	Sistemas informáticos
Ciberdefensa	Capacidad militar	MINDEF-CCFFAA-COCID	Seguridad Nacional
Ciberdelincuencia	Legislación nacional	PJ-MINJUS-MININTER-MP-PNP	Delitos informáticos
Inteligencia	Operaciones de inteligencia	DINI	Ciberinteligencia

Fuente: Astudillo (2021). Elaboración propia.

Como se ha visto en la presente tesis, cada área específica y su respectivo ente rector o articulador funciona, en la práctica, de manera independiente y con un marco normativo distinto para cada uno. Si bien no se cuestiona que se trabaje de manera especializada en cada área de operaciones para hacer frente a las diversas amenazas existentes en el ciberespacio, lo que sí se resalta es la falta de un ente rector o articulador para todas ellas. A modo de analogía, actualmente la ciberseguridad, la ciberdefensa y sus áreas específicas funcionan como si el EP, la MGP y la FAP funcionasen sin el CCFFAA, lo cual dificultaría gravemente su interoperabilidad.

Se considera necesaria la existencia de en ente rector o articulador para todo el sistema de ciberseguridad y ciberdefensa conjuntos, en tanto las amenazas existentes en el ciberespacio no se circunscriben a un solo área específica del dominio cibernético. Una entidad de este tipo serviría para orientar de manera estratégica a todos los actores relevantes en ciberseguridad y ciberdefensa hacia objetivos y metas comunes, bajo un direccionamiento y una doctrina compartidas que además faciliten el trabajo integrado y conjunto entre ellos.

Entre tanto, la atomización en las funciones de ciberseguridad y ciberdefensa nacionales representa otro factor que afecta negativamente las capacidades de preparación y respuesta conjunta que deben tener las entidades mencionadas para hacer frente a las amenazas cibernéticas que crecen en la era de la Cuarta Revolución Industrial.

Esta falta de unificación, preparación y capacidad defensiva y de respuesta ante vulneraciones cibernéticas vuelve al país, a sus instituciones, empresas, FF.AA. y su población vulnerables y hasta atractivos para ser víctimas de ataques cibernéticos como robo de información, invasión a la privacidad, sabotaje de sistema informáticos e instalaciones críticas, espionaje, soborno informático, desinformación y desestabilización social, guerra psicológica, entre otros. Esto significa una clara amenaza a la seguridad y defensa del Perú, y se considera necesario que se empiece a mejorar la situación del país al respecto.

4. Elementos a considerar para una propuesta de estrategia de política exterior que apunte al fortalecimiento de las capacidades del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas

Una propuesta de estrategia de política exterior que apunte al fortalecimiento de las capacidades en materia de ciberseguridad, ciberdefensa y amenazas híbridas debe estar orientado a integrar todos los elementos vistos anteriormente que conforman esquemas de ciberseguridad y ciberdefensa que le sean de utilidad al Estado peruano, sobre todo aquellos que, luego del análisis realizado, puedan complementar o suplir las falencias del Perú en dichos temas.

Priorizando los aspectos faltantes para que el Perú se encuentre generalmente preparado en temas de ciberseguridad y ciberdefensa, se tendría que apuntar, en el largo plazo, a tener primero un núcleo interno de comunicaciones internas que sea segura y que no dependa de proveedores externos, y de ser posible, que no dependa de tecnología de terceros. Asimismo, se requiere de una doctrina propia de ciberseguridad y ciberdefensa, que debe proyectarse al escenario internacional en base, justamente, a ella.

Esta doctrina debería venir del MINDEF o de la SEGDI. Una doctrina es necesaria en tanto le brindaría al Perú una posición común como Estado, la cual permitirá tener una Política Exterior clara en la materia tanto para asuntos bilaterales y multilaterales. En su ausencia, se puede afirmar que de todos modos es necesario apuntar hacia una menor dependencia de sistemas e infraestructuras informáticas y digitales que son proveídas por terceros, es decir, apuntar hacia un internet más soberano. Sin embargo, se tiene que pensar, además, en las posibilidades de asociatividad que tiene el Estado peruano con otros actores para poder ir mejorando sus capacidades en ciberseguridad, ciberdefensa y amenazas híbridas.

En ese sentido, una propuesta de estrategia de política exterior en estos temas debe contemplar dos ámbitos generales: la del personal, y la del desarrollo tecnológico propio. En primer lugar, el ámbito del personal debe incluir elementos como la capacitación, el entrenamiento y actualización constante en capacidades y conocimientos para actuales y futuros especialistas peruanos en ciberseguridad, ciberdefensa y amenazas híbridas. Estos especialistas, así mismo, deberían ser proveídos de los incentivos suficientes para poner su conocimiento en servicio del Estado peruano y para empezar a generar conocimiento y capacidades propias en el Perú desde una visión netamente peruana acorde a los intereses estratégicos del Estado.

En segundo lugar, el ámbito del desarrollo tecnológico propio incluye elementos como la transferencia de tecnología al Perú para poseer y desarrollar tecnologías propias, incluyendo generación de *software*, construcción de centros de procesamiento de datos y servidores propios, así como apuntar a la independencia tecnológica o el desarrollo tecnológico conjunto con aliados cercanos en materia de ciberseguridad y ciberdefensa a largo plazo.

Entonces, en vista de que el Perú es periférico en estos temas, y que quienes poseen los mayores avances son las organizaciones internacionales, centros de excelencia y Estados analizados en el segundo capítulo de la presente tesis, una propuesta de estrategia de política exterior que apunte al fortalecimiento de las capacidades mencionadas debe priorizar una alianza estratégica con alguno de aquellos actores, especialmente uno que sea capaz de proveer capacitación, entrenamiento y transferencia tecnológica al Perú.

Asimismo, debe ser un actor con el que el Perú comparta una visión similar respecto a la necesidad de contar con aliados capaces de defenderse frente a amenazas cibernéticas e híbridas que hoy en día pueden afectar a más de un Estado a la vez. Es importante que sea un actor que comparta valores similares a los Perú, ya que eso facilita la posibilidad de acercamiento y de transferencia de conocimientos, capacidades y tecnologías.

Tomando en cuenta ambos criterios, de capacidad y de visión compartida en materia de seguridad y defensa, resulta lógico y plausible que se proponga una estrategia de acercamiento y posible alianza estratégica con alguno o algunos de los siguientes actores, ya que el acercamiento con uno no implica negar el acercamiento con otro: el CCDCOE de la OTAN, la ENISA de la UE y el Hybrid CoE. Evidentemente, se trata de entidades que forman parte de organizaciones occidentales y que están compuestos por Estados que comparten valores similares a los del Perú.

Además, debido a la naturaleza multilateral o multi estatal de ellas, el Perú y sus instituciones que se asocien con dichas organizaciones podrían sacar mayor provecho del conocimiento de los varios Estados que las componen. Asimismo, el Perú no estaría sujeto a seguir una sola línea de pensamiento o una sola doctrina, lo cual sería más probable si es que se asocia con un solo Estado, por ejemplo, alguna de las potencias cibernéticas mencionadas en el capítulo segundo. Adicionalmente, el Perú estaría actualizado en cuanto a los esfuerzos multilaterales para afrontar las amenazas cibernéticas e híbridas, y como Estado podría liderar esfuerzos similares en Latinoamérica o en la OEA.

Asimismo, los especialistas enviados o que reciban capacitación y entrenamiento por parte de las organizaciones mencionadas permitirán mantener al tanto a las FF.AA., la PNP, la DINI y el MRE sobre los conflictos actuales en el ciberespacio, y les permitirá conocer el nivel de capacidad de los actores involucrados, así como podrán recibir experiencias y lecciones aprendidas de primera mano de quienes estén luchando en ciberguerras en ese momento.

Cabe resaltar que el acercamiento o la alianza con alguno de estos actores no significa que se imposibilite el acercamiento o la alianza con otros actores, incluso si aquellos terceros se consideren rivales entre sí, sobre todo si se toma en cuenta a las potencias cibernéticas mundiales y las relaciones entre ellas. Asimismo, sería ideal que a

mediano o largo plazo el Perú logre aliarse con más de uno de los actores mencionados, para evitar caer en una situación de sobre dependencia hacia uno solo de ellos.

De este modo, podría relacionarse con más de uno y dejar en claro que la relación del Perú con ellos solo se da a nivel de capacitación y entrenamiento en materia de ciberseguridad y ciberdefensa, y que ello no implica que el Perú esté necesariamente alineándose estratégica o políticamente a ellos; y que, por lo tanto, el Perú no se estaría involucrando en las relaciones entre aquellos actores ni en sus potenciales conflictos.

Finalmente, en cuanto a la situación del Perú frente al resto de países de la región, el Perú se encontraría en una situación ventajosa frente a sus vecinos y posibles rivales si es que desarrollase avanzados niveles de capacidad en ciberseguridad y ciberdefensa tanto en el aspecto defensivo como ofensivo, sobre todo considerando que hoy en día hay conflictos interestatales que se combaten enteramente en el ciberespacio, o que estos enfrentamientos en el dominio cíber son precursores para futuras acciones militares o de presión política, económica, diplomática o militar. Así, si bien el Perú no ocupa el primer puesto en cuanto a poderío militar convencional en la región, sí lo podría hacer en el quinto dominio de la guerra: el ciberespacio.

Conclusiones

- La conceptualización de la Seguridad y Defensa ha evolucionado en el tiempo. Hoy en día estos aspectos se manifiestan en diversos campos (militar, económico, político, psicosocial) y en cinco dominios (terrestre, marítimo, aéreo, espacial y ciberespacial). En ellos existen actores con intenciones y capacidades para generar algún daño a un Estado, lo cual configura una amenaza. Estas amenazas pueden ser convencionales cuando provienen de un actor estatal, no convencionales cuando proviene de un actor no estatal, o híbridas cuando proviene de actores estatales, no estatales o la combinación de ellos, con objetivos que pueden afectar diversas áreas de la seguridad humana.
- En la era de la Cuarta Revolución Industrial, resaltan las amenazas que se manifiestan en el ciberespacio, las cuales pueden afectar la seguridad, la defensa y los intereses de un Estado, así como al normal funcionamiento de la sociedad en general. Por ello, la ciberseguridad y la ciberdefensa son esenciales, en tanto sirven para proteger y responder ante ataques cibernéticos hacia la IC, las redes y los sistemas informáticos y digitales de entidades gubernamentales y de empresas, garantizando así, dentro de sus capacidades, la seguridad y la defensa de la sociedad
- Diversas organizaciones y organismos internacionales han desarrollado marcos normativos, capacidades, agendas e instituciones orientadas a la ciberseguridad, la ciberdefensa y la atención a amenazas híbridas, como la ONU, la OTAN, la UE y la OEA.
- Las grandes potencias mundiales como EE.UU., Rusia y China cuentan con avanzadas capacidades para llevar a cabo la ciberguerra en función de sus intereses. Estos países llevan a cabo constantes operaciones cibernéticas ofensivas y defensivas que, dependiendo de la naturaleza y el objetivo de éstas, pueden considerarse dentro del espectro de amenazas híbridas, ya que no sólo buscan afectar las capacidades militares convencionales de su rival, sino también influir en la toma de decisiones de alto nivel o en la opinión pública, infiltrarse y espiar sobre el adversario, sabotear sistemas esenciales de su sociedad civil, generar desorden

social y político, entre otros objetivos; y porque hacen uso de actores no estatales para la consecución de dichos objetivos.

- El Perú no cuenta con capacidades cibernéticas cercanas a las de los actores mencionados. Esto parece ser una tendencia en toda la región de América Latina, en tanto es una región periférica respecto de los conflictos cibernéticos en el mundo. Sin embargo, es una necesidad permanente poder contar con capacidades en ciberseguridad, ciberdefensa y de amenazas híbridas para poder contrarrestar cualquier ciberataque que pueda afectar al Estado, a sus intereses y a su población.
- La PNSD del Estado Peruano reconoce a las amenazas cibernéticas. En ese sentido, en el Perú existen la Ley de Delitos Informáticos (Ley N.° 30096) que penaliza crímenes en el ciberespacio, y la Ley de Ciberdefensa (Ley N.° 30999) que regula las operaciones militares peruanas en el ciberespacio. Esto se puede considerar un marco normativo inicial para futuros esfuerzos en materia de ciberseguridad y ciberdefensa.
- No obstante, no existe aún en el país una política nacional de ciberdefensa ni una entidad, estrategia o doctrina en ciberseguridad y ciberdefensa que oriente de manera integrada los esfuerzos del Estado peruano en dichos temas. Tampoco existe en vigor una ley que sea propiamente de ciberseguridad, aunque, desde el 2019 existe un dictamen de proyecto de Ley de Ciberseguridad (Proyecto de Ley No. 4237 y 4352) aún sin aprobarse.
- Los actores encargados de la ciberseguridad y ciberdefensa del país son la PCM mediante su CNSD, encargada de la ciberseguridad y seguridad digital en la Administración Pública; la DIVINDAT de la PNP, encargada de combatir la ciberdelincuencia; los cibercomandos de las FF.AA., bajo la dirección del COCID del CCFFAA, encargados de la ciberdefensa; y la DINI, encargada de la ciberinteligencia.
- El mayor uso de las tecnologías de la información por parte del Estado y por parte de la población en general no ha traído consigo una mayor concientización ni uso de herramientas de ciberseguridad para su propia protección. El Perú se encuentra en una situación vulnerable ante actores estatales y no estatales que pueden realizar

una serie de acciones contra el país en el dominio cíber, o utilizarlos con otros fines, configurando así amenazas asimétricas al Estado peruano.

- La Política Nacional de Ciberseguridad del 2017, aun por implementarse, indica que el Perú debe hacer uso de la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales que trabajan en ciberseguridad y ciberdefensa. Por ello, se considera que el Ministerio de Relaciones Exteriores tiene un rol central en este aspecto, por lo que es necesario que se elabore una estrategia de política exterior que apunte al fortalecimiento de las capacidades nacionales en materia de ciberseguridad, ciberdefensa y amenazas híbridas.
- Mediante la conformación de alianzas estratégicas con actores avanzados en ciberseguridad, ciberdefensa y amenazas híbridas; la formación y capacitación de especialistas civiles y militares en el país; la transferencia tecnológica y la generación de tecnologías propias; el Perú se encontraría, a largo plazo, en una situación ventajosa frente a sus vecinos y posibles rivales, tanto en el aspecto defensivo como ofensivo. Esto cobra mayor relevancia al considerar que hoy en día existen conflictos interestatales que se combaten enteramente en el ciberespacio, o que estos enfrentamientos en el dominio cíber son precursores para futuras acciones militares o de presión política, económica, diplomática o militar. Si bien el Perú no ocupa el primer puesto en cuanto a poderío militar convencional en la región, sí lo podría hacer en el quinto dominio de la guerra: el ciberespacio.

Bibliografía

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2021a). *Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad.* https://www.enisa.europa.eu/about-enisa/about/es

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2021b). *CSIRTs by Country – Interactive Map.* https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Spain

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2021c). *Cyber Europe.* https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2021d). *Cyber Europe 2020.* https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020

Astudillo, C. (2021, 30 de octubre). *Importancia de la Ciberdefensa en el Perú* [Ponencia]. Exposiciones EXPO CYBER 2021, Lima, Perú.

Benedet, M. (2020). Ciberseguridad en Perú hoy: realidad y acción. *Lemontech Blog.* https://blog.lemontech.com/ciberseguridad-en-peru-hoy-realidad-y-accion/

Cárdenas, W. (2015). *Ciberdefensa y ciberseguridad en el sector Defensa de Colombia* [Especialización de Seguridad Informática]. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00002590.pdf

Castillo, E. (2021, 30 de octubre). *Conversatorio entre los miembros de Ciberdefensa de las FFAA* [Ponencia]. Exposiciones EXPO CYBER 2021, Lima, Perú.

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN [CCDCOE]. (s/f). https://ccdcoe.org/

Comisión Europea. (s/f). *NIS Directive*. https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Comisión Europea. (2021a). *European cooperation network on elections.* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

Comisión Europea (2021b). *Joint Cyber Unit*. https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

Comisión Europa. (2021c). *NIS Cooperation Group.* https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Comisión Europea. (2020a). *European Democracy Action Plan*. https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

Comisión Europea (2020b). *Proposal for directive on measures for high common level of cybersecurity across the Union.* https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Comité Interamericano contra el Terrorismo [CICTE]. (2020). Plan de trabajo 2020-2021. https://translate.googleusercontent.com/translate_c?hl=en-US&sl=es&tl=en&anno=2&prev=search&u=http://scm.oas.org/doc_public/SPANISH/HIST_20/CICTE01350S03.doc&usg=ALkJrhhwx2MkFXfhuTddARlHMnWRKUc1ZA

Congreso de la República del Perú. (2019, 27 de agosto). Ley N° 30999 Ley de Ciberdefensa. *El Peruano*, 9-10. https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

Congreso de la República del Perú. (2013, 21 de octubre). Ley N° 30096 Ley de Delitos Informáticos. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Congreso de la República del Perú. (2009, 12 de mayo). Ley N° 29357 Ley de Organización y Funciones del Ministerio de Relaciones Exteriores. http://www.rree.gob.pe/elministerio/documents/ley29357.pdf

Consejo de Europa. (2001). *Convention on Cybercrime*. https://rm.coe.int/1680081561

Constantin, L. (2020). SolarWinds attack explained: And why it was so hard to detect. *CSO*. https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

Cooperación Estructurada Permanente [PESCO]. (s/f). *About PESCO*. https://pesco.europa.eu/

CSIRT Americas. (2016). CSIRT Americas. https://csirtamericas.org/

CSIRTs Network. (s/f). *CSIRTs Network*. https://csirtsnetwork.eu/

Cybersecurity & Infrastructure Security Agency [CISA]. s/f. https://www.cisa.gov/critical-infrastructure-sectors

Decreto Legislativo N° 1412. (13 de setiembre de 2018). Normas Legales, N° 14646, Diario Oficial El Peruano. https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/

Decreto Supremo N° 012-2017-DE. Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional. (22 de diciembre de 2017). Normas Legales, N° 16137, Diario Oficial El Peruano. https://busquedas.elperuano.pe/download/url/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1

Del Carpio, L. (2021, 30 de octubre). *Conversatorio entre los miembros de Ciberdefensa de las FFAA* [Ponencia]. Exposiciones EXPO CYBER 2021, Lima, Perú.

Equipo de Respuesta ante Emergencia Informáticas de la Unión Europa [CERT-EU]. (s/f). *CERT-EU*. https://cert.europa.eu/cert/plainedition/en/cert_about.html

Fatić, A. (2002). Conventional and unconventional – 'hard' and 'soft' security: the distinction. *Journal for Labour and Social Affairs in Eastern Europe*. *5*(3) 93-98.

Flournoy, M. y Sulmeyer, P. (2018). Battlefield Internet: A Plan for Securing Cyberspace. *Foreign Affairs*, *97*(5), 40-46. https://www.jstor.org/stable/43292068

García, A. (2021, 30 de octubre). *Conversatorio entre los miembros de Ciberdefensa de las FFAA* [Ponencia]. Exposiciones EXPO CYBER 2021, Lima, Perú.

Gestión. (2020). Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia? *Gestión*. https://gestion.pe/publirreportaje/ciberseguridad-en-el-peru-que-tan-preparados-estamos-para-enfrentar-la-ciberdelincuencia-noticia/?ref=gesr

Gob.pe. (2021a). *Centro Nacional de Seguridad Digital*. https://www.gob.pe/institucion/pcm/campa%C3%B1as/4730-centro-nacional-de-seguridad-digital

Gob.pe. (2021b). *Equipo de respuesta ante incidentes de seguridad digital del Perú*. https://www.gob.pe/7739-presidencia-del-consejo-de-ministros-equipo-de-respuesta-ante-incidentes-de-seguridad-digital-del-peru

Gob.pe. (2021c). *Objetivos del Centro Nacional de Seguridad Digital*. https://www.gob.pe/13907-objetivos-del-centro-nacional-de-seguridad-digital

Gob.pe. (2021d). *Reportar incidentes de seguridad digital*. https://www.gob.pe/14084-reportar-incidentes-de-seguridad-digital

Gob.pe. (2020). *Ministro de Defensa inauguró instalaciones del Comando Operacional de Ciberdefensa*. https://www.gob.pe/institucion/ccffaa/noticias/505601-ministro-de-defensa-inauguro-instalaciones-del-comando-operacional-de-ciberdefensa

Gob.pe. (2018). *Reglamento de Organización y Funciones (ROF) del Ministerio de Relaciones Exteriores*. https://www.gob.pe/institucion/rree/informes-publicaciones/1388-reglamento-de-organizacion-y-funciones-rof-del-ministerio-de-relaciones-exteriores

International Business Machines Corporation [IBM], s/f. *What is cybersecurity?* https://www.ibm.com/topics/cybersecurity

Ministerio del Interior [MININTER]. (2016). *Ciberpolicías contra delitos informáticos*. https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Multinational Capability Development Campaign [MCDC]. (2019). *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*.

Niubox. (2019). *Congreso peruano aprueba leyes de ciberdefensa y ciberseguridad*. https://niubox.legal/congreso-peruano-aprueba-leyes-de-ciberdefensa-y-ciberseguridad/?lang=en

Obando, E. (2021, 15 de setiembre). *Conferencia sobre Ciberdefensa* [Conferencia]. Lima. meet.google.com/iwh-ibmj-oqc

Oficina de Publicaciones de la Unión Europea. (s/f). *EUR-Lex*. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC*

Organización de las Naciones Unidas [ONU]. (s/f). *Office of Counter-Terrorism*. https://www.un.org/counterterrorism/about

Organización de los Estados Americanos [OEA]. (2021). *OEA*. http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Organización de los Estados Americanos [OEA]. (2003). Declaración sobre Seguridad en las Américas. http://www.oas.org/juridico/spanish/decl_security_sp.pdf

Organización del Tratado del Atlántico Norte [OTAN] (2017). Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Piqué, J. (2021). Rusia y China: un matrimonio sin amor. *Política Exterior*. *https://www.politicaexterior.com/rusia-y-china-un-matrimonio-sin-amor/?fbclid=IwAR3FoR3JDamV7OO0wUhi6a5r3dKxI7OvKgjNGsjopa63YEY5SPXRsO7Fwak*

Politico. (2021a). *EU medicines agency says hackers manipulated leaked coronavirus vaccine data*. https://www.politico.eu/article/european-medicines-agency-ema-cyberattack-coronavirus-vaccine-data/

Politico. (2021b). *EU to launch rapid response cybersecurity team.* https://www.politico.eu/article/eu-joint-cyber-unit-rapid-response-cyberattacks/

Presidencia del Consejo de Ministros [PCM]. (2019). *Perú se adhiere al Convenio de Budapest para luchar contra la ciberdelincuencia.* http://www.pcm.gob.pe/2019/02/peru-se-adhiere-al-convenio-de-budapest-para-luchar-contra-la-ciberdelincuencia/

Riordan, S. (2019). *Por qué necesitamos diplomáticos en el ciberespacio.* https://www.esglobal.org/por-que-necesitamos-diplomaticos-en-el-ciberespacio/

Robinson, P. (2008). Dictionary of International Security.

Sari, A. y Lauva, A. (2018). Hybrid Threats and the United States National Security Strategy: Prevailing in an "Arena of Continuous Competition". *Ejil: Talk!*. https://www.ejiltalk.org/hybrid-threats-and-the-united-states-national-security-strategy-prevailing-in-an-arena-of-continuous-competition/

Secretaría de Gobierno Digital. (2017). Política Nacional de Ciberseguridad. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. https://www.pdfdrive.com/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations-e180122657.html

Sosa, A. A. (2021, 30 de octubre). *El Comando Operacional de Ciberdefensa* [Ponencia]. Exposiciones EXPO CYBER 2021, Lima, Perú.

Unión Europea [UE]. (2021, 12 de octubre). *Últimos desarrollos en ciberseguridad en la UE* [Diapositivas de PowerPoint].

Valeriano-Ferrer, F. (2013). *Apuntes sobre Defensa Nacional*. https://repositorio.esup.edu.pe/handle/20.500.12927/28

Vargas, R., Recalde, L., y Reyes, R. (2017). *Ciberdefensa y ciberseguridad, más allá Del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa.* URVIO, Revista Latinoamericana de Estudios de Seguridad. http://dx.doi.org/10.17141/urvio.20.2017.2571

Wolff, J. (2021). Understanding Russia's Cyber Strategy. *Foreign Policy Research Institute*. https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/

Yu, Y. (2018). China's Hybrid Warfare and Taiwan. *The Diplomat.* https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/