MAESTRÍA EN ESTRATEGIA MILITAR

Tema: **Las Operaciones Cibernéticas**

Título: **El rol y las capacidades cibernéticas de las Fuerzas Armadas de la República Argentina en el marco de los conflictos futuros**

Autor: **Comodoro Maximiliano Luis Ravera**

Director: **Brigadier Mayor (R) Mg. Alejandro Moresi**
Co-Director **Teniente Coronel (R) Carlos Amaya**

Marzo, 2024

CONTENIDO

INTRODUCCIÓN

La República Argentina identificó la utilización del ciberespacio con fines militares como un riesgo y la no consolidación de dicho ambiente operacional como una amenaza a la defensa nacional, reconociendo la necesidad de adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional, y de aquellas que sean designadas para su preservación. Esto demanda contar con capacidades que permitan efectuar operaciones cibernéticas en forma permanente, a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

El Comando Conjunto de Ciberdefensa es quien conduce las operaciones militares en la República Argentina y coordina sus acciones con los centros específicos de las Fuerzas Armadas brindando protección cibernética a las redes informáticas de la defensa y, a orden, a las infraestructuras críticas.

La globalización y la innovación tecnológica han sido grandes generadores de cambios llevando a una mayor complejidad de la guerra que ya no se presenta de la manera tradicional sino con diferentes formas pudiendo involucrar una multiplicidad de actores entre los cuales los ejércitos regulares de un Estado pueden intervenir o no, y en los que, en determinadas áreas, hasta el momento, no existe un acuerdo en la legislación internacional.

Si bien la guerra no ha cambiado en naturaleza, si lo ha hecho su carácter y la forma de combatir. El Instrumento Militar ha perdido protagonismo en un contexto global de constante competencia que involucra todos los factores de poder de los Estados. Los nuevos principios de la guerra ya no utilizan sólo a las Fuerzas Armadas para someter la voluntad del enemigo, sino que usan todo tipo de medios, militares y no militares, letales y no letales para doblegar la voluntad del oponente. Todo ello en un campo de batalla sin fronteras, donde confiar únicamente en las Fuerzas Armadas y su armamento militar para lograr la seguridad nacional protegiendo los intereses del Estado, en el sentido estratégico más amplio, ya no es suficiente porque la guerra se ha extendido más allá de los límites (Liang & Xiangsui, 2004).

Los conflictos actuales se presentan de forma multifacética y fuera de los parámetros tradicionales, suelen ser transfronterizos, multijurisdiccionales, y sus protagonistas pueden actuar de forma pública y/o privada, civil y/o militar, legal y/o ilegal. Esto dificulta a los Estados hacerles frente con sus Fuerzas Armadas, por un lado, y sus Fuerzas de Seguridad y Policiales por otro, requiriendo ser abordadas de manera interagencial (Trama, Guerrero, & De Vergara, 2019, p. 8).

Las características de los conflictos del siglo XXI han dado lugar al surgimiento de conceptos como conflictos de zona gris[1] y guerra híbrida[2].

John Arquilla y David Ronfeldt sostienen que, la ciberguerra y la guerra de red son conceptos del nuevo espectro de conflicto surgido a raíz de la revolución de la información (Arquilla & Ronfeldt, 2001, pág. 1). La utilización de las TIC[3] para interrumpir las actividades de un Estado u organización mediante ataques cibernéticos con intenciones de sabotaje, propaganda, perturbación económica o social, denegación de servicios en general o afectación de infraestructuras críticas u objetivos estratégicos en particular, entre otras, son cada vez más notorias, aunque muchas veces no puedan ser comprobadas.

Ejemplos de casos emblemáticos han sido la primera operación cibernética rusa en Estonia en 2007, la intrusión de Stuxnet en Irán en 2010 y la operación encubierta rusa en las elecciones presidenciales de EE.UU. en 2016. Los ciberataques rusos a Estonia en 2007 afectando servicios, periódicos online, bloqueando webs gubernamentales, bancos online e infraestructuras públicas desde salud hasta los semáforos durante semanas pusieron en evidencia la vulnerabilidad del internet de las cosas[4] (McGuinness, 2017). La operación Juegos Olímpicos, que consistió en la intrusión informática del gusano israelí-estadounidense Stuxnet en la planta de enriquecimiento de uranio iraní de Natanz en 2010, no sólo se trató de haber logrado acceder desde el exterior al corazón de los sistemas de control de unas instalaciones críticas, sino de la aparición de un método novedoso que abría el camino a toda una nueva generación de virus espía capaz de actuar de forma casi autónoma sobre los sistemas de control de supervisión y adquisición de datos con un potencial aterrador (Gibney, 2016).

La intervención encubierta de piratas informáticos rusos durante la campaña electoral presidencial de los EEUU en 2016 con el hackeo de correos electrónicos y documentos del Partido Demócrata y su lenta filtración entre julio y octubre, una compleja y calculada operación de

[1] *Zona Gris:* concepto utilizado por el realismo ofensivo para enmarcar un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado. El conflicto en la zona gris gira en torno a una incompatibilidad relevante para al menos uno de los actores. Las estrategias utilizadas son multidimensionales, de implementación gradual y con objetivos a largo plazo (Jordán, 2018, pág. 133).

[2] *Guerra híbrida*: forma de lucha caracterizada por la plena integración en tiempo y espacio de procedimientos típicamente convencionales con tácticas propias de la guerra irregular, desde las clásicas emboscadas o acciones de propaganda, agitación e insurgencia hasta actividades de guerra informativa, guerra legal o ciberguerra, mezcladas éstas últimas con actos terroristas y conexiones con el crimen organizado para la obtención de apoyos y asistencia de todo tipo (Hoffman, 2009).

[3] *TIC*: Tecnologías de la Información y Comunicaciones.

[4] *Internet de las cosas (IoT)*: "Se le llama internet de las cosas, en inglés Internet of Things (IoT) a la posibilidad de interconexión y transmisión de datos entre objetos cotidianos e internet. Los aparatos eléctricos y electrónicos y los dispositivos digitales con los que convivimos tienen circuitos y sensores que les permite ejecutar programas, recolectar y compartir datos con la internet sin la intervención de personas" (Gobierno de Argentina, 2023).

desinformación en redes sociales, y una sospecha de connivencia con miembros de la campaña de Donald Trump (Noujaim & Amer, 2019), independientemente del resultado del proceso electoral, revela como mediante la utilización de la tecnología y la inteligencia artificial[5] sumado a técnicas de big data[6] y data analitycs[7] el comportamiento de grandes poblaciones puede ser modificado.

La invasión rusa a Ucrania a partir del 24 de febrero de 2022 podría catalogarse como el mayor conflicto militar a gran escala de la era cibernética, y el primero en incorporar múltiples operaciones cibernéticas en muchas partes y de manera significativa. La guerra de Ucrania nos permite visualizar como la explotación del ciberespacio incide y se complementa con otras operaciones, cinéticas o no, para poder lograr efectos favorables.

En este contexto adquiere singular importancia el ciberespacio como quinto dominio, un ámbito de circulación de información virtual que atraviesa a los espacios físicos tradicionales en donde no existen límites entre lo público y lo privado, tienen lugar las operaciones cibernéticas, constituye un ámbito de actuación operacional del Instrumento Militar junto a otros múltiples actores, ofrece una mayor libertad de acción para el manejo de la información y una nueva dimensión para conducir la guerra.

Los Estados se han vuelto más vulnerables ante el surgimiento de nuevas amenazas a través del espacio cibernético formando parte este tema de la agenda internacional. Esta preocupación se observa en sus respectivos documentos de defensa y seguridad nacional obligando a sus Fuerzas Armadas a tener que adaptarse para poder hacer frente a estos desafíos. La utilización de nuevas tecnologías asociadas a la defensa es imprescindible. El rol de las Fuerzas Armadas en la defensa ciberespacial dependerá de la participación y la utilización que cada Estado quiera darle para lograr los objetivos de la política. La distinción que hace la legislación de la República Argentina, con respecto a los conceptos seguridad[8], referido a la seguridad pública interna cuya responsabilidad es asignada a las Fuerzas de Seguridad y Policiales; y defensa[9], referido a la seguridad pública externa cuyos responsables son las Fuerzas Armadas, agrega mayor dificultad en el ambiente del espacio cibernético donde confluyen acciones de autoría anónima y sólo pueden ser mensurables por sus

[5] *Inteligencia artificial* (IA) Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico (RAE, 2023).
[6] *Big data*: se refiere a una gran cantidad de información que sólo se puede procesar mediante el uso de herramientas digitales y que sirve para responder preguntas a través del análisis de enormes volúmenes de datos (Argentina G. , 2023).
[7] *Data analitycs*: Análisis de datos implica el uso de datos, técnicas y herramientas que identifican patrones y tendencias, que a su vez generan información procesable que respalda la toma de decisiones informadas (CompTIA, 2023).
[8] Ley N° 24.059 de Seguridad Interior
[9] Ley N° 23.554 de Defensa Nacional

efectos. De acuerdo al rol asignado, las Fuerzas Armadas podrán adecuar sus estructuras y desarrollar capacidades para intervenir dentro del ambiente operacional del espacio cibernético.

La República Argentina en su actualización del Libro Blanco de la Defensa 2015 expresó su interés en avanzar en la investigación, desarrollo y aplicación de las tecnologías vinculadas al ciberespacio desde el Sistema de Defensa Nacional, considerando sus contribuciones como críticas para hacer viables los efectos pretendidos en el marco de una estrategia de carácter defensivo y esenciales, para contar con una alerta estratégica temprana frente a una eventual agresión externa, y para desarrollar eficazmente la conducción de las operaciones militares y repeler con éxito dicha agresión (Defensa, Libro Blanco, 2015, págs. 25, 32).

En tal sentido, el Ministerio de Defensa por Resolución MD N° 08/2010 estableció un Grupo de Tareas para abordar la temática específica desde el punto de vista de la Defensa Nacional, creando un Programa Nacional de Infraestructuras Críticas de la Información y de la Ciberseguridad (Resolución JGM N° 580/2011), un Elemento para tratar Proyectos, Doctrina, Organización y Competencias vinculados con la materia (Resolución EMCO N° 59/2012), la Unidad de Coordinación (Resolución N° 385/2013), el Plan Estratégico para el Instrumento Militar (Directiva EMCO N° 02/2013), hasta llegar a la creación del Comando Conjunto de Ciberdefensa, con dependencia orgánica, funcional y operacional del Estado Mayor Conjunto de las Fuerzas Armadas, y con la misión de "ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar" (Resolución MD N° 343/2014).

Al mismo tiempo, la Directiva de Política de Defensa Nacional (DPDN) Decreto N° 2645/2014 contempló el desarrollo de capacidades operacionales en la dimensión ciberespacial con el objeto de adquirir competencias en los ambientes terrestre, naval y aéreo, así como de seguridad cibernética de redes pertenecientes al Sistema de Defensa Nacional y respecto de los objetivos de valor estratégico definidos por el Nivel Estratégico Nacional y la elaboración de un Plan de Desarrollo de defensa ciberespacial para el período 2014-2017 (Capítulo III, Anexo I, Decreto PEN Nº 2645/2014)[10].

La posterior DPDN Decreto PEN N° 703/2018 estableció como un tipo de operación militar en tiempo de paz la vigilancia y control del ciberespacio a fin de anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar el Sistema de Defensa Nacional, como

[10] DPDN Decreto PEN Nº 2645/2014 (Argentina G. , 2015)

así también acciones contra las infraestructuras críticas del país o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia, observando la necesidad de fortalecer estas capacidades; y por Decreto PEN N° 150/2018 oficializó el cargo de Subsecretario de Ciberdefensa bajo la órbita de la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa para hacerse cargo de uno de los principales ejes de la Defensa a futuro (Argentina B. O., 2018).

En 2019, el Ministerio de Modernización por Resolución N° 829/2019 aprobó la Estrategia Nacional de Ciberseguridad de la República Argentina, y el Ministerio de Defensa por Resolución N° 1380/2019, la Política de Ciberdefensa de la República Argentina. Esta última, en su anexo 4, establecía entre sus objetivos "adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la Defensa" fijando como prioridad operacional "desarrollar capacidad de disuasión y aptitudes ofensivas de respuesta ante amenazas de ataque que comprometan la libertad de acción en el ciberespacio" (Argentina G. , 2019).

La última DPDN Decreto N° 457/2021 (Anexo IF-2021-60150305-APN-SSPEYPM#MD) estableció que la Ciberdefensa debe garantizar el resguardo soberano sobre la infraestructura de las TICs localizadas en el territorio nacional y minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el Instrumento Militar, en cumplimiento de la normativa vigente en materia de Defensa Nacional (Argentina G. , 2021).

En enero de 2023, la actualización de la Política de Ciberdefensa (Resolución MD N° 105/2023) estableció que "la ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el instrumento militar en cumplimiento de la normativa vigente en materia de Defensa Nacional" (Argentina G. , 2023).

La necesidad de desarrollar capacidades acordes a los objetivos planteados en estas políticas llevó a plantear la siguiente investigación ¿Cuál será el rol de las Fuerzas Armadas de la República Argentina según el carácter de los conflictos futuros y qué capacidades cibernéticas serán necesarias para enfrentar las nuevas amenazas?

El objetivo de este trabajo ha sido identificar el rol de las Fuerzas Armadas de la República Argentina en la ciberguerra y las capacidades que se necesitan para enfrentar las nuevas amenazas en los conflictos. En tanto, los objetivos específicos consistieron en determinar las implicancias del

espacio cibernético para la Defensa, los efectos del avance tecnológico en esa dimensión y la utilización militar que se le podría dar en el futuro, comprender cómo se aborda la defensa cibernética en los ámbitos global, regional y nacional y el rol de sus Fuerzas Armadas, e identificar qué capacidades de ciberguerra son necesarias para una defensa efectiva en la República Argentina.

Como intento de respuesta se planteó como hipótesis que, para obtener la victoria en la forma de combate moderno a través del ciberespacio se requiere que el IM desarrolle capacidades para conducir operaciones cibernéticas defensivas, ofensivas, de explotación y de información tanto en la paz como en la guerra que le permitan accionar desde una posición relativa favorable mediante el ejercicio de una cibersupremacia o cibersuperioridad conocida o desconocida por el adversario.

El problema se encuentra embebido en un marco jurídico muy amplio que parte de una conceptualización diferenciada de la seguridad a nivel nacional a partir de la Ley N° 23.554 de Defensa Nacional (1988), con sus normas complementarias y modificatorias, y la Ley N° 24.059 de Seguridad Interior (1992), también con sus respectivas normas complementarias. Involucra además a la Ley N° 25.520 de Inteligencia Nacional (2001), su modificación Ley Nº 27.126 Agencia Federal de Inteligencia (AFI) y normas complementarias.

Vinculados con la Defensa Nacional adicionalmente a la Ley N° 23.554 de Defensa Nacional (1988) y su reglamentación Decreto PEN N° 727/06, se consideraron el Decreto PEN N° 1691/06 Directiva de Organización y Funcionamiento de las FFAA, la Ley N° 24948 de Reestructuración de las FFAA (1998), el Decreto PEN Nº 1729/2007 Ciclo de Planeamiento de la Defensa Nacional, la Resolución MD N° 343/2014 Creación del Comando Conjunto de Ciberdefensa, el Decreto PEN N° 42/2016 Creación de la Subsecretaría de Ciberdefensa, la Directiva de Política de Defensa Nacional (DPDN) Decreto PEN N° 1714/2009 y posteriores actualizaciones (Decreto PEN Nº 2645/2014, Decreto PEN N° 703/2018, Decreto PEN Nº 571/2020, y Decreto PEN Nº 457/2021), la Resolución MD N° 1380/2019 Política de Ciberdefensa de la República Argentina y su actualización (Resolución MD N° 105/2023), la Resolución MD N° 127/2023 Plan Plurianual de Ciencia, Tecnología, Innovación y Producción para la Defensa, y la Publicación Conjunta PC 10-04 Planeamiento para la Acción Militar Conjunta – Nivel Estratégico Militar (2018).

Las normas principales dentro de la Seguridad Interior relacionadas con los delitos informáticos y ciberseguridad en general incluyen el Código Penal de la Nación Argentina, la Ley Nº 26388 de Delitos Informáticos, la Ley Nº 25326 de Protección de Datos Personales y su reglamentación (Decreto PEN Nº 1558/2001), la Ley Nº 25506 de Firma Digital y su

reglamentación (Decreto PEN Nº 2628/2002), y la Ley Nº 27411 Aprobación del Convenio (de Budapest) sobre Ciberdelito. A estas se agregan otras normas específicas relacionadas con la protección de menores y contra la pornografía infantil como la Ley Nº 26061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes y su reglamentación (Decreto PEN Nº 415/2006), la Ley Nº 26904 de Grooming, la Decisión Marco 2004-68-JAI del Consejo de Europa, la Ley Nº 863 de la Legislatura de la Ciudad Autónoma de Buenos Aires y el Código Contravencional de la Ciudad de Buenos Aires.

La normativa vinculada a la Protección de las Infraestructuras Críticas de Información abarca desde la Declaración de Panamá sobre la Protección de la Infraestructura Crítica en el Hemisferio frente al Terrorismo (OEA, 2007), la Resolución JGM Nº 580/2011 Creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI), la Disposición ONTI Nº 3/2013 Aprobación de la Política de Seguridad de la Información Modelo, la Resolución JGM Nº 1523/2019 Definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la Decisión Administrativa JGM Nº 641/2021 Requisitos mínimos de Seguridad de la Información para Organismos, y las Disposiciones de la Dirección Nacional de Ciberseguridad Nº 1/2021 Creación del Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar), y Nº 6/2021 Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras, Nº 1/2022 Aprobación del Modelo Referencial de Política de Seguridad de la Información.

Otras normativas relacionadas con la ciberseguridad consideradas fueron el Decreto PEN Nº 577 / 2017 Creación del Comité de Ciberseguridad y modificación (Decreto PEN Nº 480/2019), la Resolución JGM Nº 141/2019 Delegación de la Presidencia del Comité de Ciberseguridad, y la Resolución JGM Nº 829 / 2019 Estrategia Nacional de Ciberseguridad y su modificación (Resolución JGM Nº 44/2023).

El abordaje metodológico se apoyó en un diseño de tipo descriptivo comenzando con una lectura exploratoria de diferentes tipos de fuentes bibliográficas que incluyó libros, documentos, ensayos académicos, normas, reglamentos, manuales, doctrina, publicaciones científicas y de investigación, periódicos, sitios web y blogs, tanto del ámbito civil como militar y algunas películas documentales.

Se revisaron manuales de Doctrina Militar tanto Argentina (PC 10-04, PC 00-02) como extranjera: EEUU (JP 1, JP 3-1, AFDP 3-12, FM 3-38), y Brasil (MD31-M-07), el Libro Blanco de la Defensa (2015) y el Plan Plurianual de Ciencia, Tecnología, Innovación y Producción para la

Defensa (2023), y se analizaron diferentes estrategias de ciberdefensa y ciberseguridad además de la Argentina, incluyendo Australia, Estados Unidos, Reino Unido, Francia, Alemania, España, Rusia, China y la OTAN.

Se tuvieron en cuenta diferentes ensayos, investigaciones y escritos de diferentes académicos y especialistas, entre ellos Aguilar, Alexander, Amaya, Andress, Angstrom, Arpón, Arquilla, Arteaga, Barea, Bartolomé, Bateman, Bauer, Bauman, Beecroft, Belson, Benítez, Berás, Berdan, Bertoldi, Beskow, Bodnar, Borghello, Boulanin, Brockmann, Cañete, Carley, Castro, Cherry Clay, Colom Piella, Cronin, De Spiegeleire, De Vergara, Derleth, Dickinson, Dodge, Douhet, Efrony, Eissa, Encheva, Evans, Feliu Ortega, Fernandez Vega, Fusaro, Gastaldi, Gershgorn, Giles, Graber, Gray, Guerrero, Heller, Hoehn, Hoffman, Hollis, Hüttenrauch, Intini, Jacobsen, Jasper, Jenkins, Jordán, Kaldor, Kandiko, Karam, Kerttunen, Kiselyov, Kleinman Ruiz, Kuehl, Kugler, Kuz , Lazaruk, Levite, Liang, Libicki, Lind, Loudon, Maas, Macri, Mariani, Marr, Martinez Nuñez, Mattis, Medairy, Messe, Miguel, Moerbe, Monaghan, Monteverde, Moresi, Morozov, Motta, Münkler, Nye Jr, Parker, Pascucci, Peldán Carlsson, Poczynok, Polyakov, Pons, Raymond, Reguera, Ríos, Robledo, Romero Garat, Ronfeldt, Rugge, Russell, Saalman, Sabbagh, Saldanha Walker, Sayler, Schafer, Schelling, Schultz, Schulze, Scroxton, Serbin, Pont, Sheldon, Slayton, Smith, Sorrentino, Soula, Stevens, Strickland, Strout, Su, Swan, Sweijs, Tello, Thakkar, Theohary, Todorov, Tomé, Topychkanov, Toro Hardy, Torres, Trama, Tuters, van Creveld, Verbruggen, Vertuli, Vorobyov, Waldman, Westreicher, Wilde, Winterfield, Xiangsui, Zacarías Di Tullio, Zeng, y Zweibelson.

Se utilizó información de diferentes fuentes periodísticas digitales como elconfidencial.com, abcnews.go.com, infobae.com, elpais.com, noticiasdenavarra.com, economiatic.com, governmentciomedia.com, bbc.com, tn.com.ar, clarin.com, zona-militar.com, technologyreview.com, elanalista.com.ar, infodefensa.com, ispionline.it, theguardian.com, ssoar.info, perfil.com, zona-militar.com, urgente24.com; y de estudios y publicaciones realizadas por organizaciones como amnesty.org, carnegieendowment.org, BID, securingdemocracy.gmfus.org, sipri.org, ccdcoe.org, americanbar.org, fuerzas-armadas.mil.ar, doctrine.af.mil, comptia.org, cybercom.mil, media.defense.gov, arxiv.org, eacnur.org, eccu.edu, justsecurity.org, unq.edu.ar, enisa.europa.eu, esgcffaa.edu.ar, defensa.gob.es, press.armywarcollege.edu, frba.utn.edu.ar, smh.com.au, gov.uk, crsreports.congress.gov, digital-commons.usnwc.edu, ias.informatik.tu-darmstadt.de, iadfoundation.org, iat.es, intgovforum.org, dod.defense.gov, jid.org, jcs.mil, athenalab.org, softwarelab.org, nato.int, defensa.gob.es, arxiv.org, dle.rae.es, rand.org, nellis.af.mil, crsreports.congress.gov, secpho.org, direct.mit.edu, icrc.org,

cscis.org, politica-china.org, cip.gov.ua, itu.int, ITU, UNCTAD, cybercom.mil, WEF, weforum.org, whitehouse.gov, researchgate.net, saij.gob.ar, y pucara.org.

También se consultaron sitios web y blogs como history-computer.com, infotecs.mx, askanydifference.com, differencebetween.net, boletinoficial.gob.ar, argentina.gob.ar, aselcom.com, wired.com, cyberark.com, defence-industries.com, warontherocks.com, dqindia.com, xataka.com, ibm.com, eurozine.com, master-bigdata.com, original.antiwar.com, nic.ar, microsoft.com, onespan.com, oracle.com, pandasecurity.com, towardsdatascience.com, seguridadinternacional.es, salesforce.com, sap.com, deloitte.com, computerweekly.com, sekoia.io, techcrunch.com, c4isrnet.com, tecknexus.com, bayometric.com, blog.cloudflare.com, ceinaseg.com, securitysectorintegrity.com, techtarget.com, welivesecurity.com, vmware.com, y economipedia.com.

Entre los libros consultados estuvieron "Cyber Warfare" (2011), de Andress & Winterfield; "Networks and Netwars" (2001) de Arquilla & Ronfeldt; "Artificial Intelligence and the future of Defense" (2017) de De Spiegeleire, Maas & Sweijs, Operaciones Militares Cibernéticas (2017) de De Vergara & Trama, "The command of the air" (2019) de Dohuet, "Unrestricted Warfare" (2004) de Liang & Xiangsui, "Disrupting Deterrence" (2022) de Rand Corporation, Operaciones en el ambiente de la información (2022) de Moresi, Motta, Trama, Saldanha Walker & Amaya, Informe sobre tecnología e innovación 2021 de UNCTAD, y "Perceptions are reality" (2018) de Vertuli & Loudon; y además se analizaron las películas "Zero Days" (2016) de Gibney, y "The Great Hack" (2019) de Noujaim & Amer.

La base académica detallada antes cimentó el estado del arte conceptual para dar rienda suelta al pensamiento crítico que permitiera responder a la hipótesis basada en argumentos sólidos.

En cuanto a la organización del escrito, este fue estructurado en una introducción, cuatro capítulos, y una conclusión. La introducción proporciona el marco para plantear la problemática tratada.

En el capítulo uno, titulado "Ciberespacio, Seguridad Nacional y Defensa" se desarrollaron los conceptos relacionados con dicho ámbito y de ciberpoder, especificando además el alcance de los términos y su relación con otros dominios. Se analizaron las implicancias que tiene el uso del espacio cibernético para la seguridad nacional desarrollando los conceptos de ciberguerra, guerra de red, ciberagresión, ciberataque y ciberdefensa. Se determinaron posibles objetivos y efectos; y se describieron, además, diferentes formas de abordar la defensa en estas áreas intangibles, sin territorio fijo y donde cualquier persona puede acceder desde cualquier parte en el mundo.

En el segundo capítulo “Innovación tecnológica y su aplicación militar en el ciberespacio” se definieron conceptos clave para poder comprender las implicancias del uso de la tecnología en ese marco e identificar su aplicación, alcance y efectos en el ámbito militar.

El capítulo tres “Operaciones militares cibernéticas y marco legal” estuvo dedicado a analizar el concepto de soberanía en el ciberespacio desde diferentes enfoques, la legislación internacional y nacional respecto al uso militar del ciberespacio, las posibilidades de generar alianzas, conceptos doctrinarios y tendencias respecto a las operaciones militares en el ciberespacio y lecciones que nos ha dejado el conflicto entre Rusia y Ucrania.

En el cuarto y último capítulo “Capacidades de defensa ciberespacial en la República Argentina” se describieron las capacidades necesarias en esta área para la paz y para la guerra, la organización de la ciberdefensa y ciberseguridad en el ámbito nacional, la posibilidad de optimizarla en función de la legislación nacional y una visión del rol del Instrumento Militar argentino en el ciberespacio de cara al futuro.

Finalmente, las conclusiones permiten identificar las ideas y conceptos principales que deberían ser considerados en relación a la hipótesis planteada, y a las nuevas formas de combate futuro relacionadas con el empleo del ciberespacio.

CAPÍTULO I: CIBERESPACIO, SEGURIDAD NACIONAL Y DEFENSA

"No hay una actitud más peligrosa que presumir el hecho de que una futura guerra será igual a la última guerra, y no podemos darnos el lujo de ignorar todas las lecciones de la última"

Sir John Cotesworth Slessor[11]

Ciberespacio, ciberpoder, alcance y relación con otros dominios

El ciberespacio es el nuevo mundo del siglo XXI que se descubre cada día con las nuevas tecnologías y nos obliga a reflexionar dónde estamos y hacia dónde nos conduce, ofreciéndonos productos sorprendentes, pero no siempre con todos los valores humanos asociados. La tecnología actual nos inunda de manera ubicua, imperceptible y a la vez imprescindible (Martinez Nuñez, 2020).

Es uno de los considerados "global commons" o espacios comunes junto con las aguas internacionales, el espacio aéreo y el espacio exterior que constituye uno de los entornos en que ninguna persona o Estado puede tener su propiedad o control exclusivo y que son básicos para la vida. Esto significa que conforma un espacio fundamental de tránsito de bienes, servicios, comunicación e información de libre uso y acceso que no pertenece a ningún Estado y sobre el cual ninguna nación puede ejercer derechos de soberanía siendo el único creado artificialmente y sin una localización física (Barea, 2018).

Martínez Núñez (2020) sostiene que la soberanía en el ciberespacio es un concepto distinto del habitual. Es un bien común de la humanidad. Allí, la soberanía se ejerce o tiene más que ver con el grado de conocimiento de autonomía tecnológica de cada país, que le permita garantizar a sus ciudadanos un acceso seguro para contribuir con su innovación, su progreso, su avance y un acceso libre de amenazas.

Comprender el ciberespacio implica entender conceptos como el de teleinformática y redes de comunicación de datos. La teleinformática es una disciplina formada por la unión de la informática y las telecomunicaciones que permite unir distintos tipos de dispositivos dentro de una oficina u hogar en forma localizada, o a kilómetros de distancia en áreas más extensas. Las redes de comunicación de datos definen un conjunto de equipos interconectados que comparten información, recursos y servicios (Kuz & Ríos, 2020).

[11] *Sir John Cotesworth Slessor* (1897-1979) Mariscal británico de la Royal Air Force (RAF), se desempeñó como Jefe del Estado Mayor Aéreo desde 1950 hasta 1952 y fue uno de los arquitectos de la estrategia aérea británica durante y después de la Segunda Guerra Mundial.

Como resultado de esa unión, se desarrollaron y continúa desarrollándose una infinidad de aplicaciones en una diversidad de campos como energía, TIC, transporte, hídrico, salud, alimentación, finanzas, nuclear, químico, espacio y el mismo Estado, incluido su Instrumento Militar de la Defensa Nacional.

La idea de ciberespacio fue concebida en los años 60 por el psicólogo e informático Joseph Carl Robnett Licklider, profesor asociado del Instituto de Tecnología de Massachusetts y primer director de la Oficina de Técnicas de Procesamiento de Información de la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de los Estados Unidos, como una "red informática intergaláctica". Licklider describió una red en la que el software podría flotar sin máquinas individuales y por lo tanto los programas y los datos no vivirían en una computadora individual sino en la Red. Esta idea pudo ser materializada, comenzó a funcionar a partir de 1969 como ARPAnet y finalmente evolucionó hacia el Internet que conocemos hoy (Anónimo, 2020). Sin embargo, es importante destacar que el internet entendido como una red de área extensa o global y los elementos que la rigen constituyen sólo una parte del ciberespacio.

El Departamento de Defensa de los EE.UU. define al ciberespacio como un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de información tecnológicas y datos residentes, incluido el Internet, redes de telecomunicaciones, sistemas informáticos, y procesadores y controladores integrados (Theohary, 2020).

El ciberespacio permite también ser utilizado en combinación con otras capacidades ajenas a él, a través del espectro electromagnético. El Ejército de los Estados Unidos creó el concepto de Actividades Ciber-Electromagnéticas (CEMA) integrando actividades ciberespaciales con electromagnéticas con el fin de lograr efectos combinados sinérgicos y simultáneos denegando el uso del ciberespacio y el espectro electromagnético y protegiendo el sistema de Comando y Control de misión (FM 3-38, 2014).

La evolución de la tecnología asociada a la teleinformática, las redes de comunicación de datos y el internet de las cosas nos orienta hoy hacia la noción de ciberespacio, aunque se puede encontrar una amplia variedad de definiciones.

Dan Kuehl definió al ciberespacio como

> un dominio global dentro del entorno de la información cuyo carácter distintivo y único se enmarca en el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando tecnologías de la información y la comunicación" (Kuehl, 2009).

Algunos especialistas entienden por ciberespacio “la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan” (Miguel, 2020). Otros, como un “ambiente complejo que resulta de la interacción de personas, software y servicios, por medio de dispositivos y redes conectadas”, y que “no posee existencia física, sino que es un dominio que engloba todos los sistemas TIC” (Benítez, 2020).

El Comando Conjunto de Ciberdenfensa de la República Argentina concibe al ciberespacio como el:

> ámbito tanto físico como virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos de información digital a través de redes, software, hardware y firmware de dispositivos electrónicos cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de información y las comunicaciones con impacto sobre las tecnologías de operación, y que constituye un ámbito de actuación operacional del IMDN y otros múltiples actores cibernéticos (Intini, 2020).

Es importante destacar dentro de estos conceptos que tanto las tecnologías de operación asociadas a la evolución del internet de las cosas como las redes o dispositivos aislados por fuera de él también forman parte del ciberespacio.

Este se caracteriza por ser de naturaleza artificial, imperceptible, dinámico, transversal y de fronteras o límites poco definidos. Estas características lo distinguen de los otros ámbitos clásicos como el terrestre, marítimo, aéreo o espacial determinados por variables conocidas constituyéndolo en un quinto dominio donde tanto las telecomunicaciones como los sistemas autónomos están cada vez más relacionados y regidos dentro del ciberespacio ocasionando que los conflictos en algunos casos se resuelvan en este ámbito, o puedan ser afectados a través del mismo.

Si bien el espacio cibernético como ámbito de circulación de información no constituye un espacio en sí mismo, representa una dimensión superpuesta que atraviesa a los espacios físicos tradicionales y en donde los límites entre lo público y lo privado, y entre lo militar y civil, son difusos.

Fabio Rugge sostiene que:

> el ciberespacio es un poderoso multiplicador de los efectos desestabilizadores de la información manipulada porque ofrece una alta conectividad, un bajo costo de entrada, varios puntos de distribución sin intermediarios y completa indiferencia a la distancia física o a las fronteras nacionales. Más importante aún, el anonimato y la inhabilidad de poder atribuir un ataque a alguien con seguridad hacen al ciberespacio el dominio de la ambigüedad (Rugge, 2018).

Entre sus ventajas se distingue que el mismo es de alcance global, proporcionando acceso y permitiendo la interconexión de personal, lugares y sistemas en áreas negadas en otros dominios y mejorando, en este sentido, la capacidad de las Fuerzas Armadas. Facilita el acceso a áreas en conflicto sin exponer a los operadores. Permite la acción y concentración rápida debido a que la información se mueve a una velocidad incomparable y se pueden emplear miles de computadoras para concentrar ciberataques tanto para negar servicios como para influir y movilizar poblaciones (Cronin, 2006). Su utilización como vehículo transmisor de ideas, vector de comunicación y herramienta de propaganda le confiere un poder excepcional (Barea, 2018) permitiendo a individuos organizarse y manifestarse libremente como lo demostró el uso de las redes sociales y la Primavera Árabe de 2011. Facilita el anonimato valiéndose de que el excesivo número de usuarios de internet más allá de su concepción original dificulta seguir una ruta probatoria y por lo tanto permite una libertad de acción con una atribución limitada (Clay, 2009). Favorece la ofensiva y el ataque ante vulnerabilidades estructurales de seguridad inherentes a la arquitectura del ciberespacio (Parker, 2014). Extiende el espectro de armas no letales ofreciendo este tipo de medios como acción directa contra un adversario. Permite lograr efectos tanto en el nivel estratégico, operacional y/o táctico. Posibilita también efectuar ataques con efectos cinéticos sobre mandos de control industriales a través de las tecnologías de operación afectando infraestructuras críticas como por ejemplo plantas potabilizadoras de agua o de distribución eléctrica, ferrocarriles, señalización urbana, aeropuertos o centrales nucleares.

Entre sus limitaciones, se observa que el adversario puede usar todas las mismas ventajas antes mencionadas en contra de su oponente. Mientras más dependa un adversario del ciberespacio será más vulnerable a ciberataques y cuanto menos centrado esté en las redes menos influencia se podrá tener sobre el mismo. Los ataques dependerán mucho de los efectos imprevisibles de segundo orden (Lonsdale, 2004).

No existe la opción de aplicar la fuerza bruta por lo tanto las operaciones cibernéticas dependen de la coerción (Schelling, 2008). El éxito de las operaciones dependerá de la reacción de los adversarios ante la información suministrada, alterada o negada. Asimismo, es difícil limitar los efectos de un ataque a través del ciberespacio interconectado debido a que es imposible identificar su alcance máximo poniendo en riesgo consecuencias involuntarias. Por ejemplo, el ataque ruso contra Viasat, un proveedor de banda ancha satelital de alta velocidad cuyos módems se desconectaron al principio de la guerra de Ucrania, afectando aparentemente en forma involuntaria las comunicaciones en toda Europa (Burgess, 2022).

Se puede adoptar una postura defensiva con medidas que incrementen los niveles de protección, pero las intrusiones de ataques complejos y persistentes son inevitables. De igual manera en que este dominio virtual fue creado por el hombre con apoyo en la tecnología, podría ser destruido.

El ciberespacio puede ser definido, analizado y entendido por capas de red. Es así como dentro del mismo se distinguen tres de ellas: una capa física, que constituye el medio por donde se desplazan los datos y que involucra dos componentes, uno geoespacial (tierra, mar, aire o espacio) donde se encuentran ubicados los elementos de las redes, y otro de red física propiamente dicho, que incluye hardware, software e infraestructuras que apoyan a las redes y a los conectores físicos; otra capa lógica relacionada con la arquitectura, los servicios y las aplicaciones de red, y una tercera capa social y de información representada por las personas físicas, las cibernéticas y la propia información. En esta tercera capa es donde se origina la problemática del conflicto en el ciberespacio como dominio de actuación de los seres humanos.

El ecosistema ciberespacial involucra diversos factores entre los que se encuentran las tecnologías de la información y de la operación, la información, el software, la energía, el transporte y las personas que pueden ser afectados al estar vinculados a las redes (Intini, 2020).

El ciberespacio es entendido por Sheldon (2011) como el dominio en el que tienen lugar las operaciones cibernéticas. El ciberpoder es la suma de los efectos estratégicos generados por las operaciones cibernéticas en y desde el ciberespacio para ejercer influencia. Estos efectos se pueden sentir dentro de este, así como en otros dominios de tierra, mar, aire y espacio, y también pueden ser cognitivamente efectivos con seres humanos individuales, constituyendo una herramienta estratégica que puede ser utilizada sólo o en combinación con otros instrumentos militares y de poder nacional, generando efectos en todos los espacios de forma absoluta y simultánea.

Este mismo autor afirma que el ciberpoder puede usarse en la paz y la guerra porque, entre sus muchos otros atributos, es sigiloso y encubierto, relativamente económico, su uso favorece el delito y es difícil de atribuir al autor. Estos mismos atributos exponen las propias vulnerabilidades a ciberataques por otros. No obstante, con un conocimiento acabado de ciberseguridad y una comprensión realista de sus límites, constituye un valioso instrumento estratégico para manipular el entorno en beneficio propio y superar riesgos. En este sentido, el ciberpoder tiene un propósito estratégico relevante para lograr los objetivos de la política.

El poder cibernético es simplemente otra dimensión de la soberanía del siglo XXI, con una dinámica diferente, en la que el ciberdelito, el hacktivismo[12], la inteligencia y las operaciones militares informáticas comparten un mismo dominio y en la que el internet se ha convertido en una de las áreas de competencia más desestabilizadoras entre los Estados (Rugge, Cyberspace and Great Powers Competition, 2020). El dominio cibernético es ahora un área sensible de la seguridad de los Estados que desarrollan estrategias de ciberseguridad nacional para lograr un contexto seguro (Motta, 2022).

Desde el punto de vista estratégico las definiciones no tienen tanta importancia, "lo que en realidad más importa es percibir la esfera de información como un lugar que existe, comprender su naturaleza y considerarla como algo que puede ser manipulado y usado como una ventaja estratégica" (Lonsdale, 2004).

En este sentido, se puede definir al ciberespacio como "el dominio que existe para entrar, almacenar, transmitir y extraer información a través del uso del espectro electromagnético" que "incluye todo el hardware, software y medios de transmisión usados desde la entrada inicial" (teclado, voz, documentos escaneados), "hasta la presentación de información para la cognición de usuarios" (imágenes, sonidos, documentos) "u otra acción" (guía de un vehículo no tripulado, cerrar una válvula, etc.) (Parker, 2014), y al ciberpoder como "el potencial para usar el ciberespacio a fin de lograr el resultado deseado" (Nye, 2011), donde el contexto estratégico es clave en la comprensión de su uso**.**

Parker (2014) sostiene que a medida que el carácter de la guerra y del ciberespacio cambian, el combate se une con otros dominios y los líderes militares deben tomar decisiones sensatas sobre lo que pueden aportar para lograr los resultados deseados, considerando las oportunidades y ventajas que presenta el ciberespacio por un lado y las vulnerabilidades y limitaciones de las operaciones en dicho dominio por el otro.

Conceptos "ciber": ciberguerra y guerra de red, ciberamenaza, ciberagresión, ciberataque, ciberarma, ciberdefensa y ciberseguridad

A la dificultad de lograr consenso respecto a una gobernanza ciberespacial global (Efrony, 2021), se adiciona la falta de definiciones comunes a la hora de elaborar doctrinas. Existen muchos

[12] *Hacktivismo*: Acrónimo de hacker y activismo también conocido como ciberactivismo y se refiere a la utilización no-violenta de herramientas digitales persiguiendo fines políticos.

términos relacionados con el dominio “ciber” y sólo esta palabra por sí misma puede ser controvertida. Esto se debe a que no existe un único glosario de definiciones ni una taxonomía globalmente aceptada y como consecuencia, la mayoría de los estudios relacionados con el ciberespacio y sus aplicaciones se ven en la obligación de incluir sus propios listados de definiciones.

La Junta Interamericana de Defensa (JID) ha observado tres casos predominantes: uso de la palabra “ciber” o “cibernético” como un adjetivo (ciber arma, arma ciber, arma cibernética), como un prefijo con guión (ciber-arma) o con prefijo sin guión (ciberarma) y recomienda su uso de acuerdo a las normas de escritura de los prefijos de la Real Academia Española “como un elemento compositivo que indica relación con la informática”, o el adjetivo ciberespacial (fuerza ciberespacial, ecosistema ciberespacial) con el significado de pertenencia o relación con el ciberespacio (JID, 2020).

Respecto a un consenso a nivel regional, se puede decir que la Unión Europea es la más avanzada en la materia, en particular los países que forman parte de la OTAN, y que existe también una intención en este sentido en otras regiones como el continente americano con el apoyo de La Fundación Interamericana de Defensa (FID) y la JID.

Identificando el término “ciber” como un prefijo que indica relación con el ciberespacio se desarrollarán a continuación algunos conceptos:

El Licenciado Hugo Miguel define la ciberguerra como las

> acciones defensivas y/u ofensivas que tienen por fin asegurar y/o afectar el uso efectivo y el mantenimiento de las capacidades, la libertad de acción y el sostenimiento de la iniciativa sobre el ciberespacio del Sistema de Defensa Nacional, además de negar el uso del mismo a intereses ajenos, contrapuestos y/u hostiles (2020).

De acuerdo a la doctrina militar de la República Federativa de Brasil ciberguerra

> corresponde al uso ofensivo y defensivo de información y sistemas de información para negar, explotar, corromper, degradar o destruir las capacidades de comando y control (C^2) del oponente en el contexto del planeamiento militar a nivel operacional o táctico de una operación militar. Comprende acciones que involucran herramientas de tecnología de la información y comunicaciones (TIC) para desestabilizar o aprovechar los sistemas de tecnología de la información y las comunicaciones y el comando y Control ($STIC^2$) del oponente y defender el $STIC^2$ propio. Cubre esencialmente las acciones cibernéticas. La oportunidad para el empleo de estas acciones o la efectividad de su utilización será proporcional a la dependencia del oponente en relación a las TIC (MD31-M-07, 2014).

Para la corporación RAND ciberguerra “implica las acciones de un Estado-Nación u organización internacional para atacar e intentar dañar las computadoras o redes de información de

otra nación a través de, por ejemplo, virus informáticos o ataques de denegación de servicio" (2016).

Por otra parte, existe el término "netwar" o guerra de redes, que según Arquilla & Ronfeldt se refiere a un modo emergente de conflicto (y crimen) en los niveles sociales, a excepción de la guerra militar tradicional, en la que los protagonistas utilizan formas de organización en red y doctrinas, estrategias y tecnologías relacionadas en sintonía con la era de la información", en la que "es probable que estos protagonistas consistan en organizaciones dispersas, pequeños grupos e individuos que se comunican, coordinan y llevan a cabo sus campañas en Internet, a menudo sin un comando central preciso". Esta "difiere de los modos de conflicto y crimen en los que los protagonistas prefieren desarrollar organizaciones, doctrinas y estrategias formales, independientes y jerárquicas (2001).

De los conceptos mencionados se puede afirmar que el primero demanda la participación formal de un Estado y por obligación su Instrumento Militar de la Defensa Nacional; mientras el segundo, es mucho más informal y abarcador respecto a los actores intervinientes.

Otros términos con prefijo "ciber" importantes de conceptualizar son ciberamenaza, ciberagresión, ciberataque y ciberarma.

La JID define ciberamenaza como "una fuente potencial de perjuicio, externa o interna, a algún activo de la organización que se materializa a través del ciberespacio" (JID, 2020, p. 14).

Para el Reino Unido es "cualquier cosa capaz de arriesgar la seguridad de, o causar daño a los sistemas de información y dispositivos interconectados (incluidos el hardware, software e infraestructura asociada), los datos en ellos y los servicios que brindan, ante todo por medios cibernéticos" (Gov.UK, 2016), mientras que para Brasil es toda "causa potencial de un incidente no deseado que puede provocar daños en el ciberespacio de interés" (MD31-M-07, 2014).

Por su parte, el Comando Conjunto de Ciberdefensa República Argentina identifica a una ciberamenaza como un:

> factor externo representado por la posibilidad que ocurra un fenómeno o evento adverso en el ciberambiente de interés, en un momento, lugar específico, con una magnitud determinada y que podría ocasionar daños a las personas y/o a las instalaciones o medios TIC, la pérdida de personal o medios de vida y/o trastornos al empleo del Instrumento Militar,
>
> y por ciberagresión una
>
> acción ofensiva, voluntaria o no, que se ejecuta en el ciberespacio, sobre una infraestructura crítica o activo de información del Sistema de Defensa Nacional y ocasiona, como

> consecuencia, daños a su disponibilidad, integridad y confidencialidad afectando el desarrollo de las operaciones que ejecuta en cumplimiento de su misión (Intini, 2020).

Un ciberataque consiste en la "explotación deliberada de sistemas informáticos, empresas y redes que dependen del mundo digital para causar daños" (Gov.UK, 2016); o las "medidas adoptadas a través del uso de las redes informáticas para interrumpir, negar, degradar o destruir información albergada en estaciones de trabajo y redes informáticas del adversario, o las estaciones de trabajo y las redes mismas", que "pueden ser consolidadas en grupos que materializan acciones de infiltración, maniobra o ataque" (Sorrentino, 2020).

Una ciberarma se define como un "software específicamente diseñado para causar un daño o efecto perjudicial a un elemento del ciberespacio pudiendo tener consecuencias físicas en los ámbitos de operaciones" (BID, 2016).

Por último, es importante comprender los conceptos de ciberdefensa y ciberseguridad.

De acuerdo a la doctrina militar conjunta argentina la ciberdefensa es el "conjunto de acciones desarrolladas en el ciberespacio de interés del sistema de defensa para prevenir y/o contrarrestar toda amenaza o agresión cibernética" (PC 00-02, 2015).

La doctrina militar conjunta brasilera la define como el

> conjunto de acciones ofensivas, defensivas y exploratorias, llevada a cabo en el Ciberespacio, en el contexto de la planificación a nivel estratégico nacional, coordinado e integrado por el Ministerio de Defensa, con el propósito de proteger los sistemas de información de interés para la Defensa Nacional, obtener datos para la producción de conocimiento de Inteligencia y comprometer los sistemas de información del adversario (MD31-M-07, 2014).

Para el Comando Conjunto de Ciberdefensa República Argentina es

> la integración y acción coordinada de las capacidades del Estado Nacional para adoptar medidas tendientes a prevenir, proteger y responder toda ciberamenaza (…) que afecte o intente afectar las infraestructuras críticas[13], ejecutadas de manera disuasiva o efectiva por el Instrumento Militar (IM)". Para el componente del IM vinculado a la ciberdefensa "implica el planeamiento y ejecución de operaciones militares en el ciberespacio (Intini, 2020).

El Servicio de Ciberdefensa y Seguridad de la Información de la Armada agrega que

> se puede definir a la ciberdefensa como el ámbito propicio para que la ciberseguridad alcance su grado máximo de desarrollo y maduración", y que "debe estar dirigida a

[13] *Infraestructura Crítica del Sistema de Defensa Nacional*: Instalaciones, redes, servicios y medios técnicos y de tecnologías de la información y comunicaciones, que proporcionan un servicio esencial al Sistema de Defensa Nacional y cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes. Abarca los sistemas de comando y control, los sistemas de armas, el sistema de control SCADA, los sistemas de comunicaciones y los sistemas informatizados.

> combatir o contrarrestar una amenaza, sea esta inmediata, latente o potencial, originada en adversarios, enemigos, organizaciones criminales o individuos aislados, que pretenda atentar contra los principios de confidencialidad, integridad y disponibilidad de la información, debiendo considerarse como una función defensiva-ofensiva (Sorrentino, 2020).

Por otra parte, ciberseguridad es definida como un "conjunto organizado de medidas destinadas a prevenir, evitar y minimizar potenciales daños a redes y sistemas de información propios" (JID, 2020), y como "una herramienta cuyo objeto es salvaguardar los atributos básicos de seguridad de los activos de la información (confidencialidad, integridad y disponibilidad)" (Sorrentino, 2020).

O según la doctrina del Reino Unido como

> la protección de sistemas interconectados (incluidos el hardware, software y la infraestructura asociada), los datos en ellos y los servicios que brindan, de acceso no autorizado, daños o uso indebido. Esto incluye los daños causados intencionalmente por el operador del sistema, o accidentalmente, como resultado de no seguir los procedimientos de seguridad o ser manipulado para no hacerlo (Gov.UK, 2016).

De este último concepto deriva el de ciberseguridad social, vinculado con la seguridad nacional, referido al ser humano y definido como

> un área científica de desarrollo que utiliza la ciencia para caracterizar, entender y prever cambios impulsados por los medios cibernéticos en el comportamiento humano, la sociedad, la cultura y la política, y para construir la infraestructura cibernética necesaria que permita a la sociedad retener su carácter esencial en medio de un entorno de información cibernético que se encuentra bajo cambios y enfrenta amenazas cibernéticas sociales actuales o inminentes (Beskow & Carley, 2019).

La diferencia entre la ciberseguridad tradicional y la social radica en que, en la primera, los seres humanos utilizan la tecnología para hackear[14] la misma tecnología, en cambio en la segunda, los seres humanos utilizan la tecnología para hacerlo a otros seres humanos (hackeo cognitivo).

Utilización del espacio cibernético e implicancias para la seguridad nacional

El ciberespacio, dentro de la globalización y la revolución tecnológica, ofrece una mayor libertad de acción para el acceso y manejo de la información. Quien logre dominar u obtener la superioridad logrará una posición relativa favorable, pero así y todo será igualmente vulnerable.

El libre acceso que este facilita a infinidad de posibilidades y espacios comunes se ha transformado en una necesidad y un derecho social, y por lo tanto en una obligación ineludible por salvaguardarlo (Barea, 2018).

[14] *Hackear*: Introducirse de forma no autorizada en un sistema informático.

Esta nueva dimensión, que atraviesa los espacios físicos, se ha convertido en un nuevo ámbito de competencia donde diferentes actores mediante el acceso y empleo de nuevas tecnologías pueden vulnerar la seguridad y la defensa de un Estado.

El Informe de Percepción de Riesgos Globales 2023 del Foro Económico Mundial ubica a la ciberdelincuencia generalizada y la ciberinseguridad en la posición octava de riesgos globales clasificados por gravedad a corto y largo plazo. El informe pronostica que, en los próximos diez años, la a tecnología exacerbará las desigualdades, mientras que los riesgos de la ciberseguridad seguirán siendo una preocupación constante. Junto con un aumento en el delito cibernético, los intentos de interrumpir los recursos y servicios críticos habilitados por tecnología serán más comunes, y anticipa ataques contra la agricultura y el agua, los sistemas financieros, la seguridad pública, el transporte, la energía y la infraestructura de comunicación doméstica, espacial y submarina. Los riesgos tecnológicos no se limitarán únicamente a los actores deshonestos, y el análisis sofisticado de conjuntos de datos más grandes permitirá el uso indebido de información personal a través de mecanismos legales legítimos, debilitando la soberanía digital individual y el derecho a la privacidad, incluso en regímenes democráticos bien regulados (WEF, 2023).

Garantizar el libre acceso al ciberespacio en contraposición a la amenaza constante por un adversario hipotético que logre impedirlo, aunque fuera de manera temporal, se ha constituido en una necesidad de importancia estratégica (Barea, 2018).

Esta situación no ha pasado desapercibida. Por el contrario, forma parte de la agenda internacional y preocupa a los Estados que lo manifiestan en sus respectivos documentos de defensa y seguridad nacional.

La política o estrategia de seguridad nacional describe cómo una Nación proporciona seguridad para el estado y sus ciudadanos. Consiste en una descripción formal de la comprensión de sus principios rectores, valores, intereses, objetivos, entorno estratégico, amenazas, riesgos y desafíos con el fin de proteger y promover la seguridad nacional, basada generalmente en la constitución, los documentos fundacionales y la legislación. Esta política aclara los comportamientos y las responsabilidades de las instituciones estatales para proporcionar seguridad y defender el estado de derecho. La política de defensa es parte de la política o estrategia de seguridad nacional del Estado, cubre desde los fines hasta las formas y medios para lograr los objetivos de defensa nacional y se guía por códigos y principios allí integrados (UN Security Sector Reform Task Force, 2012).

Durante décadas, los Estados han utilizado como mecanismo para dirimir los conflictos que alcanzaban su máximo estadio el enfrentamiento de sus Fuerzas Armadas en la guerra, mediante operaciones convencionales para lograr imponer su voluntad en función de sus intereses y/o proteger sus intereses vitales, utilizando teorías, medios, estrategias y tácticas tradicionales en el contexto de un conflicto armado entre dos o más Estados o alianzas abiertamente hostiles.

Los efectos de la posmodernidad y la innovación tecnológica en el siglo XXI han llevado a la a una mayor complejidad de la guerra, ya sin poder ser entendida únicamente en su forma más tradicional como un conflicto armado de alta intensidad o total. El espectro que abarca es mucho más amplio y los actores involucrados en ella ya no son únicamente ejércitos regulares pertenecientes a un Estado-Nación.

De acuerdo a la doctrina militar conjunta estadounidense, la guerra es el cómo del conflicto armado contra un enemigo y su carácter variable se transforma por los instrumentos del poder nacional (Diplomático, Informacional, Militar y Económico) y otros factores sociales, de infraestructura, físicos y cronológicos. En la competencia global, las operaciones por debajo del umbral que provocaría una respuesta militar mediante la manipulación de las percepciones populares y el uso de medios no militares en oposición a los intereses y fines de seguridad de su país los ha llevado a redefinir el espectro de relaciones estratégicas como el continuo de la competencia (competition continuum). El continuo de la competencia describe estados de cooperación, competencia por debajo del conflicto armado y conflicto armado para distinguir las relaciones estratégicas entre los actores y aclarar las opciones dentro de cada contexto. El Instrumento Militar, como medio para garantizar, disuadir, compeler o forzar a un oponente, posibilitará y reforzará la aplicación de los demás instrumentos del poder nacional enmarcado en los principios constitucionales, las normas para la profesión de las armas y el derecho de la guerra (Joint Chiefs of Staff, 2022).

El espacio cibernético ofrece una mayor libertad de acción para el manejo de la información y una nueva dimensión para conducir la guerra. Los Estados se han vuelto más vulnerables ante el surgimiento de nuevas amenazas obligando a sus Fuerzas Armadas a tener que adaptarse para poder hacer frente a estos desafíos y la utilización de nuevas tecnologías asociadas a la defensa es imprescindible.

El ambiente de seguridad complejo de la actualidad requiere una presencia incrementada en el ciberespacio ya que el mismo es considerado un ambiente operacional con características propias

que lo distinguen, con ventajas y limitaciones que requieren ser evaluadas en los posibles contextos estratégicos debido a los cambios en la forma de la guerra (Parker, 2014).

El control de los espacios comunes ya no es exclusivo de una gran potencia. La soberanía e independencia de los países y organizaciones supranacionales están ligadas a la libertad de acción asociada al empleo de estos espacios y el ciberespacio es uno de ellos. La interrelación e interdependencia que existe entre ellos demanda que se controlen de manera simultánea y el nuevo concepto de Operaciones Multi-Dominio se centra en desarrollar capacidades para ello. El desafío supone encontrar un punto de equilibrio entre seguridad y libertad por un lado y competición y colaboración por el otro en donde tanto la inacción o pasividad como la actitud belicosa o agresiva son contraproducentes (Barea, 2018).

En el ciberespacio chocan múltiples intereses. Esto obliga a los formuladores de política a abordar conceptos tradicionalmente difíciles de resolver generando tensiones de manera similar a la política exterior entre volver al realismo en un sistema no gobernado y anárquico, y aspirar al ideal liberal de seguridad a través del reconocimiento recíproco de derechos naturales. La política en el ámbito ciberespacial requiere establecer prioridades basadas en valores como los derechos de la propiedad intelectual, el papel del gobierno en los asuntos de negocios, presentar a los criminales ante la justicia, libertad de expresión, intereses de seguridad nacional y privacidad personal, que no son nuevos, pero se presentan desde otra perspectiva (Parker, 2014).

El acceso a internet genera además un dilema de política exterior permitiendo ayudar a movilizar y habilitar disidentes bajo gobiernos opresivos o proporcionar más herramientas de control de la población a los líderes autoritarios (Morozov, 2011).

La tecnología actual permite manipular las creencias e ideas a escala mundial y a la velocidad de los algoritmos, transformando el campo de batalla en todos los niveles de la guerra y en la que la guerra de la información se está convirtiendo en un fin en sí mismo. De aquí surge como un subdominio emergente de la seguridad nacional el concepto de ciberseguridad social, diferente a la ciberseguridad tradicional (Beskow & Carley, 2019).

Estos autores han observado que, si bien la geografía todavía es relevante, se ha producido un cambio en el centro de gravedad estratégico orientado hacia la población, destacando que existen ya actores estatales y no estatales que han comenzado a explotar la idea de manipular poblaciones u organizaciones a través del ciberespacio influyendo directamente en el tejido social. Afirman que, para poder proteger esta debilidad interna de sufrir manipulaciones externas, es imprescindible que los líderes entiendan este concepto.

Según lo observado, el ciberespacio permite un amplio abanico de posibilidades de empleo, que, traducido en intenciones, puede constituir una amenaza para la seguridad nacional de un Estado. En consecuencia, los Estados deben determinar políticas y estrategias que permitan abordar los temas mencionados.

El hecho que EEUU describa en su Estrategia de Seguridad Nacional al ciberespacio como un instrumento clave de su política exterior y de seguridad, cuya defensa es una prioridad, representa un claro indicador de la importancia estratégica que posee (Whitehouse, 2022), y debería encender una alarma en el panel de control de la seguridad nacional de todos los países.

Empleo militar del ciberespacio. Estrategias, objetivos y efectos

El ciberespacio permite realizar múltiples operaciones como: engaño, disuasión, interferencia de sistemas de comando y control, utilización de drones, confundir sistemas de información militar y/o civil, anular servidores para que no puedan emplearse determinadas computadoras y redes, causar eventos o fenómenos naturales que obliguen al oponente a distraer tropas, confundir sistemas logísticos gobernados por computadoras, descriptar códigos criptográficos, interferir el tráfico aéreo, los sistemas de distribución eléctrica o de salud, alterar sistemas bancarios, difundir propaganda o conducir operaciones de acción psicológica y generar percepciones erróneas en la mente del oponente (Trama, Operaciones cibernéticas, 2017).

Para ejercer el poder militar el propósito de la ciberdefensa debe ser preservar la capacidad de librar la guerra y realizar otras formas de defensa frente a un ataque. Si no fuera posible las cualidades mínimas del sistema deberían ser la robustez (que incluye la recuperabilidad), la integridad y la confidencialidad. Por otra parte, discernir el propósito de los ciberataques puede ofrecer una idea de lo que el atacante está tratando de lograr y permitir que el objetivo tome medidas para asegurarse de que el atacante sea empujado más lejos de su objetivo. Esto puede ser disuasorio si convence al atacante de que ha fracasado pudiendo incluso llegar a revelar sus objetivos (Libicki, 2009).

Si bien el ciberespacio en sí mismo ofrece una gran libertad de acción para el empleo del Instrumento Militar (IM), este podrá estar condicionado por los lineamientos políticos que cada Estado establezca en su Estrategia de Seguridad Nacional, y el rol y el área de responsabilidad que le asigne. Tanto el empleo del IM en el ciberespacio como el desarrollo de capacidades para poder accionar en él serán determinados por el planeamiento estratégico militar que decante de los

objetivos fijados por la Estrategia Nacional (PC 10-04, 2018). Sin embargo, es muy importante al momento de desarrollar una doctrina de ciberdefensa, comprender todas las posibilidades que el ciberespacio como quinto dominio ofrece, más allá de las leyes nacionales, y las políticas limitantes que puedan determinar los líderes de cada Estado en particular, y a las cuales se beberá adecuar la estrategia. Las regulaciones y las políticas nacionales pueden limitar el desarrollo de ciertas capacidades, pero no deberían condicionar el conocimiento del alcance que el ciberespacio puede ofrecer al Instrumento Militar ni las formas en que los desarrollos de ciertas capacidades pueden ser explotadas en un conflicto armado por otro adversario que no esté sujeto a las mismas limitaciones.

La Defensa se basa principalmente en la disuasión, fundamentada por un lado, en la capacidad de respuesta de forma que el potencial atacante renuncie a materializar su amenaza por los perjuicios que podría recibir a cambio; por otro, en la protección, por la capacidad de resistencia a los ataques de manera que resulten infructuosos o sus efectos se minimicen, y además, en la prevención o previsión, en base a la libertad de acción para poder tomar medidas y ejecutar acciones de protección y /o de respuesta en el momento y modo adecuados. En todas ellas, pero en la última en especial, la inteligencia juega un papel decisivo sobre las amenazas y los riesgos a la que la seguridad está expuesta (Feliu Ortega, 2012). La disuasión no podrá ser efectiva si no se conoce al enemigo, sus intenciones, su objetivo, sus límites, sus capacidades y sus razones para atacar. Esta información de inteligencia permitirá generar credibilidad en las amenazas y garantizar una respuesta apropiada que influya en las acciones del atacante.

La redundancia y réplica son estrategias de resiliencia que pueden disuadir a los presuntos agresores al hacer fútiles los ataques (Nye, 2011). Las respuestas de represalia por medio del ciberespacio u otros medios también pueden mejorar la disuasión (Kugler, 2009).

La disuasión con la amenaza del uso de la fuerza como estrategia de ciberseguridad plantea fallas en su efectividad. El problema de la atribución dificulta identificar a un enemigo a quién realizar la amenaza del uso de la fuerza. Además, los actores detrás de un ciberataque pueden no ser Estados sino grupos extremistas, dispuestos a aceptar las consecuencias por su causa, o individuos a quienes se le vulnerarían sus derechos (Torres, 2019).

Scott Jasper sostuvo que la disuasión surge de la creencia del adversario de que existe una amenaza de represalia, que la acción prevista no puede tener éxito o que los costos superan los beneficios de actuar; que su efectividad dependerá de poder lograrse tres condiciones: capacidades, credibilidad y comunicación; y requerirá la determinación nacional de comprometer recursos, mejorar la cooperación o usar la fuerza cuando sea necesario (Jasper, 2015, pág. 65).

Explicó que puede ser planteada con diferentes enfoques o estrategias: el de disuasión por enredo a través de la cooperación basada en intereses mutuos; bajo el concepto de defensa activa mediante la utilización de tecnologías automatizadas para interceptar, aislar o eliminar los vectores de amenazas incluyendo acciones ofensivas con fines defensivos; por negación de beneficios, basada tanto en la seguridad como en la resistencia de las redes y los sistemas; o por represalia o castigo basado en el derecho de una nación a utilizar todos los medios necesarios para defenderse a sí misma, a sus aliados y socios, y sus intereses; y que un enfoque integral puede lograr estrategias complementarias para la disuasión de la ciberagresión. (Jasper, 2015, págs. 67-74).

Aclaró que la disuasión, como elemento de la política de ciberseguridad, proporciona una respuesta estratégica que se sustenta en esta asociación y cooperación; y que garantizar la capacidad de responder mediante represalias se complica por la dificultad de monitorear el ciberespacio, identificar intrusiones y ubicar la fuente con un alto grado de confianza y de manera oportuna. Observó que las Amenazas Persistentes Avanzadas[15] (APT) ocultan la detección de las identidades de los atacantes y permiten una negación plausible, pero si pudiera obtenerse una atribución definitiva, las Fuerzas Armadas de un Estado podrían actuar dentro de su autoridad prescrita en defensa propia contra un ataque armado equivalente en el ciberespacio (Jasper, 2015, pág. 75).

Además, agregó, que un enfoque de defensa en profundidad enfatiza la implementación continua de soluciones reactivas para proteger múltiples puntos de amenaza; y que las operaciones cibernéticas ofensivas en defensa propia, por el alcance, duración e intensidad de la respuesta, probablemente causarán un daño cinético significativo por lo cual exige una total certeza de atribución (Jasper, 2015, pág. 69).

Joseph Nye Jr. manifestó que los ciberataques estratégicos no son tan fáciles de lograr como parecen, porque deben enfrentar la complejidad de las redes y la posibilidad de consecuencias no deseadas dejando una incertidumbre residual en la mente de los atacantes sobre su efectividad (Nye Jr, 2016, pág. 48).

Sostuvo además, que las ambigüedades de atribución y la diversidad de adversarios no imposibilitan la disuasión por miedo al castigo, que este es posible tanto contra los estados como contra los delincuentes, pero los problemas de atribución a menudo ralentizan y mitigan sus efectos disuasorios; que la negación juega un papel más importante en el trato con actores no estatales que

[15] *Amenaza Persistente Avanzada (APT)* Grupo organizado de expertos, normalmente asociado a un Estado, que utiliza sofisticados conocimientos, herramientas y TTPs (técnicas, tácticas y procedimientos) para (de manera anónima, sigilosa y desapercibida) infiltrarse, tomar el control y perpetuarse en una red ajena, con el objeto de tener acceso a la información de su interés y obtener ventajas estratégicas (JID, 2020, pág. 14).

con los principales estados cuyos servicios de inteligencia pueden formular una APT; y que con tiempo y esfuerzo, es probable que una importante agencia militar o de inteligencia penetre en la mayoría de las defensas, aunque la combinación de una amenaza de castigo más una defensa eficaz puede influir en los cálculos de costos y beneficios (Nye Jr, 2016, pág. 68).

Finalmente recomendó no limitarse a los instrumentos clásicos de castigo y negación al evaluar la posibilidad de disuasión sino prestar atención a los mecanismos de entrelazamiento (Nye Jr, 2016, pág. 68).

En la actualidad se observa una ventaja de la estrategia ofensiva sobre la defensiva por encontrarse libre de complicaciones en el ciberespacio. Nye Jr. observó que esta ventaja puede cambiar con el tiempo a medida que los Estados y las organizaciones comprendan mejor las limitaciones de los ataques cibernéticos y la creciente importancia de Internet para su bienestar económico y los cálculos de costo-beneficio de la utilidad de la guerra cibernética (Nye Jr, 2016, pág. 71). Los actores de APT de hoy en día están capacitados para derrotar las defensas reactivas de ciberseguridad basadas en reglas al desarrollar continuamente sus herramientas, técnicas y procedimientos maliciosos y suelen participar en campañas a largo plazo para comprometer las redes de destino, buscando primero ganar y luego mantener una presencia oculta. La única forma en que las organizaciones pueden protegerse, es mediante el uso de técnicas cibernéticas ofensivas para descubrir adversarios avanzados en sus redes con un enfoque de "caza de ciberamenazas"[16]. Para ello, las organizaciones deben mejorar su postura de seguridad antes de ser atacados basados en tres elementos claves: herramientas analíticas, analistas de amenazas talentosos y un proceso de búsqueda estandarizado integrado en una estrategia de seguridad más amplia (Messe & Medairy, 2018).

China y Rusia son los dos estados que han desarrollado mayor cantidad de APT y herramientas de espionaje. Otros países que también se destacan son Corea del Norte, Irán, Paquistán, Estados Unidos e Israel (Borghello, 2020).

Jeppe Jacobsen (2014), apoyado en antiguos conceptos del libro de Clausewitz "On War" (1832), planteó que las amenazas y las oportunidades de los ciberataques son muy exageradas y que la ciberguerra no reemplazará a las guerras convencionales porque los Estados fuertes, atacados a través del ciberespacio, son más propensos a tomar represalias usando armas convencionales, debido a la capacidad inferior de los ciberataques para causar daño físico.

[16] *Caza de ciberamenazas*. Proceso dinámico y proactivo de ciberdefensa orientado a la detección y aislamiento de amenazas avanzadas que evaden las soluciones de seguridad tradicionales basadas en la gestión de eventos e información de seguridad (SIEM) y dispositivos de ciberseguridad perimetral (firewalls, IDS, IPS, sandboxing, etc.) (JID, 2020, pág. 14)

Por su parte, Martin Libicki sostuvo que la tecnología cibernética "puede ser un multiplicador de fuerza decisivo si se emplea con cuidado, discriminación y precisamente en el momento adecuado" (Libicki, 2009, pág. 139).

El empleo del ciberespacio involucra tanto el nivel estratégico, como el operacional y/ o táctico permitiendo accionar sobre las diferentes capas que lo componen y producir efectos en el plano físico, digital o cognitivo.

En el plano físico los efectos se pueden lograr sobre el hardware: equipamiento integrado a las redes o alguno de sus componentes (incluidos cables), asociados a las tecnologías de la información u operación. Aquí adquieren vital importancia las infraestructuras críticas de un Estado, que cuanto más dependientes de la tecnología son, se vuelven más vulnerables. En el plano digital los efectos pueden lograrse sobre los datos, pudiendo ser negados, sustraídos o develados mediante la utilización de software. Aquí los datos constituyen el elemento crítico, para algunos será el botín, para otros el tesoro más preciado, y para otros el elemento necesario para poder proyectarse hacia los otros planos del ciberespacio. Es en este plano donde cobran protagonismo las APT, se librarán las batallas y en donde tanto la defensa como la seguridad deberán actuar para evitar daños. En el plano cognitivo se puede influenciar a las personas para formarles opiniones y orientarlas hacia un objetivo, pudiendo lograr movilizarlas y actuar en sintonía con el mismo. Aquí la Inteligencia debe entender para proteger los intereses del Estado.

Ulises Kandiko ha detallado algunos ejemplos. Se puede utilizar software para alterar el rostro de una persona en un cuerpo diferente y utilizar grabaciones y datos físicos de videos en línea para crear discursos que nunca sucedieron (fusión de lo falso con lo real) y utilizar pods de interferencia montados en aviones o drones para explotar direcciones IP, interceptar comunicaciones o manipular mensajes enemigos. Las armas cibernéticas pueden ser cuidadosamente diseñadas para fines específicos como borrar datos de discos duros (virus Shamoon) o sabotear los sistemas de control industrial (ICS) de una instalación nuclear en forma automática, una vez dentro de su sistema de control, para regular la velocidad de sus centrifugadoras de uranio haciendo que fallen lentamente (gusano Stuxnet), o de una instalación petroquímica a control remoto por internet, para intentar desencadenar una explosión, generando un ataque de alto impacto con consecuencias físicas (malware Triton) (Kandiko, 2018).

Los efectos a lograr tanto en el plano físico como cognitivo a través del ciberespacio estarán asociados necesariamente al plano digital y el manejo de datos. Los efectos que pudieran llegar a alcanzarse en los planos antes mencionados, sin la utilización de datos, no corresponden al empleo

del ciberespacio sino a operaciones de los dominios físicos del tipo cinéticas, por ejemplo, el seccionamiento de un cableado de internet en el lecho marino o las actividades de propaganda en la vía pública mediante panfletos.

En el ámbito de la información, el propósito estratégico gira en torno a la capacidad en la paz y la guerra de manipular las percepciones del entorno estratégico en beneficio propio y, al mismo tiempo, degradar la capacidad de un adversario para comprender ese mismo entorno. Con el avance tecnológico, el acceso a internet y las redes sociales el ciberespacio juega un papel muy importante.

Desde la perspectiva militar, la importancia de la toma de decisiones y la dependencia tecnológica de las redes para el Comando y Control de las operaciones es vital.

> Los líderes visualizan y entienden el entorno operativo a través de la información que, como elemento de poder de combate, permite la toma de decisiones y su transmisión oportuna ayuda a las operaciones decisivas. La innovación tecnológica aumenta significativamente la velocidad, el volumen y el acceso a la información; y al mismo tiempo, permite interrumpir, manipular, distorsionar y negar información (Vertuli & Loudon, 2018, pág. xii).

El Departamento de Defensa de los Estados Unidos bajo la dirección del Estado Mayor Conjunto e impulsado principalmente por la Fuerza Aérea se encuentra desarrollando una nueva arquitectura de datos para el Comando y Control de operaciones multidominio de todas sus Fuerzas Armadas llamado JADC2 (Comando y Control Conjunto de Todos los Dominios) que mediante una sola red de "internet de las cosas" permita conectar numerosos sensores con sistemas de armas, utilizando algoritmos de inteligencia artificial para ayudar a mejorar la toma de decisiones. JADC2 garantizará que los datos recopilados por los sensores, independientemente del dominio, puedan procesarse, transferirse a un nodo de Comando y Control donde se puedan fusionar con otros datos de otros sensores y distribuirse al tirador apropiado en casi tiempo real (Strout, 2020).

Hoehn sostiene que el desarrollo de capacidades sofisticadas de Anti-Acceso / Denegación de Área (A2/AD) en el entorno operativo de combate futuro que incluyen guerra electrónica, armas cibernéticas, misiles de largo alcance y defensas aéreas avanzadas, para contrarrestar las ventajas militares tradicionales, requiere un enfoque de múltiples dominios en el que el acceso a la información será fundamental (Hoehn, 2022).

Al respecto, Russel había observado que

> las operaciones estratégicas A2/AD en el ciberespacio pueden lograrse mediante la degradación o destrucción de la red física y la infraestructura que sustenta el ciberespacio (…) de una manera que impida que un adversario acceda al dominio o, si ya está presente, disminuya su capacidad para utilizar plenamente sus capacidades. Los satélites y los cables

> de fibra óptica son esenciales para esta red de comunicaciones y pueden ser dañados o destruidos por asalto físico (Russell, 2017).

La pérdida de redes o capacidad de automatización podría provocar la parálisis. Sería un error subestimar el peligro y suponer que las redes y los sistemas de información permanecerán relativamente libres de interferencia enemiga durante un conflicto. Es por ello que una defensa cibernética robusta, redundante y resiliente puede ser adecuada pero no suficiente. Es necesario también contar con cibercapacidades para interrumpir, denegar, degradar o destruir redes de computadores o dispositivos interconectados que puedan afectar al enemigo de forma tal de afectar su toma de decisiones y lograr la anticipación y la ventaja.

> Por otra parte
>
> el aspecto único de la utilización de la información durante las actividades militares es que sus efectos son potencialmente de naturaleza global, esfumando o diluyendo las líneas entre los niveles tácticos, operacionales y estratégicos del conflicto. Los líderes pueden emplear el uso de información para afectar los resultados en las formaciones militares adversarias (De Vergara, 2020).

El conflicto de Ucrania ha permitido por primera vez observar el rol del ciberespacio en un conflicto armado a gran escala. Ariel Levite observó, en el periodo previo a la invasión rusa, entre 2014 y febrero de 2022, la preminencia de la inteligencia cibernética no solo en los esfuerzos de recopilación, sino también en operaciones encubiertas, misiones de influencia y guerra de información. El incremento en el dominio digital y la dependencia de los activos digitales de Ucrania, reforzada por la asistencia masiva de gobiernos y corporaciones extranjeras a partir de 2021, hicieron de la inteligencia cibernética un factor constante en la confrontación con Rusia (Levite, 2023).

Sin embargo, Levite afirma que mientras las operaciones cibernéticas pueden ocupar un lugar central en un período anterior a la guerra, una vez que la confrontación militar es abierta, la guerra cibernética queda relegada a un papel auxiliar debido a que a través del ciberespacio no se puede ocupar territorio, ni matar o destruir constantemente a escala industrial. Sus efectos y radio de explosión son mucho menos predecibles que los de sus equivalentes cinéticos, e incluso las ganancias cibernéticas suelen ser efímeras, transitorias y reversibles, menos medibles y menos visibles que las ganancias físicas. En este punto, las herramientas cibernéticas ofensivas solo pueden facilitar y complementar las operaciones cinéticas al desviar temporalmente la atención, incapacitar o desequilibrar a un adversario, o intimidarlo. Una vez iniciada la guerra, los medios cibernéticos de combate se convierten en parte de un esfuerzo integral para monitorear, interferir y proteger las transmisiones de señales electrónicas, la recepción, la interpretación y la explotación (Levite, 2023).

Asimismo, Nick Beecroft sostiene que la guerra dejó expuesto el enorme papel del sector privado en la defensa de las redes digitales a escala nacional, con algunas preocupaciones entre los aliados occidentales como si la coalición ad hoc desplegada para defender a Ucrania podría replicarse en otros lugares y si sólo confiar en un "paraguas cibernético" proporcionado por un puñado de corporaciones estadounidenses (Bateman, Beecroft, & Wilde, 2022). Observó además que los logros operacionales no equivalen a estructuras duraderas y de base amplia para la defensa colectiva en el ciberespacio, y que la guerra no ha resuelto cuestiones profundas relacionadas con la soberanía, la rendición de cuentas y el reparto de la carga (Beecroft, 2022).

Diferentes formas de abordar la defensa ciberespacial en el mundo

La ausencia de una gobernanza global del ciberespacio ha conducido a muchos Estados a adoptar alianzas y coordinar políticas para poder defenderse. En 2004, Estonia propuso a la OTAN el concepto de un centro de ciberexcelencia que se pudo materializar el 14 de mayo de 2008 junto con otras seis naciones (Alemania, Italia, Letonia, Lituania, República Eslovaca y España) con el nombre de “Cooperative Cyber Defence Centre of Excellence (CCDCOE)[17]”de la OTAN. Entre sus mayores logros se encuentra el proceso del Manual de Tallin sobre el derecho internacional aplicable a las operaciones cibernéticas, lanzado en 2009 y publicado en 2013, mejorado y completado en 2017 en su versión 2.0, y actualmente se encuentra en su proceso de revisión y actualización a la versión 3.0 (CCDCOE, 2023).

La OTAN no solo ha hecho del ciberespacio un dominio operacional al mismo nivel que los tradicionales declarándolo oficialmente el 16 de junio de 2016 como una zona de guerra, sino que ha asumido que un ataque cibernético podría llegar a superar el umbral para la invocación del Artículo 5 del Tratado del Atlántico Norte. Según el mismo, las Partes convienen en que un ataque armado contra una o varias de ellas ocurrido tanto en Europa como en América del Norte será considerado como un ataque dirigido contra todas. En consecuencia, si se produjera, cada una de ellas, en el ejercicio del derecho de legítima defensa, individual o colectiva, reconocido por el art. 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes atacadas tomando individualmente, y de acuerdo con las otras, las medidas que juzgue necesarias, comprendido el empleo de las fuerzas armadas para restablecer la seguridad en la región del Atlántico Norte.

[17] Centro de Excelencia Cooperativa de Ciberdefensa.

El objetivo principal de la OTAN en materia de ciberdefensa es proteger sus propias redes, operar en el ciberespacio, ayudar a los aliados a mejorar su resiliencia nacional y proporcionar una plataforma para la consulta política y la acción colectiva. En la Cumbre celebrada en Bruselas en 2021, los aliados respaldaron una nueva Política Integral de Ciberdefensa, que apoya las tareas centrales de la OTAN y la postura general de disuasión y defensa para mejorar aún más la resiliencia de la Alianza. La OTAN está promoviendo un ciberespacio libre, abierto, pacífico y seguro, y realizando esfuerzos para mejorar la estabilidad y reducir el riesgo de conflicto mediante el apoyo al derecho internacional y las normas voluntarias de comportamiento responsable del Estado en el ciberespacio (OTAN, 2023).

De igual manera, la UE reconoció que la cadena de ciberdefensa es tan fuerte como el eslabón más débil y desarrolló algunos tipos de respuesta más allá de los doctrinales y técnicos como la diplomacia cibernética, que dio lugar por primera vez a sanciones a empresas e individuos por un comportamiento inadecuado o delictivo en las redes, o medidas como la Unidad Conjunta de Ciberseguridad , o una plataforma europea para el conocimiento del entorno cibernético (Martinez Nuñez, 2020) . En 2020, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), desarrolló un marco para ayudar a los Estados miembros a comprender su nivel de madurez mediante la evaluación de sus objetivos de Estrategias Nacionales de Ciberseguridad, que les ayudará a mejorar y desarrollar capacidades tanto a nivel estratégico como operativo (ENISA, 2023).

La postura defensiva de Alemania comenzó a cambiar en 2015, después de que la red interna del Bundestag alemán se viera comprometida por operadores respaldados por Rusia. Eso llevó al país a revisar su estrategia de ciberseguridad, emitiendo un documento más ofensivo en 2016. En 2017, Alemania creó el Comando del Espacio de Información y Ciber (Kdo CIR), un comando conjunto con tres elementos subordinados: el Comando de Inteligencia Estratégica, el Comando Técnico de la Información y el Centro de Geoinformación, que proporciona apoyo de ciberdefensa a sus Fuerzas Armadas. Kdo CIR Constituyó logró la mayor interoperabilidad de sus medios (personal y material) a través de la integración de las capacidades de comunicaciones, informática, inteligencia, guerra electrónica, ciberdefensa, operaciones psicológicas y geoinformación en sus Fuerzas Armadas (Cañete, 2020). En 2020, Alemania puso en marcha la “Cyberagentur”, una ciberagencia encargada en el campo de la seguridad informática en la misma línea de la estrategia de seguridad informática de la UE (Anónimo, 2020). En 2021, la Estrategia de Seguridad Cibernética alemana se centró en cuatro áreas de acción: sociedad, industria privada, gobierno y asuntos internacionales / de la UE. En julio de 2023, Alemania publicó una Estrategia para China,

reconociendo su creciente asertividad y prácticas desleales, pero con un concepto de reducción de riesgos poco claro.

La Estrategia Nacional Cibernética 2022 del Reino Unido plantea un enfoque nuevo e integral para fortalecer su posición como una potencia cibernética. Se complementa con una Estrategia de Seguridad Cibernética del gobierno: 2022 a 2030 para construir un sector público ciberresiliente, una que describe cómo la función digital de Defensa permitirá el acceso a los datos mediante la entrega de una red troncal digital segura, singular y moderna, una Estrategia de Datos para la Defensa que describe la visión de datos, las reglas de datos y los planes del Ministerio de Defensa en toda la Defensa, y una Estrategia de Ciberresiliencia para la Defensa describe la visión del Ministerio de Defensa para construir una defensa más fuerte y ciberresiliente (GOV.UK, 2022). UK pretende contar para 2025 con una red troncal digital segura, singular y moderna que le permita conectar sensores, efectores y decisores en dominios militares y comerciales y con socios, impulsando la integración y la interoperabilidad entre dominios y plataformas, y liberar el poder de los Datos de Defensa, explotando la Inteligencia Artificial y otras tecnologías revolucionarias. Concibe a la columna vertebral digital de Defensa como un ecosistema que combina personas, proceso, datos y tecnología (GOV.UK, 2021).

La Estrategia Cibernética Militar Francesa, consta de dos documentos separados: la Política Ministerial para la Guerra Cibernética Defensiva y los Elementos Públicos para la Doctrina de la Guerra Cibernética Militar Ambos describen la doctrina del Ministerio de Defensa francés sobre la guerra cibernética defensiva y ofensiva. La ciberdefensa en general es responsabilidad del director general de la Agencia Nacional de Ciberseguridad de Francia (ANSSI), mientras que el comandante de la ciberdefensa (COMCYBER) está exclusivamente a cargo de la ciberdefensa del Ministerio de Defensa. En su compromiso con la OTAN, Francia mantiene una postura cooperativa en la guerra cibernética ofensiva, pero a la vez independiente, manteniendo el control total sobre sus operaciones y capacidades (Delerue, Desforges, & Gery, 2019).

La Directiva de Defensa Nacional de España (2020) definió a los datos como un nuevo recurso crítico de la economía mundial, objeto de competición geoestratégica e identificó como un reto las acciones de desinformación y las agresiones en el ciberespacio. Con el objeto de obtener una visión unificada para la obtención de sistemas de ciberdefensa, el Ministerio de Defensa español creó en 2020 la Jefatura de Sistemas Satelitales y de Ciberdefensa (JSSAT-CIBER) que agrupa dos iniciativas, la vinculadas con el desarrollo del segmento de vuelo de los programas espaciales de navegación, vigilancia y comunicaciones; y los proyectos relacionados con el componente del dominio de la ciberdefensa (Pons, 2021).

Por otra parte, diferentes documentos de dominio público sumados a la historia reciente, han demostrado un patrón común en la estrategia de Rusia y China al intentar combinar métodos de guerra convencionales y no tradicionales, para socavar el consenso de que existe un estado de guerra creando ambigüedad en la naturaleza del mismo conflicto. El conflicto cibernético se desprende en gran medida de los conceptos operacionales de ambos estados (Moerbe, 2017).

La Estrategia de Seguridad Nacional de la Federación Rusa (2015) planteaba que los objetivos estratégicos de defensa nacional debían alcanzarse en el marco de implementar la política militar a través de la disuasión estratégica y la prevención de conflictos armados, mejorar la organización militar del estado y las formas y métodos para desplegar sus Fuerzas Armadas, otras tropas, formaciones militares y agencias, incrementando el estado de alistamiento para la movilización de la Federación Rusa y la preparación de las fuerzas y los recursos de la defensa civil. Contemplaba además el desarrollo e implementación de medidas políticas, militares, técnico-militares, diplomáticas, económicas, informativas y otras interrelacionadas para garantizar la disuasión estratégica, la prevención de conflictos armados y el uso de otras fuerzas armadas, para proteger su soberanía e integridad territorial. La disuasión estratégica y la prevención de conflictos armados se logran manteniendo la capacidad de disuasión nuclear en un nivel suficiente, y las Fuerzas Armadas de la Federación de Rusia, otras tropas, y formaciones militares y cuerpos en el nivel requerido de preparación para el combate.

Keir Giles (2016) resaltó una distinción fundamental entre el enfoque de la doctrina rusa y occidental de las actividades de información respecto a la categorización de las operaciones en red de computadoras y otras actividades en el ciberespacio, en el que el término “ciber” como una función o dominio separado no es un concepto ruso. En lugar de ciberespacio, Rusia se refiere al “espacio de información” e incluye en este espacio el procesamiento de información.

Fabio Rugge (2018) observó que la doctrina rusa de la "Guerra de Nueva Generación"[18] ha generado un contexto en el que los “ataques informativos” se convierten en el “integrador de sistemas” de medios militares tanto cinéticos como no cinéticos, así como de actores gubernamentales y no gubernamentales; se libran durante tiempos de paz y de guerra en los dominios de los medios de comunicación nacionales, del adversario e internacionales, y se perciben como una de las herramientas más rentables de coerción no nuclear y un instrumento esencial para

[18] *Guerra de Nueva Generación (de Rusia)*: conocida como "doctrina Gerasimov", consagra una combinación de poder duro y blando (que abarca también la guerra económica, el chantaje energético y la diplomacia de oleoductos, el apoyo a oposiciones políticas y agentes de influencia en el extranjero, y otras medidas activas) en diferentes dominios y mediante una hábil aplicación de herramientas militares, diplomáticas y económicas coordinadas (Masarellas, 2022, p. 2).

minimizar los enfrentamientos cinéticos. La doctrina rusa enfatiza la guerra de la información y el uso de medios no cinéticos a fin de dar forma al campo de batalla para el combate físico.

La guerra de Ucrania expuso las profundas diferencias en el enfoque ruso y estadounidense de las operaciones cibernéticas ofensivas evidenciando que a Rusia poco le importa el retroceso de sus operaciones cibernéticas ofensivas, y menos las revelaciones sobre su conducta cibernética. Las operaciones cibernéticas ofensivas rusas en Ucrania se han ajustado a un mismo patrón de comportamiento empleado contra Estonia en 2007 y en las elecciones estadounidenses de 2016 en tiempos de paz, constituyéndose en instrumentos políticos de acoso, subversión y / o coerción para proyectar su influencia y moldear favorablemente el entorno político. En cambio, las acciones cibernéticas estadounidenses e israelíes como la operación Juegos Olímpicos, fueron diseñadas cuidadosamente para producir efectos temporales, precisos y localizados en activos e instalaciones utilizables militarmente (Levite, 2023).

Por el lado de China, en 2010 publicó el Libro Blanco titulado “Internet en China” y en 2017 la “Estrategia Internacional de Cooperación en el Ciberespacio”, estableciendo que “el principio de soberanía consagrado en la Carta de las Naciones Unidas cubre todos los aspectos de las relaciones de Estado a Estado, incluido el ciberespacio. La posterior “Directriz Estratégica Militar para una Nueva Era”, planteó la seguridad cibernética como un desafío global y una grave amenaza, observando que sus fuerzas armadas debían acelerar la construcción de sus capacidades en el ciberespacio, desarrollando medios de ciberseguridad y defensa, determinando capacidades de ciberdefensa, reforzando la defensa nacional de las fronteras cibernéticas, protegiendo la información y la seguridad cibernética.

La República Popular China cuenta además con una Ley de Ciberseguridad, formulada con el fin de proteger las operaciones, salvaguardar la soberanía del ciberespacio, la seguridad nacional y los intereses públicos sociales, salvaguardar los derechos e intereses legítimos de los ciudadanos, personas jurídicas y otras organizaciones, y promover el sano desarrollo de la informatización económica y social.

En Asia, China está intentando articular una alianza militar y utiliza el Foro de Cooperación Económica Asia-Pacífico, el grupo BRICS, la Conferencia sobre Interacción y Medidas de Fomento de la Confianza en Asia (CICA) y la Organización de Cooperación de Shanghái para avanzar en una “estructura de seguridad”, probablemente como estrategia de defensa ante el incremento de la presencia de EEUU en Taiwán. Esta iniciativa fue propuesta por el presidente chino Xi Jinping en junio de 2019 durante una reunión de la CICA en Dusambé e interpretada por algunos analistas

como una especie de “OTAN asiática”. En aquella ocasión, su par ruso Vladímir Putin proclamó que Rusia, China y Mongolia cumplían una importante tarea común: “garantizar juntos la estabilidad en el espacio eurasiático". Por otra parte, tras haber incrementado sus inversiones en toda África desde 2013 a través del proyecto de Iniciativa del Cinturón y la Ruta, conocido como la “Nueva Ruta de la Seda”, y haber superado a EEUU como el mayor socio comercial de África desde 2010, China plantea también una alianza militar de cooperación con África.

En oposición, EEUU ha buscado influir en los países vecinos para contener a China, utilizando a Japón y Australia (U24 Asia, 2019). Los verdaderos aliados de EEUU integran un grupo de mini coaliciones superpuestas: El Quad (Diálogo de Seguridad Cuadrilateral), la alianza de inteligencia de los Cinco Ojos y el AUKUS, y son cinco: Japón, Australia, India, Nueva Zelanda y Canadá (Toro Hardy, 2022).

África alberga los 10 países más pobres de todo el mundo, es el hogar de más de 18 millones de refugiados y desplazados (EACNUR, 2017), y su índice de adopción de Internet en diciembre de 2021 era del 43 % (Internet Society, 2022). El Departamento de Paz y Seguridad de la Unión Africana es el encargado de llevar a cabo los objetivos de alcanzar paz, seguridad y estabilidad. La UE ha intentado fortalecer las relaciones con África y su consideración de socio estratégico, pero al mismo tiempo se ha transformado en un escenario de competencia de las grandes potencias. Marruecos por su parte, renovó una alianza militar con EEUU hasta 2030.

Australia en su Libro Blanco 2016 observó el incremento de ciberataques utilizando ciberoperaciones ofensivas con impactos más allá de la Defensa, y con el potencial para atacar a otras agencias gubernamentales, todos los sectores de Australia economía e infraestructura crítica y, en el caso de los actores estatales, llevar a cabo espionaje estatal, incluso contra la industria de la defensa. Su Estrategia de Ciberseguridad de Defensa 2020 reconoce el valor estratégico y la ventaja de la inversión en capacidades cibernéticas ofensivas como una herramienta crítica para la seguridad cibernética. Se orienta hacia una defensa ciberresiliente y los principios para mantener una postura sólida de ciberseguridad en un entorno estratégico cambiante (AGD, 2023).

Estados Unidos, cambió de una postura defensiva y reactiva a una postura más efectiva y proactiva llamada "Compromiso Persistente", una estrategia que implica ejecutar operaciones fuera de las redes militares para defenderlas e incluye misiones de "caza avanzada[19]" en las que el

[19] *Caza avanzada*: se refiere a la caza de amenazas, una medida de seguridad proactiva que implica la búsqueda activa de amenazas potenciales dentro de la red de una organización, combinando técnicas manuales y análisis de la actividad maliciosa con el uso de software automatizado para descubrir posibles amenazas y mitigar los riesgos. Constituye una parte esencial de una estrategia de ciberseguridad sólida, y requiere profesionales cualificados, herramientas avanzadas y un análisis exhaustivo de los datos para tener éxito (Moes, 2023).

personal de su Comando Cibernético (CYBERCOM) trabaja con naciones amigas para investigar signos de amenazas cibernéticas y mejorar las defensas. Se complementa con la estrategia "Defender hacia Adelante", una estrategia de defensa y tácticas ofensivas en el ciberespacio que reconoce las ventajas inherentes a las tácticas de ataque y las operaciones proactivas en el ciberespacio integrándolas en una estrategia defensiva.

En 2022, la Administración Biden-Harris de los Estados Unidos actualizó la Estrategia de Seguridad Nacional y la Estrategia de Defensa Nacional, junto con una serie de medidas para proteger el ciberespacio, su ecosistema digital, y los sistemas de control de infraestructura crítica, promover el liderazgo en computación cuántica al tiempo que mitiga los riesgos para sistemas criptográficos vulnerables, y mover al gobierno hacia una arquitectura de confianza cero, un nuevo paradigma que asume que las redes ya están comprometidas y, como resultado, requieren una validación continua de usuarios y dispositivos. En línea con esta última estrategia, el Departamento de Defensa intenta sumar a sus socios de “Five Eyes”: Australia, Canadá, Nueva Zelanda y el Reino Unido (Demarest, 2023).

En marzo de 2023, publicó su Estrategia Nacional de Ciberseguridad basada en cinco pilares: defender la infraestructura crítica, interrumpir y desmantelar los actores amenazantes, dar forma a las fuerzas del mercado para impulsar la seguridad y la resiliencia, invertir en un futuro resiliente, y forjar alianzas internacionales para perseguir objetivos compartidos (Whitehouse, 2023).

Subordinada a las anteriores estrategias, el Departamento de Defensa elevó al Congreso en mayo su Estrategia Cibernética 2023, enfocada en maximizar sus capacidades operativas cibernéticas en apoyo de la disuasión integrada, hacer campaña en y a través del ciberespacio por debajo del nivel de conflicto armado, y proteger y reforzar la red global de aliados y socios. Reconoce como amenazas a China, Rusia Corea del Norte, Irán, las organizaciones extremistas violentas (“VEOs”), y las organizaciones criminales transnacionales. Además, identifica como líneas de esfuerzo complementarias defender la nación, prepararse para combatir y ganar guerras, proteger el dominio cibernético con aliados y socios, y construir ventajas duraderas en el ciberespacio.

El 18 de Julio de 2023 el Senado estadounidense publicó un proyecto de ley para que el Departamento de Defensa desarrolle una estrategia para la guerra cibernética y electrónica convergente (USCongress, 2023). Requiere recomendaciones sobre las relaciones y procesos de comando y control, des conflicto y coordinación entre los comandantes del Teatro de Operaciones y

el Comando Cibernético con respecto a las operaciones cibernéticas tácticas y las operaciones convergentes de guerra cibernética y electrónica realizadas antes y durante el conflicto armado (Pomerleau, 2022).

Respecto a la Política Hemisférica de Ciberseguridad en América Latina, las disparidades jurídicas y los problemas de la transnacionalización de los delitos dificultan las estrategias nacionales por la poca coordinación de los ordenamientos jurídicos de los países afectos a la ciberdelincuencia. El atraso y desigualdad entre el desarrollo de los países y su acceso a la red, ha provocado grandes trabas al avance de la ciberseguridad en América Latina no existiendo un marco regulatorio común para los países, a pesar de que la OEA y el BID han trabajado constantemente fomentando la coordinación regional.

Según el Índice Nacional de Ciberseguridad de la "E-Governance Academy", Latinoamérica se encuentra en el sexto lugar de las regiones que han priorizado el desarrollo de las cibercapacidades, solo por encima de África y Oceanía. Por encima se encuentran los países de la OTAN, los aliados de la OTAN, el resto de Europa, Asia, y Medio Oriente (Aguilar Antonio, 2021).

El sector privado, en especial el empresarial, ha colaborado en parte mientras que los Estados latinoamericanos adaptan sus políticas al siglo XXI, ya que muy pocos cuentan con un marco regulatorio actualizado sobre el ciberespacio. América Latina presenta grandes problemas de coordinación entre los actores internacionales involucrados en la seguridad del ciberespacio. Los esfuerzos han sido canalizados a partir de la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), y las reuniones periódicas en los foros internacionales, no logrando reducir los altos índices de ciberataques, ni aumentar las bajas tasas de reacción oportuna.

Se destaca positivamente la cooperación entre las organizaciones internacionales como INTERPOL en el combate efectivo de la delincuencia cibernética. Los Estados han comenzado a aprovechar la capacidad de sus fuerzas armadas nacionales y/o agencias de defensa relacionadas para defender a su país cinéticamente y proporcionar una defensa similar a través del ciberespacio, en respuesta a las amenazas de seguridad cibernética (Castro & Monteverde, 2018).

Entre los Estados que poseen organizaciones de ciberdefensa se encuentra Brasil, con su Comando de Defensa Cibernética; Colombia, con su Comando Conjunto Cibernético; Argentina, con su Comando Conjunto de Ciberdefensa; y Perú, con su Departamento de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas Peruanas. Un estudio publicado en 2021 por el portal de Revistas Académicas de la Universidad de Chile destaca que las Fuerzas Armadas mejor

capacitadas para realizar ciberoperaciones son las de los países antes mencionados (Aguilar Antonio, 2021).

Un informe del BID sobre ciberseguridad del año 2016 observó que bajo la dirección del Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad y en coordinación con diversos organismos, instituciones académicas y el sector privado, el gobierno de Argentina había desarrollado un proyecto de Estrategia Nacional de Seguridad Cibernética que se encontraba en espera de adopción. Asimismo, reconocía que sus Fuerzas Armadas realizaban anualmente Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos para compartir mejores prácticas y revisar funciones de mando y control, pero con una capacidad limitada de resiliencia cibernética (BID, 2016).

Tras la aprobación de la Estrategia de Seguridad Nacional del año 2008, la República Federativa de Brasil reconoció dos campos distintos de la ciberdefensa: la ciberseguridad a cargo de la Presidencia de la República y la Ciberdefensa, a cargo del Ministerio de Defensa, a través de las Fuerzas Armadas (MD31-M-07, 2014).

La JID y la Fundación Interamericana de Defensa, con el apoyo del Gobierno de Canadá, lanzaron el Programa de Ciberdefensa para brindar capacitación a los países miembros con el propósito de fortalecer las capacidades de ciberdefensa individual y colectiva entre las instituciones militares de la región. Durante la II Conferencia de Defensa Cibernética en 2020, incluyeron entre sus objetivos fortalecer las estrategias de ciberdefensa y la capacidad de respuesta en el hemisferio occidental; mejorar la colaboración, la comunicación y el intercambio de información dentro y entre las instituciones militares y los gobiernos de las Américas; promocionar los intereses multilaterales; fortalecer las relaciones y promocionar el aprendizaje; y apoyar el establecimiento del Marco de Cooperación para la Defensa Cibernética en las Américas. Del Programa de Ciberdefensa de la JID participan Argentina, Colombia, Guatemala, México, Perú y República Dominicana (IADF, 2023).

En el primer capítulo se ha podido caracterizar al ciberespacio, se definieron conceptos clave de la temática, se analizaron aspectos relacionados con su utilización e incidencia en temas de seguridad nacional y defensa, las posibles estrategias a ser aplicadas y como algunos países enfrentan este desafío en la actualidad. El próximo capítulo estará vinculado con los aspectos tecnológicos; se definirán conceptos claves, se analizarán diferentes herramientas disponibles, la posibilidad de su aplicación en el ámbito militar y las tendencias tecnológicas para su aplicación en los futuros conflictos.

CAPÍTULO II: INNOVACIÓN TECNOLÓGICA Y SU APLICACIÓN MILITAR EN EL CIBERESPACIO

"La victoria sonríe a quienes anticipan los cambios en el carácter de la guerra, no a quienes esperan para adaptarse después de que ocurran los cambios".

Giulio Douhet[20]

La proliferación de las TIC cambia la forma en que los humanos interactúan entre sí y con su entorno, y donde la movilidad adquiere protagonismo en nuestra vida líquida, en la que la comunicación móvil, internet móvil, y la navegación se realizan con conexión inalámbrica en el espectro electromagnético.

Las fuerzas armadas modernas también operan en un mundo cada vez más basado en redes inalámbricas, y utilizan una amplia gama de dispositivos electrónicos en el espectro electromagnético para comunicaciones, control de armas, inteligencia, vigilancia, navegación y protección de fuerzas en el campo de batalla. Estos dispositivos funcionan en este entorno de información a través del campo electromagnético, lo que hace necesario intensificar las capacidades de interoperabilidad entre ellos (Haig, 2015).

El uso del espectro electromagnético y la operación en el ciberespacio son esenciales en la guerra moderna. Las fuerzas militares usan redes informáticas inalámbricas para coordinar operaciones, usan sensores aéreos y terrestres para detectar y ubicar al enemigo, usan radios para comunicarse entre sí y usan bloqueadores electrónicos para cegar los radares enemigos o interrumpir sus comunicaciones. Con enrutadores inalámbricos o radios tácticos como parte de casi todas las redes informáticas, el ciberespacio y el espectro electromagnético ahora forman un entorno continuo y coherente. El espectro electromagnético y el ciberespacio como entorno de información específico son fundamentales para las operaciones militares. La dependencia existente entre el ciberespacio y el espectro electromagnético puede traducirse en efectos multidisciplinarios que, mediante actividades técnicas de información armonizadas, coordinadas e integradas, y los desarrollos tecnológicos permitirá aumentar esta convergencia (Haig, 2015).

En la sesión inaugural del XXXII Seminario Internacional de Seguridad y Defensa realizado en España en septiembre del año 2020, el Almirante (R) Martinez Nuñez afirmaba que la tecnología está cambiando dramáticamente el mundo, pero continúa siendo aún una herramienta de diseño en

[20] *Douhet, G*., & Ferrari, D. (2019). The command of the air (Air University Press edition). Air University Press, p. 27.

manos de los seres humanos. El ciberespacio es un producto del ser humano y seguirá siéndolo en la medida que así lo desee (Martinez Nuñez, 2020).

El Informe sobre Tecnología e Información 2021 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) expresaba que

> Vivimos en una época de espectaculares avances tecnológicos, concentrados en su mayoría en los países desarrollados (…) El mundo está llegando al final de la fase de implantación de la "Era de las TIC" e inicia la fase de instalación de un nuevo paradigma, que incluye tecnologías de frontera, revolución a veces denominada cuarta revolución industrial o Industria 4.0 (…) El desarrollo humano en las últimas décadas ha sido acompañado de rápidos cambios en la tecnología y de una creciente proliferación de dispositivos y servicios digitalizados, (esperando que) el ritmo del cambio se acelere de la mano de las "tecnologías de frontera", (…) un grupo de nuevas tecnologías que aprovechan la digitalización y la conectividad, lo que les permite combinarse para multiplicar sus impactos (UNCTAD, 2021, págs. 4,8-9).

En este contexto, la ciberdefensa se concibe como un conjunto de capas sucesivas que comienzan en el individuo y se extienden a redes más amplias, en donde el componente humano de la defensa no pierde su importancia, ni a pesar de los avances tecnológicos, ni gracias a ellos, no pudiendo sustituir hasta el momento la empatía, el espíritu de sacrificio, el espíritu de servicio a los demás, ni el sentido del deber (Martinez Nuñez, 2020).

Conceptos de innovación tecnológica, Internet de las cosas, TIC, TI y TO, Industria 4.0 y tecnologías de frontera

Innovación tecnológica es el cambio de índole técnico o científico que se introduce al bien o servicio que ofrece una empresa u organización, a los procesos que se desarrollan dentro de la misma, a fin de alcanzar mayor competitividad. Se puede clasificar de diferentes formas: radical, es aquella completamente original y novedosa; incremental, la que en base a algo ya existente permite mejorar los productos o servicios ofrecidos; y cambio de paradigma, aquella que hace alusión a un cambio de percepción respecto a las tecnologías (Westreicher, 2020).

El concepto de innovación tecnológica se encuentra asociado al de "internet de las cosas" ("IoT"), tecnologías de la información y las comunicaciones (TIC), tecnologías de la información (TI) y tecnologías de operación (TO), tecnologías de frontera e industria 4.0.

Internet se define como una gran “red de redes”, es decir, una red conectada a otra de manera continua y simultánea donde todos los dispositivos están conectados entre sí a través de un mismo protocolo o “lenguaje en común” (NIC, 2018).

Para interconectar dispositivos de red en Internet se utiliza un conjunto de protocolos de comunicación por ejemplo el “Protocolo de Control de Transmisión / Protocolo de Internet” (TCP/IP[21]) (CCNA, 2023). La mayoría de ellos se estructuran como series de capas o pila de protocolos. Cada capa está diseñada para una finalidad específica, existe tanto en los sistemas de envío como en los de recepción, envía o recibe exactamente el mismo objeto que envía o recibe el proceso equivalente de otro sistema, lo hace independientemente de las demás capas del mismo sistema y en paralelo con la misma capa en otros sistemas (Studocu, 2023). La Organización Internacional para la Estandarización (ISO) diseñó un modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que utiliza una estructura con siete capas para las actividades de red. Cada capa tiene asociados uno o más protocolos. El modelo TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas (Oracle Corporation, 2010).

Internet es una red de redes con alcance mundial. Si bien todos los equipos conectados a ella no lo están directamente entre sí, conforman pequeñas redes que a su vez se van vinculando con otras de forma descentralizada. La gran mayoría contrata el servicio de un proveedor de telefonía móvil o banda ancha hogareña o empresarial para poder acceder a la misma. En el hogar o la oficina, la computadora portátil, tableta o teléfono celular se vinculan a un dispositivo inalámbrico, que luego se conecta a la red de fibra óptica de la empresa que brinda el servicio de Internet. Éste se comunica a la red de otro Proveedor de Servicios de Internet (ISP: “Internet Service Provider”) más grande y así sucesivamente hasta llegar a los proveedores de acceso internacional, que se interconectan con los denominados “Carriers”, a través de fibras ópticas transcontinentales y satélites, entre otros (NIC, 2018).

En lugares donde no existe o es insuficiente la estructura de la banda ancha existen alternativas sin necesidad de instalaciones con cableado como el internet de microondas o el internet satelital.

Internet de las cosas (IoT: “Internet of Things”) es un concepto abstracto que involucra las cosas cotidianas que se conectan a Internet, potenciando objetos que antiguamente no estaban conectados a una red o que se conectaban mediante circuito cerrado, y que hoy permiten comunicarse globalmente mediante el uso de la red de redes.

[21] El protocolo TCP/IP es de los que se encuentran más en la superficie del modelo OSI, en las capas inferiores existes otros protocolos de comunicación y algunos muy específicos para tiempo real como el 1553.

Los aparatos más modernos, eléctricos y electrónicos, y los dispositivos digitales con los que convivimos actualmente como computadoras y celulares, heladeras, juguetes, automóviles, lavarropas, sensores, cafeteras, cámaras, calefacción, casas inteligentes, iluminación, asistentes inteligentes, etc., tienen circuitos y sensores que les permite ejecutar programas, recolectar y compartir datos con el internet sin la intervención de personas.

El desarrollo del IoT se enfoca específicamente en la generación de sensores incorporados a los objetos para la recolección y envío de datos (Argentina.gob.ar, 2021). Los objetos parecen inteligentes, aunque en realidad están obedeciendo un programa o software que les permite realizar acciones en base a los datos recolectados: encender luces, riego de plantas, una cafetera, etc (innovacionenunclick, 2023).

En resumen, se le llama Internet de las cosas a la posibilidad de interconexión y transmisión de datos entre objetos cotidianos e internet (Argentina.gob.ar, 2021)

La Unión Internacional de Telecomunicaciones (UIT) estableció que "...IoT puede ser considerada una infraestructura global para la sociedad de la información, permitiendo servicios avanzados para interconectar (física y virtualmente) cosas, basadas en tecnologías de la información y las comunicaciones interoperables. A través de la identificación, captura de datos, capacidades de comunicaciones y procesamiento, IoT hace un uso integral de las cosas para ofrecer servicios para todo tipo de aplicaciones mientras asegura que los requisitos de seguridad y privacidad sean cumplimentados" (UIT-T Y.2060, 2012).

El concepto de Tecnologías de la Información y la Comunicación (TIC) hace referencia a las teorías, las herramientas y las técnicas utilizadas en el tratamiento y la transmisión de la información: informática, internet y telecomunicaciones (Hdez, 2021). Otros conceptos igualmente aceptados, pero menos utilizados son Nuevas Tecnologías de la Información y la Comunicación (NTIC) o Tecnologías de la Información (TI), aunque este último resulta incompleto por su alcance.

Se puede definir a las TIC como el "conjunto de recursos necesarios para tratar información a través de ordenadores y dispositivos electrónicos, aplicaciones informáticas y redes para convertirla, almacenarla, administrarla y transmitirla" (Gorrín, 2020). En el nivel de usuario, individuo u organización, las TIC forman el conjunto de herramientas tecnológicas que permiten un mejor acceso y clasificación de la información como medio tecnológico para el desarrollo de su actividad (Hdez, 2021).

Los términos TIC y TI no deben confundirse entre sí. TIC es un término extensivo de TI usado en el ámbito académico. Las TIC se usan en la configuración académica, y las TI en

organizaciones más complejas y grandes, como empresas y grandes corporaciones. Mientras que las TIC están asociadas al campo educativo, las TI están asociadas al campo de las computadoras, software, redes y el procesamiento de datos. Las TIC se utilizan principalmente en la configuración académica, mientras que las TI se utilizan en organizaciones más complejas y grandes, como empresas y grandes corporaciones (Anónimo, differencebetween.net).

La TI: Tecnología de la Información (IT: "Information Technology") es una industria en sí misma. Se asocia al empleo de software, hardware, y equipos de telecomunicaciones, con el propósito de almacenar, proteger, recuperar y procesar datos electrónicamente.

La TO: Tecnología Operacional, Operativa o de Operaciones, (OT: "Operational Technology"), se refiere al empleo de soluciones, tanto de hardware como de software, para monitorear, cambiar o controlar dispositivos físicos, procesos y eventos dentro de una empresa u organización (Brainly, 2022). Esta especialidad tecnológica se usa con mayor frecuencia en entornos industriales e involucra, por lo general, dispositivos que tienen mayor autonomía que los empleados por la TI.

Los Sistemas de Control Industrial (ICS: "Industrial Control Systems"), que abarcan varios tipos de procedimientos de control e instrumentos, utilizados en la supervisión de procesos industriales, son un ejemplo de TO. Los ICS, en general, son administrados por sistemas SCADA ("Supervisory Control And Data Acquisition", o Control de Supervisión y Adquisición de Datos), que pueden proporcionar a los usuarios una interfaz gráfica, permitiendo observar el estado actual del sistema, ingresar ajustes para administrar el proceso, y reaccionar oportunamente ante cualquier alarma que indique que algo anda mal.

Los ICS, que permiten monitorear y controlar de forma remota las diferentes variables del proceso industrial, incluyen sistemas de seguridad (SIS – "Safety Instrumented Systems"). Los SIS se usan para proteger a los humanos, las plantas industriales y el medio ambiente si un proceso supervisado supera los márgenes de control permitidos. Son los que controlan las operaciones en instalaciones nucleares, plantas de petróleo y gas, instalaciones de tratamiento de agua y más cuando se detectan condiciones peligrosas y representan la última línea de defensa. El enfoque tradicional de las redes ICS era segregar la infraestructura de comunicación de los activos de control. Sin embargo, la tendencia de la última década hacia la integración de la infraestructura de red, colocando los sistemas de control de procesos y los controladores SIS en la misma red de propósito general, combinados con ingeniería de acceso remoto, los ha vuelto mucho más vulnerables (De Nimrod, 2018).

Por otra parte, la OT depende de dispositivos como los PLC (“Programmable Logic Controller” o Controladores Lógicos Programables), que reciben información de dispositivos de entrada o sensores, procesan los datos, y realizan tareas específicas, como monitorear la productividad de una máquina, rastrear la temperatura de operación, detener o iniciar procesos automáticamente, o activar alarmas, entre otras acciones. El acceso a estos dispositivos suele ser restringido a un grupo pequeño de especialistas altamente capacitados dentro de una organización, no suelen actualizarse ni cambiarse durante mucho tiempo y requieren un software personalizado para su funcionamiento.

La innovación digital requiere que los sistemas de TO y TI anteriormente con roles bastante separados, deban interactuar e integrarse. La conexión de componentes de red de la OT como los PLC, SCADA y las redes industriales, a componentes de la red de IT, como procesadores, almacenamiento y administración de sistemas, permite utilizar los datos que recopila el equipo físico y los dispositivos de internet industrial de las cosas para identificar problemas o aumentar la eficiencia.

Si bien la mayor conectividad e integración de dispositivos en red producto de la convergencia de OT e IT es muy beneficioso para el análisis y el control inteligentes, significa también más oportunidades para los “agujeros” de ciberseguridad (Anónimo, 2021).

El concepto de Industria 4.0 extiende la conectividad digital al mundo físico y sus tecnologías combinan información digital de muchas fuentes y ubicaciones físicas y digitales diferentes, incluida la Internet de las cosas (IoT) y el análisis, la fabricación aditiva, la robótica, la informática de alto rendimiento, la inteligencia artificial y las tecnologías cognitivas, los materiales avanzados y la realidad aumentada. Estas fuentes de datos se unen para mejorar las operaciones en un ciclo continuo conocido como bucle de físico a digital a físico (PDP). A lo largo de este ciclo, el acceso en tiempo real a los datos y la inteligencia está impulsado por el flujo continuo y cíclico de información y acciones entre los mundos físico y digital (Deloitte, 2023). Sin embargo, es el salto de lo digital a lo físico, de las tecnologías digitales conectadas a la acción en el mundo físico, lo que constituye la esencia de la Industria 4.0 (Schultz, Mariani, Jenkins, Strickland, & Raymond, 2018).

El término Industria 4.0 o Cuarta Revolución Industrial ha sido ampliamente utilizado en los últimos años y una de las áreas en donde encuentra una gran difusión a nivel global es el ámbito de la producción militar o de armamento. Es aquí donde primero se han probado e implementado todos los logros científicos y técnicos de la humanidad a lo largo de los siglos, donde la mayoría de los países y empresas líderes en la industria están ponen en práctica los últimos descubrimientos y

desarrollos y donde se encuentran las aplicaciones de la tecnología láser, el desarrollo de hardware y software, las ondas electromagnéticas, la fusión y la división de isótopos radiactivos y otros logros de nuestro tiempo.

La plataforma de la Industria 4.0 permite producir bienes individuales a costa de los producidos en serie con la más alta calidad. La base de este tipo de producción es la infraestructura de sistemas y procesos de fabricación inteligentes acoplados digitalmente. Así, Industria 4.0 se refiere a todo el ciclo de producción de un producto: desde la idea de desarrollo, pasando por la producción, distribución y uso, hasta el reciclaje.

Las innovaciones tecnológicas como Internet de las cosas, las redes de comunicaciones 5G, la computación en la nube, el análisis de datos y la robótica están cambiando los productos, procesos y modelos comerciales en todos los sectores y creando nuevas estructuras industriales a medida que cambian las cadenas de valor globales. La digitalización de la producción tiende a conducir en gran medida a la automatización de la industria, permitiendo la libre circulación de la producción industrial en todo el mundo.

Las tecnologías clave identificadas inicialmente en las estrategias industriales que llevaron al desarrollo de la Industria 4.0 fueron: Internet industrial de las cosas (IIoT: Industrial Internet of Things), simulaciones, realidad aumentada / virtual (VR / AR), robots autónomos, tecnologías en la nube o computación en la nube ("cloud computing"), ciberseguridad, impresión 3D, integración de sistemas horizontal y vertical, análisis de macrodatos (Big Data). Esta lista se complementa con otras nuevas soluciones tecnológicas como: inteligencia artificial y sistemas cognitivos, aprendizaje automático, aplicaciones móviles inteligentes, tecnologías de cadena de bloques ("blockchain"), plataformas digitales y más. La lista de tecnologías que tendrán un impacto significativo en el futuro cercano no puede ser exhaustiva porque constantemente surgen nuevas oportunidades y necesidades (Todorov & Encheva, 2020).

Las "tecnologías de frontera" son un grupo de nuevas tecnologías que aprovechan la digitalización y la conectividad, lo que les permite combinarse para multiplicar sus impactos. Naciones Unidas identificó la inteligencia artificial (IA), el internet de las cosas (IoT), los macrodatos (Big Data), la cadena de bloques (Blockchain), la telefonía de quinta generación (5G), la impresión tridimensional (3D), la robótica, los drones, la edición genómica, la nanotecnología y la energía solar fotovoltaica, como tecnologías que pueden utilizarse para aumentar la productividad con un enorme potencial para mejorar la vida de las personas y proteger el planeta (UNCTAD, 2021).

Los países en desarrollo no pueden permitirse el lujo de no subirse a esta nueva ola de cambio tecnológico. Cada país necesitará una política de ciencia, tecnología e innovación que se adecúe a su fase de desarrollo (UNCTAD, 2021). El Ministerio de Defensa y las Fuerzas Armadas deberán adaptarse a esta transformación incluyendo la planificación y gestión de los recursos materiales, el seguimiento de los programas de armamento y la logística durante todo el ciclo de vida completo transformando sus estructuras e infraestructuras hacia el concepto de Defensa 4.0 (de Paula Romero Garat, 2018).

Según la Asociación de la Industria de la Tecnología de la Computación (CompTIA) las diez principales tecnologías emergentes con mayor potencial de impacto a corto plazo que cambiarán nuestro mundo son la Inteligencia Artificial (IA), el 5G e Internet de las Cosas, la computación en la nube, la biometría, la realidad virtual / aumentada, la cadena de bloques, la robótica, el procesamiento natural del lenguaje y la computación cuántica (Dickinson, 2021).

Nuevas tecnologías: Inteligencia Artificial, Aprendizaje Automático y Aprendizaje Profundo, Biometría, Realidad Virtual y Aumentada, Telefonía de Quinta Generación, Macrodatos, Minería de Datos, Procesamiento Natural del Lenguaje y Computación en la Nube, Cadena de Bloques, Computación Cuántica, Robots y Drones Autónomos

El concepto de Inteligencia Artificial (IA) fue acuñado a mediados de la década de 1950 por John McCarthy, docente e investigador informático, quien lo definió en términos generales como la "ciencia e ingeniería para fabricar máquinas inteligentes". Hoy en día se utiliza como término general para un amplio conjunto de técnicas computacionales que permiten que las computadoras y los robots imiten capacidades que generalmente están asociadas con la inteligencia humana, como observar el mundo a través de la visión, procesar el lenguaje natural y el aprendizaje. La IA no es una tecnología definida y singular en la forma en que lo es la tecnología de las armas nucleares; es una tecnología de propósito general que abarca una amplia variedad de aplicaciones habilitadoras que pueden usarse para proporcionar alguna forma de capacidades cognitivas para “reconocer” múltiples tipos de tecnología, incluidos los sistemas de armas (Saalman, Topychkanov, Su, & Peldán Carlsson, 2020, p. 7).

Desde la década de 1950, el campo de la IA ha pasado por varios “ciclos de exageración”, caracterizados por un período de gran éxito seguido inevitablemente por un período de desilusión al

no lograr el nuevo y prometedor enfoque de la IA cumplir con las expectativas iniciales. Estos desenlaces ocasionaron recortes en la financiación de programas de investigación y en la inversión en aplicaciones comerciales. Desde principios de la década de 2010, el campo de la IA ha experimentado un nuevo pico en las expectativas, debido a la conjunción de varios factores: importantes avances en el poder computacional; rápidos avances en el aprendizaje automático, en particular el "aprendizaje profundo"; y el aumento en la disponibilidad de los datos digitales en los que se pueden entrenar los sistemas de aprendizaje automático (Saalman, Topychkanov, Su, & Peldán Carlsson, 2020, p. 8).

Actualmente, el enfoque de la ingeniería de IA que ha despertado un gran interés y ha canalizado una gran inversión es el aprendizaje automático o “machine learning”. Su fortaleza radica en su capacidad para abstraer las relaciones estadísticas de los datos. Es un enfoque extremadamente poderoso para automatizar tareas que requieren un reconocimiento de patrones avanzados. Estas tareas incluyen: percepción de la máquina, clasificación de datos, predicción, detección de anomalías, optimización y generación de datos creativos (Brockmann, Bauer, & Boulanin, 2019, pág. 13).

Boulanin & Verbruggen explicaron que el aprendizaje automático es un enfoque de la ingeniería de IA que, a diferencia de los métodos tradicionales de programación en que un humano codifica la forma en que los sistemas deben ejecutar las tareas, permite construir sistemas que pueden enseñarse por sí mismos. Si bien su estudio se mantuvo en un campo marginal, y con un uso práctico limitado, durante los años 60 y 70, el interés se reavivó a partir de los 80 con la digitalización de muchas industrias y la utilización de grandes conjuntos de datos que inspiraron el desarrollo de nuevas técnicas de aprendizaje automático incluyendo una “red neuronal artificial” basada en el conocimiento del cerebro, la estadística y las matemáticas aplicadas.

Sin embargo, no fue hasta principios de la década de 2010 que se produjo un verdadero avance con la adaptación exitosa al aprendizaje profundo o “deep learning” como técnica de aprendizaje automático basado en redes neuronales artificiales grandes, y apoyado por dos tendencias, la comercialización generalizada de unidades de procesamiento gráfico (GPU) basadas en un chip de computadora de fácil adaptación, y el desarrollo de Internet y las redes sociales que provocó una explosión en los volúmenes de datos digitales para el entrenamiento de algoritmos (Boulanin & Verbruggen, 2017).

La capacidad de las computadoras y los robots para percibir el mundo se ha mejorado drásticamente gracias a los avances en el aprendizaje automático (Gershgorn, 2016). En el campo

de la visión por computadora, la importancia del aprendizaje profundo se midió concretamente mediante una disminución de diez veces en la tasa de error de los sistemas de reconocimiento de imágenes entre 2010 y 2017, del 25% a alrededor del 2% (Gershgorn, 2017). Los sistemas de visión por computadora que funcionan con aprendizaje profundo ahora pueden competir con los humanos, o simplemente superarlos, en el reconocimiento de objetos y rostros (Dodge & Karam, 2017). En el sector de la salud, el aprendizaje profundo está creando nuevas posibilidades para automatizar el análisis de imágenes médicas, como rayos X y resonancia magnética, como, por ejemplo, para diagnosticar los síntomas de ceguera mediante la lectura de escáneres de retina (Regalado, 2018).

Los métodos de aprendizaje automático se pueden utilizar para clasificar cualquier tipo de datos digitales al dar sentido a conjuntos de datos grandes y heterogéneos, desde imágenes hasta registros médicos. Los grandes proveedores de servicios de Internet como Google, Facebook y YouTube utilizan el aprendizaje automático para etiquetar y organizar el contenido, desde texto hasta imágenes y videos (Marr, 2017).

La forma en que el aprendizaje automático encuentra correlaciones en los datos también se puede utilizar para realizar predicciones estadísticas sobre el comportamiento futuro. Empresas de comercio electrónico como Google, Amazon y Netflix utilizan el aprendizaje automático para generar recomendaciones para los clientes rellenando automáticamente los términos de búsqueda o mediante marketing dirigido (Marr, 2018). En el campo de la medicina, se puede utilizar para procesar los registros de los pacientes y descubrir personas con un mayor riesgo de un ataque cardíaco o diabetes (Shu, 2018).

La capacidad del aprendizaje automático para identificar patrones también se puede utilizar para detectar anomalías en grandes conjuntos de datos. En ciberseguridad, el aprendizaje automático podría utilizarse para mejorar la detección de vulnerabilidades de día cero[22] en los sistemas informáticos y de nuevo malware[23] con una firma que aún no se conoce bien (Polyakov, 2018).

El aprendizaje automático se puede utilizar también para optimizar el rendimiento de sistemas o tareas complejos, como mejorar el control de enjambres de robots, que son grupos de

[22] *Vulnerabilidad de día cero*: es un agujero o falla en un programa de software para el cual no hay un parche o una solución, generalmente porque el proveedor de software desconoce la vulnerabilidad (https://www.burrosabio.com/que-es-una-vulnerabilidad-de-dia-cero/).

[23] *Malware* o "software malicioso" es un término amplio que describe cualquier programa o código malicioso (ej: virus, troyano, spyware, ransomware, etc.) diseñado para infiltrarse en un sistema informático con el fin de dañar o robar datos e información.

sistemas idénticos, generalmente pequeños y de bajo costo, que operan como una entidad coherente (Hüttenrauch, 2016, págs. 24-28).

Brockmann, Bauer, & Boulanin observaron que uno de los logros del aprendizaje automático tiene que ver con la creatividad, basados en experimentos conocidos como redes generativas adversarias (GAN), que llevaron al desarrollo de sistemas de inteligencia artificial capaces de crear imágenes, sonidos o historias escritas originales y ultrarrealistas, con implicaciones tanto positivas como negativas, como ayudar a un sistema de aprendizaje automático a generar nuevos datos para capacitarse a sí mismo; o, por otro lado, creando falsificaciones digitales con fines de guerra de información o delictivas (Brockmann, Bauer, & Boulanin, 2019, pág. 14).

Destacaron entre las limitaciones del aprendizaje automático, primero, la dependencia de grandes volúmenes de datos y de calidad para un entrenamiento efectivo. Segundo, la fragilidad y confiabilidad de los sistemas de aprendizaje automático basado en una programación acotada a un entorno operativo previsto, carente de sentido común básico que puede ser engañado fácilmente. Tercero, su inmadurez tecnológica desde una perspectiva de seguridad debido a que los sistemas que dependen de redes neuronales profundas trabajan como cajas negras cuyo funcionamiento interno está oculto o resulta difícil de entender para los humanos siendo potencialmente impredecibles (Brockmann, Bauer, & Boulanin, 2019, págs. 14-15).

Los avances recientes en IA han sido impulsados por el sector civil. Las empresas con experiencia en tecnologías de la información y las comunicaciones (TIC), como Apple, Intel y Microsoft, y los gigantes de Internet, como Google, Amazon, Baidu y Facebook, están liderando la innovación. Tienen grandes recursos financieros a su disposición, lo que les permite contratar a los investigadores e ingenieros de inteligencia artificial más talentosos y adquirir empresas emergentes innovadoras. También tienen acceso a conjuntos de datos gigantes que les permiten entrenar potentes algoritmos de aprendizaje automático. Muchas de estas empresas tienen su sede en EE. UU. o China. Sin embargo, también hay empresas innovadoras en otros países, y se llevan a cabo importantes actividades de I + D en todo el mundo, incluidos los países en desarrollo. La IA es una tecnología con una barrera de entrada baja, ya que no requiere necesariamente grandes recursos financieros o infraestructura. Un estudiante de IA podría desarrollar un algoritmo revolucionario desde su habitación. La comunidad de IA también está abierta con respecto a la difusión de hallazgos. La información para diseñar herramientas de inteligencia artificial, como los sistemas de reconocimiento facial, está ampliamente disponible en línea. Solo dos factores limitan a un actor, ya sea estatal o no estatal, de hacer avances en IA: acceso a expertos en IA y acceso a datos. Los países que lideran en IA son aquellos que tienen universidades, instituciones de investigación y empresas

que pueden formar y retener ingenieros de IA competentes y tienen un gran volumen de datos de alta calidad sobre los que se pueden entrenar sistemas (Brockmann, Bauer, & Boulanin, 2019, pág. 15).

"Biometría es un término técnico para referirse a los rasgos físicos o de comportamiento de los humanos" (OneSpan, 2023). Involucra medidas y cálculos corporales relacionados con las características humanas. Las características distintivas y mensurables que se utilizan para etiquetar y describir a las personas se denominan identificadores biométricos. Se clasifican en fisiológicos, relacionados con la forma del cuerpo (huellas dactilares, venas de la palma, reconocimiento facial, ADN, impresión de la palma, geometría de la mano, reconocimiento del iris, retina y olor / aroma) y de comportamiento, relacionados con el patrón de comportamiento de una persona (ritmo de mecanografía, marcha, pulsación de teclas, firma, perfil de comportamiento y voz) (OneSpan, 2023).

El panorama tecnológico actual ha generado que las personas se cambien a servicios a los que se puede acceder a través de Internet en sus dispositivos personales, como teléfonos inteligentes y computadoras, requiriendo que el usuario autentique su identidad cada vez que inicie sesión en un servicio o cambie a otros servicios. Incluso para proteger sus propios dispositivos, los usuarios utilizan algún tipo de método de autenticación. Los factores de autenticación pueden basarse en el conocimiento (PIN, contraseñas, etc.), posesión (tokens, tarjetas de identificación, etc.) o herencia (huella digital, patrón de iris, etc.). La introducción de contraseñas complicadas o tokens que apenas pueden recordar ralentiza todo el proceso de autenticación y desaprueba la experiencia del usuario. La biometría elimina todas esas deficiencias y proporciona una experiencia de autenticación que no toma más de un segundo en la que los usuarios solo tienen que escanear su identificador biométrico. Un toque en el escáner de huellas dactilares o simplemente mirar el escáner de iris es todo el esfuerzo de autenticación requerido por el usuario y pueden tomar la decisión de otorgar o denegar el acceso al instante (Thakkar, 2021).

La autenticación biométrica es un concepto en seguridad de datos en informática como una forma de identificación y control de acceso, pero también se utiliza para identificar individuos en grupos que están bajo vigilancia.

La biometría conductual es un nuevo enfoque de la ciberseguridad que utiliza algoritmos de aprendizaje automático para analizar el comportamiento del usuario. Esta tecnología puede detectar patrones en la forma en que los usuarios interactúan con los dispositivos, como la velocidad de escritura, el movimiento del mouse y la navegación. Al analizar estos patrones, la biometría

conductual puede identificar amenazas potenciales, como los piratas informáticos que han obtenido acceso a la cuenta de un usuario (EC-Council University, 2023).

La Realidad Virtual (RV) y la Realidad Aumentada (RA) son herramientas muy potentes que pueden ayudarnos a experimentar la realidad de una manera que puede cambiar dramáticamente nuestra percepción del mundo. Aunque son dos tecnologías parecidas, difieren en términos de la "presencia" del usuario. Mientras en la RV el usuario se transpone a un mundo virtual y se desconecta con el mundo que le rodea, la RA sólo altera la realidad actual para el usuario y le ayuda a añadir elementos digitales en el mundo real para proporcionar más claridad a su realidad existente sin alterar su presencia de ninguna manera (Aselcom, 2020).

> Las realidades aumentadas y virtuales aprovechan algunos de los mismos tipos de tecnología y existen para servir al usuario con una experiencia mejorada o enriquecida. La realidad virtual generalmente se entrega al usuario a través de un controlador montado en la cabeza o de mano. Este equipo conecta a las personas con la RV y les permite controlar y navegar sus acciones en un entorno destinado a simular el mundo real (TICNegocios, 2023).

La RV se utiliza principalmente para crear una realidad imaginaria, desarrollar proyectos virtualmente para poder verlos antes de que existan físicamente y mejorar la capacitación en entornos de la vida real mediante la creación de una simulación de la realidad donde las personas pueden practicar de antemano. Constituye una herramienta clave para la generación de gemelos digitales[24]. Por su parte, la RA superpone componentes virtuales como imágenes digitales, gráficos o sensaciones como una nueva capa de interacción con el mundo real. Esta tecnología mantiene el mundo real en el centro, pero lo mejora con otros detalles digitales, superponiendo estratos de percepción y complementando su realidad o entorno (TICNegocios, 2023).

La RV y la RA no siempre operan de forma independiente, y de hecho a menudo se combinan para generar una experiencia aún más inmersiva. Existe una tercera opción, que es la que plantean los nuevos dispositivos de Realidad Mixta (RM), permitiendo crear mundos 100% virtuales en los que también es posible interactuar con elementos digitales. No solo se trata de "estar" en el mundo digital, sino también de poder manipularlo (IAT, 2021).

La telefonía móvil ha sido una auténtica revolución, no solo como medio de comunicación, sino como herramienta para otras utilidades que afectan a todas las capas de nuestra sociedad a través de diferentes tipos de dispositivos electrónicos como teléfonos inteligentes, tabletas y sus aplicaciones. La telefonía de quinta generación (5G) es una nueva generación de la red móvil cuyos estándares han evolucionado, destacándose entre sus capacidades la alta velocidad, menor latencia y

[24] *Gemelo digital (o digital twin)* es una representación digital de un objeto, proceso o servicio físico. Estas réplicas virtuales son utilizadas para hacer simulaciones antes de que se creen e implementen en la realidad, con el fin de recopilar datos para predecir cómo funcionarán y permitir ahorrar tiempo y dinero (Herranz, 2021).

alta concentración de dispositivos. Al brindar mayor ancho de banda para bajar y subir contenidos y una menor latencia o tiempo de respuesta, permite desarrollar con mayor eficiencia el llamado IoT o internet de las cosas (Arpón & Berás, 2020).

La tecnología 5G es 20 veces más rápida que su predecesora la 4G LTE, ofrece una conexión más estable por tener baja interferencia e incrementa significativamente el número de dispositivos conectados en forma simultánea a una antena (más de un millón). Asimismo, su implementación requiere una inversión en infraestructura básica mucho más costosa (entre 30 y 50% superior) ya que se deben instalar más antenas por unidad de superficie. Además, consume entre dos y tres veces más energía y su costo de mantenimiento también es superior (Fusaro, 2021).

Según Huawei[25], se espera que para 2025 haya conectados hasta 100.000 millones de dispositivos (Romero Garat, 2018). Esto debería encender una alerta desde el punto de vista de la ciberseguridad y la ciberdefensa. Las redes de comunicaciones actuales enfrentan ataques cibernéticos diarios que emplean puertas traseras para capturar información o desactivar capacidades. En el futuro, la red 5G estará conectada a miles de millones en lugar de millones de personas y cosas, esto incluirá el acceso a la infraestructura vital y la información de una nación. En la red 5G, habrá más equipos y puntos de entrada que serán difíciles de monitorear debido al volumen masivo de datos y al aumento dramático de nodos.

Los Macrodatos, Datos Masivos, Inteligencia de Datos o "Big Data" es un concepto que hace referencia a "aquellos conjuntos de datos cuyo tamaño, velocidad de crecimiento y variabilidad hacen que sean difíciles de analizar por medio de tecnologías convencionales" (IAT, 2021). Cuando la cantidad de información superó la capacidad de almacenamiento y las herramientas tradicionales de análisis para gestionar y procesar estos datos no fue suficiente surgió la necesidad de contar con tecnologías analíticas capaces de trabajar con grandes volúmenes de información en el menor tiempo posible.

El término Big Data como se lo conoce hoy se utilizó por primera vez a finales de los 1989 por Erik Larson coincidiendo con la creación de internet, abriéndose los primeros caminos para la generación masiva de datos, de donde deriva la aparición de los primeros sistemas de gestión y almacenamiento de información en 1992 (master-bigdata, 2023).

De acuerdo al sitio IAT, los Macro Datos poseen cinco características (5 V's): volumen, variedad, velocidad, veracidad y valor; y su funcionamiento se basa en tres etapas: la recolección e

[25] *Huawei Technologies Co*: empresa tecnológica multinacional china, fundada en 1987 por Ren Zhengfei, proveedor líder global de soluciones de Tecnologías de la Información y Comunicación (TIC).

integración de información, la gestión interna respecto al almacenamiento de datos masivos y el posterior procesamiento o análisis de patrones, para lo cual se suelen utilizar algoritmos avanzados o IA basada en el aprendizaje automático o aprendizaje profundo, permitiendo crear modelos de datos aplicables al mundo real. Se obtienen de las personas que los generan, de transacciones de información, de mercadotecnia en línea, de las comunicaciones máquina a máquina (M2M) o de datos biométricos; y entre las metodologías de análisis de datos utilizados se encuentran la asociación, la minería de datos, la agrupación y el análisis de textos (IAT, 2021).

La asociación permite establecer, en base relaciones entre diferentes variables, patrones de causalidad para predecir el comportamiento de otras variables. La minería de datos o "data mining", mediante la combinación de métodos estadísticos, IA y almacenamiento en bases de datos, busca patrones en grandes volúmenes de datos para predecir comportamientos. La agrupación de datos o "clustering" es una variante de la minería de datos que busca similitudes en grandes volúmenes de información para dividirlos en grupos más pequeños y así crear una estructura previa de los datos en función de las cualidades que los definen (IAT, 2021).

El análisis de texto o "text analytics" permite extraer datos valiosos de la información en formato de texto utilizados por una herramienta de IA denominada "language processing" o procesamiento del lenguaje natural, que también se usa para el lenguaje oral y que aporta soluciones efectivas al momento de comprender el lenguaje humano y su complejidad (IAT, 2021).

Otra de las herramientas que ha favorecido el análisis de Macrodatos, es el servicio de computación en la nube o "cloud computing". Este servicio tecnológico permite acceso remoto a softwares, almacenamiento de archivos y procesamiento de datos por Internet, sin instalar aplicaciones localmente en computadoras. Proporciona mayor flexibilidad en relación a los propios datos e informaciones, a los que se pueden acceder desde cualquier lugar y en cualquier momento mediante una conexión a internet, y ofrece tanto a individuos como a organizaciones de cualquier tamaño la capacidad de un pool de recursos de computación con buen mantenimiento, seguro, de fácil acceso y bajo demanda, como servidores, almacenamiento de datos y solución de aplicaciones. De esta manera constituye una alternativa a la ejecución en una computadora personal o servidor local, ofreciendo mayor capacidad de almacenamiento, acceso desde cualquier dispositivo con internet y menor gasto en infraestructura y equipos (Salesforce, 2021).

La computación en la nube utiliza una capa de red para conectar los dispositivos de punto periférico de los usuarios, como computadoras, smartphones y accesorios portátiles, a recursos

centralizados en el data center y permite liberarse de problemas relacionados con el mantenimiento de infraestructura de servidores y profesionales de TI (Salesforce, 2021).

El servicio de computación en la nube ha abierto la puerta a una multiplicidad de soluciones y aplicaciones para muchos sectores a través de internet. Las aplicaciones basadas en la nube o software como servicio (SaaS) se ejecutan en sistemas distantes "en la nube", pertenecientes y administrados por otros, que están conectados a los sistemas de usuario a través de un navegador web. La plataforma como servicio (PaaS) ofrece un entorno basado en la nube con todos los requisitos para dar soporte al ciclo de vida de creación y puesta en marcha de aplicaciones web, sin coste y complejidad de comprar y gestionar el hardware, software, aprovisionamiento y alojamiento necesario. La infraestructura como servicio (IaaS) proporciona a las empresas recursos informáticos, incluyendo servidores, redes, almacenamiento y espacio en centro de datos con pago en función del uso (IBM, 2021).

El servicio de computación en la nube debería llamar a la reflexión sobre la privacidad y resguardo de los datos sensibles que si se pierden o develan pueden afectar o dañar a la organización y la consecución de sus objetivos. Desde la perspectiva militar, podría implicar contar con un servicio propio, con servidores propios, bajo control y dominio propios.

Otro tipo de tecnología que permite gestionar un registro encriptado descentralizado de todo tipo de transacciones generando confianza entre las partes es el de cadena de bloques o “blockchain”. Se trata de un registro fiable y difícil de hackear de las transacciones y propiedad, llamado también “libro mayor”. Consiste en una base de datos con información almacenada en bloques, idénticos y sincronizados entre sí, los cuales se pueden copiar y replicar en ordenadores individuales.

Se basa en lo que se denomina tecnología de registro distribuido, en donde todos los miembros de la red P2P[26] que componen estos registros pueden ver la misma información en bloques individuales (SAP, 2021). Una transacción que se graba en un ordenador o nodo es visible para cada uno de los ordenadores en la red digital. Todos pueden ver los mismos datos. Es más, pueden rechazar o verificar lo que ven. La información se comunica a todos los otros bloques de la cadena (SAP, 2021). Esto hace que esta tecnología sea muy difícil de hackear ya que ningún ordenador controla los datos, y modificarlos en un bloque significaría que toda la cadena debería hacerlo también (SAP, 2021).

[26] *P2P*: Las tecnologías “peer to peer” (P2P) hacen referencia a un tipo de arquitectura para la comunicación entre aplicaciones que permite a individuos comunicarse y compartir información con otros individuos sin necesidad de un servidor central que facilite la comunicación (Panda, 2021).

> Los registros de cadena de bloques pueden incorporar una amplia gama de documentos, como ser préstamos, títulos inmobiliarios, manifiestos de logística y casi cualquier cosa de valor. La información de Macrodatos puede ser compartida en un entorno de verificación múltiple ideal para compartir información segura y en tiempo real (SAP, 2021).

La tecnología de cadena de bloques permite mejorar la transparencia y la responsabilidad en toda la cadena de suministro. Blockchain como servicio (BaaS) basado en la nube reduce los costos y aumenta la seguridad y la eficiencia a la vez, sin utilizar recursos internos (SAP, 2021).

La computación cuántica es una vertiente de la computación que hace uso de fenómenos de la mecánica cuántica tales como átomos, superposición, amplitudes de probabilidad o entrelazamiento cuántico (Velez, 2020). Su desarrollo data a partir de los años setenta y las cualidades cuánticas del entrelazamiento y la superposición permiten el manejo y procesamiento de grandes cantidades de información de forma mucho más eficiente que los computadores clásicos. Los problemas encontrados, además de una base física y matemática compleja y abstracta, han sido la falta de investigación y desarrollo de software para los sistemas informáticos cuánticos y la duda en que pueda resolver aquellos problemas que la computación clásica no puede, concepto apodado por Google como "supremacía cuántica" (Preskill, 2012). Hasta ahora no se ha demostrado esta supremacía cuántica.

Las computadoras cuánticas pueden realizar cálculos y procesar información masiva rápidamente, tareas que mediante otro método demandarían tiempos extremos difíciles de mensurar. El primer ordenador cuántico fue desarrollado por IBM en el 2000 y en la actualidad estos dispositivos comienzan a estar disponibles para el uso y desarrollo de software para ingenieros y desarrolladores, existiendo una oferta interesante de simuladores y librerías cuánticas para el diseño, ejecución y análisis de circuitos y algoritmos cuánticos (Kleinman Ruiz, 2019).

Actualmente existe una dependencia vital en el uso de las redes que vincula todo tipo de sistemas los cuales son segurizados[27] mediante encriptación basada en las tecnologías de computadores que resultan difíciles de vulnerar. La computación cuántica posee el potencial de romper la mayoría de los actuales algoritmos de cifrado, encriptar en forma totalmente segura y constituye una tecnología emergente con infinidad de aplicaciones. Sus avances coexisten con las llamadas tecnologías híbridas[28], desarrolladas en paralelo con los algoritmos cuánticos, dispositivos de redes y formas de almacenamiento y la forma de transmisión no convencional de la información

[27] *Segurizados*: Elementos que se encuentran protegidos de ser interferidos por un sistema específico de red (vmware, 2023).

[28] *Tecnologías híbridas*: Tecnologías que surgen de emplear conjuntamente dos tecnologías pre-existentes complementarias con un único fin y con el objeto de beneficiarse de sus ventajas respectivas y paliar las posibles desventajas de cada una de ellas por separado (https://www.madrimasd.org/notiweb/analisis/tecnologias-hibridas-un-cambio-paradigma-cientifico-tecnologico).

tipo fotónica[29]. El desarrollo de computadores cuánticos podría ser el disparador de diferentes desarrollos tecnológicos de uso dual[30] para nuestro país (Bertoldi, 2020).

Finalmente, de la mano de la IA y el 5G, se proyecta el desarrollo de robots y drones autónomos en infinidad de campos y sectores, tanto comerciales como de seguridad y defensa. Esta situación, sobre todo en el campo militar, plantea un dilema ético y legal a nivel internacional respecto de la autonomía de las máquinas versus el poder de veto del factor humano.

Cada vez más, los "cobots" o robots colaborativos están transformando prácticamente cualquier sector de la actividad humana y su implementación no deja de crecer, proyectándose para el año 2025 que el mercado alcance el 175% de su nivel actual. Los drones, vehículos aéreos no tripulados y dirigidos remotamente, están sirviendo de catalizadores de innovación en numerosos campos científicos e industriales, ofreciendo nuevos servicios y extendiendo sus posibilidades de operación a sectores productivos tan dispares como agricultura, construcción y minería, movilidad, seguridad y salvamento, paquetería, energía, telecomunicaciones o sector inmobiliario. Hoy se puede observar su utilización para realizar inspecciones, fumigar campos de cultivo o trazar mapas de territorios de forma semiautónoma (SECPHO, 2021).

El empleo individual o en conjunto de las herramientas tecnológicas mencionadas anteriormente, que implica el uso de hardware, software, una red de datos interconectada, una fuente de energía y, por ahora, personal capacitado para operar, configurar, programar y/o supervisar las acciones, expone al mismo tiempo una vulnerabilidad en común por el simple hecho de utilizar el ciberespacio: el riesgo de ser hackeadas o sufrir un ciberataque a través de la red.

Las ciberarmas, apoyadas en la capacidad de control remoto a través de internet, que permiten a un atacante reaccionar en tiempo real y cambiar sus intenciones a medida que avanza, y la capacidad de ocultarse dentro del sistema durante largos períodos de tiempo, a pesar de ser digitales, pueden tener impacto directo en la seguridad humana afectando las infraestructuras críticas de un Estado (Kandiko, 2018).

Utilización militar de las nuevas tecnologías a través del ciberespacio y tendencias

[29] *Transmisión fotónica*: Consiste en el uso de la luz para transmitir datos en lugar de la electricidad. La fotónica de silicio se utiliza en los centros de datos para conectar sistemas que se encuentran separados a grandes distancias mediante transceptores ópticos en cada sistema, los cuales convierten las señales eléctricas en señales ópticas que viajan por los cables de fibra óptica (https://hardzone.es/reportajes/que-es/fotonica/).

[30] *Tecnologías de uso dual*: Son aquellas tecnologías que encuentran aplicaciones tanto en el ámbito de la Defensa y de la Seguridad como en el sector civil.

La Industria de Defensa (Ochre Media) observó como las TIC introdujeron una gran variedad de transformaciones en la industria de la defensa en términos de avance en las armas inteligentes y en la conducción de las operaciones dentro del campo de batalla apoyado en redes centralizadas, superioridad aérea y espacial, vigilancia de combate en tiempo real y multiplicadores de fuerza basados en software (Defense Industries, 2023).

El desarrollo de armas inteligentes eficientes y de muy alta precisión permitió realizar ataques quirúrgicos sobre objetivos seleccionados reduciendo significativamente los daños colaterales. Los avances realizados en IA aplicada a la industria de la defensa han impulsado la producción de robots para reemplazar a los seres humanos en el campo de batalla. El enfoque de gestión del campo de batalla centrado en la red utilizando las ventajas de las TIC le permite a un comandante militar controlar su ejército, observar la posición de las fuerzas militares, sus bajas, el nivel de suministro de municiones y decidir el mejor modo de acción en función de información actualizada. Asimismo, la utilización de dispositivos electrónicos inalámbricos centrados en la red facilita la vigilancia y ayudan a mejorar la comunicación entre tropas, identificar y clasificar las fuerzas armadas amigas y fuerzas enemigas hostiles en el terreno enviando información al centro de comando en tiempo real.

El mayor avance de las TIC para la industria de la defensa lo identificó en el desarrollo de dispositivos, componentes electrónicos y la producción de equipos militares de muy alta gama para el mantenimiento de la superioridad aérea y espacial, como aviones interceptores, vehículos aéreos no tripulados y satélites para el monitoreo continuo de objetivos militares.

La introducción de las TIC en la industria de la defensa provocó un cambio de enfoque en los multiplicadores de fuerza pasando de los basados en hardware a los basados en software. La mayoría de las empresas de la industria de la defensa poseen departamentos separados especializados para el desarrollo de software militar aplicado a muchos equipos de hardware como sistemas de gestión del campo de batalla, radares de largo alcance, sistemas de guía activa de misiles y sistemas de posicionamiento global. Su contribución en el desarrollo de software es muy alta y la mejor opción para aquellas empresas que quieran incursionar en la industria de la defensa global por el alcance que tienen las TIC (Defense Industries, 2023).

Los sectores de Defensa e Inteligencia estadounidenses identificaron como tecnologías emergentes con efecto disruptivo futuro a la inteligencia artificial, los sistemas letales de armas autónomas, las armas hipersónicas, las armas de energía dirigida, la biotecnología, y la tecnología cuántica (Sayler, 2022).

En relación a los efectos de las tecnologías en la disuasión estratégica en el siglo XXI, la Corporación RAND concluyó que tecnologías emergentes, especialmente en los ámbitos de la agresión y manipulación de la información, la automatización, los sistemas hipersónicos y los sistemas no tripulados, tienen implicaciones significativas tanto para la efectividad como para la estabilidad de la disuasión y que la transición emergente hacia nuevas formas de hacer la guerra, potenciada por estas mismas tecnologías emergentes, plantea riesgos más generales para las políticas de disuasión que cualquier tecnología por sí sola. Las capacidades cibernéticas, las tecnologías de manipulación de la información, los sistemas no tripulados, las herramientas biológicas e incluso los sistemas de soporte de decisiones (DSS) impulsados por inteligencia artificial (IA) podrían fortalecer y aumentar la frecuencia de las acciones bélicas en la zona gris (RAND, 2022).

Con relación a la "Inteligencia Artificial y el futuro de la Defensa", un estudio del Centro de Estudios Estratégicos de La Haya sostiene que la aplicación de la IA para fines militares no se limita únicamente a mejorar las funciones "cinéticas" o de "poder duro" en un contexto táctico, sino también aplicaciones de apoyo, logísticas y estratégicas que brindan a las fuerzas una ventaja cualitativa, información y poder de permanencia, citando como casos de uso concretos los siguientes:

1º) Operaciones cibernéticas automáticas. Explotación de la capacidad de la IA a través del ciberespacio para examinar grandes cantidades de datos y captar señales que permitan fortalecer la seguridad utilizando algoritmos de aprendizaje automático para defenderse de los "bots" de amenazas persistentes avanzadas o identificar "exploits" de seguridad del día cero y rastrearlos a medida que se propagan por la comunidad de hackers e investigadores (De Spiegeleire, Maas, & Sweijs, 2017, págs. 87-88).

2º) Selección algorítmica de objetivos. Desarrollo de sistemas de reconocimiento automático de objetivos rápidos y precisos que faciliten a pilotos o UAV a encontrar y comprometerse con objetivos en tiempo real, y que puedan funcionar con los sistemas de radar existentes, para proporcionar capacidades de focalización de largo alcance o para vigilancia táctica aerotransportada. En entornos de combate complejos, a nivel del teatro, la integración de sistemas de aprendizaje automático para procesar información diversa puede permitir tomar decisiones dentro del ciclo de selección de objetivos más rápidas, más efectivas y más precisas (De Spiegeleire, Maas, & Sweijs, 2017, págs. 88-89).

3º) Transferencia de misión. A corto plazo, la IA puede ofrecer a la unidad entrante durante su despliegue y rotación la oportunidad de contar con toda la información generada por la unidad saliente (incluidos los informes posteriores a la acción y de inteligencia, los materiales informativos, etc.), proporcionando una base de conocimientos mejorada que facilite la continuidad y mejore la seguridad operativa del proceso (De Spiegeleire, Maas, & Sweijs, 2017, págs. 89-90).

4º) Conciencia situacional y comprensión. Los sistemas de IA pueden aumentar en gran medida la seguridad y la eficacia de las fuerzas que operan en el campo de batalla, en entornos extranjeros o culturas desconocidas, mediante sistemas de traducción mejorados, para reducir errores de comunicación o percepción; y sistemas de reconocimiento facial y emocional como módulos de vigilancia de mirada persistente, para evaluar una situación, identificar una amenaza y determinar una intención hostil o pacífica (De Spiegeleire, Maas, & Sweijs, 2017, págs. 90-91).

5º) Planificación automatizada y asignación de personal. Los sistemas de aprendizaje automático a partir de datos de pruebas de capacidad de soldados, y su desempeño grupal o individual, podrían formular modelos elaborados, sobre la base de los cuales, se podría alinear el talento humano con los requisitos de la misión y optimizar la composición de equipos para misiones específicas, según la experiencia, personalidad y/o el rendimiento pasado (De Spiegeleire, Maas, & Sweijs, 2017, págs. 91-92).

6º) Análisis de sistemas objetivo / Análisis de audiencia objetivo. IA aplicada al análisis de sistemas y audiencia objetivo mediante algoritmos de aprendizaje automático para el análisis de datos clasificados y de código abierto como métodos relacionados con las actividades de inteligencia de alerta e inteligencia estratégica que se utilizan para desarrollar una comprensión profunda de las áreas potenciales de operaciones (De Spiegeleire, Maas, & Sweijs, 2017, págs. 92-93).

7º) Lecciones aprendidas: operativas y no operativas. IA aplicada a sistemas inteligentes que permitan encontrar lecciones aprendidas y aplicarlas contribuyendo al proceso de mejora continua, y sistemas de tutoría inteligente, para el desarrollo de programas de enseñanza de manera rentable adaptables a las necesidades de aprendizaje de cada individuo (De Spiegeleire, Maas, & Sweijs, 2017, pág. 93).

8º) Análisis de opciones para el desarrollo de capacidades. Utilización de la IA para mejorar la rigurosidad del análisis y emplear análisis de compensación para acelerar el proceso de desarrollo de capacidades (De Spiegeleire, Maas, & Sweijs, 2017, págs. 95-94).

9º) Análisis de registros médicos electrónicos y optimización de Medevac. Empleo de un sistema de razonamiento clínico que mediante técnicas de aprendizaje automático, identifica y clasifica automáticamente los problemas de salud más importantes por los que un paciente debe ser atendido, y que, en un contexto táctico de combate, podría ayudar en la evacuación médica del personal herido de áreas inseguras combinando información sobre la gravedad de las lesiones, rutas de exfiltración disponibles, lugares de aterrizaje y condiciones climáticas, pudiendo determinar el medio óptimo de evacuación y aumentando la eficiencia y seguridad de las evacuaciones médicas (De Spiegeleire, Maas, & Sweijs, 2017, pág. 94).

10º) Clasificación de documentos e intercambio de información encriptada de inteligencia. IA aplicada a sistemas entrenados de aprendizaje profundo que permitan la encriptación y el intercambio de datos o información altamente clasificados de inteligencia (De Spiegeleire, Maas, & Sweijs, 2017, págs. 94-95).

11º) Prevención de conflictos (P4): predictiva, preventiva, personalizada y participativa. Utilización combinada de big data, capacidades computacionales y algorítmicas de IA orientada al conocimiento más profundo sobre los impulsores del conflicto e incidir sobre ellos (De Spiegeleire, Maas, & Sweijs, 2017, págs. 95-97).

12º) Potenciación de la resiliencia social. IA aplicada, en el ámbito del conflicto, a prevenirlo y detenerlo, y en el ámbito de la resiliencia, mediante el empleo de la capacidad para rastrear y comprender la dinámica que conduce a una resiliencia social fortalecida o debilitada basada en una combinación de big data, capacidades computacionales y algorítmicas de inteligencia artificial cada vez más poderosas es probable que aumente exponencialmente (De Spiegeleire, Maas, & Sweijs, 2017, págs. 97-98).

La aplicación militar de IA incluye, pero no se limitan a inteligencia, vigilancia y reconocimiento; logística; operaciones cibernéticas; comando y control; y vehículos autónomos y semiautónomos. Estas tecnologías están destinadas en parte a aumentar o reemplazar a los operadores humanos, liberándolos para realizar un trabajo más complejo y cognitivamente exigente. Además, permitirían reaccionar significativamente más rápido que los sistemas que dependen de la entrada del operador, hacer frente a un aumento exponencial en la cantidad de datos disponibles para el análisis y habilitar nuevos conceptos de operaciones, como enjambre (comportamiento cooperativo en el que los vehículos no tripulados se coordinan de forma autónoma para lograr una tarea) que podría conferir una ventaja en la guerra al abrumar a los sistemas defensivos del adversario. Al mismo tiempo, la IA plantea una serie de desafíos como sistemas sujetos a sesgos

algorítmicos como resultado de sus datos imprecisos o modelos de entrenamiento, y el uso de la IA para engañar la IA del adversario (Sayler, 2022).

La realidad virtual en el ámbito militar puede utilizarse para el entrenamiento militar en diferentes escenarios sin costos adicionales. Los simulacros de guerra pueden ser estimulados para que los soldados puedan entender cómo es realmente toda la acción. Su característica flexible permite ser adaptado para todo tipo de divisiones. La RV puede utilizarse también para impartir formación sobre seguridad, resolución de conflictos y manejo de crisis. La realidad aumentada, por su parte, hace más rápido, fácil y eficiente la fabricación permitiendo también diagnosticar visualmente los problemas de planta y reducir el tiempo de inactividad; y facilita el sistema logístico optimizando los procesos de localización, escaneado y registro de productos (Aselcom, 2020). El Ejército de los EEUU se encuentra probando un prototipo de visor de realidad aumentada, el IVAS versión 1.2 de Microsoft, que permite aumentar la conciencia situacional del combatiente en el terreno permitiéndole ver a través de cortinas de humo, en la oscuridad y alrededor de esquinas (Redacción, 2023).

Los sistemas de armas autónomos letales (LAWS) son una clase de sistemas de armas capaces de identificar un objetivo de forma independiente y emplear un sistema de armas a bordo para atacar y destruir el objetivo sin control humano manual. LAWS requiere algoritmos informáticos y conjuntos de sensores para clasificar un objeto como hostil, tomar una decisión de enfrentamiento y guiar un arma hacia el objetivo. Esta capacidad permitiría que el sistema funcione en entornos con comunicaciones degradadas o denegadas donde los sistemas tradicionales tal vez no puedan funcionar (Sayler, 2022). La utilización de LAWS o drones de ataque evita poner en riesgo a los propios soldados mediante un gran despliegue militar, evita ofrecer a los habitantes incentivos para unirse a grupos insurgentes, y las operaciones con drones son infinitamente más económicas que todo lo anterior (Barro, 2021).

La tecnología cuántica podría tener implicaciones significativas para el futuro de las tecnologías de encriptación y sigilo. Las comunicaciones cuánticas podrían permitir a los desarrollar comunicaciones seguras que no podría ser interceptada ni descifrada, descifrar información del adversario, mejorar la detección de submarinos, y proporcionar opciones alternativas de posicionamiento, navegación y temporización, permitiendo continuar operando a pleno rendimiento en entornos con GPS degradado o sin GPS (Sayler, 2022).

El Sistema Avanzado de Gestión de Batalla (ABMS) es el último esfuerzo de la Fuerza Aérea de los EEUU para crear un sistema de comando y control (C2) de próxima generación.

ABMS propone el uso de entornos en la nube y nuevos métodos de comunicación para permitir que los sistemas de la Fuerza Aérea y la Fuerza Espacial compartan datos sin problemas utilizando inteligencia artificial para permitir una toma de decisiones más rápida. La Fuerza Aérea describe ABMS como su esfuerzo por crear una Internet de las cosas, lo que permitiría que los sensores y los sistemas C2 se desagreguen entre sí (al contrario de cómo la Fuerza Aérea ha realizado tradicionalmente C2). Este programa es la contribución de la Fuerza Aérea al esfuerzo conjunto de comando y control de todos los dominios (JADC2) del DOD centrado en modernizar los procesos de toma de decisiones del DOD para las operaciones de combate (Hoehn, 2022).

Al mismo tiempo, la USAF se encuentra desarrollando el Programa Dominio Aéreo de Próxima Generación (NGAD) que tiene por objetivo reemplazar al F-22 Raptor con un caza avanzado de sexta generación que pueda lograr superioridad aérea mientras opera junto con drones y otros aviones de combate. NGAD incluye una combinación de aeronaves tripuladas y no tripuladas, con otros sistemas y sensores (Hoehn, 2022).

El segundo capítulo ha permitido identificar las nuevas tecnologías relacionadas con el ciberespacio, cómo funcionan, qué aplicación tienen, como se pueden interrelacionar o complementar, que uso militar tienen o se les puede dar y que impacto futuro pueden llegar a tener de acuerdo a su evolución en los futuros conflictos. El próximo capítulo abordará cuestiones dentro del marco legal donde transcurren las operaciones militares cibernéticas, implicancias al momento de constituir alianzas, conceptos doctrinarios y lecciones sobre la guerra de Ucrania.

CAPÍTULO III: OPERACIONES MILITARES CIBERNÉTICAS Y MARCO LEGAL

"El valor de la ciencia está en la previsión: los nuevos desafíos exigen repensar las formas y métodos de llevar a cabo las operaciones de combate" (MilitaryReview, 2016).

General Valery Gerasimov[31]

El ciberespacio constituye una nueva arena de interacción, cooperación y conflicto de la política global, y está plenamente aceptado como un ámbito de las operaciones militares, pero sería un error considerarlo como un ámbito aislado. Desde principios de los tiempos los ejércitos han basado sus operaciones en la capacidad de integración de elementos muy distintos. Lo digital impregna hoy la mayoría de las operaciones militares (Martinez Nuñez, 2020).

A través del ciberespacio pueden realizarse múltiples operaciones como: engaño, disuasión, interferencia de sistemas de comando y control, utilización de drones, confundir sistemas de información militar y/o civil, anular servidores para que no puedan emplearse determinadas computadoras y redes, causar eventos o fenómenos naturales que obliguen al oponente a distraer tropas, confundir sistemas logísticos gobernados por computadoras, desencriptar códigos, interferir el tráfico aéreo, los sistemas de distribución eléctrica o de salud, alterar sistemas bancarios, difundir propaganda o conducir operaciones de acción psicológica y generar percepciones erróneas en la mente del oponente (Trama G. , 2017).

La tecnología ha permitido desarrollar y emplear a través del ciberespacio herramientas cada vez más sofisticadas para realizar espionaje cibernético (operaciones de explotación) y sabotaje en línea (operaciones cibernéticas ofensivas) sin necesidad de exponer fuentes humanas o desplegar fuerzas militares (Kandiko, 2018).

La redundancia y réplica son estrategias de resiliencia que pueden disuadir a los presuntos agresores al hacer fútiles los ataques (Nye, 2011) Las respuestas de represalia por medio del ciberespacio u otros medios también pueden mejorar la disuasión (Kugler, 2009). Actualmente la defensiva está en desventaja, pero la ofensiva está libre de complicaciones en el ciberespacio.

Soberanía, legislación internacional y operaciones militares en el ciberespacio

[31] Citado Por Robert Coalson, James Madison College - Michigan State University , *General Valery Gerasimov*, Jefe de Estado Mayor General de las FF.AA. de la Federación Rusa desde el 9 de noviembre de 2012.

El ciberespacio es un bien común de la humanidad. Ahí la soberanía tiene mucho más que ver con el grado de conocimiento y con la autonomía tecnológica y de infraestructura, que tenga cada país, aquélla que le permita garantizar a sus ciudadanos un acceso seguro, libre de amenazas y que contribuya a su innovación y progreso. El ciberespacio, como "bien de interés público global", requiere de normas que sean aprobadas con el mayor consenso. La seguridad en el ciberespacio no se limita a un simple aspecto técnico, sobre él descansan importantes pilares de la economía y la seguridad de una nación. Además, no es un problema sólo del Estado ya que un gran número de infraestructuras críticas son controladas por las empresas privadas y esto provoca que la seguridad informática sea una de sus máximas preocupaciones debido a que son depositarias de un gran número de aspectos relacionados con el bienestar de los ciudadanos (Reguera, 2015).

Como resulta ser la Organización de Aviación Civil Internacional (OACI) para el dominio aéreo, o la Organización Marítima Internacional (OMI) para el dominio marítimo, existe una Agencia de las Naciones Unidas especializada para las TICs denominada Unión Internacional de Telecomunicaciones (UIT) con competencia en el ciberespacio. Este organismo a nivel mundial promueve las comunicaciones, la normalización, el desarrollo y la innovación en materia de telecomunicaciones, obteniendo acuerdos respecto de las tecnologías, los servicios y la atribución de recursos globales tales como el espectro de radiofrecuencias y las posiciones orbitales de los satélites, para crear un sistema permanente de comunicación global robusto, fiable y en continua evolución (UIT, 2023).

Otras organizaciones internacionales que abordan cuestiones como la seguridad, la gobernanza y la cooperación en el ciberespacio son el Foro de las Naciones Unidas para la Gobernanza de Internet (IGF), el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG), el Grupo de Trabajo de Composición Abierta de las Naciones Unidas (GTCA), el Centro para el Ciberespacio Estratégico + Estudios Internacionales (CSCIS) y la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Desde 2014, bajo el liderazgo de Xi Jinping, China ha promovido activamente la "soberanía de Internet" como un medio para remodelar el discurso y las prácticas de la gobernanza cibernética global (Zeng & Stevens, 2017). Su enfoque sobre la soberanía cibernética se extiende a la infraestructura cibernética, las actividades en línea, las personas y la información dentro de China.

La soberanía en el ciberespacio es un tema complejo por tratarse de un dominio virtual, sin fronteras físicas, donde no es posible aplicar directamente los principios tradicionales de soberanía

territorial, generando un debate sobre quién tiene control y jurisdicción sobre activos, datos y actividades digitales específicos. Conceptualizar la soberanía dentro del ciberespacio requiere considerar aspectos importantes como la jurisdicción nacional, el territorio cibernético, normas, tratados internacionales y gobernanza global, incluidos actores no estatales, y disuasión en el ciberespacio, lo que le permitirá desarrollar capacidades cibernéticas como parte de su estrategia de defensa nacional para disuadir a los adversarios potenciales de realizar operaciones cibernéticas maliciosas contra ellos.

La idea de soberanía en el ciberespacio puede no alinearse precisamente con la soberanía territorial tradicional. Como Internet es una plataforma política, militar, económica, cultural y social nacional, es de esperar que los Estados no permitan que Internet se desordene sin gestión, poniendo en peligro sus propios intereses sin vigilancia. La evolución del ciberespacio asociado a las nuevas tecnologías requiere del consenso entre los Estados para abordar una forma de control y gobernanza del dominio digital y sus problemas asociados.

Con pocas excepciones, como la Convención de Budapest sobre el Delito Cibernético y la Convención de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales, el derecho internacional no tiene reglas a medida para regular el ciberespacio. La mayoría de los Estados y varias organizaciones internacionales, incluida la Primera Comisión de Desarme y Seguridad Internacional de la Asamblea General de las Naciones Unidas, el G20, la Unión Europea, la ASEAN y la OEA, han afirmado que el derecho internacional existente se aplica a las tecnologías de la información y la comunicación por parte de los Estados (Hollis, 2021).

La OTAN no sólo ha hecho del ciberespacio un dominio operacional del mismo nivel que los tradicionales de tierra, mar y aire, o el nuevo del espacio, sino que ha asumido que un ataque cibernético podría llegar incluso a superar el umbral que llevaría a la invocación del Artículo 5 del Tratado del Atlántico Norte, con todo lo que eso conlleva.

En relación con la soberanía en el ciberespacio, el Colegio de Abogados de los Estados Unidos (ABA) identificó varios acontecimientos significativos en la última década:

1) El 23 de mayo de 2018, en uno de los discursos más significativos sobre el derecho internacional en el ciberespacio, el fiscal general británico Jeremy Wright, declaró públicamente la posición de su país sobre la cuestión de la soberanía, no reconociendo una norma específica de soberanía en el derecho internacional aplicable en el ciberespacio.

2) En 2019, el Ministerio de los Ejércitos francés publicó una declaración detallada sobre las opiniones de Francia sobre el derecho internacional aplicable a las acciones estatales en

el ciberespacio reconociendo el principio de soberanía. Francia ejerce su soberanía sobre los sistemas de información situados en su territorio. La gravedad de una violación de la soberanía se evaluará caso por caso de acuerdo con los acuerdos franceses de gobernanza de la ciberdefensa para determinar posibles respuestas de conformidad con el derecho internacional.

3) En 2020, Paul Ney, asesor general del Departamento de Defensa estadounidense, en un discurso en la conferencia legal anual del Comando Cibernético de los Estados Unidos reiteró la importancia de mirar la práctica de los Estados y la opinio juris[32] para determinar cómo está evolucionando el derecho internacional con respecto a las operaciones cibernéticas, y se refirió a la soberanía como un principio, en lugar de una regla. Ese mismo año, Roy Schöndorf, fiscal general Adjunto de Derecho Internacional de Israel, sin articular una posición, proporcionó algunas consideraciones para evaluar por qué la soberanía es importante, como la necesidad de un Estado de proteger la infraestructura ubicada en su territorio.

4) En 2021, la Asamblea General de la ONU publicó en un Informe del Compendio del Grupo de Expertos Gubernamentales que no existe una práctica estatal amplia ni una opinio juris suficiente para generar una nueva norma internacional consuetudinaria que permita la violación de la soberanía estatal por medio de las TIC; que las violaciones de la soberanía estatal por parte de otro Estado por medio de las TIC constituyen un hecho internacionalmente ilícito y conllevan la responsabilidad internacional del Estado que las viola; y que las interceptaciones de telecomunicaciones se considerarían un hecho internacionalmente ilícito porque violan la soberanía estatal. Del mismo modo, las operaciones cibernéticas contra sistemas de información ubicados en el territorio de otro Estado o que produzcan efectos extraterritoriales también pueden constituir una violación de la soberanía.

5) En 2022, Canadá adoptó la posición de que la soberanía territorial es una norma de derecho internacional pero que no requiere consentimiento para toda actividad cibernética que tenga efectos, incluida cierta pérdida de funcionalidad, en otro Estado. En mayo de ese mismo año, Suella Braverman, fiscal general británica, reafirmó la posición del Reino Unido de que el derecho internacional no reconoce una regla de soberanía, y propuso que las actividades cibernéticas que son perjudiciales para un Estado podrían ser coercitivas constituyendo una intervención prohibida y pudiendo empujar los límites de cómo un Estado podría entender el principio de no intervención.

[32] *Opinio juris*: es una forma abreviada de la frase latina opinio juris sive necessitatis, que significa "una opinión de ley o necesidad". En el derecho internacional consuetudinario, la opinio juris es el segundo elemento necesario para establecer una costumbre jurídicamente vinculante. Opinio juris denota una obligación subjetiva, un sentido en nombre de un Estado de que está obligado a la ley en cuestión. La Corte Internacional de Justicia refleja esta norma en el artículo 38(1)(b) del Estatuto de la CIJ al reflejar que la costumbre que ha de aplicarse debe ser "aceptada como ley".
Al igual que con el derecho internacional consuetudinario, la opinio juris es una noción no resuelta y debatida en el derecho internacional.

ABA supone que a medida que más Estados desarrollen y empleen capacidades cibernéticas, se desarrolle tanto la práctica de los Estados como la opinio juris con respecto al derecho internacional y las actividades cibernéticas, abordando la cuestión de la soberanía como regla o principio del derecho internacional (Cherry & Pascucci, 2023).

Kevin Heller sostiene que los Estados actualmente respaldan tres posiciones diferentes con respecto a la ilicitud internacional de las operaciones cibernéticas que penetran los sistemas informáticos ubicados en el territorio de otro estado pero que no alcanzan el nivel de uso de la fuerza o intervención prohibida. La primera posición, defendida por el Reino Unido y EEUU, es que las operaciones cibernéticas de baja intensidad nunca violan la soberanía porque la soberanía funciona en el ciberespacio como un principio, no como una regla. Esta idea es simplemente irreconciliable con la naturaleza del derecho internacional, con la práctica estatal y la opinio juris de lo contrario. Las dos siguientes ven la soberanía como una regla que se aplica en el ciberespacio. La segunda posición, la puramente soberanista, es que todas las operaciones cibernéticas de baja intensidad violan la soberanía porque la soberanía prohíbe cualquier penetración no consensuada de un sistema informático ubicado en el territorio de otro estado. La tercera posición, la soberanista relativa, es que solo algunas operaciones cibernéticas de baja intensidad violan la soberanía del estado objetivo: aquellas que (1) causan daños físicos o una pérdida equivalente de la funcionalidad de la infraestructura cibernética, o (2) interfieren o usurpan funciones inherentemente gubernamentales. En la práctica, la diferencia entre las dos últimas posiciones se refiere al ciberespionaje, que la soberanía pura prohíbe categóricamente y la soberanía relativa generalmente permite (Heller, 2021).

Ariel Levite observó que algunas de las potencias cibernéticas más importantes parecen haber llegado a la conclusión de que las acciones cibernéticas ofensivas en tiempos de paz, incluso aquellas que van mucho más allá de la recopilación de inteligencia, no constituyen automáticamente ataques armados, y mucho menos actos de guerra. Hasta ahora, ni el carácter de las operaciones cibernéticas, ni el contexto altamente conflictivo en el que ocurren, ni sus objetivos y efectos (incluso cuando incapacitan instalaciones tan sensibles como la infraestructura crítica) han demostrado ser suficientes para lograr que la comunidad internacional les otorgue el estatus de un "ataque armado", y mucho menos un "acto de guerra".

Levite sostuvo que incluso los propios protagonistas parecen estar de acuerdo, como se puede ver en los intercambios cibernéticos ofensivos cada vez mayores entre Irán e Israel que ninguna de las partes consideró que entraran en estas categorías. De hecho, las acciones y la diplomacia de aquellos que emplean medios cibernéticos ofensivos, así como de aquellos en el

extremo receptor, ahora han creado un patrón claro y consistente y una serie de precedentes que sugieren que los protagonistas cibernéticos desean dejarse una libertad considerable para interpretar la acción cibernética ofensiva de sus adversarios caso por caso. No menos importante, el comportamiento de estas partes revela que muchos prefieren conservar una amplia libertad para emprender tales acciones por sí mismos.

A pesar de esta similitud, es probable que las partes difieran un poco sobre dónde y cómo trazan la línea. En consecuencia, no se puede excluir la posibilidad de que, si el ciberespacio se utilizara como medio principal para un ataque estratégico que causara una pérdida significativa de vidas, podría considerarse un ataque armado. La OTAN, ha evolucionado en su enfoque para reflejar ese pensamiento. Si esta postura puede resultar atractiva desde una perspectiva política, el nivel de criterios que deben cumplirse para que la acción cibernética ofensiva se considere seriamente bélica es bastante alto, dejando a juicio posterior del hecho determinar si se cumplieron (y cuándo), restando así parte de su valor normativo y disuasorio (Levite, 2023).

En 2021, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE), lanzó un proyecto a cinco años del Manual de Tallin 3.0, para la revisión de los capítulos existentes y la exploración de nuevos temas de importancia para los Estados como la cuestión de la soberanía como regla o principio del derecho, la protección de los datos en virtud del derecho internacional humanitario; si un ataque a los sistemas financieros constituye una intervención prohibida o un uso de la fuerza; en qué medida una campaña de información o desinformación alcanza el nivel de una intervención prohibida; y si las contramedidas colectivas son lícitas en el contexto del ciberespacio. Sin embargo, esta nueva versión del manual seguirá siendo un trabajo académico no jurídicamente vinculante destinado a proporcionar una reafirmación objetiva del derecho internacional aplicado en el contexto cibernético (CCDCOE, 2023).

Martinez Nuñez observó que, pese a haber alcanzado niveles de libertad muy altos en internet, existe mucha desigualdad en el acceso y la seguridad; y que los valores y las reglas del mundo que hemos creado todavía no han permeado la suficiente razón por la cual el mundo cibernético necesita de una gobernanza más eficaz. Al mismo tiempo sostuvo que el conflicto de intereses en la escena global se ve traducido en un desprecio al orden internacional basado en reglas como una consecuencia sociológica del internet, y que el enorme potencial destructivo que existe a través de este, que puede permanecer oculto y latente, obliga a un cambio muy profundo de paradigma de cómo se debe tratar a un competidor estratégico. Actualmente la disuasión y diálogo no son suficientes y es necesario como una tercera vía la corresponsabilidad, involucrando a las

primeras potencias a que se sientan dueñas del futuro de todos ante la amenaza de que este potencial latente destructivo pueda ser utilizado (Martinez Nuñez, 2020).

La carencia de una percepción global común sobre el quinto dominio deriva en diferentes visiones y perspectivas en el análisis y estudio del ciberespacio y, en particular, de las operaciones militares a través del mismo, desarrollándose doctrinas, definiciones y taxonomías con diferentes enfoques y en algunos casos de difícil compatibilidad.

La República Argentina no se ha expedido de manera explícita y oficial acerca de la soberanía en el ciberespacio y su posición respecto a la ilicitud internacional de las operaciones cibernéticas. Sin embargo, reconoce la importancia del ciberespacio como un dominio crítico que requiere una adecuada gobernanza, medidas de seguridad y cooperación internacional. Argentina ha desarrollado una Estrategia Nacional de Ciberseguridad[33] para abordar los desafíos que plantean las ciberamenazas y proteger su infraestructura digital enfocada en mejorar las capacidades de seguridad cibernética del país, promover la resiliencia cibernética y salvaguardar los intereses nacionales en el ciberespacio. Al mismo tiempo, el gobierno argentino trabaja en la elaboración de leyes y reglamentos para proteger la privacidad de los ciudadanos, combatir el ciberdelito y definir las funciones y responsabilidades de las diferentes partes interesadas en el ámbito del ciberespacio. Argentina también reconoce la naturaleza global del ciberespacio y la importancia de la cooperación internacional para abordar las ciberamenazas transfronterizas, participando en iniciativas, congresos y foros regionales e internacionales relacionados con la ciberseguridad y la gobernanza del ciberespacio; y prioriza la protección de su infraestructura crítica frente a amenazas cibernéticas mientras las fuerzas armadas y de seguridad argentinas han estado desarrollando capacidades de defensa cibernéticas para proteger los intereses y activos nacionales de posibles ataques cibernéticos. Basados en la postura estratégica defensiva, cooperativa y autónoma, y su adhesión al derecho internacional, podemos inferir que la República Argentina ve la soberanía como una regla que se aplica en el ciberespacio, y por lo tanto requiere de capacidades para controlarlo y protegerlo.

Ante la falta de consenso global y la ausencia de un marco regulatorio común, resulta de vital importancia que la comunidad internacional aborde los desafíos que plantea el ciberespacio y trabaje para desarrollar políticas y normas de ciberseguridad efectivas para mejorar la estabilidad y la seguridad en este ámbito.

[33] IF-2023-81810563-APN-SSTI#JGM (Anexo I de la RESOL-2023-44-APN-SIP#JGM).

Legislación nacional y el empleo del Instrumento Militar en el ciberespacio

La ciberseguridad y ciberdefensa de un país está vinculada a la concepción de defensa y seguridad que tiene. En la República Argentina, seguridad se refiere a la seguridad pública interna y defensa a la seguridad pública externa asignando la responsabilidad de la seguridad pública interna a las Fuerzas de Seguridad y Policiales; y la responsabilidad de la defensa, entendida como seguridad pública externa a las Fuerzas Armadas. Esta distinción incide en la preparación integral y multidimensional de toda la nación para la guerra, sus Fuerzas Armadas y los métodos para conducirla afectando la doctrina militar para la obtención de poder de combate en términos de capacidades militares (Moresi, Motta, Trama, Saldanha Walker, & Amaya, 2022, págs. 42-43).

El Instrumento Militar será empleado para conjurar y repeler toda "agresión de origen militar estatal externo", entendiendo el uso de Fuerzas Armadas pertenecientes a otro/s Estado/s contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas (Decreto PEN Nº 727, 2006).

El primer problema que se plantea respecto al empleo del IM en el ciberespacio es el de la atribución ante un ciberataque (individuo o Estado) y la definición de reglas de empañamiento claras al momento de responder. La dificultad para identificar al agresor puede limitar el accionar del IM al momento de defenderse y garantizar su autopreservación, o para restablecer el orden dentro de su área de responsabilidad.

La Ley de Seguridad Interior Nº 24.059 contempla que las Fuerzas Armadas puedan actuar en operaciones de apoyo logístico por disposición del Ministro de Defensa; en operaciones destinadas a su auto preservación y al restablecimiento del orden dentro de la jurisdicción militar, en caso de atentado en tiempo de paz a dicha jurisdicción; o, por disposición del Presidente de la Nación, y previa declaración del estado de sitio, para el restablecimiento de la normal situación de seguridad interior en aquellos casos excepcionales en situaciones de extrema gravedad, sin influir en la doctrina, organización, equipamiento y capacitación de las Fuerzas Armadas (Argentina G. , 1991). Por esta razón y dadas las características que plantea el ciberespacio como nuevo dominio de conflicto, sería conveniente la aprobación legal de normas específicas para el empleo del IM en el ciberespacio.

Por otra parte, la Ley de Defensa Nacional Nº 23.554 establece que "las cuestiones relativas a la política interna del país no podrán constituir en ningún caso hipótesis de trabajo de organismos

de inteligencia militares" (Argentina G. , 1988), y la Ley de Inteligencia Nacional Nº 25.520 indica que la Dirección Nacional de Inteligencia Estratégica Militar está a cargo de la producción de inteligencia estratégica militar, referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la defensa nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar; y los organismos de inteligencia de las Fuerzas Armadas producen la inteligencia estratégica operacional y la inteligencia táctica necesarias para el planeamiento y conducción de operaciones militares y de la inteligencia técnica específica (Argentina G. , 2001).

Nuevamente el empleo del IM en el ciberespacio plantea un problema de libertad de acción para las actividades de inteligencia militar ya que constituye un ámbito de información ilimitado y la mayor fuente abierta para la obtención de datos, pero a su vez, su accionar en ese mismo ámbito es restringido y limitado por el marco jurídico nacional.

El Decreto PEN Nº 1691/2006 Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas resalta la importancia de considerar los factores de diseño y la determinación de capacidades. La priorización de las capacidades del IM debe guardar coherencia con la concepción, el posicionamiento, la actitud estratégica de la Nación, y la misión asignada al IM. Entre los criterios para la priorización se encuentra promover la integración y coordinación, incluidas las capacidades relacionadas al concreto desarrollo de las operaciones militares de combate, y asegurar los niveles necesarios de compatibilidad, interoperabilidad y complementariedad militar efectiva con los países de la subregión.

Al mismo tiempo, el diseño de fuerzas por capacidades del IM implica lograr la "aptitud de ejecutar en forma autónoma la completa gama de operaciones que demandan todas las formas genéricas de agresión que se manifiestan en los conflictos convencionales de origen externo generados por actores estatales" (Argentina G. , 2006).

El diseño de capacidades de la defensa ciberespacial para lograr la interoperabilidad e integración militar efectiva, primero entre fuerzas, y luego entre países aliados, requiere tecnologías y doctrinas de empleo compatibles, un detalle no menor, cuando se debe asesorar al decisor de la política exterior.

Entender a las operaciones ofensivas militares dentro del ciberespacio como contrarias a la postura estratégica defensiva nacional y asociar a la ciberdefensa sólo con las operaciones defensivas en el ciberespacio son conceptos erróneos. Las operaciones ofensivas militares dentro

del ciberespacio representan un tipo de operación dentro del abanico de posibilidades del IM que le permitirá incrementar su libertad de maniobra mediante la proyección de poder y obtener la ventaja durante el combate. Las operaciones ofensivas en el ciberespacio permiten afectar el Comando y Control del enemigo, demorar su toma de decisiones, y por ende su tiempo de reacción, o afectar alguna infraestructura critica del enemigo que proporcione una ventaja estratégica. Al mismo tiempo, las Operaciones de Información a través del ciberespacio o ciberinfluencia, permiten distorsionar la información de enemigo, engañarlo e inducirlo a equivocarse. Privar al IM de este tipo de operaciones, además de desaprovechar las ventajas que ofrece este dominio, sería como quitarle al guerrero su espada y dejarlo sólo con el escudo para defenderse. El IM necesita de las operaciones ofensivas y de información en el ciberespacio para poder explotarlo en su favor en apoyo a las operaciones cinéticas en los otros dominios.

Scott Graber sostiene que, en los dominios cinéticos, a nivel estratégico, la ofensiva y la defensa se relacionan con la captura y protección del territorio respectivamente; mientras que "atacar" y "proteger" se refieren al nivel táctico, y que muchas tácticas de ataque y protección se pueden utilizar con fines estratégicos ofensivos y defensivos. En cambio, en el ciberespacio, las tácticas defensivas son mucho más limitadas porque ni las defensas cibernéticas activas, ni las pasivas, dañan al adversario, como si lo hacen muchas defensas cinéticas. Una protección pasiva, como un cortafuego, simplemente intenta bloquear la amenaza. Una defensa cibernética activa proporciona capacidad en tiempo real para descubrir, detectar, analizar y mitigar amenazas y vulnerabilidades, pero no daña al atacante. Se debe sumar el problema de la atribución, que limita aún más la posibilidad de disuasión en la defensa cibernética y reduce la posibilidad de contraataques como parte de una estrategia defensiva de ataque (Graber, 2021).

En una estrategia defensiva las protecciones pasivas son un aspecto importante, pero el dominio cibernético está inherentemente orientado hacia tácticas de ataque. Por esta razón, las tácticas de ataque deben incluirse en una estrategia defensiva, o la estrategia se pone en grave desventaja. Las tácticas de ataque agresivas en redes externas pueden interrumpir a los adversarios de maneras que las medidas de protección pasiva no lo hacen. Las tácticas de ataque proactivas u operaciones ofensivas son necesarias para hacerlo, incluso en una estrategia defensiva. La distinción entre una defensa activa y un ataque ofensivo puede diferir según el ojo del espectador. El dominio cibernético ofrece un área ambigua o zona gris para operar, con leyes aún en constante cambio, que está entre el espionaje y la guerra, pero que también podría considerarse contraespionaje como alternativa al uso de la fuerza militar, y a la que una estrategia de defensa de

un Estado podría adaptarse para explotar las ventajas ofensivas inherentes y características únicas del mismo (Graber, 2021).

Si bien el marco normativo vigente en la República Argentina define las cuestiones referidas a la defensa, la seguridad, y la inteligencia, el ciberespacio, por su particularidad, requiere de una normativa al más alto nivel actualizada aplicable a las operaciones en el ciberespacio, que especifique además la asignación de roles y áreas de responsabilidad a fin de optimizar el empleo de recursos y capacidades y hacer más eficiente la defensa en todos los dominios, incluido el ciberespacio.

Alianzas militares de defensa ciberespacial y limitaciones

La cooperación internacional adquiere una relevancia especial en la ciberdefensa debido al carácter ubicuo (ataques desde cualquier parte del mundo a través de redes secuestradas) y anónimo (sin firma reconocida) de los ciberataques, siendo necesaria la participación de otros países para la identificación del origen de la ciberamenaza y para la respuesta eficaz. Esta se puede lograr mediante acuerdos bilaterales con otras fuerzas o a través de alianzas internacionales de defensa colectiva basados en entornos de confianza mutua (JID, 2020, pág. 55).

Tanto la confianza cero[34] como la cooperación internacional son fundamentales para la filosofía de Comando y Control Conjunto de Todos los Dominios o JADC2 que sostiene los EEUU, y que prevé fuerzas y bases de datos interconectadas en tierra, aire, mar, espacio y ciberespacio (Macri, 2022).

La falta de un consenso global en la gobernanza del ciberespacio repercute en visiones diferentes de los Estados en la forma de organizar las estructuras nacionales para defender el ciberespacio, y consecuentemente, estas estructuras organizativas diferentes, que responden a normas y regulaciones nacionales particulares, pueden dificultar la colaboración nacional e internacional tan necesaria en el ámbito de la ciberdefensa, y constituir una limitación al momento de intentar generar alianzas.

[34] *Confianza Cero o Zero Trust*: Es un modelo de seguridad informático que en lugar de asumir que todo lo que hay detrás de un firewall corporativo es seguro, asume la violación y verifica cada solicitud como si se originara en una red abierta, independientemente de dónde se origine la solicitud o a qué recurso acceda, De esta manera, cada solicitud de acceso está completamente autenticada, autorizada y cifrada antes de conceder acceso (Microsoft, 2023).

Por otra parte, la postergación del desarrollo de capacidades de las Fuerzas Armadas de un Estado como el caso de la República Argentina, independientemente de sus razones, puede generar una brecha tecnológica contraria a la requerida para lograr la convergencia, integración e interoperabilidad con los Instrumentos Militares de otros Estados dentro de una Alianza. Esta brecha tecnológica no solo se refiere al desarrollo puntual de capacidades en el ciberespacio, sino también en los otros dominios de guerra donde los medios tecnológicos requieren estar integrados a través del ciberespacio para la nueva forma de combate moderno que este dominio plantea. El problema se agravará aún más, cuando la opción tecnológica elegida por un Estado en línea con su estrategia política exterior sea incompatible con otros aliados de un mismo bloque.

En el presente, pensar en un Instrumento Militar de un Estado desvinculado del ciberespacio es inconcebible, porque el ciberespacio se ha transformado en un dominio de guerra que, independientemente de la postura estratégica que un Estado asuma, es indispensable tanto para el accionar militar conjunto, como para su integración en alianzas o coaliciones con otros países.

Los acuerdos binacionales entre Estados permiten al personal militar y sus medios participar de capacitaciones o ejercicios en otros países. Las academias militares de las grandes potencias como los EEUU son bastante reacias a compartir información respecto a sus capacidades cibernéticas y nuevos conceptos de empleo. La participación en cursos de capacitación y ejercicios en el ámbito ciberespacial requiere de permisos de seguridad concedidos por su Departamento de Defensa, y restringidos a determinados tipo de aliados. Sin embargo, la participación en ejercicios militares multinacionales en otros dominios, independientemente de las capacidades y limitaciones individuales de cada Estado, permiten observar de alguna manera el estado del arte y los avances tecnológicos en la forma del combate moderno, constituyendo una gran oportunidad para recopilar información a partir de la cual cada Estado podría intentar adquirir o desarrollar nuevas capacidades y anticipar su estrategia defensiva en el arte de la guerra.

Lamentablemente, la República Argentina no ha sabido aprovechar todas estas oportunidades. La ausencia de sus Fuerzas Armadas en ejercicios multinacionales como el Resolute Sentinel 2023 o el Ejercicio UNITAS LXIII 2022 por la participación del Reino Unido (zona-militar, 2023), posiblemente respondiendo a razones válidas de la política exterior, son claros ejemplos. También lo es la ausencia de la Fuerza Aérea Argentina, aunque sea como observador, en los ejercicios de entrenamiento de combate aéreo RED FLAG (RFNAFB, 2023), que se llevan a cabo en la base de la USAF en Nellis, sede del Centro de Guerra de los EEUU y la Escuela de Armas de la USAF, y en donde se validan tácticas y doctrinas en el empleo del Poder Aeroespacial.

Por otra parte, el Comando Cibernético de los Estados Unidos (CYBERCOM) organiza anualmente el ejercicio táctico multinacional conocido como CYBER FLAG (USCYBERCOM, 2022), en el que también participa el Reino Unido. Considerando el actual contexto internacional de competencia entre EEUU y China, en el que sus estrategias de Seguridad Nacional y Defensa apuntan a la disuasión integrada y están ávidos por sumar aliados y socios, la República Argentina debería evaluar la conveniencia de un posible acercamiento en función de sus propios intereses y participar en este tipo de ejercicios de cara al futuro, independientemente de la participación del Reino Unido. Los problemas de soberanía que la República Argentina mantiene con el Reino Unido no deberían distanciarnos en la relación con los Estados Unidos, quien continúa liderando el bloque occidental en materia tecnológica y militar.

La gran competencia de poder entre EE. UU. y China puede crear oportunidades para que Argentina se comprometa con múltiples aliados cibernéticos y busque asociaciones beneficiosas, y al mismo tiempo, puede presentar desafíos en términos de equilibrar los intereses económicos, la alineación de políticas y las prioridades regionales de seguridad cibernética. El enfoque de Argentina hacia las alianzas y la cooperación cibernética probablemente dependerá de sus consideraciones estratégicas, intereses económicos y compromiso con las iniciativas regionales de seguridad cibernética.

Conceptos doctrinarios de las operaciones militares cibernéticas

Las disciplinas que se asocian con la ciberdefensa son las ciberoperaciones, las operaciones sobre redes TIC, la ciberseguridad, las operaciones de información, la guerra electrónica, las operaciones psicológicas y la comunicación estratégica, y pueden diferenciarse según el objeto que las motiva. La ciberdefensa incluye como eje central a las ciberoperaciones, pero también todas las capacidades de mando, técnicas, logísticas y administrativas requeridas para la planificación y conducción de las mismas. Las ciberoperaciones se centran en la misión y en el efecto que se pretende alcanzar según los objetivos de la misma. El aprovechamiento del éxito se logra a través de alcanzar una situación de cibersupremacía[35] o cibersuperioridad[36] conocida o desconocida por el adversario (JID, 2020, págs. 41,80).

[35] *Cibersupremacía* se alcanza cuando se tiene control absoluto del ciberespacio de confrontación. Las ciberfuerzas adversarias son incapaces de ejercer ninguna interferencia efectiva sobre el ciberespacio de confrontación. La libertad de acción propia es total mientras que la del adversario es mínima (JID, 2020, pág. 37)

La República Argentina no ha publicado oficialmente una doctrina de ciberdefensa militar, aunque continúa trabajando activamente en el desarrollo de sus capacidades de seguridad cibernética y ha formulado lineamientos, procedimientos y planes internos para manejar las amenazas cibernéticas específicas de su dominio, guiados por estrategias y políticas nacionales de seguridad cibernética más amplias.

La mayoría de los académicos y formuladores de políticas afirman que el ciberespacio favorece la ofensiva y una minoría no está de acuerdo. El equilibrio ofensiva-defensa en el ciberespacio solo puede evaluarse con respecto a habilidades y tecnologías organizativas específicas. Se define en términos diádicos, el valor menos los costos de las operaciones ofensivas y el valor menos los costos de las operaciones defensivas. Los costos de las operaciones cibernéticas están conformados principalmente por las habilidades organizativas necesarias para crear y administrar tecnología de información compleja de manera eficiente. El éxito actual de la ofensiva resulta principalmente de una mala gestión defensiva y los objetivos relativamente más simples de la ofensiva. Puede ser muy costoso ejercer efectos físicos precisos utilizando armas cibernéticas. Un análisis empírico demostró que los ataques cibernéticos de Stuxnet contra las instalaciones nucleares de Irán muy probablemente costaron mucho más a la ofensiva que a la defensa. Además, los beneficios percibidos tanto de la ofensiva como de la defensa fueron ambos probablemente de mayor magnitud que los costos percibidos, por lo que es poco probable que los tomadores de decisiones se hayan centrado en los costos (Slayton, 2017).

Actualmente existe una tendencia en los Estados democráticos a ejecutar operaciones de explotación con miras a desarrollar y poseer capacidades ofensivas de consideración en caso de ser requeridas como una estrategia de ciberseguridad nacional para disuadir a los agresores que intenten realizar ciberataques. Esto manifiesta un cambio desde la lógica de la resiliencia a la lógica de la disuasión producto de la proliferación de ciberataques tanto de origen estatal como no estatal sobre países, instituciones, procesos electorales e intereses vitales. Entre los países que ya disponen de capacidades ofensivas y defensivas adecuadas y doctrina de empleo desarrollada se encuentran EEUU, China, Rusia, Israel, Reino Unido, Irán, Corea del Norte, Australia y Francia (Arteaga, 2019).

"Las ciberoperaciones son acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones" (JID, 2020, pág. 42). La clasificación de las

[36] *Cibersuperioridad* se alcanza cuando se dispone de una posición más favorable sobre el adversario en el ciberespacio de confrontación. La libertad de acción propia es mayor que la del adversario (JID, 2020, pág. 37)

operaciones cibernéticas puede variar o superponerse según los Estados y sus estructuras organizativas. Las terminologías empleadas también pueden variar.

La Junta Interamericana de Defensa distingue seis tipos de ciberoperaciones, de acuerdo a su naturaleza, objetivo y entorno en donde se desarrollan: defensivas pasivas, defensivas activas, de explotación pasivas, de explotación activas, de respuesta y ofensivas. Las ciberoperaciones defensivas pasivas, se ejecutan en las redes propias exclusivamente para la prevención, protección y resiliencia del ciberespacio propio sin tomar acciones específicas contra otros. Las ciberoperaciones defensivas activas son de tipo intrusiva u ofensiva, y también se ejecutan en las redes propias para la búsqueda de vulnerabilidades y riesgos, y la evaluación del estado de seguridad del ciberespacio propio. Las ciberoperaciones de explotación pasivas, son de tipo no intrusivas y se ejecutan en las redes propias o redes públicas abiertas para la obtención de información para la planificación y conducción de ciberoperaciones defensivas, ofensivas u otras operaciones convencionales. Las ciberoperaciones de explotación activas, son de tipo intrusivas en las redes de adversarios o de terceros para obtener información para la planificación y conducción de ciberoperaciones defensivas, ofensivas o convencionales. Las ciberoperaciones de respuesta, son del tipo ofensivas y se ejecutan en las redes de adversarios o de terceros para prevenir, anticipar o reaccionar ante ciberataques a las redes propias. Las ciberoperaciones ofensivas, son ejecutadas en el marco de un conflicto declarado en las redes de adversarios o de terceros para causar un ciberefecto o un efecto físico (JID, 2020, págs. 42-43).

Asimismo, las operaciones en redes se enfocan exclusivamente en los ciberefectos, no considerando los efectos físicos a personas o instalaciones, la ciberseguridad se centra en la protección y recuperación de los sistemas TIC propios, las operaciones de información se centran en conseguir la superioridad de la información y la influencia, incluyendo la protección de la información propia y afectar a la del adversario, la guerra electrónica se enfoca exclusivamente en actividades que utilizan el espectro electromagnético o la energía dirigida para atacar o protegerse través del mismo, las operaciones psicológicas se centran en las personas y sirven de gran apoyo en la conducción de ciberoperaciones, y la comunicación estratégica se centra en la comunicación en este caso a través del ciberespacio (JID, 2020, pág. 41).

De acuerdo a la doctrina militar de la fuerza aérea estadounidense (USAF), las operaciones en el ciberespacio se llevan a cabo a lo largo de la competencia continua para lograr los objetivos asignados y asegurar los intereses nacionales. Estas operaciones se pueden utilizar de forma independiente o integrada con operaciones en otros dominios, para lograr efectos primarios, complementarios o habilitadores. Además, permiten asegurar la confidencialidad, integridad y

disponibilidad de las redes vitales de Comando y Control. El control en el ciberespacio brinda a la fuerza conjunta libertad de acción y reduce la vulnerabilidad a los ataques del enemigo dentro del ciberespacio como a través de otros dominios. Lograr y mantener una ventaja en el ciberespacio es un componente fundamental de la ventaja operativa y estratégica general, especialmente para las operaciones contra adversarios similares. Debido a la complejidad del ciberespacio, la superioridad global no es alcanzable, e incluso la superioridad localizada puede resultar poco práctica. Para garantizar el éxito en las Operaciones Conjuntas de Todos los Dominios (JADO), los comandantes deben esperar operaciones en el ciberespacio impugnadas y dar cuenta de la degradación anticipada de las capacidades.

EEUU clasifica sus operaciones militares en el ciberespacio en tres tipos: Operaciones Ciberespaciales Ofensivas (OCO), misiones destinadas a proyectar poder en y a través del ciberespacio; Operaciones Ciberespaciales Defensivas (DCO), misiones para preservar las capacidades amigables del ciberespacio y proteger datos, redes, dispositivos y otros sistemas designados al derrotar la actividad ciberespacial maliciosa en curso o inminente; y Operaciones de la Red de Información del Departamento de Defensa (DODIN), operaciones para asegurar, configurar, operar, extender, mantener y sustentar el ciberespacio DOD para crear y preservar la confidencialidad, disponibilidad e integridad del DODIN (AFDP 3-12, 2023, pág. 6).

Las OCO son misiones destinadas a proyectar poder en y a través del ciberespacio del enemigo y zona gris a través de acciones realizadas en apoyo al comandante combatiente o de los objetivos nacionales. Pueden orientarse a funciones del ciberespacio enemigo o a crear efectos de primer orden para iniciar efectos de negación en cascada controlados en los dominios físicos para afectar los sistemas de armas, procesos de C2, nodos logísticos y otros objetivos valiosos. Incluyen todas las misiones de operaciones cibernéticas realizadas fuera del ciberespacio amigo con una intención distinta a la de defender el ciberespacio amigo de una amenaza cibernética actual o inminente (AFDP 3-12, 2023, pág. 7).

Las OCO consisten en operaciones de Inteligencia, Vigilancia y Reconocimiento (ISR) en el ciberespacio, para recopilar información de inteligencia, operaciones Preparación Operativa del Entorno en el Ciberespacio (C-OPE), para operaciones militares de seguimiento, Operaciones de efectos como negación, degradación, interrupción o destrucción en el ciberespacio, y acciones de negación en los dominios físicos, pudiendo llevarse a cabo en conjunto con otros componentes o fuerzas de operaciones especiales. Pueden orientarse exclusivamente a las funciones del ciberespacio del adversario o crear efectos en el ciberespacio con manifestaciones en dominios físicos contra los sistemas de armas del adversario, los procesos C2, los nodos logísticos, etc.,

Deben considerarse como una aplicación de fuerza que puede llegar al mismo nivel que el daño físico o la destrucción de los sistemas y equipos del adversario, y requieren una consideración cuidadosa con respecto al alcance de las operaciones, las reglas de enfrentamiento (ROE), las posibles repercusiones y el progreso medible hacia los objetivos del comandante (AFDP 3-12, 2023, pág. 7)

Las misiones DCO se ejecutan para defender el ciberespacio amigo de amenazas inminentes o activas que han eludido, violado o amenazan con violar las medidas de seguridad, lo que las distingue de las operaciones DODIN, que se esfuerzan por proteger el ciberespacio del Departamento de Defensa de toda amenaza en forma anticipada. Las acciones de DCO son conceptualmente similares a las de contrainteligencia y generalmente consisten en DCO de protección, para minimizar el riesgo para las redes, los sistemas y los datos a través de acciones de seguridad en el ciberespacio basadas en amenazas, DCO de investigación, para identifica, iluminar y caracterizar las amenazas que han violado las redes y brindan opciones de respuesta, y DCO de respuesta, dentro o fuera de los sistemas DODIN en un terreno ciberespacial controlado por amigos o adversarios. Cuando una actividad DCO de protección, investigación o respuesta se lleva a cabo en un terreno amigable del ciberespacio, constituye una misión de medidas defensivas internas DCO (DCO-IDM), y cuando una actividad de respuesta DCO se lleva a cabo fuera de la red defendida, en un ciberespacio extranjero y sin el permiso del propietario del sistema afectado, se considera una misión de acción de respuesta DCO (DCO-RA) (AFDP 3-12, 2023, pág. 8).

> Los adversarios rara vez actúan abiertamente cuando realizan actividades de inteligencia u operaciones ofensivas en el ciberespacio. Por esta razón, se debe tener cuidado adicional para evaluar deliberadamente la efectividad operativa de DCO. La falta de evidencia de una violación no significa que la red sea segura. Una evaluación adecuada ayuda a los comandantes a evitar errores que resultan de la mala interpretación de los datos. La evaluación operativa deliberada de la misión y el terreno que se está protegiendo, y las capacidades defensivas del ciberespacio disponibles, proporciona a los comandantes operacionales una descripción precisa de los riesgos del ciberespacio para la misión (AFDP 3-12, 2023, pág. 8).

Las operaciones DODIN son misiones permanentes que involucran operaciones diarias de seguridad y mantenimiento, respuesta a amenazas y apoyo a las fuerzas DCO. Aunque muchas de estas actividades son eventos programados con regularidad, no pueden considerarse de rutina, ya que sus efectos agregados establecen el marco para la mayoría de las misiones. Además de los esfuerzos regulares de seguridad, la respuesta efectiva a las intrusiones u otras actividades maliciosas requieren una acción coordinada con las fuerzas del DCO. Muchas tareas asociadas entre las operaciones DCO y DODIN pueden superponerse o requerir eliminación de conflictos. El apoyo

a las fuerzas de DCO puede incluir garantizar los niveles apropiados de acceso y permisos para completar las misiones defensivas asignadas (AFDP 3-12, 2023, pág. 8).

La información también es un recurso militar fundamental porque puede proporcionar una ventaja operativa. La fuerza conjunta utiliza la información para realizar muchas actividades simultáneas e integradas, y para mejorar la comprensión, la toma de decisiones y la comunicación. Los comandantes utilizan la información para visualizar y comprender el entorno operacional (OE), y dirigir y coordinar acciones. La fuerza conjunta también puede aprovechar la información para afectar las percepciones, actitudes, toma de decisiones y comportamiento de los actores relevantes. (AFDP 3-12, 2023, pág. 2).

Para la USAF, las operaciones en el ciberespacio se consideran una de las seis principales capacidades de guerra de información (IW) presentadas a la fuerza conjunta para realizar y apoyar operaciones en el entorno de información (OIE). Debido a que el ciberespacio se define como totalmente contenido dentro del entorno de la información (IE), las OIE combinan operaciones en el ciberespacio y otras actividades y capacidades de información para crear efectos en apoyo de operaciones conjuntas en todo el entorno operativo. Las operaciones del ciberespacio se pueden realizar de forma independiente o sincronizadas, integradas y desconcertadas con otras capacidades y actividades de información para una OIE más eficaz (AFDP 3-12, 2023, pág. 2).

Ariel Levite observó que el éxito de las operaciones cibernéticas ofensivas demandará prolongadas operaciones preparatorias con mucha anticipación y bastante extensa a lo largo de la Cadena de Muerte Cibernética con el objeto de crear una infraestructura clandestina para penetrar en las redes adversarias, establecer un punto de apoyo secreto, reconocer toda la red y establecer un aparato de comando y control. También será esencial efectuar preparaciones integrales adicionales para convertir este punto de apoyo en un ataque físico a activos digitales valiosos que los neutralizarán o los asumirán y los aprovecharán para realizar ataques digitales de seguimiento. Sin importar el caso, los preparativos deberán desarrollar opciones completas para generar los impactos deseados, ya sea cuando se cumplan ciertos criterios o bajo demanda. En Ucrania, esto implicó que Rusia sondeara y probara repetidamente las capacidades y rutinas de los defensores cibernéticos (Levite, 2023).

Los preparativos avanzados para ataques cibernéticos parecerían crear una poderosa ventaja de primer golpe. El incentivo para lanzar ataques cibernéticos temprano, antes de que comience la confrontación convencional, se basa en dos consideraciones: ayudar a llevar a cabo operaciones convencionales posteriores y hacerlo antes de que los desarrollos operativos disminuyan la

probabilidad de que los ataques cibernéticos planificados logren los efectos deseados (Levite, 2023).

Operaciones cibernéticas y lecciones de la guerra de Ucrania

Levite resaltó los beneficios significativos en la guerra de Ucrania que representaron los desarrollos tecnológicos, junto con las inversiones masivas en herramientas y capacidades de alerta temprana y conciencia situacional, sobre todo en los ámbitos cibernético, de inteligencia artificial y de fusión de datos, para comprender la situación sobre el terreno y anticipar desarrollos inmediatos. Destacó además que a Ucrania y sus aliados occidentales les ha ido mucho mejor que a Rusia en la competencia por la defensa cibernética, la alerta temprana, el conocimiento de la situación del campo de batalla y la información sobre objetivos debido en gran parte a la riqueza y sofisticación de las capacidades técnicas aportadas por los gobiernos de Estados Unidos y el Reino Unido, así como por varias entidades comerciales (incluidas SpaceX, Palantir, Microsoft, Amazon, y Mandiant), algunas subvencionadas por ellos. Todos estos actores acudieron en ayuda de Ucrania con inteligencia, sensores de reconocimiento espacial, telecomunicaciones y otros activos técnicos y capacidades para fusionar información y derivar señales operativas que los ucranianos supieron tejer hábilmente con sus recursos autóctonos. Sin embargo, subrayó la importancia de saber distinguir entre la capacidad de mejorar en gran medida la conciencia situacional a través de la fusión sofisticada de diversos sensores digitales y la capacidad de anticipar el resultado de los encuentros en el campo de batalla y más allá (Levite, 2023, pág. 14).

Observó que, en Ucrania, contario a los preconceptos existentes al rol que cada parte asigna a las operaciones cibernéticas y orienta sus efectos deseados (Rusia cognitivo y Occidente físicos), todas las partes asignaron al ciberespacio un papel disruptivo en lugar de destructivo cuando buscaron efectos físicos. Los efectos de destrucción buscados se asignaban a operaciones cinéticas, aunque en algunos casos precedidas por una interrupción cibernética. Esto genera la incertidumbre de si el ciberespacio seguirá siendo una herramienta principalmente disruptiva en el futuro y si otras naciones involucradas en conflictos también suscribirán el mismo enfoque (Levite, 2023, pág. 22).

El conflicto de Ucrania puso en evidencia la relativa agilidad de la infraestructura digital (telecomunicaciones, computadoras y datos) en comparación con la infraestructura física. Si bien los ataques físicos, electromagnéticos y cibernéticos pueden, interrumpir e incluso destruir activos digitales clave y socavar o disminuir la eficacia de las misiones que sirven, la infraestructura digital

ucraniana (especialmente sus torres celulares y servidores de datos) fueron capaces de absorber misiles rusos en forma masiva, así como ataques cibernéticos, y continuar funcionando, a pesar de algunos contratiempos temporales. Este éxito en parte es atribuible a la experiencia previa de Ucrania con la agresión cibernética rusa, a su sistema de alerta temprana, y a la asistencia extranjera de gobiernos, corporaciones, y expatriados. Además, a las redes de tecnología digital modernas basadas en comunicaciones móviles y satelitales, y una infraestructura de computación en la nube más robustas y resistentes que la infraestructura anterior, que permitió una reconstitución, preservación y reutilización relativamente rápidas de activos y funciones clave (Levite, 2023, pág. 17).

Otra característica del conflicto de Ucrania es la creciente fusión entre el espacio y el ciberespacio y entre la infraestructura digital en tierra y en el espacio. La información digital, las telecomunicaciones, la navegación y los activos de comunicación masiva son vitales para la guerra moderna, y muchos hoy operan en o a través del espacio. En el conflicto de Ucrania permitió detectar signos tempranos de que atacar y defender los activos espaciales no solo está profundamente integrado con la guerra en el aire, el mar y la tierra, sino que también está fuertemente entrelazado con la confrontación digital en otros dominios. El control (o, por el contrario, la interrupción o desactivación) de los activos digitales en el espacio comienza a demostrar ser indispensable para ganar ventaja en el campo de batalla y en el esfuerzo de guerra en general, y las operaciones cibernéticas y electromagnéticas están emergiendo como medios preferidos para proyectar el poder en el espacio para obtener una ventaja en la campaña. El ataque a Viasat, así como los esfuerzos para interferir las comunicaciones por satélite, sugieren que, por ahora, los activos espaciales comerciales, incluso los de propiedad de no combatientes, se consideran un juego justo si brindan servicios a cualquiera de los protagonistas (Levite, 2023, págs. 17-18).

La guerra entre Rusia y Ucrania dejó expuestos algunos conceptos respecto a la utilización de las operaciones en el ciberespacio. Las operaciones cibernéticas pudieron ser integradas a estrategias de guerra híbrida más amplias, utilizando ataques cibernéticos junto a acciones militares tradicionales, guerra de información y manipulación política.

Tanto Rusia como Ucrania dirigieron ataques a las infraestructuras críticas, incluyendo redes de energía, transporte y comunicación con el potencial de causar interrupciones significativas y afectar el bienestar de la población, llamando la atención en los círculos de seguridad internacional y exponiendo el concepto del uso de las infraestructuras críticas como arma, y como un instrumento de guerra hibrida de estados más débiles contra superpotencias (Evans, 2020).

Las operaciones cibernéticas no lograron hasta el momento efectos estratégicos disruptivos o destructivos significativos que reduzcan la capacidad de resistencia del adversario, pero si han demostrado mayor valor en sus funciones de inteligencia, reconocimiento y capacidades psicológicas (Schulze & Kerttunen, 2023, pág. 3). Las actividades cibernéticas rusas se centraron en la recopilación de inteligencia, la destrucción de datos, y ataques de denegación de servicio a infraestructuras críticas (Schulze & Kerttunen, 2023, pág. 7). Al respecto, Libicki ya había apreciado que la ciberguerra no podía desarmar y menos destruir al enemigo ya que las operaciones cibernéticas por si solas no permiten obtener ganancias territoriales y resulta muy dificultoso someter la voluntad del enemigo basado solo en medios digitales (Libicki, 2009, pág. 119). Los ataques rusos orientados a la infraestructura civil para a reducir la voluntad de resistir de los ucranianos, tuvieron un efecto contrario, provocando un fuerte apoyo a su presidente Volodymyr Zelensky. El Internet en Ucrania se convirtió en un campo de batalla, pero demostró ser excepcionalmente resistente (Tomé, Belson, & Berdan, 2023), y la ejecución de operaciones de información le permitió a Ucrania ganar corazones y mentes (Alexander, 2022). Ucrania demostró una gran ciberresiliencia basada en el almacenamiento de datos gubernamentales en la nube (Microsoft, 2023), intercambio de información sobre inteligencia y actividades de búsqueda de amenazas (CYBERCOM, 2023), y una ciberdefensa ágil, proactiva y flexible (Schulze & Kerttunen, 2023, pág. 7).

Ha resultado difícil de coordinar la aplicación conjunta y combinada de las operaciones cibernéticas en apoyo a las operaciones convencionales en el campo de batalla con el objeto de lograr un efecto facilitador/multiplicador de fuerzas. Esto se debe a diferencias en los tiempos de planificación y ritmos operativos, a geografías diferentes de los campos de batalla digitales y convencionales, a interferencias activas de guerra electrónica en el entorno de combate sobre conexiones de comando y control en vivo para la ejecución de malware, y a objetivos conflictivos respecto al efecto deseado entre descubrirse y quemar la capacidad de acceso para actividades de inteligencia a largo plazo, o lograr un efecto cibernético a corto plazo (Schulze & Kerttunen, 2023, págs. 2-3). Un informe de Microsoft observó que los actores estatales rusos de ATP llevaron intrusiones cibernéticas junto con acciones militares cinéticas, pero los diferentes tipos de ataques no funcionaron bien en conjunto (Microsoft, 2022). Bateman lo atribuyó a una mala planificación estratégica, inteligencia insuficiente y una sobrecarga de secretismo y desconfianza (Bateman, Beecroft, & Wilde, 2022).

Rusia invadió Ucrania el 24 de febrero de 2022, pero la preparación del campo de batalla por parte de la inteligencia rusa y las operaciones cibernéticas comenzó mucho antes. El grupo

Nobelium/ATP29[37] fue identificado como un actor activo desde mayo de 2021. Rusia también intentó moldear la percepción pública presentando a Ucrania como atacante mediante operaciones de información en Telegram y Twitter (Bodnar, Schafer, & Soula, 2023). Estas operaciones fueron desacreditadas por fuentes abiertas de inteligencia (Lazaruk & Tuters, 2022) y la comunidad de inteligencia de los EEUU (Crawford, 2022). El día anterior a la invasión, la agencia de inteligencia militar rusa lanzó varios ciberataques destructivos de eliminación de datos contra el gobierno ucraniano y otras organizaciones financieras, de energía y de TI destinados a apoyar los próximos ataques terrestres y aéreos, y el día de la invasión, interrumpió las comunicaciones por satélite Viasat sobre Ucrania y Europa, creando efectos indirectos no deseados al desactivar los módems satelitales de la red de turbinas eólicas alemanas (Waldman, 2022).

Durante los primeros seis meses de guerra, el Equipo de Respuesta a Emergencias Informáticas del Gobierno de Ucrania CERT-UA registró 1.123 ataques cibernéticos (Ucrania, 2022), un valor tres veces mayor al período anterior a la guerra (Sabbagh, 2023); y durante 2022, respondió a 2.194 incidentes cibernéticos, el 25% dirigidos al gobierno, autoridades locales, sectores de defensa y seguridad, energía, servicios financieros, TI y telecomunicaciones y logística (Scroxton, 2023).

El conflicto también demostró lo difícil que resulta lograr efectos físicos con medios cibernéticos, siendo los medios convencionales más rápidos, económicos y precisos (Schulze & Kerttunen, 2023, pág. 6). En abril de 2022, los ucranianos lograron descubrir y desactivar, antes que se iniciara el temporizador programado, el malware Industroyer2[38] diseñado para afectar los sistemas de control industrial dentro de la red de energía eléctrica de Ucrania, un desarrollo que puede demandar años. Sin embargo, para octubre de 2022, al menos el 40% de las instalaciones eléctricas ucranianas habían sido dañadas, y para diciembre, el 50% de la población carecía de suministro eléctrico producto de los bombardeos convencionales (Amnesty, 2022).

En un informe de ciberinteligencia de CSCIS[39] de septiembre de 2023, el Director del Centro de Defensa Cibernética David Swan resaltó que las fuerzas cibernéticas rusas, incluidos hackers aliados y de apoyo, refinaron tanto su objetivo como su metodología, lanzando campañas sobre infraestructuras críticas, infraestructura industrial, organizaciones políticas y de medios, como

[37] *ATP29, Nobelium o Cozy Bear*: grupo de ciberespionaje vinculado al Servicio de Inteligencia Exterior de la Federación Rusa conocido por realizar ciberataques sofisticados y dirigidos contra gobiernos y organizaciones no gubernamentales, empresas, grupos de expertos, militares, proveedores de servicios de TI, tecnología e investigación sanitaria, proveedores de telecomunicaciones y otras organizaciones (sekoia, 2023).

[38] *Industroyer2*: variante del malware Industroyer utilizado en 2016 por el grupo Sandworm APT para cortar el suministro eléctrico en Ucrania, y en este caso, para afectar sus subestaciones eléctricas de alto voltaje (welivesecurity, 2022).

[39] *CSCIS* Centre for Strategic Ciberspace + International Studies (cscis.org).

así también objetivos de oportunidad, tanto ucranianos como de sus aliados. Los indicadores se basaron en la focalización de los ataques y en el uso más selectivo de malware y TTP[40] (Swan, 2023).

El conflicto entre Rusia y Ucrania expuso cómo el ciberespacio constituye un dominio cada vez más disputado en la guerra moderna, y seguramente lo será aún más en el futuro, a medida que la tecnología y las capacidades cibernéticas continúen evolucionando. Entre las lecciones aprendidas Schulze y Kerttunen destacaron que:

1º) Las ciberoperaciones ofensivas plantean como debilidad el tiempo de preparación anticipada requerido, la dependencia de su objetivo y la posibilidad de fallar ante una ciberdefensa ágil y proactiva.

2º) El éxito en el ciberespacio requiere flexibilidad, velocidad, visión de futuro, inteligencia útil sobre amenazas, procesos interministeriales simplificados que minimicen los silos de información, ejercitaciones, capacitación y una planificación bajo un enfoque que incluya al gobierno y la industria.

3º) La línea de acción debería orientarse a alinear mejor las operaciones de red con las de guerra electrónica, las operaciones de información, las operaciones de inteligencia y la destrucción física de nodos clave de comunicación, comando y control, y logística del adversario.

4º) La planificación debe evitar cadenas de ataques demasiado complejas en las que las operaciones convencionales dependan en gran medida de las operaciones cibernéticas (Schulze & Kerttunen, 2023, págs. 7-8).

Por último, el conflicto evidencia la necesidad de contar con normas y acuerdos internacionales sólidos con respecto al comportamiento responsable de los Estados en el ciberespacio y la importancia de las respuestas internacionales coordinadas a las amenazas y ataques cibernéticos, en un entorno percibido como de competencia estratégica donde, según el derecho internacional, las operaciones cibernéticas no se consideran que cumplan con los criterios legales de uso de la fuerza o un ataque armado y por lo tanto no justifican la cláusula de legítima defensa prevista en el artículo 51 de la Carta de la ONU, y habilita su uso por debajo del umbral de la guerra y dentro de la zona gris sin correr riesgos de escalada o represalias armados o violentas (Schulze & Kerttunen, 2023, pág. 3).

El tercer capítulo permitió conceptualizar diferentes enfoques de soberanía en el ciberespacio, analizar el marco jurídico, comprender como impactan en la doctrina de ciberdefensa,

[40] *TTP* Tácticas, Técnicas y Procedimientos

en la concepción de las operaciones ciberespaciales, y en la posibilidad de integrar alianzas. Además, la guerra de Ucrania proporcionó ejemplos prácticos del uso del dominio ciberespacial en un conflicto a gran escala, resaltando importantes detalles y tendencias de la forma de combate moderno. El último capítulo se centrará en las capacidades necesarias para la ciberdefensa, la planificación y organización de la ciberdefensa y ciberseguridad en la República Argentina y el rol de su Instrumento militar de cara al futuro.

CAPÍTULO IV: CAPACIDADES DE DEFENSA CIBERESPACIAL EN LA REPÚBLICA ARGENTINA

"Diseñar una nueva forma de actuar en la guerra requiere nuestro diseño de cómo y por qué pensamos. Hacerlo nos permite innovar formas de considerar lo inimaginable, irrealizable e inexplorado justo fuera de nuestro marco actual".

Ben Zweibelson[41]

"Para provocar una revolución en asuntos militares, normalmente se necesitan dos cosas: un desarrollo objetivo que lo haga posible; y un hombre que tomará ese desarrollo por los cuernos, lo montará y lo dirigirá".

Martin van Creveld [42]

A partir del 2006, la República Argentina reemplazó para el diseño de su Instrumento Militar el modelo de hipótesis de conflicto por el modelo de planeamiento por capacidades conceptualizado en la Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas (Decreto PEN Nº 1691/2006), y adoptado a partir de la DPDN Decreto PEN Nº 1714/2009. El ciberespacio como nuevo ámbito operacional de la defensa quedó incorporado con la posterior DPDN Decreto PEN Nº 2645/2014.

El modelo de planeamiento estratégico militar por capacidades pretende lograr la aptitud necesaria para ejecutar en forma autónoma la gama completa de operaciones que permita enfrentar cualquier tipo de agresión. Al mismo tiempo, consciente de las propias limitaciones y recursos disponibles, intenta apelar a la pauta de capacidad suficiente y el concepto de fuerza activa sustancial[43], adaptándolos a la forma de combate moderno asociada a las nuevas tecnologías.

Se enfoca en el desarrollo y la consolidación de las capacidades de vigilancia, comando, control, comunicaciones, informática e inteligencia, un alto grado de movilidad estratégica y táctica, de sostén logístico, y las relacionadas al concreto desarrollo de las operaciones militares de combate, en coherencia con la concepción, el posicionamiento y la actitud estratégica de la nación del tipo defensiva, cooperativa y autónoma.

[41] Ben Zweibelson,"Beyond the Pale - Designing Military Decision-Making Anew," Air University Press, 2023, p. xxviii.
[42] *Martin van Creveld*, "Napoleon and the Dawn of Operational Warfare", en La evolución del arte operacional: desde Napoleón hasta el presente,ed. John Andreas Olsen y Martin van Creveld (Oxford: Oxford University Press, 2011).
[43] *Fuerza activa sustancial*: "mínima organización que, en forma sistémica, posee todos los atributos que le permiten desarrollar de manera autónoma todas las operaciones inherentes a la potencialidad de que se trate".

Entre los criterios para desarrollar capacidades están asegurar una operatividad razonable y un control efectivo, ajustarse al concepto de diseño polifuncional, priorizando desarrollos nacionales, la generación propia de conocimiento, la dualidad de aplicaciones, y niveles mínimos de interoperabilidad multilateral y regional que permitan avanzar en los procesos de integración.

El Plan Plurianual de Ciencia, Tecnología, Innovación y Producción para la Defensa (2022-2025) incluye entre sus líneas de acción promover y consolidar programas tecnológicos transversales priorizando entre otros la ciberdefensa (Defensa, 2023, pág. 42).

El desarrollo de capacidades del IM de la República Argentina para la defensa del ciberespacio se encuentra asociado a tres retos principales en general que hoy enfrentan los países en desarrollo para acceder a los beneficios de las nuevas tecnologías: pobreza económica, la brecha digital y la escasez de habilidades (UNCTAD, 2021). La falta de inversión en capacidades tecnológicas asociadas al ciberespacio puede acrecentar la brecha digital en desmedro de la integración. En el plano militar y de forma similar, la desinversión en estas capacidades sólo hará más difícil la compatibilidad, interoperabilidad y complementariedad afectando la integración y convergencia de los medios militares entre sí, entre fuerzas conjuntas, y entre aliados y socios.

Para enfrentar estos desafíos la Argentina cuenta con el Fondo Nacional de la Defensa[44] (FONDEF), creado en el año 2020 para financiar el proceso de reequipamiento de las Fuerzas Armadas, y el Instituto de Ciberdefensa de las Fuerzas Armadas[45], creado en 2021 para facilitar la capacitación integral de personal que desempeña funciones en el ámbito de la Ciberdefensa. En cuanto a achicar la brecha digital y darle conectividad a toda la ciudadanía, la Argentina cuenta con sectores que producen tecnología de Redes de Acceso de Radio Abierta (Open RAN) 5G que compiten en el mercado global (Technexus, 2021) y firmó en febrero de 2022 un memorándum de entendimiento con China adhiriéndose a la Nueva Ruta de la Seda que incluye proyectos de cooperación en infraestructura de conectividad en telecomunicaciones (Lopez, 2022). Para Fusaro, la tecnología 5G, IP versión 6 e Internet 2, permitirá a los países y las empresas que lo posean estar a la vanguardia, no pudiéndose competir contra ellos, aunque el internet que tenemos hoy en Argentina no trabaja con estas redes de alta velocidad, baja latencia y alta concentración de

[44] Ley Nº 27.565 (IF-2020-62357072-APN-DSGA#SLYT), sancionada por el Honorable Consejo de la Nación el 16 de Septiembre de 2020, y promulgada por Decreto Nº 782/2020 del Poder Ejecutivo Nacional (P.E.N.) el 30 de Septiembre de 2020.

[45] Creado el 18 de marzo, en el marco de la 10ma Reunión del Consejo de Dirección de la Universidad de la Defensa Nacional (UNDEF), presidida por el Ministro de Defensa, Agustín Rossi; el Jefe del Estado Mayor Conjunto de las FFAA, General de División Juan Martín Paleo; el Jefe del Ejército, General de División Agustín Cejas; el Jefe de la Armada, Vicealmirante Julio Guardia; el Jefe de la Fuerza Aérea, Brigadier Mayor Xavier Isaac; el Comandante Conjunto de Ciberdefensa, General de Brigada Aníbal Intini; y el rector de UNDEF, Jorge Battaglino.

dispositivos, sino trabaja en su mayoría con IP versión 4, y tampoco están dadas las condiciones para su implementación porque a las empresas les resultaría muy difícil recuperar el capital invertido (Fusaro, 2021). Por otra parte, existen al menos ocho casos de emprendimientos argentinos dentro del segmento "spacetech[46]", algunos de ellos vinculados a servicios de conectividad satelital que dan una luz de esperanza (Murua, 2023).

El 07 de septiembre de 2023, el Ministro de Defensa, Jorge Taiana, inauguró una red de fibra óptica exclusiva para el Sistema de Defensa, para brindar "comunicaciones seguras, redundantes, confidenciales y de alta disponibilidad", que se suma a un software de desarrollo nacional para las FFAA, y que forma parte de un proyecto para contar con una red soberana que incluya, con la intervención de la empresa ARSAT, capacidades militares satelitales, y que integre el "Sistema de Ciberdefensa con tecnología auditable, controlable y desarrollada en el país por profesionales egresados de nuestras universidades" (Argentina, 2023). Si bien lo logrado no es suficiente, representa un buen comienzo y señala un camino de avance para el país.

Sin embargo, existen otros desafíos particulares más profundos a nivel nacional, que son de índole legal y político, y que la Argentina también debe enfrentar al momento de optar por el desarrollo de capacidades de su IM para la defensa del ciberespacio. El marco normativo nacional y una conceptualización errónea del término defensa asociado a la postura estratégica determinada por el poder político, y adoptada por el IM pueden limitar el desarrollo de algunas capacidades y poner a la Nación en desventaja a nivel global.

La limitación de jurisdicción para el empleo efectivo del IM demanda un gran esfuerzo de coordinación entre agencias y actores a nivel estatal al momento de aplicar una defensa integral en el ciberespacio. La asignación de las infraestructuras críticas a defenderse como área de responsabilidad es un factor esencial a considerar reglas de empeñamiento claras que habiliten el uso del IM en el ciberespacio.

En el contexto mundial de competencia continua donde actores occidentales como los EEUU, la OTAN, y particularmente el Reino Unido, reafirman el valor de la geopolítica y las visiones realistas, mantener una postura netamente defensiva, cooperativa y autónoma, sostenida en una visión constructivista y de alguna manera sesgada, que no permita el desarrollo de capacidades ofensivas, pone en mayor riesgo no solo la soberanía, sino también los recursos naturales y estratégicos, y raya entre la ingenuidad y la irresponsabilidad. La diplomacia como factor de poder es siempre un medio válido para defender o luchar por los intereses nacionales,

[46] Spacetech o tecnología espacial, se refiere al uso de la tecnología para la exploración e investigación espacial que incluye todo, desde vehículos de lanzamiento de cohetes y satélites hasta robótica y software informático.

inclusive embebido dentro de una estrategia de disuasión por enredo o basada en normas, pero también es la alternativa de los actores más débiles, que no pueden proyectar poder duro, ni disuadir por miedo al castigo o represalia. La disuasión por negación apoyada en la defensa también resulta insuficiente si restringe la posibilidad de desarrollar capacidades ofensivas. Una estrategia de disuasión aplicada al ciberespacio debe contemplar todas las alternativas posibles (Nye Jr., 2017). No desarrollar el conjunto pleno de capacidades militares que habilita el uso del ciberespacio en línea con las de otros dominios es un error que puede llegar a pagarse muy caro. Las capacidades para proyectar poder militar y atacar dentro o fuera de las fronteras son necesarias para el IM argentino, más aún, existiendo una potencia nuclear ocupando nuestro territorio insular en el Atlántico Sur, e independientemente de que nuestra Constitución Nacional es clara al señalar cómo recuperar nuestras islas usurpadas. Además, no debemos desatender tampoco los intereses encontrados que tienen nuestro país con Chile y el Reino Unido por su proyección hacia la Antártida que seguramente nos afectará en un futuro no muy lejano.

La decisión estratégica de acercarnos a China puede beneficiarnos en muchos aspectos, pero debemos considerar también que hará alejarnos del marco de integración y cooperación militar regional con los países de occidente, sobre todo si no se actúa como un bloque. Nuestro país debe enfrentar un dilema, la competencia tecnológica entre los EEUU/OTAN y China impiden compatibilizar equipamiento militar, y por otra parte, la prohibición del Reino Unido para adquirir tecnologías de uso militar o dual a la Argentina bajo la mirada indiferente de la OTAN dificulta su desarrollo. La integración al bloque BRICS puede ser una alternativa, pero también tiene consecuencias geopolíticas que deberán ser evaluadas.

Para que la República Argentina pueda converger y avanzar tecnológicamente será necesario diversificar su base productiva en función del dominio de las tecnologías existentes, y al mismo tiempo adoptar nuevas tecnologías o tecnologías de frontera. Por el momento, lograr la autonomía tecnológica basada en desarrollos propios de uso dual que disminuya la dependencia de las grandes potencias es algo inalcanzable en el corto plazo, pero que debería ser considerado en un plan muy a largo plazo o Gran Estrategia que la República Argentina como Nación hasta el momento lamentablemente no posee. Al mismo tiempo, el desarrollo de las futuras capacidades de ciberdefensa estará ligado no solo a la tecnología, sino también a la decisión estratégica nacional de como interactuar con el mundo y limitar o no la libertad de acción de su IM en la arena ciberespacial, con consecuencias también en otras dimensiones físicas interrelacionadas.

Capacidades de defensa cibernéticas necesarias para la paz y para la guerra

"La dicotomía entre la guerra y la paz ya no es un concepto útil para pensar en la seguridad nacional o en las operaciones tácticas (porque) estamos en un estado de competencia y conflicto que es continuo y dinámico" (Derleth, 2021, pág. 23).

A los efectos de la cuantificación y dimensionamiento de las capacidades militares en la República Argentina, uno de los criterios, aún vigentes, que estableció la Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas[47] para su priorización, fue "que se correspondan con el perfil y la naturaleza defensiva que se pretende asignar al Instrumento Militar". Luego, el Decreto PEN Nº 1714/2009 Directiva Política de Defensa Nacional también fijó como criterio orientador para la estructuración y desarrollo del IM "la vigencia de una concepción, posicionamiento y actitud estratégica de naturaleza defensiva", las mismas que se mantienen vigentes hasta la actualidad[48].

Asumir al IM de un Estado como un factor de poder de "naturaleza defensiva" resulta ser una falacia de dicotomía falsa[49], porque contrario a lo que pueda interpretarse por el término defensa nacional, la naturaleza del poder militar conceptualmente es ofensiva, o si ayuda mejor a la interpretación, de proyección de fuerza o de poder. El IM, en esencia, es agresivo porque su fin último es proyectar fuerza o poder duro para dejar fuera de combate a un adversario, tanto en ataque como en defensa, doblegar su voluntad de lucha, o imponer la propia voluntad e intereses. Sin embargo, será la conducción política al más alto nivel de cada Estado quien determine la organización y empleo de su IM. La concepción estratégica del mismo podrá responder a diferentes teorías de las relaciones internacionales, realismo (ofensivo o defensivo), liberalismo o constructivismo, y el rol y el alcance que se le dará al mismo dependerá en parte ello. Cada Estado será quien determine una estrategia, de actitud - no naturaleza- defensiva u ofensiva, en el marco de su propia Constitución y legislación nacional. Restringir, limitar u oponerse al desarrollo de capacidades ofensivas de proyección de poder duro, como suele ser el caso de la República Argentina, justificándolo en una postura estratégica defensiva-cooperativa basada en la convivencia pacífica en la región pese a claros intereses contrapuestos con vecinos sobre la

[47] Decreto PEN Nº 1691/2006
[48] Decreto PEN Nº 457/2021 (DCTO-2021-457-APN-PTE)
[49] *Falacia de falso dilema, dicotomía falsa o falsa disyuntiva* es un error de razonamiento en el que se presenta una situación que busca limitar las opciones disponibles y restringir el debate, evitando que se consideren otras alternativas razonables, y que a menudo se utiliza como una táctica persuasiva para manipular la opinión pública o para respaldar una postura particular (Aparicio, 2023).

Antártida y territorios usurpados, resulta ser una visión bastante ingenua, muy arriesgada, y desde la óptica militar, hasta irresponsable. La defensa de la soberanía, el propio territorio, y sus recursos naturales y estratégicos, hace indispensable contar con capacidades para proyectar fuerza dentro del propio territorio o más allá de sus fronteras si fuera necesario. Son estas capacidades ofensivas las que permiten ejercer el control efectivo. No comprender esto significa mal interpretar el concepto de defensa nacional, ya que solo contar con capacidades defensivas en sentido estricto pueden permitir sostener un sistema de alerta temprana y vigilancia, robustez o resiliencia, hasta quizás una capacidad de proyección de fuerza limitada en el caso de una defensa activa, pero nunca proyectar poder duro en todo su potencial con libertad de maniobra suficiente para ejercer el pleno control efectivo con el objeto de imponer la voluntad o los interese propios. Desarrollar capacidades ofensivas favorecerá además a la disuasión. Luego, la decisión de empeñar esas capacidades ofensivas o no hacerlo, y apostar en su lugar a la disuasión, dependerá de la estrategia adoptada por cada Estado. Pero no invertir en estas capacidades pone a un Estado en desventaja. Incluso no contar con estas capacidades pueden hacer que la disuasión no funcione, o directamente no exista.

Clausewitz expresó que la guerra es la continuación de la política por otros medios. El IM es uno de esos medios, y constituye el brazo armado de un Estado para proyectar poder duro cuando los otros instrumentos del poder nacional como el diplomático, el de la información, o el económico se vuelven insuficientes. Luego, se puede definir y adoptar una estrategia para su utilización, que puede tener un actitud defensiva y disuasiva, de alcance limitado o contra un enemigo caracterizado, pero que de ninguna manera debería alejarnos de su fin último, no solo para garantizar la existencia del Estado, sino para, llegado el caso, imponer sus intereses. Esto demandará desarrollar la mayor cantidad de capacidades posibles que proporcionen la mayor libertad de acción para actuar cuando sea requerido, independientemente de la estrategia formal adoptada, y por supuesto, bajo la conducción civil del Estado Nacional. La doctrina estadounidense, por ejemplo, contempla cuatro usos estratégicos del IM: aseguramiento de la fuerza, la disuasión y la compulsión como dos formas de coerción, y la acción forzosa (JP1, 2020).

El entorno global actual debe interpretarse no como un ambiente de paz, crisis o guerra, sino como un ambiente de competencia continua en el que el ciberespacio constituye un habilitador, y a través del cual, tanto adversarios estatales como no estatales, pueden operar por debajo del nivel de conflicto armado. Por otra parte, las operaciones cibernéticas serán aplicables sin importar la intensidad del conflicto armado que podrá variar desde la respuesta a una crisis y operaciones de contingencia limitadas hasta operaciones de combate a gran escala (JP1, 2020). La

experiencia de la guerra entre Rusia y Ucrania expuso la necesidad de contar con capacidades cibernéticas de todo tipo para poder hacer frente al enemigo, tanto para incidir en el teatro del conflicto previo al enfrentamiento cinético o contrarrestar sus efectos, como para luego apoyar o afectar las operaciones cinéticas en los otros dominios. Por esta razón, independientemente del nivel de conflicto, en la paz o en guerra, se hace necesario contar con capacidades que permitan abarcar todo el espectro de posibilidades en el ciberespacio.

En el marco de la disuasión en el ciberespacio, Jasper sugirió una combinación de estrategias y capacidades basado en la imposición de consecuencias reales (represalias), el empleo de defensas reactivas (negación), el mantenimiento de la perseverancia diplomática (enredo) y la consideración de la adaptación legal (defensa activa), para llevar a un actor a decidir no actuar por temor a una combinación de costos, fallas o consecuencias (Jasper, 2015, pág. 78).

Sin embargo, Graber sostuvo que en el ciberespacio las tácticas defensivas son mucho más limitadas porque ni las defensas cibernéticas activas, ni las pasivas, dañan al atacante, y porque el problema de la atribución limita aún más la disuasión y reduce la posibilidad de contraataques como parte de una estrategia defensiva. Por lo tanto, las tácticas de ataque proactivas u operaciones ofensivas deberían ser consideradas en la estrategia de un Estado para explotar las ventajas que la zona gris en el dominio cibernético ofrece (Graber, 2021).

Por su parte, Torres afirmó que

> la disuasión no puede ser usada si no se conoce al enemigo, sus intenciones, hasta donde está dispuesto a llegar, cuál es su objetivo y sus razones para atacar, ya que no habría manera de generar credibilidad en las amenazas, ni se puede garantizar una respuesta apropiada que influya en las acciones del atacante. Cuando el campo de batalla es el ciberespacio, un Estado debe saber defender y atacar por los mismos medios y en las mismas condiciones (Torres, 2019).

La caracterización de los ataques cibernéticos que afecta a la defensa nacional como una operación de guerra según la legislación argentina donde existe un oponente claramente identificado como una fuerza armada de otro estado agresor externo o una vinculación con un estado de guerra declarado no resulta fácilmente aplicable en la arena ciberespacial. Restringir el desarrollo de capacidades militares basadas en argumentos que no aceptan conceptos como el de seguridad ampliada o nuevas amenazas y observan una tendencia a la militarización de las cuestiones públicas que amenaza el ejercicio del control civil sobre lo militar y despierta viejas remembranzas históricas representan una visión sesgada para los desafíos del mundo de hoy y las nuevas formas en que han evolucionado los conflictos de la mano de la tecnología. Esta situación exige revisar el marco legislativo y el papel que el Estado nacional debería asignarle a su IM, basado en las nuevas formas

de combate. Un enfoque para la intervención militar en el ciberespacio basado en efectos y definido no por quien produce el ataque cibernético, sino sobre la base de que infraestructura crítica está siendo afectada es importante, pero resulta insuficiente. No solo se trata de defender sino de contar con plena libertad de acción para proyectar poder duro. La guerra entre Rusia y Ucrania nos permite observar los efectos reales de las operaciones cibernéticas en un conflicto bélico a gran escala aportando conocimiento práctico. La convergencia tecnológica en la forma de conducir la guerra nos lleva a la necesidad de desarrollar un amplio espectro de capacidades en el ciberespacio sin restricciones y amparado en un marco legal al más alto nivel que garantice la legitimidad de las operaciones y responsabilidades.

El IM de la República Argentina debería desarrollar capacidades que le permitan ejecutar operaciones de todo tipo en el ciberespacio, más allá de las restricciones políticas o legales nacionales, incluyendo operaciones ofensivas, defensivas, de explotación y de información. Capacidades que permitan, como expresó Levite, conducir de manera quirúrgica operaciones cibernéticas en tiempos de paz o antes de la guerra más allá de la recopilación de inteligencia, y estén diseñadas para balancear entre lograr el impacto deseado y evitar efectos excesivos que desencadenen una dura represalia o comprometan las capacidades cibernéticas propias. Operaciones limitadas en su alcance, duración y efectos, que puedan espaciarse cuando sean diseñadas para transmitir señales, y que permitan que sus mensajes sean notados e internalizados. Operaciones cibernéticas defensivas y ofensivas efectivas capaces de entregar los efectos deseados en el objetivo previsto, en el momento adecuado y durante la duración buscada, limitar estos efectos al objetivo previsto, y evitar el desbordamiento y el contagio, ya sea por los efectos en cascada del ataque, la exposición de la vulnerabilidad explotada en la operación, el compromiso de las herramientas y modalidades utilizadas, o alguna combinación de estas. Estos parámetros de éxito serán importantes para definir el espacio operativo de las operaciones cibernéticas, el nivel de dependencia y los recursos asignados a los operadores cibernéticos. Además, deberá considerarse que estos parámetros podrán ser subjetivos, reflejando prioridades y sesgos culturales, políticos e institucionales, dinámicos y específicos del contexto (Levite, 2023). El desarrollo de capacidades de empleo ofensivas en el ciberespacio debería ser incluida como parte de una estrategia de disuasión que le permita al Estado argentino reservarse el derecho a emplearlas eventualmente de la misma manera en que la OTAN lo considera actualmente.

Si bien las operaciones de información no fueron analizadas en profundidad en este trabajo, al poder emplear el ciberespacio como medio habilitador para su ejecución merece la pena considerar desarrollar también este tipo de capacidades que permitan, como expuso Robledo,

promover percepciones, actitudes y comportamientos favorables a las operaciones propias e influir en la toma de decisiones humanas o automatizadas del adversario. Operaciones fundamentales para apoyar la narrativa y los mensajes clave de la comunicación estratégica como así también respaldar la legitimidad de una operación, y diseñadas para afectar las capacidades, la comprensión y la voluntad de una audiencia objetivo mediante efectos no sólo físicos sino también psicológicos. Operaciones que permitan anular o degradar enlaces de comunicación, nodos o sistemas de información, afectar la percepción, el conocimiento y la opinión mediante la denegación, degradación, interrupción o presentación de información, e influir sobre la voluntad e idealmente el comportamiento; y operaciones que, al mismo tiempo, sirvan para proteger tanto la información como los sistemas de información propios (Robledo, 2022).

Organización de la ciberdefensa y ciberseguridad en la República Argentina

Al definir las operaciones en el ciberespacio no hay acuerdos conceptuales y de consenso global. Esto repercute en la forma de organizar las estructuras nacionales de ciberdefensa, y dificulta la colaboración nacional e internacional en este ámbito. Al mismo tiempo, puede generar que queden tareas sin resolver por no determinar un responsable específico, o tareas en disputa entre diferentes organizaciones que ocasionen conflictos o duplicación de esfuerzos, afectando su eficacia y eficiencia.

La JID reconoce que

> la ciberdefensa militar constituye la capacidad principal a través del cual el gobierno de una nación implementa la ciberdefensa nacional como parte de la política de defensa, que, en coordinación con el resto de los instrumentos del poder nacional, contribuye a la seguridad nacional. Pero no siempre es evidente si una amenaza o un ciberataque son responsabilidad de la ciberdefensa militar, la ciberdefensa nacional o la ciberseguridad nacional (JID, 2020, pág. 55).

La República Argentina diferencia los ámbitos de Defensa y Seguridad a partir de la Ley N° 23.554 de Defensa Nacional y la Ley N° 24.059 de Seguridad Interior, por lo tanto, los ámbitos de actuación en el ciberespacio están divididos en Ciberdefensa y Ciberseguridad. Excepto algunos casos particulares, las Fuerzas Armadas no poseen atribución para involucrarse en aspectos que sucedan en el ámbito de la Seguridad Interior, incluyendo la protección cibernética. En este marco normativo, la Ciberdefensa en la República Argentina forma parte de un sistema mayor constituido por otros organismos del Estado, que permiten a la Nación ejercer su soberanía.

Compete al Ministerio de Defensa entender en la determinación de los objetivos y políticas del área de su competencia, los estudios y trabajos técnicos, y la formulación y ejecución de las políticas nacionales referidas a la defensa nacional (Decreto PEN Nº 577/2017).

Compete al Ministerio del Interior entender en la determinación de los objetivos y políticas del área de su competencia, la determinación de la política criminal, la elaboración de planes y programas para su aplicación y prevención del delito, y la coordinación de las acciones tendientes a solucionar situaciones extraordinarias o emergencias dentro del territorio nacional (Decreto PEN Nº 577/2017).

La seguridad nacional en el ciberespacio, en sentido holístico y por descarte, está en manos del Comité de Ciberseguridad[50], creado para convocar a los representantes de las principales áreas de gobierno, elaborar una estrategia nacional de ciberseguridad, entendida en sentido amplio, y desarrollar un plan de implementación. Actualmente, este comité está integrado por seis organismos: la Secretaría de Innovación Pública dependiente de la Jefatura de Gabinete de Ministros, que es quien lo preside, el Ministerio de Defensa, el Ministerio de Seguridad, el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, el Ministerio de Justicia y Derechos Humanos, y la Secretaría de Asuntos Estratégicos dependiente de la Presidencia de la Nación (Argentina, 2022). Resulta llamativo la ausencia de la Agencia Federal de Inteligencia (AFI) cuando la temática de las ciberamenazas forma parte de los lineamientos estratégicos del Sistema de Inteligencia Nacional (SIN) dentro del Plan de Inteligencia Nacional (Argentina, 2020).

Una unidad ejecutiva coordina la agenda y registro de las reuniones del Comité Nacional de Ciberseguridad en la órbita de la Subsecretaría de Tecnologías de la Información de la Secretaría de Innovación Pública, encargada de elaborar, promover y dar seguimiento al Plan de Acción de la Estrategia Nacional de Ciberseguridad (RESOL-2023-44-APN-SIP#JGM).

La Dirección Nacional de Ciberseguridad, dependiente de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros, es quien entiende en los aspectos relativos a la ciberseguridad, a la protección de las infraestructuras críticas de la información[51], interviene en la formulación y ejecución de planes de capacitación, y se encarga de generar y mejorar las capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática a nivel nacional (Argentina, 2023). En el ámbito de esta dirección, fue creado el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar.), para "coordinar la gestión de

[50] Decreto Poder Ejecutivo Nacional Nº 577/2017 (Creación del Comité de Ciberseguridad).
[51] *Infraestructuras Críticas de Información*: "son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas" (Anexo I, RESOL-2019-1523-APN-SGM#JGM).

incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del Sector Público Nacional (e) Infraestructuras Críticas de Información, declaradas como tales" (Artículo 1, DI-2021-1-APN-DNCIB#JGM).

El Ministerio de Seguridad de la Nación cuenta con un Comité de Respuesta de Incidentes de Seguridad Informática (CSIRT) conformado por personal de las cuatro fuerzas de seguridad federales (Gendarmería Nacional, Prefectura Naval, Policía de Seguridad Aeroportuaria y Policía Federal), con el objeto de "coordinar las actuaciones centralizadas ante usos nocivos y/o ilícitos de las infraestructuras tecnológicas, las redes y los sistemas de información y de telecomunicaciones (y) colaborar en la protección de las infraestructuras críticas del Ministerio de Seguridad y sus órganos dependientes" (Resolución Ministerio de Seguridad Nº 1107-E/2017).

En el ámbito de la Defensa Nacional, la función principal del sistema de ciberdefensa es proteger las redes, los sistemas y las infraestructuras críticas del país bajo su jurisdicción, de las amenazas y los ataques cibernéticos. Para ello, las Direcciones de Ciberdefensa y fracciones de ciberdefensa tácticas de las FFAA son responsables de proteger sus respectivas redes militares y activos críticos de las ciberamenazas, y se enfocan en implementar medidas defensivas, realizar ejercicios cibernéticos y responder a incidentes cibernéticos dentro de su ámbito.

Por su parte, el Comando Conjunto de Ciberdefensa, creado en el año 2014, tiene por misión "ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del IM de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar" (Resol MD 343/2014). Entre sus funciones esta coordinar sus acciones con las Direcciones de Ciberdefensa de las FFAA, establecer los criterios rectores, a nivel del IM, para la determinación de Infraestructuras Críticas a ser protegidas, establecer las políticas, estándares y procedimientos de Ciberdefensa, criptografía e informática forense, y determinar las operaciones de Ciberdefensa necesarias para el cumplimiento de la misión del Comando. También entiende en la conducción y ejecución de las ciberoperaciones necesarias para la protección de las operaciones del Instrumento Militar y, a orden, de las Infraestructuras Críticas Nacionales que se le asignen, y la ejecución de las acciones necesarias y suficientes para operar en la eventualidad de un ambiente degradado desde el punto de vista cibernético y recuperar las capacidades afectadas por incidentes; e interviene en la elaboración, experimentación, revisión y/o reelaboración de doctrina conjunta y/o combinada básica, derivada y de procedimientos relativa a la Ciberdefensa (Ciberdefensa, 2023).

Luego, mediante Decreto PEN N° 42/2016, se creó en la órbita del Ministerio de Defensa, la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares, con Control Funcional sobre el Comando Conjunto de Ciberdefensa.

Posteriormente, en enero de 2023, por Resolución N° 105/2023, el Ministerio de Defensa actualizó la Política de Ciberdefensa creando, bajo la órbita de la Subsecretaría de Ciberdefensa, el Comité de Infraestructuras Críticas de la Información de la Defensa, para identificar los Activos Digitales Críticos que soportan el normal funcionamiento de las Infraestructuras Críticas del Sistema de Defensa Nacional y el Centro de Supervisión y Control de Gestión de Ciberdefensa, para centralizar y gestionar la información y prevención de incidentes cibernéticos en la jurisdicción. También resaltó entre los considerandos que "la ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el instrumento militar en cumplimiento de la normativa vigente en materia de Defensa Nacional[52]".

Además, a favor del multilateralismo en las relaciones internacionales, la República Argentina colabora en ciberseguridad mediante foros, conferencias e iniciativas regionales e internacionales para compartir conocimientos, mejores prácticas e inteligencia de amenazas con otros países y organizaciones internacionales.

Finalmente, ya que el entorno de la ciberdefensa y seguridad se encuentra en constante evolución, es de esperar que la estructura organizacional y los roles de los actores involucrados puedan cambiar con el tiempo para adaptarse a las amenazas y desafíos emergentes.

El rol del Instrumento Militar argentino en el ciberespacio de cara al futuro

El accionar de las Fuerzas Armadas argentinas en el sistema de defensa nacional se encuentra enmarcado dentro de un plexo legal que involucra la Ley N° 23.554 de Defensa Nacional, su Decreto Reglamentario N° 727/06, el Decreto N° 1691/06 Directiva de Organización y Funcionamiento de las FFAA y la Ley N° 24948 de Reestructuración de las FFAA. Este marco normativo limita y restringe el empleo del IM en asuntos de seguridad interior. La misión principal del IM es conjurar y repeler toda agresión externa perpetrada por fuerzas armadas de otro Estado[53].

[52] RESOL-2023-105-APN-MD, "Actualización de la Política de Ciberdefensa," Ministerio de Defensa, 30 enero 2023.
[53] Decreto PEN 1691/2006, Anexo I - Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas

Cuando nos referimos al empleo específico del IM en el ciberespacio, Eissa, Gastaldi, Poczynok y Zacarías Di Tullio observaron a priori que las operaciones ciberespaciales sin un objetivo específicamente militar, "correspondería caracterizarlas como operaciones delictivas que exceden el ámbito de la defensa nacional, y que deben ser tratadas por otros organismos del Estado (…) y agencias estatales que hacen a la seguridad pública", y que "la ciberdefensa debe abocarse exclusivamente a aquellos ataques cibernéticos cuyo objetivo es afectar las capacidades militares de los Estados", orientados a quebrantar la infraestructura, la logística y la cadena de suministros, o distraer, confundir e inhabilitar el C4IVR[54] (Eissa, Gastaldi, Poczynok, & Zacarías Di Tullio, 2014, págs. 186-188). Sin embargo, un ciberataque que afecta los intereses nacionales o las infraestructuras críticas debería ser considerado un problema de defensa nacional y de sus Fuerzas Armadas por añadidura.

En 2018, la Publicación Conjunta PC 10–04 Planeamiento para la Acción Militar Conjunta – Nivel Estratégico Militar estableció que, si no hay escenarios relacionados con la misión principal y objetivos explícitos del IM, o complementarios, se deberán usar otras herramientas para atenuar la falta de precisiones. Al mismo tiempo, la ausencia de escenarios concretos no implica en absoluto que deban obviarse las responsabilidades para el cumplimiento de la misión principal (10-04, 2018, pág. 21), defendiendo o atacando, más allá de la adopción de una postura u actitud estratégica defensiva como Nación bajo un lineamiento político.

En este sentido, la República Argentina necesitará desarrollar capacidades cibernéticas que le permitan al IM la libertad de acción suficiente para conducir operaciones efectivas en el ciberespacio del tipo defensivas, ofensivas, de explotación, o de información, para lograr efectos físicos, digitales o cognitivos que permitan garantizar la seguridad de las infraestructuras críticas asignadas, sostener el Comando y Control propio, degradar el del enemigo, complementar el esfuerzo operacional de proyección de poder militar en los dominios cinéticos o en el espectro electromagnético, o accionar en cumplimiento de los objetivos estratégicos asignados, Estas capacidades son esenciales tanto para las nuevas formas de combate moderno como para sobrevivir en el ambiente global de competencia continua ligado a los nuevos desarrollos tecnológicos en el que no existen hasta el momento reglas claras y en que las amenazas ya no necesariamente visten uniforme. Negar este hecho y no evolucionar en consecuencia implica desaprovechar la actual ventaja que hoy brinda el ciberespacio para actuar. Demorarse en el tiempo incrementa la brecha tecnológica que nos separa de los países más desarrollados y las posibilidades de integración y

[54] *C4IVR* Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento.

convergencia nacional e internacional bajo el concepto JADO o multidominio occidental. El ciberespacio hoy afecta a todos los dominios en la forma de combate.

Es indispensable por las características que poseen las amenazas a través del ciberespacio un enfoque integral para enfrentarlas, independientemente de los responsables y encargados de llevar a cabo la seguridad y/o defensa del ciberespacio. Es aquí donde se observa el primer obstáculo a resolver: ¿quién debe ejercer el liderazgo operativo del accionar integral en el ciberespacio?

Analizando los criterios rectores fijados en la segunda Estrategia Nacional de Ciberseguridad de la República Argentina[55], respecto a la primera[56], se observa que el liderazgo fue eliminado de la lista, y que la integración internacional fue suplantada por la cooperación, visualizando un cambio de actitud que va de la "intención de unir fuerzas" a "articular acciones oportunas" para generar sinergia. Respecto a los objetivos fijados, se agregó el fortalecimiento del sistema institucional y la protección de las infraestructuras críticas nacionales, pero aún sin identificar puntualmente dentro de los sectores que, si se hicieron en el año 2019,[57] y que son: energía, TIC, transporte, hídrico, salud, alimentación, finanzas, nuclear, químico, espacio y Estado.

Al mismo tiempo, la visión integradora o cooperadora que plantean ambas estrategias respecto al accionar del IM se encuentra limitada a la ciberdefensa en función de su misión principal según el marco regulatorio vigente, dándole participación en el Comité Nacional de Ciberseguridad[58], presidido por la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros.

Se observa que el enfoque holístico que debería dársele a la ciberseguridad nacional, entendida en concepto amplio, se encuentra sumido en una vorágine burocrática que le impide pasar de lo teórico a lo práctico, y que cuando se pretende bajarlo a la realidad no existe una operacionalización interagencial integrada porque aún existen muchas indefiniciones que incluyen entre otras la determinación específica de las infraestructuras críticas, áreas de responsabilidad según actores, reglas de empeñamiento, estructura de la organización, comando de misión y liderazgo.

Hasta tanto y en cuanto no se definan las cuestiones antes mencionadas, no se podrá pasar de la fase conceptual o teórica a la fase operacional, mientras los avances tecnológicos, que no esperan, plantean mayores desafíos y agravan la exposición de nuestras vulnerabilidades.

[55] IF-2023-81810563-APN-SSTI#JGM (Anexo I de la RESOL-2023-44-APN-SIP#JGM).
[56] IF-2019-49036224-APN-SGM#JGM (Anexo I de la RESOL-2019-829-APN-SGM#JGM).
[57] IF-2019-78452510-APN-SGM#JGM (Anexo I de la RESOL-2019-1523-APN-SGM#JGM).
[58] Decreto Poder Ejecutivo Nacional Nº 577/2017 (Creación del Comité de Ciberseguridad).

Finalmente, el desafío que plantea mantener el marco de la actual legislación, demandará de los actores involucrados una relación cívico-militar madura, sin sesgos con la gobernanza, que se focalice en los problemas de hoy y del futuro, donde se puedan optimizar todos los acotados recursos que tiene el Estado para poder ser empleados en forma interagencial de manera eficaz y eficiente, y en donde el IM como factor de poder del Estado participe atacando, defendiendo o apoyando de acuerdo a la tarea que le sea asignada.

La defensa ciberespacial desde una perspectiva de seguridad nacional, una visión "fuera de la caja"

El ciberespacio es parte de los bienes comunes globales o "Global Commons" (DQI, 2012), e Internet es un servicio público. Las actividades realizadas a través del ciberespacio en la República Argentina dependen de una conexión externa de la cual somos altamente dependientes. Esta interdependencia con servidores fuera de una red propia y soberana sobre la cual podamos ejercer el control nos hace altamente vulnerables. Por lo tanto, resulta prioritario, por un lado, contar con una red propia y soberana que facilite ejercer el control en el ciberespacio de jurisdicción, y por el otro, determinar puntualmente aquellas infraestructuras críticas de la información cuyas conexiones y actividades son esenciales y podrían ser afectadas, a los fines de mitigar riesgos.

Por el año 2011, Jason Andress visionaba de la mano de la globalización el incremento futuro de ataques, operaciones de influencia y espionaje a través del ciberespacio hasta el punto de afectar los elementos del poder nacional, donde la legislación cibernética estaría por detrás de la tecnología hasta tener un impacto marginal, donde continuarían los ataques cibernéticos aislados que podrían catalogarse como actos de guerra pero donde la ONU no actuaría, ni los países querrían comprometerse en establecer estándares o establecer tratados para deber cumplir luego restringiéndoles o impidiéndoles obtener ventajas competitivas, y donde la inacción podría conducir a una atrofia tecnológica hasta que una catástrofe cibernética significativa los obligue a un cambio. Haciendo una analogía con la guerra biológica, el marco de respuesta cibernética eficaz recomendado incluía crear el equivalente cibernético nacional a los Centros para el Control de Enfermedades, para monitorear, informar, coordinar y colaborar sobre amenazas y tendencias cibernéticas, a nivel nacional e internacional; una Agencia Federal para el Manejo de Emergencias Cibernéticas, para gestionar la respuesta a eventos cibernéticos de trascendencia nacional; y un

Marco Nacional de Respuesta Cibernética, para prevenir, planificar y abordar la gama completa de amenazas cibernéticas bajo funciones y responsabilidades claramente definidas (Andress & Winterfield, 2011, págs. 266-268).

Andress observó que entre las herramientas claves utilizadas en aquel momento en los Estados Unidos para abordar la problemática (investigación, agencias de aplicación de la ley, Departamento de Seguridad Nacional, Comando Cibernético, Agencia de Seguridad Nacional y Legislación), todos tenían una parte, pero ninguno estaba a cargo; y para dar una respuesta correcta a la organización recomendó la fórmula: Agregación de capacidades + Innovaciones + Recursos + Liderazgo = Ventaja estratégica (Andress & Winterfield, 2011, pág. 271).

Por su parte, en el año 2013, los rusos Vorobyev & Kiselyov sostenían que "la información ahora es un arma (que) no solo complementa los ataques y las maniobras de fuego, sino que los transforma y los une, (por lo que) la información se está convirtiendo en una lucha armada por derecho propio" (Vorobyov & Kiselyov, 2013, pág. 56).

Actualmente, las tecnologías emergentes aplicadas incrementan cada vez más, y en mayor medida, los desafíos y las amenazas a la seguridad nacional en el entorno de competencia global. Moresi afirma que la capacidad que posee la IA de poder perfilar al ser humano permitirá no solo influir sino llegar a controlar sus decisiones (Moresi, Motta, Trama, Saldanha Walker, & Amaya, 2022, pág. 107).

Encontrar la solución al problema es complejo. En la República Argentina, de Vergara y Trama señalaron en 2017 la necesidad de definir líneas y reglas claras en la relación entre el gobierno y el sector privado, explicitar responsabilidades, capacidades y autoridades, y aprender a trabajar interagencialmente en un ambiente de cooperación para enfrentar las amenazas en el ciberespacio (de Vergara & Trama, 2017, págs. 265-266).

Moresi planteó como una estrategia de integración civil-militar a explorar el desarrollo de un concepto de Poder Ciberespacial Nacional que involucre y coordine los esfuerzos sinérgicos en todas las áreas (Moresi, Motta, Trama, Saldanha Walker, & Amaya, 2022, pág. 114).

En este sentido, este Poder Ciberespacial Nacional requerirá de un liderazgo e unidad de comando al más alto nivel bajo una visión de seguridad nacional en sentido amplio con control operacional interagencial que integre las áreas defensa, seguridad interior e inteligencia, y que permita tomar decisiones en los niveles estratégico, operacional y táctico, sustentado por un marco jurídico adecuado que involucre recursos cívico-militares y que habilite tanto a las FFAA como a las FFSS, el desarrollo de capacidades para conducir operaciones defensivas, ofensivas, de

explotación y de información a través del ciberespacio, integrado a un Sistema de Inteligencia Nacional (SIN) basado en fuentes abiertas que permita tanto la anticipación y alerta estratégica, como la mitigación de ciberoperaciones que dentro del entorno de la información pretendan afectar cognitivamente a su población.

Al mismo tiempo, será necesario contar con una ciberseguridad nacional robusta basada en los tres pilares indicados por la JID: ciberresiliencia, ciberprotección y ciberdefensa, en estrecha colaboración y cooperación, al igual que con sus homólogos internacionales. Ciberresiliencia gestionada a través de los CERTs de ámbito gubernamental, militar, infraestructuras críticas, unidades y sector privado; ciberprotección, ejercida por unidades especializadas de las fuerzas y cuerpos de seguridad del Estado; y ciberdefensa, llevada a cabo por una fuerza ciberespacial[59], conformada por unidades de ciberdefensa de las FFAA con capacidades defensivas, ofensivas y de explotación, y apoyada por otros poderes del Estado (Diplomático, Información, y Económico) en caso de ser requerido (JID, 2020, págs. 84-85); en donde resulta esencial la cooperación en todas sus facetas: internacional, nacional, con el sector industrial y académico, con los ciudadanos, y la cooperación interna dentro de la propia fuerza ciberespacial (JID, 2020, pág. 54).

Por el momento, la metodología de planeamiento estratégico militar como fase del Planeamiento de la Defensa de la República Argentina, y el diseño de fuerzas derivado del mismo, deberá ajustarse al criterio de capacidades militares establecido por la Directiva Política de Defensa Nacional Decreto PEN Nº 2645/2014 (Argentina G. , 2015), priorizando el análisis y determinación de ciertos factores particulares que son esenciales y que conforman el MIRILADO (Medios, Información, Recursos Humanos, Infraestructura, Logística, Adiestramiento, Doctrina y Organización). Para desarrollar capacidades de ciberdefensa debería considerarse:

- Medios (M) de hardware y software para ejecutar operaciones en todos los dominios tanto físicos (tierra, mar, aire y espacio) como virtual, actualizados y acorde al estado del arte en la materia, priorizando los desarrollos nacionales (de uso dual o no, según corresponda), y que tiendan al auto sostenimiento e independencia de las tecnologías externas, en la medida de lo posible. Los desarrollos o adquisiciones deberían apuntar a la convergencia tecnológica considerando tecnologías emergentes como la inteligencia artificial, la computación cuántica, y los cambios que se producen tanto en los servicios de comunicaciones como en las características de las tecnologías de la información, tanto en el ámbito local como global (Moresi, Motta, Trama, Saldanha Walker, & Amaya, 2022, pág. 116).

[59] *Fuerza ciberespacial*: conjunto de unidades de las fuerzas armadas, organizadas bajo un mismo mandó único, responsables del planeamiento y la conducción de las operaciones militares en el ciberespacio (JID, 2020, pág. 15).

La fuerza ciberespacial debería disponer de unas capacidades orientadas a la conducción de ciberoperaciones, en sus tres facetas (defensiva, explotación y ofensiva); como la gestión de eventos de seguridad, la inteligencia operativa, la respuesta, la investigación forense digital y la ciberdefensa desplegable (JID, 2020, pág. 59), (y) sus sistemas deben permitir altos niveles de conciencia situacional, ser robustos, ágiles, proactivos, resilientes, generando modelos que permitan la adecuada toma de decisiones sobre datos e información confiables y seguros. (Moresi, Motta, Trama, Saldanha Walker, & Amaya, 2022, pág. 115).

También debería considerarse desarrollar capacidades para realizar operaciones de información a través del ciberespacio.

- Información (I) actualizada obtenida no sólo a través de medios de inteligencia, sino utilizando otros recursos de fuentes abiertas como el observatorio argentino del ciberespacio (ESGCFFAA, 2023) y afines, y la participación en foros, actividades educativas u operativas.
- Recursos Humanos (R) formados, capacitados y actualizados para llevar a cabo las operaciones ciberespaciales, ordenados bajo un plan de carrera, y acompañados con una política de retención de personal acorde, para conservar los mismos a lo largo del tiempo, y facilitar el traspaso de conocimientos y experiencias entre ellos.
- Infraestructura (I) robusta, redundante, y preferentemente propia y soberana en su extensión, que permita ejercer control a través del ciberespacio dentro de su área de responsabilidad o jurisdicción.
- Logística (L) del tipo fija y móvil, de la que participen tanto el ámbito público como privado, en todas las dimensiones físicas y digital, que contribuya no solo a ejecutar operaciones, sino también a generar resiliencia en caso de verse afectada la infraestructura o sus medios.
- Adiestramiento (A) a partir de ejercitaciones conjuntas y combinadas dentro y fuera del país, y en función de las actividades operativas diarias, no solo a nivel nacional, sino también a través de mecanismos de cooperación regional e internacional.
- Doctrina (D) específica propia, acorde al estado del arte en el ambiente ciberespacial global, que permita ser considerada tanto por las doctrinas convencionales como la conjunta, sin limitaciones políticas que afecten la libertad de acción ni pongan al IM en desventaja o a la nación en mayor riesgo haciéndola más vulnerable, y respaldada por un marco jurídico acorde para su empleo. Amparada bajo una norma legal del rango más alto posible que garantice la legitimidad de las misiones, responsabilidades, cometidos, actividades y acciones de la fuerza ciberespacial, y que incluya como mínimo, el ámbito de actuación, la misión, los cometidos, la organización y la dependencia de la fuerza ciberespacial (JID, 2020, pág. 46).
- Organización (O) bajo unidad de comando al más alto nivel, de carácter interagencial, con una estructura bien definida, al igual que las áreas de responsabilidad de sus

participantes, sus roles y funciones, y con reglas de empeñamiento claras. Esta organización bien entendida trascenderá la órbita militar bajo un enfoque de seguridad nacional en sentido amplio donde, tal vez, el IM podría asumir el liderazgo, al menos inicial, como ya lo ha hecho antes en otras áreas y oportunidades históricas que incluyen desde el control cívico-militar aeroespacial[60], hasta el manejo de crisis de la pandemia del COVID 19[61].

Buscar la innovación e intentar llevar a la práctica conceptos nuevos implica ir más allá de los límites institucionales dentro de un marco socialmente construido y utilizado para dar sentido a la realidad (Zweibelson, 2023, pág. xxix).

En este sentido, avanzar en el concepto de un Poder Ciberespacial Nacional, organizado bajo una estructura de comando y control militar, subordinado al Poder Ejecutivo, donde participen otras agencias y organismos del Estado, y organizada tal vez sobre la base del Comando Conjunto de Ciberdefensa, podría llegar a ser el primer paso en la búsqueda de la mejor solución.

El cuarto capítulo habló de la defensa ciberespacial en la República Argentina, analizando las capacidades necesarias para la paz y la guerra, describiendo la ciberseguridad y la ciberdefensa en nuestro país, que debería tener el IM para actuar en el ciberespacio de cara al futuro y que podría ser una solución para optimizarla desde una perspectiva de seguridad nacional en sentido amplio.

[60] Vasallo, C. (s. f.). *Control del Espacio Aéreo en la República Argentina*. SAIJ. Recuperado 9 de octubre de 2023, de http://www.saij.gob.ar/doctrina/dacf080092-vassallo-control_espacio_aereo_en.htm%3Bjsessionid=el1a0negeh3fppq327uq3y5e?0.

[61] Rivas, S. (2021, julio 14). *Actividades de las Fuerzas Armadas Argentinas en la gestión de la pandemia Covid 19*. Pucará Defensa. https://www.pucara.org/post/actividades-de-las-fuerzas-armadas-argentinas-en-la-gestión-de-la-pandemia-covid-19.

CONCLUSIONES

El presente trabajo académico pretende dar respuesta al desafío que plantea hoy la defensa del ciberespacio para la República Argentina, intentando determinar el rol y las capacidades cibernéticas de sus Fuerzas Armadas en el marco de los conflictos futuros. La hipótesis presentada sostiene que la victoria en el ciberespacio de acuerdo a la forma de combate moderno podrá lograrse mediante el desarrollo de capacidades que le permitan a su IM conducir operaciones cibernéticas defensivas, ofensivas, de explotación y de información en todos los niveles de la guerra y con la libertad de acción suficiente para sostener la cibersupremacía o cibersuperioridad, conocida o no por el enemigo, para producir los efectos deseados.

El primer objetivo específico consistió en determinar las implicancias del espacio cibernético para la Defensa, los efectos del avance tecnológico en esa dimensión y la utilización militar que se le podría dar en el futuro. De este trabajo surge que:

1º) La explotación del ciberespacio permite producir efectos tanto en todos los planos (físico, digital y cognitivo), como en todos los niveles (estratégico, operacional y táctico). La atribución es una característica que limita la defensa y que puede explotarse en un ataque inmediato, pero que también podría descubrirse a largo plazo. Al mismo tiempo, hasta el momento resulta complicado medir y limitar los efectos de segundo y tercer orden de un ciberataque.

2º) Las tecnologías emergentes aplicadas a la guerra moderna tienden a la interoperabilidad, la integración y la convergencia, conceptos que requieren de una interconexión a una red, que además de ser un requisito mandatorio, plantea una vulnerabilidad en común e insalvable hasta el momento. Estos factores pueden influir y constituir una limitación al momento de generar alianzas o acuerdos de cooperación entre naciones. Los líderes militares deben comprender cómo se desarrollan, adaptan y emplean estas nuevas tecnologías que son relevantes para el ámbito de combate, y orientar tanto a quienes desarrollan tales capacidades como a quienes tienen poder decisión acerca de donde se invierten los recursos de la defensa nacional.

3º) El conflicto entre Rusia y Ucrania ha demostrado hasta el momento que las capacidades cibernéticas no han permitido producir efectos cinéticos estratégicos en la misma magnitud a los que pueden ejecutarse a través de los otros dominios (tierra, mar, aire y espacio) y aplicarse por el empleo del poder duro. Aun así, por su interrelación con ellos, cada vez más

dependiente tecnológicamente, es de esperar que las acciones a través del ciberespacio puedan llegar a incidir en los efectos buscados en estos dominios físicos hacia el futuro. La guerra también dejó expuesto al ciberespacio como un ámbito de combate en el que se ha desplegado todo el abanico de posibilidades, empleando ciberoperaciones ofensivas, defensivas, de explotación y de información.

4º) Al mismo tiempo, el ciberespacio, por ser parte del espectro electromagnético dentro del entorno de la información, y por sobreponerse con el ámbito de aplicación de la guerra electrónica, nos lleva a plantearnos si desde un enfoque más operativo no sería más conveniente referirnos en su conjunto como dominio ciber-electromagnético.

Basado en los puntos expuestos precedentemente se da por cumplido el primer objetivo específico, avanzando sobre el segundo, que fue comprender cómo es abordada la defensa cibernética en los ámbitos global, regional y nacional y el rol de sus Fuerzas Armadas. Para ello se observó que:

1º) El ciberespacio es parte de los bienes comunes globales con la particularidad de ser un dominio de carácter virtual creado por el hombre. Los Estados difieren en la forma de conceptualizar la soberanía en el ciberespacio y no existe un consenso a nivel internacional respecto a normas, reglas y límites en el empleo del mismo, en el que intervienen actores estatales y no estatales. También difieren en las estrategias planteadas y la forma de organizarse para actuar y defenderlo.

2º) Mientras algunos estados adoptan una postura defensiva limitada a defender las infraestructuras críticas y basado en la robustez, resiliencia y redundancia, otros países como EEUU, China, Rusia, Israel, Reino Unido, Irán, Corea del Norte, Australia y Francia, prefieren desarrollar capacidades ofensivas apostando a la disuasión y reservándose su empleo en caso de ser necesario.

3º) Cuando nos referimos a ciberdefensa no se trata de defender toda la red en forma constante, porque resulta prácticamente imposible. El ciberespacio hace a todos los Estados vulnerables. Sostener el dominio o la superioridad en forma continua resulta prácticamente imposible. El objetivo será crear entonces una ventana de oportunidad suficiente que permita ejecutar la tarea o la operación mientras los adversarios intentan interrumpir o alterar los datos o la información en el ciberespacio.

4º) La disuasión en el ciberespacio en sentido estricto tampoco resulta posible por las características antes mencionadas, aunque puede llegar a servir de paliativo. Adoptar una actitud estratégica defensiva basada en una estructura robusta, redundante, ágil y resiliente, resulta

insuficiente porque restringe la libertad de acción y pone a un Estado en desventaja. Tanto la defensa pasiva como la defensa activa en el ciberespacio no pueden frustrar el comportamiento del enemigo en el ciberespacio.

Con estas conclusiones parciales se da por cumplimentado el segundo objetivo específico y se pasa al tercero que ha sido identificar qué capacidades de ciberguerra son necesarias para una defensa efectiva en la República Argentina. Con tal fin se identifificó lo siguiente:

1º) La ciberdefensa requiere tener el abanico completo de capacidades al actuar, independientemente de las limitaciones políticas que pudieran imponerse, que deben entenderse como de carácter temporal según la óptica del liderazgo de turno. Tanto las operaciones ciberespaciales ofensivas como las operaciones de información en el ciberespacio empleadas como tácticas de ataque proactivas son necesarias para la ciberdefensa, incluso con una postura estrategia defensiva; y ambas son válidas en el actual entorno de competencia continua internacional sin regular y sin consensos. Al mismo tiempo, las ciberoperaciones de explotación son vitales para poder contar con la anticipación y alerta estratégicas necesarias para poder absorber y minimizar los embates del adversario.

2º) La actuación del IM de la República Argentina en la ciberdefensa se encuentra limitada por el marco legal vigente. Este no solo condiciona su ámbito de operación sino también restringe el desarrollo de sus capacidades en función de una postura estratégica mal interpretada. Por un lado, sus FFAA no pueden involucrarse en asuntos de seguridad interior y las operaciones de inteligencia deben focalizarse sólo en aspectos militares. Por otro lado, la “naturaleza defensiva” de su actitud estratégica le impide el desarrollo de todas las capacidades en su máximo potencial.

3º) La ciberdefensa desde una perspectiva de seguridad nacional en sentido amplio debería considerar una organización integral e interagencial para ser más eficaz y eficiente en su faz operacional. Esto implicará contar con una estructura de Ciberpoder Nacional con unidad de comando, amparada por un marco legal al más alto nivel y bajo una autoridad de ejecución con control operacional sobre todos los actores con competencia en el ciberespacio de jurisdicción nacional, que permita optimizar la utilización de todos los recursos que tiene el Estado basado en una relación cívico-militar madura y sin sesgos.

4º) Esta organización podría iniciarse bajo la estructura del Comando Conjunto de Ciberdefensa, por haber sido el IM de la nación, por su preparación y aptitudes, el pionero en operacionalizar e implementar históricamente numerosas iniciativas por necesidad del país.

5º) Los desafíos de cara al futuro para nuestra Nación son enormes, y el diseño de la nueva estructura demandará considerar en detalle los factores del MIRILADO (Medios,

Información, Recursos Humanos, Infraestructura, Logística, Adiestramiento, Doctrina y Organización) que serán esenciales para el desarrollo de capacidades para la ciberdefensa y ciberseguridad integradas.

De esta manera se da por cumplimentado el tercer objetivo específico, y se concluye como respuesta a la hipótesis planteada que la República Argentina necesitará desarrollar capacidades cibernéticas que le permitan al IM la libertad de acción suficiente para conducir operaciones efectivas en el ciberespacio del tipo defensivas, ofensivas, de explotación, o de información, para lograr efectos físicos, digitales o cognitivos que permitan garantizar la seguridad de las infraestructuras críticas asignadas, sostener el Comando y Control propio, degradar el del enemigo, complementar el esfuerzo operacional de proyección de poder militar en los dominios cinéticos o en el espectro electromagnético, o accionar en cumplimiento de los objetivos estratégicos asignados.

Para finalizar, y a modo de reflexión, la naturaleza de la guerra no ha cambiado pese al avance de la tecnología, pero si lo ha hecho su carácter, en dónde el ciberespacio irrumpe como habilitador de un nuevo ámbito de combate o competencia continua donde los efectos pueden no ser tan notorios hoy, pero con seguridad serán mucho más significativos mañana. Dependerá de nuestra decisión como país de tomar una actitud proactiva y actuar en consecuencia, o esperar a una catástrofe cibernética - como indicaba Andress - que nos obligue al cambio.

BIBLIOGRAFÍA

AFDP 3-12. (1 de Febrero de 2023). *doctrine.af.mil*. Recuperado el 1 de Agosto de 2023, de https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-12-Cyberspace-Ops/

AGD. (2023). *defense.gov.au*. Recuperado el 21 de Julio de 2023, de https://www.defence.gov.au/about/strategic-planning/defence-cyber-security-strategy

Aguilar Antonio, J. M. (Enero de 2021). *Estudios Internacionales*. Recuperado el 20 de Julio de 2023, de https://revistaei.uchile.cl/index.php/REI/article/view/57067/

Alexander, C. (11 de Marzo de 2022). Recuperado el 4 de Octubre de 2023, de https://theconversation.com/ukraine-is-well-ahead-in-the-global-battle-for-hearts-and-minds-but-russia-knew-this-would-happen-179043

Amnesty. (21 de Diciembre de 2022). Obtenido de https://www.amnesty.org/en/latest/news/2022/12/ukraine-devastating-power-cuts-undermining-civilian-life-as-christmas-approaches/

Andress, J., & Winterfield, S. (2011). *Cyber Warfare.* Waltham: Elsevier.

Angstrom, J. (2005). Introduction. Debating the nature of modern war. En I. Duyvesteyn, *Rethinking the Nature of War* (págs. 1-27). Londres, Reino Unido: Taylor and Francis.

Anónimo. (2020). *History-computer.com*. Recuperado el 19 de Octubre de 2020, de https://history-computer.com/Internet/Birth/Licklider.html

Anónimo. (30 de Junio de 2020). La oposición rechazó la reforma militar que impulsa el Gobierno. *Infobae*. Obtenido de https://www.infobae.com/politica/2020/06/30/la-oposicion-rechazo-la-reforma-militar-que-impulsa-el-gobierno/

Anónimo. (12 de Agosto de 2020). *Noticias de Navarra*. Obtenido de https://www.noticiasdenavarra.com/actualidad/politica/2020/08/12/alemania-abre-agencia-velara-ciberseguridad/1069752.html

Anónimo. (22 de Febrero de 2021). *Infotecs*. Recuperado el 27 de Septiembre de 2021, de https://infotecs.mx/blog/tecnologia-operacional.html

Anónimo. (s.f.). *askanydifference.com*. Recuperado el 10 de octubre de 2021, de https://askanydifference.com/difference-between-ict-and-it/

Anónimo. (s.f.). *differencebetween.net*. Recuperado el 10 de Octubre de 2021, de http://www.differencebetween.net/technology/difference-between-ict-and-it/

Argentina, B. O. (23 de Febrero de 2018). Recuperado el 23 de Septiembre de 2021, de https://www.boletinoficial.gob.ar/detalleAviso/primera/179214/20180223

Argentina, G. (26 de Abril de 1988). Recuperado el 27 de Julio de 2023, de https://www.argentina.gob.ar/normativa/nacional/ley-23554-20988/actualizacion

Argentina, G. (18 de Diciembre de 1991). Obtenido de https://www.argentina.gob.ar/normativa/nacional/ley-24059-458/texto

Argentina, G. (3 de Diciembre de 2001). Recuperado el 27 de Julio de 2023, de https://www.argentina.gob.ar/normativa/nacional/ley-25520-70496/actualizacion

Argentina, G. (29 de Noviembre de 2006). Recuperado el 27 de Julio de 2003, de https://www.argentina.gob.ar/normativa/nacional/decreto-1691-2006-122503/texto

Argentina, G. (19 de Enero de 2015). Recuperado el 24 de Septiembre de 2023, de https://www.argentina.gob.ar/normativa/nacional/decreto-2645-2014-240966/texto

Argentina, G. (29 de Octubre de 2019). Recuperado el 24 de Septiembre de 2023, de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1380-2019-330819/texto

Argentina, G. (19 de Julio de 2021). Recuperado el 24 de Septiembre de 2023, de https://www.argentina.gob.ar/normativa/nacional/decreto-457-2021-352107/texto

Argentina, G. (30 de Enero de 2023). Recuperado el 24 de Septiembre de 2023, de https://www.argentina.gob.ar/noticias/actualizacion-de-la-politica-de-ciberdefensa-y-creacion-de-dos-areas-para-la-supervision-y#:~:text=Esta%20resoluci%C3%B3n%20%28Nro.%20105%2F2023%29%20se%20inscribe%20en%20el,de%20la%20Pol%C3%ADtica%20Militar%20de%20la

Argentina, G. (2023). Recuperado el 25 de Septiembre de 2023, de https://www.argentina.gob.ar/jefatura/innovacion-publica/telecomunicaciones-y-conectividad/grupo-de-trabajo-de-servicios-de-6

Argentina, G. d. (8 de Octubre de 2020). Obtenido de https://www.argentina.gob.ar/noticias/el-presidente-recibio-los-organismos-integrantes-del-sistema-de-inteligencia-nacional

Argentina, G. d. (30 de Noviembre de 2022). Recuperado el 17 de Septiembre de 2023, de https://www.argentina.gob.ar/noticias/nueva-reunion-del-comite-nacional-de-ciberseguridad

Argentina, G. d. (2023). Recuperado el 17 de Septiembre de 2023, de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/objetivos-de-la-direccion#:~:text=Las%20acciones%20primarias%20que%20tiene%20la%20Direcci%C3%B3n%20Nacional,incidentes%20de%20seguridad%20inform%C3%A1tica%20

Argentina, G. d. (7 de Septiembre de 2023). *argentina.gob.ar*. Recuperado el 16 de Septiembre de 2023, de https://www.argentina.gob.ar/noticias/taiana-inauguro-la-red-de-fibra-optica-de-la-defensa-que-brindara-comunicaciones-seguras

Argentina.gob.ar. (2021). *argentina.gob.ar*. Recuperado el 2021 de Septiembre de 20, de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-internet-de-las-cosas

Arpón, M., & Berás, A. (19 de Septiembre de 2020). *eldiario.es*. Recuperado el 11 de Octubre de 2021, de https://www.eldiario.es/red/que-es/tecnologia-5g_1_6231620.html

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars - The Future of Terror, Crime, and Militancy.* Santa Mónica: National Defense Research Institute - RAND.

Arteaga, F. (10 de Septiembre de 2019). *Real Instituto elcano*. Recuperado el 2020 de Mayo de 23, de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari92-2019-arteaga-capacidades-ofensivas-disuasion-y-ciberdefensa

Aselcom. (18 de Agosto de 2020). *aselcom.com*. Recuperado el 10 de Octubre de 2021, de https://www.aselcom.com/2020/08/18/realidad-virtual-vs-realidad-aumentada/

Barea, A. (2018). El control sobre los "global commons" en el mundo actual. *Military Review*, 24-29.

Barro, A. (29 de Septiembre de 2021). *elconfidencial.com*. Recuperado el 10 de Octubre de 2021, de https://www.elconfidencial.com/mundo/2021-09-29/drones-afganistan-nueva-guerra-remota-joe-biden_3296947/

Bartolomé, M. C. (2006). *La seguridad interncional en el siglo XXI, más allá de Westfalia y Clausewitz.* Chile: ANEPE.

Bateman, J., Beecroft, N., & Wilde, G. (19 de Diciembre de 2022). *carnegieendowment.org*. Recuperado el 21 de Julio de 2023, de https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667

Bauman, Z. (2006). Obtenido de https://www.lecturalia.com/libro/18018/vida-liquida

Beecroft, N. (3 de Noviembre de 2022). *carnegieendowment.org*. Recuperado el 21 de Julio de 2023, de https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322

Benítez, J. J. (8 de Octubre de 2020). Pricipios y Sistemas de Gestión de la Ciberdefensa. Respuesta "preventiva". CABA, Buenos Aires, Argentina.

Bertoldi, E. (2020). Importancia del desarrollo de la tecnología cuántica para la seguridad (ofensiva y defensiva) de las redes de comando y control de la FAA. *Revista de la Escuela Superior de Guerra Aérea*(245), 34-42.

Beskow, D., & Carley, K. (2019). La ciberseguridad social. Un ámbiro emergente de la seguridad nacional. *Military Review*, 23-33.

BID. (2016). *Informe Ciberseguridad.* Banco Interamericano de Desarrollo.

Bodnar, J., Schafer, B., & Soula, E. (24 de Febrero de 2023). *GMC*. Obtenido de https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/

Borghello, L. C. (05 de Noviembre de 2020). Los estados mas famosos y peligrosos desarrolladores de malware ATP. CABA, Buenos Aires, Argentina.

Boulanin, V., & Verbruggen, M. (Noviembre de 2017). *sipri.org.* Obtenido de https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf

Brainly. (17 de Marzo de 2022). Obtenido de https://brainly.lat/tarea/60876193

Brockmann, K., Bauer, S., & Boulanin, V. (Marzo de 2019). *sipri.org.* Recuperado el 10 de Octubre de 2021, de https://sipri.org/sites/default/files/2019-03/sipri2019_bioplusx_0.pdf

Burgess, M. (23 de Marzo de 2022). Recuperado el 22 de Septiembre de 2023, de https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

Cañete, P. (2020). El comando de ciberdefensa alemán. Un claro ejemplo de integración. *Vision Conjunta*, 14-20.

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

CCDCOE. (2023). *ccdcoe.org*. Recuperado el 25 de Julio de 2023, de https://ccdcoe.org/research/tallinn-manual/

CCNA. (2023). Obtenido de https://ccnadesdecero.es/que-es-tcp-ip/

Cherry, L., & Pascucci, P. (27 de Enero de 2023). Recuperado el 26 de Julio de 2023, de https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/

Cherry, L., & Pascucci, P. (27 de Enero de 2023). *americanbar.org*. Recuperado el 26 de Julio de 2023, de https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/

Ciberdefensa, C. C. (2023). *ffaa.mil.ar*. Recuperado el 17 de Septiembre de 2023, de https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/mision.html

Clay, W. (2009). Cyber Crime. En F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (págs. 1-22). Washington DC: National Defense University Press.

Colom Piella, G. (Junio de 2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova, 10*(10), 77-90.

Colom Piella, G. (2018). Guerras Híbridas - Cuando el concepto lo es todo. *Revista Ejercito*, 38-44.

Colom Piella, G. (Junio de 2018). Guerras Híbridas.Cuando el concepto lo es todo. *Revista Ejército*(927), 38-44.

CompTIA. (2023). Recuperado el 25 de Septiembre de 2023, de https://www.comptia.org/content/guides/what-is-data-analytics

Crawford, S. (14 de Abril de 2022). Obtenido de https://abcnews.go.com/Politics/preemptive-public-us-strikes-winning-intelligence-war-russia/story?id=84015518

Cronin, A. K. (2006). Cyber Mobilization: The New Levée en Masse. *Parameters*, 77-87.

CYBERCOM. (23 de Marzo de 2023). Recuperado el 4 de Octubre de 2023, de https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/

De Nimrod, S. (8 de Febrero de 2018). *cyberark.com*. Recuperado el 14 de Octubre de 2021, de https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack

de Paula Romero Garat, C. d. (01 de Febrero de 2018). *infodefensa.com*. Recuperado el 20 de Septiembre de 2021, de http://www.infodefensa.com/es/2018/02/01/opinion-adaptacion-defensa-fuerzas-armadas-concepto-industria.php

De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *ARTIFICIAL INTELLIGENCE AND THE FUTURE OF DEFENSE:STRATEGIC IMPLICATIONS FOR SMALL- AND MEDIUM-SIZED FORCE PROVIDERS.* The Hague: The Hague Centre for Strategic Studies (HCSS).

De Vergara, E. (3 de Septiembre de 2020). Las operaciones de información en el espacio cibernético. CABA, Buenos Aires, Argentina.

de Vergara, E., & Trama, G. A. (2017). *Operaciones Militares Cibernéticas.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Decreto PEN Nº 727, R. d. (12 de Junio de 2006). *argentina.gob.ar*. Recuperado el 27 de Julio de 2023, de https://www.argentina.gob.ar/normativa/nacional/decreto-727-2006-116997

Defensa, M. d. (2015). *Libro Blanco.* Ciudad Autónoma de Buenos Aires: Ministerio de Defensa.

Defensa, M. d. (2023). *Plan Plurianual de Ciencia, Tecnología, Innovación y Producción para la Defensa.* CABA: Secretaría de Investigación, Política Industrial y Producción para la Defensa.

Defense Industries. (11 de Julio de 2016). *blog.defense-industries.com*. Recuperado el 20 de Septiembre de 2021, de http://blog.defence-industries.com/significant-scenarios-introduced-in-ict-era-for-defense-industry/

Defense Industries. (2023). *defense-industries.com*. Recuperado el 23 de Julio de 2023, de http://blog.defence-industries.com/significant-scenarios-introduced-in-ict-era-for-defense-industry/

Delerue, F., Desforges, A., & Gery, A. (23 de Abril de 2019). *warontherocks.com*. Recuperado el 22 de Julio de 2023, de https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

Deloitte. (2023). Obtenido de https://www2.deloitte.com/cl/es/pages/manufacturing/articles/que-es-la-industria-40.html

Demarest, C. (6 de Enero de 2023). *C4ISRNET.com*. Recuperado el 20 de Julio de 2023, de https://www.c4isrnet.com/cyber/2023/01/06/pentagon-hosts-five-eyes-partners-for-zero-trust-cybersecurity-talks/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

Derleth, J. (2021). La guerra de nueva generación de Rusia. *Military Review*, 13-26.

Dickinson, K. (31 de Mayo de 2021). *bigthink.* Recuperado el 28 de Septiembre de 2021, de https://bigthink.com/the-future/10-emerging-technologies-change-world/

Dinatale, M. (30 de Junio de 2020). El Gobierno prepara una profunda reforma militar para limitar el accionar de las Fuerzas Armadas. *Infobae*.

DOD, E. (2018). *media.defense.com.* Obtenido de https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Dodge, S., & Karam, L. (6 de Mayo de 2017). *arvix.org.* Obtenido de https://arxiv.org/pdf/1705.02498.pdf

Douhet, G. (2019). *The command of the air.* Alabama: Air University Press.

DQI, B. (27 de Julio de 2012). *dqindia.com*. Recuperado el 17 de Septiembre de 2023, de https://www.dqindia.com/cyberspace-global-commons-the-challenges-1/

EACNUR. (18 de Octubre de 2017). *eacnur.org*. Recuperado el 20 de Julio de 2023, de https://eacnur.org/es/actualidad/noticias/emergencias/africa-el-continente-con-mas-paises-en-conflicto

EC-Council University. (27 de Febrero de 2023). *eccu.edu*. Recuperado el 23 de Julio de 2023, de https://www.eccu.edu/blog/technology/the-latest-cybersecurity-technologies-and-trends/#:~:text=What%20is%20the%20latest%20technology,Cloud%20Security%2C%20and%20IoT%20Security

Efrony, D. (16 de Julio de 2021). Recuperado el 22 de Septiembre de 2023, de https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

Eissa, S., Gastaldi, S., Poczynok, I., & Zacarías Di Tullio, E. (2014). unq.edu.ar. *Revista de las Ciencias Sociales*, 181-197. Obtenido de http://www.unq.edu.ar/advf/documentos/593955b92ae2c.pdf

ENISA. (2023). *enisa.europea.eu*. Recuperado el 22 de Julio de 2023, de https://www.enisa.europa.eu/topics/national-cyber-security-strategies

Enzensberger, H. (1996). *Perspectivas de guerra civil.* Estados Unidos: Anagrama. Recuperado el 22 de Junio de 2020, de https://elpais.com/diario/1993/11/28/cultura/754441217_850215.html

ESGCFFAA. (2023). Obtenido de https://www.esgcffaa.edu.ar/esp/oac-proyecto.php

España. (11 de Junio de 2020). *defensa.gob.es.* Obtenido de https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf

Evans, C. (15 de Mayo de 2020). *press.armywarcollege.edu.* Obtenido de https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1017&context=parameters

Feliu Ortega, L. (2012). La ciberseguridad y la ciberdefensa. En M. d. CESEDEN, *El ciberspacio nuevo escenario de confrontacion* (Vol. 126, pág. 41). Ministerio de Defensa de España.

Fernandez Vega, J. (2005). *Las guerras de la política - Clauzewitz de Maquiavelo a Perón.* Buenos Aires: Edhasa.

FM 3-38, U. A. (2014). *Cyber Electromagnetic Activities.* Washington: US Army.

Fusaro, R. (03 de Agosto de 2021). *frba.utn.edu.ar*. Recuperado el 14 de Octubre de 2021, de https://www.frba.utn.edu.ar/el-futuro-de-la-industria-argentina-es-trabajar-con-tecnologia-5g/

Galloway, A. (6 de Agosto de 2020). *The Sidney Morning Herald*. Obtenido de https://www.smh.com.au/politics/federal/cyber-spy-agency-to-be-called-in-to-protect-critical-infrastructure-20200806-p55j6m.html

Gershgorn, D. (31 de Mayo de 2016). *popsci.com*. Obtenido de https://www.popsci.com/this-is-difference-one-year-makes-in-artificial-intelligence-research/

Gershgorn, D. (26 de Julio de 2017). Obtenido de https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world

Gibney, A. (Dirección). (2016). *Zero Days* [Película].

Giles, K. (2016). *Manual de guerra de información rusa.* Roma: OTAN.

Gobierno de Argentina. (2023). *argentina.gob.ar*. Recuperado el 13 de Septiembre de 2023, de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-internet-de-las-cosas

Gorrín, H. (26 de Mayo de 2020). Obtenido de https://tictoecw.blogspot.com/2020/05/concepto-de-tic.html

GOV.UK. (27 de Mayo de 2021). *gov.uk*. Recuperado el 22 de Julio de 2023, de https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data

GOV.UK. (15 de Diciembre de 2022). Obtenido de https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Gov.UK, H. G. (1 de Noviembre de 2016). *www.gov.uk*. Recuperado el 3 de Marzo de 2020, de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf

Graber, S. (20 de Julio de 2021). *cyber.forum.yale.edu*. Recuperado el 30 de Julio de 2023, de https://www.cyber.forum.yale.edu/blog/2021/7/20/defend-forward-adapting-offense-and-defense-strategy-to-cyberspace

Gray, C. S. (2007). *Another Blody Century - Future Warfare.* Phoenix: Phoenix Press.

Haig, Z. (2015). Electronic Warfare in Cyberspace. *Security and Defence Quarterly*, 22-35.

Hdez, A. (2021). *economiatic.com*. Recuperado el 2021 de Septiembre de 20, de https://economiatic.com/concepto-de-tic/

Heller, K. (2021). *In Defense of Pure Sovereignty* . Recuperado el 26 de Julio de 2023, de https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils

Herranz, A. (26 de Mayo de 2021). *xataka.com*. Obtenido de https://www.xataka.com/pro/digital-twins-que-sirven-cuales-beneficios-problemas-gemelos-digitales

Hoehn, J. R. (21 de Enero de 2022). Recuperado el 18 de Julio de 2023

Hoehn, J. R. (21 de Enero de 2022). Recuperado el 18 de Julio de 2023, de https://www.bing.com/ck/a?!&&p=72dc49fe274dd1fbJmltdHM9MTY4OTYzODQwMCZpZ3VpZD0wOGI1MmRjNi0yYzMyLTYyMmYtMDU1MC0zYzQ1MmRlZjYzMmImaW5zaWQ9NTE3NQ&ptn=3&hsh=3&fclid=08b52dc6-2c32-622f-0550-3c452def632b&psq=confresional+research+service+jadoc2&u=a1aHR0cHM6Ly9jc

Hoehn, J. R. (21 de Enero de 2022). Recuperado el 24 de Julio de 2023, de https://crsreports.congress.gov/product/pdf/IF/IF11493

Hoehn, J. R. (23 de Junio de 2022). Recuperado el 24 de Julio de 2023, de https://sgp.fas.org/crs/weapons/IF11659.pdf

Hoehn, J. R. (15 de Febrero de 2022). *Congressional Research Service.* Recuperado el 19 de Julio de 2023, de https://crsreports.congress.gov/product/pdf/IF/IF11866

Hoffman, F. (2009). Hybrid Warfare and Challenges. (N. D. Press, Ed.) *Joint Force Quarterly (JFQ), 1st Quarter*(52), 34-39.

Hollis, D. (14 de Junio de 2021). *carnegieendowment.org*. Recuperado el 26 de Julio de 2023, de https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Hüttenrauch, M. (7 de Agosto de 2016). *ias.informatik.* Obtenido de https://www.ias.informatik.tu-darmstadt.de/uploads/Site/EditPublication/Httenrauch_MSc2016.pdf

IADF. (2020). *Fundación Interamericana de Defensa*. Recuperado el 4 de Noviembre de 2020, de https://www.iadfoundation.org/es/ciberdefensa/

IADF. (2023). *iadfoundation.org*. Recuperado el 20 de Julio de 2023, de https://www.iadfoundation.org/es/ciberdefensa/

IAT. (2021). *iat.es*. Recuperado el 11 de Octubre de 2021, de https://iat.es/tecnologias/big-data/

IAT. (2021). *iat.es*. Recuperado el 10 de Octubre de 2021, de https://iat.es/tecnologias/realidad-aumentada/diferencias-realidad-virtual/

IBM. (23 de Octubre de 2021). *ibm.com*. Recuperado el 23 de Octubre de 2021, de https://www.ibm.com/es-es/cloud/learn/cloud-computing-gbl

IGF. (2023). Recuperado el 22 de Septiembre de 2023, de https://www.intgovforum.org/en

innovacionenunclick. (2023). Obtenido de https://innovacionenunclick.blogspot.com/p/seguridad_15.html

Internet Society. (9 de Junio de 2022). *internetsociety.org*. Recuperado el 20 de Julio de 2023, de https://www.internetsociety.org/es/news/comunicados-de-prensa/2022/internet-society-se-compromete-a-ampliar-el-acceso-a-internet-en-africa/

Intini, G. A. (15 de Octubre de 2020). El Comando Conjunto de Ciberdefensa. CABA, Buenos Aires, Argentina.

Jacobsen, J. (Junio de 2014). *www.diis.dk.*

Jasper, S. (2015). *Strategic Studies Quarterly*, 60-85.

Jasper, S. (2015). Disuadir a los maliciosos. Comportamiento en el ciberespacio. *Strategic Studies Quarterly*, 60-85. Obtenido de https://www.jstor.org/stable/26270834

JID. (2020). *Guía de Ciberdefensa.* Gobierno de Canadá.

JID. (2020). *jid.org.* Recuperado el 21 de Septiembre de 2023, de https://www.jid.org/ciberdefensa-2/

JOAC, J. O. (17 de Enero de 2012). Recuperado el 24 de Septiembre de 2023, de https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf

Joint Chiefs of Staff. (2022). *JP1 Joint Warfighting.* Washington DC: Joint Electronic Library Plus.

Joint Chiefs of Staff Publication, 3.-1. (8 de Junio de 2018). Cyberspace Operations. EE.UU.

Jordán, J. (2018). El conflicto internacional en la zona gris. *Revista española de ciencia política*(48), 129-151.

JP1. (29 de Junio de 2020). *jcs.mil.* Recuperado el 12 de Agosto de 2023, de https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/Capstone-Series/

Kaldor, M. (2012). *New and old wars - Organizad violence in a global era* (3ra ed.). Stanford: Stanford University Press.

Kandiko, U. (24 de Abril de 2018). *cxo-community.com*. Recuperado el 14 de Octubre de 2021, de https://www.cxo-community.com/2018/04/armas-ciberneticas-sistemas-fuera-de.html

Kleinman Ruiz, I. E. (Octubre de 2019). *researchgate.net.* Recuperado el 01 de Noviembre de 2021, de https://www.researchgate.net/profile/Ignacio-Kleinman-Ruiz/publication/337758188_Computacion_cuantica_Aplicaciones_practicas_que_la_computacion_clasica_no_puede_solucionar/links/5de8ae094585159aa462d589/Computacion-cuantica-Aplicaciones-practicas-que-la-c

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. En F. D. Kramer, *Cyberpower & National Security* (págs. 24-42). University of Nebraska Press.

Kugler, R. L. (2009). *Deterrence of Cyber Attacks.* Washington DC: Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz.

Kuz, A., & Ríos, J. (1 de Octubre de 2020). Tecnologías de Redes. CABA, Buenos Aires, Argentina.

Lazaruk, K., & Tuters, M. (19 de Diciembre de 2022). Obtenido de https://www.eurozine.com/weaponized-osint/

Levite, A. (18 de Abril de 2023). *Carnegie Endowment for International Peace*. Recuperado el 18 de Julio de 2023, de https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544

Liang, Q., & Xiangsui, W. (2004). *Unrestricted Warfare.* Beijing: Filament Books Inc.

Libicki, M. C. (2009). Ciberdefensa. En M. C. Libicki, *Cyberdeterrence and Cyberwar* (págs. 159-175). Santa Mónica: Rand Corporation.

Lind, W. (15 de Enero de 2004). *Antiwar.com*. Recuperado el 22 de Junio de 2020, de https://original.antiwar.com/lind/2004/01/15/understanding-fourth-generation-war/

Lonsdale, D. J. (2004). *The Nature of War in the Information Age: Clausewitzian Future*. Londres: Frank Class.

Lopez, P. (16 de Marzo de 2022). *tn.com.ar*. Recuperado el 12 de Agosto de 2023, de https://tn.com.ar/economia/2022/03/16/la-letra-chica-del-acuerdo-por-el-que-la-argentina-ingreso-a-la-ruta-de-la-seda-china/

Macri, K. (25 de Abril de 2022). Obtenido de https://governmentciomedia.com/zero-trust-essential-and-integral-jadc2

Marr, B. (8 de Agosto de 2017). Obtenido de https://www.forbes.com/sites/bernardmarr/2017/08/08/the-amazing-ways-how-google-uses-deep-learning-ai/?sh=13f36a0e3204

Marr, B. (9 de Abril de 2018). *forbes*. Obtenido de https://www.forbes.com/sites/bernardmarr/2018/04/09/the-amazing-ways-google-uses-artificial-intelligence-and-satellite-data-to-prevent-illegal-fishing/?sh=18d9e0d71c14

Martinez Nuñez, J. (17 de Septiembre de 2020). Amenazas desde el Ciberespacio. Madrid, España.

Masarellas, M. (24 de Febrero de 2022). *AthenaLab*. Recuperado el 17 de Octubre de 2021, de https://athenalab.org/rusia-ucrania-y-la-doctrina-gerasimov/

master-bigdata. (2023). Obtenido de https://master-bigdata.com/origen-big-data/

Mattis, J., & Hoffman, F. (2005). Future Warfare: The Rise of Hybrid Wars. *US Naval Institute, 132*.

McGuinness, D. (6 de Mayo de 2017). *bbc.com*. Recuperado el 11 de Septiembre de 2020, de https://www.bbc.com/mundo/noticias-39800133

MD31-M-07. (2014). *Manual de Doctrina Militar de Ciberdefensa EMC RFB.* Brasilia: Ministerio de Defensa.

Messe, A., & Medairy, B. (2018). El futuro de la ciberdefensa ... Pasar a la ofensiva. *LA REVISIÓN DE LA DEFENSA CIBERNÉTICA*, 37-40.

Microsoft. (27 de Abril de 2022). Obtenido de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Microsoft. (2023). Recuperado el 30 de Septiembre de 2023, de https://www.microsoft.com/en-us/security/business/zero-trust#:~:text=Instead%20of%20assuming%20everything%20behind%20the,us%20to%20%E2%80%9Cnever%20trust%2C%20always%20verify.%E2%80%9D.&text=Instead%20of%20assuming%20everything,%E2%80%9Cnever%20trust%2C%2

Microsoft. (20 de Enero de 2023). Recuperado el 4 de Octubre de 2023, de https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/

Miguel, H. (25 de Agosto de 2020). Las Armas y el Ciberespacio. CABA, Bs As, Argentina.

MilitaryReview. (Marzo de 2016). Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi5iZPx4PCBAxVkGLkGHf4xCNUQFnoECBMQAQ&url=https%3A%2F%2Fwww.armyupress.army.mil%2FPortals%2F7%2Fmilitary-review%2FArchives%2FSpanish%2FMilitaryReview_20160430_art010SP

Modernización, M. d. (s.f.). *Secretaría de Tecnologías de la Información y las Comunicaciones.* Recuperado el 2021 de Septiembre de 20, de https://www.argentina.gob.ar/sites/default/files/paperbenchmarkinternacional-iot.pdf

Moerbe, W. (2017). Maneras más curiosas y sutiles de matar. El proceso de operaciones en la guerra futura. *Military Review*, 80-88.

Moes, T. (Julio de 2023). *softwarelab.org*. Obtenido de https://softwarelab.org/es/blog/que-es-la-caza-de-amenazas/

Monaghan, S. (2019). Countering Hybrid Warfare. *PRISM, 8*(2), 82-89.
Moresi, A., Motta, G., Trama, G., Saldanha Walker, M., & Amaya, C. (2022). *Operaciones en el Ambiente de la Información.* Buenos Aires: Visión Conjunta.
Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom.* Nueva York: Public Affairs.
Motta, G. (2022). Obtenido de https://www.politicayestrategia.cl/index.php/rpye/article/view/996
Münkler, H. (2005). *Nuevas y viejas guerras: asimetría y privatización de la violencia.* Madrid: Siglo XXI.
Murua, H. (2 de Septiembre de 2023). *clarin.com*. Recuperado el 3 de Septiembre de 2023, de https://www.clarin.com/economia/emprendedores-argentinos-carrera-espacial_0_litVqW8Tgx.html
NIC, A. (Mayo de 2018). *nic.ar*. Recuperado el 2021 de Septiembre de 20, de Dirección Nacional del Registro de Dominios de Internet: https://nic.ar/es/enterate/novedades/que-es-internet
Noujaim, J., & Amer, K. (Dirección). (2019). *The Great Hack* [Película].
Nye Jr, J. (2016). Deterrence and dissuasion in ciberspace. *International Security*, 44-71.
Nye Jr., J. (1 de Enero de 2017). *direct.mit.edu*. Recuperado el 16 de Septiembre de 2023, de https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace
Nye, J. S. (2011). *The Future of Power.* Nueva York: Public Affairs.
OneSpan. (2023). Obtenido de https://www.onespan.com/es/topics/autenticacion-biometrica
Oracle Corporation. (2010). *docs.oracle.com*. Obtenido de Introducción al conjunto de protocolos TCP/IP: https://docs.oracle.com/cd/E19957-01/820-2981/ipov-6/index.html
OTAN. (22 de Junio de 2023). *nato.int*. Recuperado el 22 de Julio de 2023, de https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO%27s%20main%20focus%20in%20cyber%20defence%20is%20to,a%20platform%20for%20political%20consultation%20and%20collective%20action.
Panda. (2021). *pandasecurity.com*. Recuperado el 23 de Octubre de 2021, de http://resources.pandasecurity.com/enterprise/solutions/8.%20WP%20PCIP%20que%20es%20p2p.pdf
Parker, K. L. (2014). El uso del ciberespacio. *Military Review*, 50-59.
PC 00-02. (2015). *Glosario de Términos de Empleo Militar para la Acción Militar Conjunta PC 00-02.* Buenos Aires: Estado Mayor Conjunto.
PC 10-04. (2018). *Planeamiento para la Acción Militar Conjunta - Nivel Estratégico Militar*. Buenos Aires: Estado Mayor Conjunto.
Polyakov, A. (4 de Octubre de 2018). *towardsdatascience*. Obtenido de https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b
Pomerleau, M. (20 de Julio de 2022). Obtenido de https://fedscoop.com/senate-wants-tighter-cyber-electronic-warfare-integration-clarity-on-organizations-for-cyber-ops/
Pons, J. (25 de Mayo de 2021). *defensa.gov.es*. Recuperado el 22 de Julio de 2023, de https://www.defensa.gob.es/comun/slider/2021/05/210525-ciberdefensa-red.html
Preskill, J. (26 de Marzo de 2012). *arxiv.org*. Recuperado el 01 de Noviembre de 2021, de https://arxiv.org/abs/1203.5813v3
RAE. (2023). Recuperado el 25 de Septiembre de 2023, de https://dle.rae.es/inteligencia
RAND. (Febrero de 2016). *rand.org*. Obtenido de https://www.rand.org/topics/cyber-warfare.html
RAND. (2022). *Disrupting Deterrence.* Santa Monica, CA: Rand Corporation.
Redacción. (30 de Julio de 2023). *zona-militar.com*. Obtenido de https://www.zona-militar.com/2023/07/30/luego-de-retrasos-microsoft-entrega-al-ejercito-de-ee-uu-la-nueva-version-del-visor-de-realidad-aumentada-ivas/
Regalado, A. (23 de Octubre de 2018). *tecnologyreview*. Obtenido de https://www.technologyreview.com/2018/10/23/139378/look-how-far-precision-medicine-has-come/

Reguera, J. (18 de Marzo de 2015). *GESI*. Recuperado el 26 de Julio de 2023, de http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

RFNAFB. (2023). Obtenido de https://www.nellis.af.mil/About/High-End-Training/Red-Flag-Nellis/

Robledo, M. (3 de Febrero de 2022). *elanalista.com.ar*. Recuperado el 13 de Agosto de 2023, de https://elanalista.com.ar/la-inteligencia-en-las-operaciones-de-informacion/

Romero Garat, F. d. (26 de Marzo de 2018). *infodefensa.com*. Recuperado el 11 de Octubre de 2021, de https://www.infodefensa.com/texto-diario/mostrar/3118358/aplicacion-defensa-40-tecnologias-informacion-comunicaciones-1

Rugge, F. (11 de Enero de 2018). Obtenido de https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414

Rugge, F. (2020). Cyberspace and Great Powers Competition. En I. R. 2020, *Work in Progress - The end of a World Part II* (págs. 74-76). Milan: A. Colombo and P. Magri .

Russell, A. (2017). *Strategic A2/AD in Cyberspace*. Cambridge: Cambridge University Press.

Saalman, L., Topychkanov, P., Su, F., & Peldán Carlsson, M. (Junio de 2020). *SIPRI*. Recuperado el 30 de Septiembre de 2023, de https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk

Sabbagh, D. (19 de Enero de 2023). Obtenido de https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency

Salesforce. (2021 de Octubre de 2021). *salesforce.com*. Recuperado el 23 de Octubre de 2021, de https://www.salesforce.com/mx/cloud-computing/

SAP. (2021). *sap.com*. Recuperado el 23 de Octubre de 2021, de https://www.sap.com/latinamerica/insights/what-is-blockchain.html

Sayler, K. (14 de Noviembre de 2022). *Congressional Research Service*. Recuperado el 23 de Julio de 2023, de https://crsreports.congress.gov/product/pdf/IF/IF11105

Schelling, T. C. (2008). *Arms and Influence.* Connecticut: New Haven.

Schultz, D., Mariani, J., Jenkins, I., Strickland, F., & Raymond, L. (16 de Julio de 2018). *www2.deloitte.com*. Recuperado el 20 de Septiembre de 2021, de https://www2.deloitte.com/us/en/insights/focus/industry-4-0/reframing-defense-military-readiness.html

Schulze, M., & Kerttunen, M. (Abril de 2023). *ssoar.info.* Recuperado el 3 de Octubre de 2023, de https://www.ssoar.info/ssoar/bitstream/handle/document/88112/88112_1.pdf?sequence=1

Scroxton, A. (18 de Enero de 2023). Obtenido de https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022

SECPHO. (2021). *secpho.org*. Recuperado el 3 de Noviembre de 2021, de https://www.secpho.org/robotica-y-drones/

sekoia. (2023). Obtenido de https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/

Serbin Pont, A. (03 de Julio de 2020). Fuerzas Armadas del siglo pasado. *Perfil*. Obtenido de https://www.perfil.com/noticias/opinion/fuerzas-armadas-siglo-pasado.phtml

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly, 5*(2), 95-112.

Shu, C. (28 de Noviembre de 2018). *techcrunch*. Obtenido de https://techcrunch.com/2018/11/27/amazons-newest-service-uses-machine-learning-to-extract-medical-data-from-patient-records/

Slayton, R. (2017). *direc.mit.edu.* Recuperado el 30 de Julio de 2023, de https://direct.mit.edu/isec/article-abstract/41/3/72/12149/What-Is-the-Cyber-Offense-Defense-Balance?redirectedFrom=fulltext#.WKICNm8rK70

Smith, R. (Diciembre de 2006). Métodos de guerra. *International Review of the Red Cross*(864), 1-11. Obtenido de https://www.icrc.org/es/doc/assets/files/other/irrc_864_smith.pdf

Sorrentino, C. P. (22 de Octubre de 2020). Conferencia: Ciberespacio y Ciberdefensa . CABA, Buenos Aires, Argentina.

Strout, N. (2 de Junio de 2020). *C4ISRNET*. Obtenido de https://www.c4isrnet.com/battlefield-tech/it-networks/2020/06/02/air-force-to-dole-out-nearly-1-billion-for-abms-development/

Studocu. (2023). Obtenido de https://www.studocu.com/es-mx/document/universidad-autonoma-de-nuevo-leon/administracion-de-redes/protocolos-de-red-modelos-y-sus-capas-protocolo-osi-y-tcpip/16848039

Swan, D. (15 de Septiembre de 2023). *cscis.org*. Recuperado el 01 de Octubre de 2023O, de https://cscis.org/2023/09/16/russia-vs-ukraine-russia-focuses-attacks/

Technexus. (22 de Junio de 2021). *technexus.com*. Recuperado el 12 de Agosto de 2023, de https://tecknexus.com/5g-network/current-state-of-open-ran-americas/

Tello, A. (2011). Actualidad de la guerra y conflictos de cuarta generación. *Relaciones Internacionales, 20*(40), 321-335.

Thakkar, D. (2021). *bayometric.com*. Recuperado el 10 de Octubre de 2021, de https://www.bayometric.com/authentication-vs-authorization-biometric-technology/

Theohary, C. A. (14 de Enero de 2020). *Congressional Research Service*. Recuperado el 22 de Mayo de 2020, de https://fas.org/sgp/crs/natsec/IF10537.pdf

TICNegocios. (2023). Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/realidad-virtual-vs-realidad-aumentada-los-conceptos-clave/

Todorov, N., & Encheva, B. (2020). Aplication of Industry 4.0 in military production in Bulgaria. En I. Conference, *Process Management and Scientific Development* (págs. 121-130). Birmingham: Novotel Birmingham Centre.

Tomé, J., Belson, D., & Berdan, K. (23 de Febrero de 2023). Obtenido de https://blog.cloudflare.com/one-year-of-war-in-ukraine/

Toro Hardy, A. (20 de Junio de 2022). *https://politica-china.org/*. Recuperado el 20 de Julio de 2023, de https://politica-china.org/areas/politica-exterior/estados-unidos-y-sus-aliados-frente-a-china#:~:text=No%20resultar%C3%ADa%20exagerado%20decir%2C%20por%20tanto%2C%20que%20los,inteligencia%20de%20los%20Cinco%20Ojos%20y%20el%20AUKUS.

Torres, V. (8 de Diciembre de 2019). *ceinaseg.com*. Obtenido de https://ceinaseg.com/ciberseguridad-y-disuasion-una-estrategia-inadecuada-para-el-ciberespacio/

Trama, G. (2017). Operaciones cibernéticas. *Visión Conjunta*, 54-59.

Trama, G., Guerrero, G., & De Vergara, E. (2019). *Visión Conjunta*, 3-8.

U24 Asia. (15 de Julio de 2019). *Urgente 24*. Obtenido de https://urgente24.com/mundo/u24-asia/rusia-advierte-china-los-limites-de-una-alianza-militar-en-asia

Ucrania. (26 de Agosto de 2022). *gov.ua*. Obtenido de https://cip.gov.ua/en/news/bilshe-tisyachi-raziv-atakuvali-ukrayinu-vorozhi-khakeri-za-chas-viini

UIT. (2023). Recuperado el 22 de Septiembre de 2023, de https://www.itu.int/es/about/Pages/vision.aspx

UIT-T Y.2060, U. I. (Junio de 2012). *Unión Internacional de Telecomunicaciones.* Recuperado el 2021 de Septiembre de 20, de file:///C:/Users/pc/Downloads/T-REC-Y.2060-201206-I!!PDF-S.pdf

UN Security Sector Reform Task Force. (2012). *DCAF - Geneva Centre for Security Sector Governance*. Obtenido de https://securitysectorintegrity.com/defence-management/policy/

UNCTAD. (2021). *Informe sobre Tecnología e Información 2021 - Panorama General.* Nueva York: Naciones Unidas.

UNCTAD, C. d. (2021). *Informe sobre tecnología e innovavión 2021*. Ginebra: Naciones Unidas.
USCongress. (18 de Julio de 2023). Obtenido de https://www.congress.gov/118/crec/2023/07/18/169/123/CREC-2023-07-18-pt1-PgS3005-2.pdf
USCYBERCOM. (4 de Noviembre de 2022). Obtenido de https://www.cybercom.mil/Media/News/Article/3209896/cybercom-concludes-cyber-flag-23-exercise/
van Creveld, M. (2007). *La transformación de la guerra.* Buenos Aires: José Luis Uceda.
Velez, W. A. (Diciembre de 2020). Obtenido de https://www.researchgate.net/publication/347112503_PRINCIPIOS_FUNDAMENTALES_DE_COMPUTACION_CUANTICA
Vertuli, M. D., & Loudon, B. S. (2018). *Perceptions are reality.* Kansas: Army University Press.
vmware. (2023). Obtenido de https://www.vmware.com/es/topics/glossary/content/network-security.html
Vorobyov, I., & Kiselyov, V. (2013). Russian Military Theory: Past and Present. *Pensamiento Militar*, 56.
Waldman, A. (30 de Marzo de 2022). Obtenido de https://www.techtarget.com/searchsecurity/news/252515351/Viasat-confirms-cyber-attack-on-Ukraine-customers
WEF. (2023). *World Economic Forum.* Recuperado el 18 de Julio de 2023, de https://es.weforum.org/reports/global-risks-report-2023
WEF. (2023). *World Economic Forum.* Recuperado el 18 de Julio de 2023, de https://es.weforum.org/reports/global-risks-report-2023
welivesecurity. (12 de Abril de 2022). Obtenido de https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
Westreicher, G. (26 de Mayo de 2020). *Economipedia.com*. Recuperado el 20 de Septiembre de 2021, de https://economipedia.com/definiciones/innovacion-tecnologica.html#:~:text=La%20innovaci%C3%B3n%20tecnol%C3%B3gica%20es%20el%20cambio%20de%20%C3%ADndole,misma.%20Esto%2C%20a%20fin%20de%20alcanzar%20mayor%20competitividad.
Whitehouse. (2 de marzo de 2023). *Whitehouse.gov*. Recuperado el 20 de julio de 2023, de https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
Whitehouse, E. (Septiembre de 2018). *whitehouse.gov.* Obtenido de https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
Whitehouse, E. (Octubre de 2022). Obtenido de https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
Zeng, J., & Stevens, T. &. (2017). *researchgate.com.* Recuperado el 30 de Julio de 2023, de https://www.researchgate.net/publication/317834062_China's_Solution_to_Global_Cyber_Governance_Unpacking_the_Domestic_Discourse_of_Internet_Sovereignty
zona-militar. (3 de Julio de 2023). Obtenido de https://www.zona-militar.com/2023/07/03/con-la-presencia-del-reino-unido-y-sin-la-argentina-comenzo-en-peru-el-ejercicio-multinacional-resolute-sentinel-2023/
Zweibelson, B. (2023). *Beyond the Pale - Designing Military Decision-Making Anew*. Montgomery: Air University Press.