TRABAJO FINAL INTEGRADOR

TEMA:

IMPLICANCIAS LEGALES EN LA EJECUCIÓN DE OPERACIONES MILITARES (CONJUNTAS Y COMBINADAS) EN EL CIBERESPACIO.

TÍTULO:

LAS OPERACIONES EN EL CIBERESPACIO Y SUS LIMITACIONES LEGALES PARA EL NIVEL OPERACIONAL.

AUTOR: MAYOR (EA) CARLOS EMANUEL ZAMORATO

TUTOR: CORONEL (AUD) ÁLVARO RIBEIRO MENDONÇA

Año 2022

Resumen.

La evolución tecnológica para el control y dominio de la información, continúa rebasando límites día tras día, vulnerando diferentes sistemas que operan dentro del ciberespacio y que buscan obtener información crítica y degradar o afectar el flujo de la misma, neutralizar sistemas de comando y control, de armas, infraestructuras críticas y aquellas críticas de información; y a su vez poseer capacidades para poder contrarrestar estas afecciones buscadas.

Los Estados actualmente reconocen la relevancia e importancia, respecto del control y dominio del ciberespacio, como así también para las Fuerzas Armadas; respecto a esto podemos decir que el ciberespacio es parte de la soberanía de los estados, y como tal, se debe mantener su integridad. Por tal razón, el marco normativo debe estar actualizado, otorgar las posibilidades que permitan a aquellos que se ocupen de la protección del mismo, ejecutar acciones defensivas u ofensivas para asegurarlo y mantenerlo.

Este trabajo plantea realizar un análisis y desarrollo del plexo normativo, en lo que respecta a la ciberseguridad y ciberdefensa, enmarcado en el nivel operacional, y contemplando tanto el marco jurídico nacional como el internacional, circunscrito a las acciones específicas a ejecutarse en el dominio del ciberespacio.

Dicho análisis normativo, la relación y dependencias y las restricciones que impone el sistema legal en la ejecución de operaciones en el ciberespacio, propende a focalizar la investigación en aquellas implicancias legales que pueden surgir en el momento de la decisión de actuar. Es por ello que es necesario destacar claramente y dentro de las posibilidades que permite la intangibilidad y los límites difusos del ciberespacio, sobre aquellos procedimientos y/u operaciones que se deben ejecutar en el mencionado nivel de la conducción.

Palabras clave.

Ciberdefensa – Ciberoperaciones – Ciberseguridad – Marco normativo.

Índice de contenidos.

Índice de figuras.

Índice de anexos.

Introducción.

Las nuevas tecnologías están cambiando radicalmente la interacción humana, sin dejar de lado los conflictos armados. Desde las últimas dos décadas, y previo a lanzarse un conflicto armado, durante y después de los mismos; o sin tener que suceder alguno, se están empleando herramientas cibernéticas y de inteligencia artificial, buscando sistemas de armas cada vez más autónomos.

Sabiendo que los avances tecnológicos implican tanto beneficios, como factores negativos en el desarrollo de una guerra; el impacto que causa una acción cibernética sobre un estado o sus fuerzas; afectando, degradando o destruyendo una capacidad determinada por la detección de una vulnerabilidad en algún requerimiento o capacidad crítica, es el nuevo desafío que poseen los estados y sus fuerzas armadas para repeler y poseer la capacidad de afrontar estas acciones.

La actualización de las concepciones en todos los niveles, ya sea en implementación de políticas, en la adquisición de medios, en capacitación, en educación, en procedimientos en el marco que ampare todo lo anteriormente mencionado. Refiriéndonos de políticas, al nivel estratégico nacional, que es donde se deben desarrollar e implementar, para poder analizar este nuevo tipo de conflictos, contemplar las necesidades que van a surgir, y principalmente dónde nos encontramos a nivel nacional, regional y mundial; qué tipo de afecciones sufrimos, para poder así, determinar las infraestructuras críticas de información a resguardar.

Las capacidades a desarrollar para implementar estas políticas, desprenderán planeamientos para quienes intervengan en forma directa e indirectamente para lograr alcanzar el estándar, que permita iniciar con la educación, capacitación y procedimientos que buscarán realizar acciones en el ciberespacio para proteger, mantener y reducir las acciones externas o internas y que sucedan en un tiempo específico o no.

Por ello, es importante destacar el desarrollo de un modelo jurídico actualizado, basado en las leyes nacionales, doctrina de las Fuerzas Armadas, y consecuentes también con el ámbito internacional, favorezca al desarrollo de operaciones en el ciberespacio; y que esto sea un imperativo para los responsables e intervinientes de sistema de ciberseguridad en todo nivel, y no una necesidad que acompañe el contraste entre el avance tecnológico y tienda a reducir el tramo del plano jurídico para este ámbito.

Desde esta perspectiva, el análisis del plexo normativo respecto a las actividades de uso del ciberespacio como dominio militar es necesario para poder determinar aquellas limitaciones que posee la fuerza de las acciones a realizar en el plano de la ciberdefensa, y en operaciones, para el control del ciberespacio y del ambiente informacional.

Por Resolución del Ministerio de Defensa N° 364/2016, se crea el Comité de Seguridad de la Información del Ministerio de Defensa, integrado por las áreas con competencia en materia de política, planes y programas, presupuesto, tecnología, asuntos jurídicos, recursos humanos, administración y despacho (Ministerio de Defensa, 2006). Siendo este el primer antecedente normativo dentro del Ministerio de Defensa referido a la ciberdefensa.

Dentro de la estructura del Gobierno Nacional se encuentra la Dirección Nacional de Ciberseguridad, la misma contempla el control funcional del planeamiento y ejecución de los órganos de ciberdefensa del Ministerio de Defensa, el Comando Conjunto de Ciberdefensa; creado por la Resolución N° 343/2014; a través de la ejecución de ciberdefensa, como protección de las infraestructuras críticas del Instrumento Militar y todos aquellos designados como objetivos de valor estratégicos (OVA) y/o activos críticos de información (ACI) asignados al y por el Ministerio de Defensa al Comando Conjunto de Ciberdefensa. El cual debe ejercer la conducción de la ciberdefensa durante el desarrollo de operaciones militares en el ciberespacio en forma permanente, a fin de garantizar al instrumento militar la defensa nacional y cumplir su misión orientado por los establecido en el planeamiento estratégico militar (Ministerio de Defensa, 2014).

La Resolución N° 385/2013 que establece la Unidad de Coordinación Cibernética y las Direcciones de Ciberdefensa del Ejército Argentino, de la Armada de la República Argentina y de la Fuerza Aérea Argentina, en el marco específico y dependientes de las Direcciones Generales de Comunicaciones e Informática, responsables de la implementación de las políticas establecidas de ciberseguridad en cada fuerza específica (Ministerio de Defensa, 2013).

La ciberseguridad establece las políticas nacionales para lograr la protección, confidencialidad, integridad y disponibilidad de la información correspondiente a las infraestructuras críticas e infraestructuras críticas de información, que sean esenciales para la Nación. Por esto y a nivel nacional se crea por Decreto N° 577/2017 el Comité de Ciberseguridad, entidad *ad hoc* dependiente de la Jefatura de Gabinete de Ministros con representantes de todos los Ministerios Nacionales, cuyo principal objetivo es establecer y/o actualizar la Estrategia Nacional de Ciberseguridad, que desarrolle las previsiones en materia de protección del ciberespacio, para implementar coherente y estructuradamente aquellas acciones de prevención, detección, respuesta, defensa y recuperación frente a las amenazas cibernéticas que atenten con la seguridad de la información nacional (Presidencia de la Nación, 2017).

Según el Decreto N° 703/2018, la Directiva de Política de Defensa Nacional, consideraba al ciberespacio como un ambiente operacional militar que configura una amenaza de interés estratégico para la Defensa Nacional (Ministerio de Defensa, 2018). La característica de la

Directiva de Política de Defensa Nacional vigente desde el 2014 y hasta el 2018, fue actualizada a mediados del 2020, derogando la vigente desde el 2018 por Decreto Nro 571/2020, la misma no contemplaba el uso del ciberespacio con fines militares; es decir, limitaba para realizar acciones de ciberdefensa con fines militares (Presidencia de la Nación, 2017). El Comité de Ciberdefensa y la actual directiva de defensa, contemplan este ambiente operacional, ya que los decretos que en sus anexos establecen el vocabulario técnico temático y el propio comité, no fueron derogados aún, como el mencionado decreto.

La concepción vigente, en afinidad con las políticas de ciberseguridad, y respecto al marco mundial y regional, en el análisis del ciberespacio, que en el marco legal para la defensa y la seguridad interior, operan en forma interagencial dentro del ciberespacio; el primer problema suscita en la definición acotada del ciberespacio sólo con el plano virtual y no abarca el plano físico y el plano social. Así mismo continúan en vigencia la Resolución N° 1523/2019 que establece el glosario de términos relacionados con la Ciberseguridad y la Resolución N° 829/2019 Estrategia Nacional de Ciberseguridad que "sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio" (Secretaría de Gobierno de Modernización, 2019).

En relación a las características del ciberespacio y su vinculación dentro del ambiente operacional, encontramos en forma interrelacionada al ambiente informacional, que puede ser definido como "la sumatoria de individuos, organizaciones y sistemas que obtienen, procesan, difunden o actúan sobre la información" (Spretz, 2018). En cuestión de ciberdefensa Casarino y Ortiz (2019), definen la última como "el conjunto de actividades que apuntan a obtener conocimiento previo de amenazas y vulnerabilidades a los sistemas de comunicación de información a través de una variedad de medios técnicos" (p. 51).

Aspectos ya investigados por otros autores, donde observan o definen al ciberespacio, su conformación y como las tecnologías de la información y comunicación, adquieren dentro del ambiente operacional una dimensión especial desde el punto de vista militar; la concepción de estos aspectos está evolucionando velozmente, modificando variables, llegando a concebir al ciberespacio como un Teatro de Operaciones, dice Baretto (2017), donde la lucha por la información y el factor humano tienen un papel trascendental, ya que el control de estas variables; hombre, información y espacio; es limitado a diferencia de los tradicionales dominios de la guerra (p. 10).

Es destacable lo aportado por otros investigadores, referido a la capacitación, perfeccionamiento y adiestramiento; tanto de profesionales militares como civiles en el área de ciberde-

fensa, en las áreas de ciencias sociales y humanas sobre entornos complejos y difusos, vinculadas estas a su aplicación directa sobre la Defensa Nacional. La relevancia del conocimiento de cuándo y cómo actuar, está relacionado en su totalidad con el marco jurídico que imponga la legislación nacional, para poder operar en el nivel operacional y su posible adecuación a un marco combinado.

Esto favorecerá a tener personal que logre un análisis profundo y sistémico del manejo de la información, protección y explotación bajo las nuevas concepciones de aplicación militar de la defensa cibernética y determinado alcances dentro del ambiente operacional. Estas capacitaciones, según Fonseca y Ansorena G. (2017) deben tener como núcleo el trabajo y aprendizaje en equipo de una organización inteligente, que abarque las operaciones de información y la ciberdefensa, y las interrelaciones potenciando un efecto sinérgico en los resultados (p. 35).

El obstáculo legal normativo no es sólo nacional, sino también regional e internacional, la influencia de la tecnología y su evolución cotidiana, sumado a la necesidad de grandes procesamientos de información, y su control y protección, han generado gran número de conflictos que modificaron y complejizaron los hechos delictivos y amenazas en el sistema de redes informáticas, alcanzando sectores estatales y sus factores de poder, que por causa de la inexistencia de reglas, normas o dictámenes, no han llegado a estar en tiempo con las medidas a adoptar que permitan anticiparse a las acciones ejecutadas por diversos actores en diferentes ámbitos.

La falta de una normativa ha llevado a la adopción de políticas de Estado para poder visualizar los riesgos, amenazas y aquellas oportunidades a explotar los matices que el ciberespacio ha generado para comprender sobre cómo ha evolucionado y cuáles han sido en las que se pueden encontrar los lineamientos particulares o claves en la búsqueda de minimizar los riesgos y amenazas. Este análisis es fundamental y sus causas, por consiguiente, exigen la concepción de una estrategia nacional sobre la ciberseguridad que establezca una estructura que ponga límites territoriales debido a su intangibilidad.

El Convenio de Budapest del año 2001, cuya finalidad es: “armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos” se suma a esta la segunda de cita que según y referido al derecho procesal penal “los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico”, y finalmente la tercera de “establecer un régimen rápido y eficaz de cooperación internacional” (Convenio de Budapest, 2001).

La adaptación del derecho internacional también ha sido un gran avance, podemos mencionar el caso de la interpretación dada por las Naciones Unidad en lo referido a la temática de la información, el ciberespacio y la ciberseguridad, de la Carta de las Naciones Unidas del 26 de junio de 1945 y su última enmienda en 1973, en el "Capítulo VII – Acción en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión", en su Artículo 41 y 51, que establece que una agresión a un estado, cualquiera sea su forma, total o parcial, económica, diplomática, entre otras; y si se encuadran en lo prescripto en este documento, permite la legítima defensa sobre el atacante o agresor; esto significa que un estado conociendo a la atribución del ataque cibernético puede responder, manteniendo las medidas tomadas en forma legítima para contrarrestar las agresiones para que "la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales" (Carta de las Naciones Unidad, 1945, pp. 13 y 16).

Respecto al derecho internacional aplicable a la guerra cibernética en el año 2013 y realizado por expertos en la materia pertenecientes a la Organización del Tratado del Atlántico Norte (OTAN), se configura el Manual de *Tallin*, el cual expresa: "el objeto es regular la ley internacional de seguridad cibernética y de los ciberconflictos armados, poseyendo algunas reglas respecto al jus ad bellum y del jus in bello, ya que una operación cibernética puede causar lesiones o muerte a personas o daños a objetos" (Tallin Manual 1.0, 2013).

Asimismo el Derecho Internacional de los Conflictos Armados (DICA) ha servido para ordenar y humanizar, dentro de las posibilidades, el control o conducta de las hostilidades de los conflictos; si bien estas normas de *ius ad bellum* y el *ius in bello*, han cumplido su función con limitaciones, previniendo y evitando vulnerar derechos y tratar de ordenar el desarrollo de los mismos, permite enmarcar estas acciones del ciberespacio protegiendo a los individuos, sus derechos y su privacidad, incluyendo a los estados y organizaciones públicas y privadas que se vean afectadas (p. 90).

Actualmente se planifica a nivel Nacional sobre una Estrategia Nacional de Ciberseguridad desde el año 2017, la cual impulsa medidas preventivas y acciones defensivas ante amenazas existentes y nuevas amenazas, entrelazando agencias públicas y privadas para obtener resultados más eficaces en el control del ciberespacio nacional.

Dicha estrategia de ciberseguridad, contempla en su proyecto, la implementación, el planeamiento y coordinación del Estado Mayor Conjunto; y a cada Fuerza Armada a nivel Dirección de Ciberdefensa, enmarcado bajo la Ley N° 23554 de Defensa Nacional, Ley Nº 24059 de Seguridad Interior y Ley N° 25520 de Inteligencia Nacional, el sistema de ciberdefensa de

las Fuerzas Armadas y Estado Mayor Conjunto, con dicha estrategia se implementa con la nueva Directiva de Política de Defensa Nacional 2021.

De esta manera y a partir de esos momentos "la ciberdefensa comenzó a formar parte de un nuevo escenario de luchas, tensiones, intereses y negociaciones: entre otros, la protección de todo tipo de infraestructuras críticas el diseño de políticas públicas orientadas fortalecer la seguridad de la información, la soberanía territorial y su particular relación con el ciberespacio" e identifica a las infraestructuras críticas como "redes, recursos y servicios que -en caso de sufrir un ataque- podrían causar gran impacto en la seguridad de la población" (Eissa y Gastaldi, 2014).

La propia actualización de la Directiva de Política de Defensa Nacional vigente por el Decreto N° 457/2021, da relevancia al empleo del ciberespacio, considerándolo como dominio y de principal afectación por los avances tecnológicos, cibernéticos y de inteligencia artificial. La directiva establece que en base a este nuevo paradigma que la defensa debe encarar, dice que "de modo más específico, resulta crucial tomar en consideración las dimensiones de la defensa relacionadas al ciberespacio". Por otro lado establece que "este ámbito ha generado replanteos sobre las tradicionales categorías con las que se abordaba la "guerra real", exigiendo una rápida adaptación por parte de los sistemas de defensa" (Presidencia de la Nación, 2021).

Continuando con el análisis del tablero transnacional de la directiva, menciona que "en las últimas décadas, muchos países han reorientado esfuerzos y recursos para resguardar su ámbito ciberespacial" (Presidencia de la Nación, 2021); con esto la necesidad de contar con legislación y doctrina actualizada y específica del ciberespacio y su control, tal como lo menciona en el capítulo segundo, donde toma lineamientos jurídicos adaptables, citados en la Carta de las Naciones Unidas, referentes a la legítima defensa y agresión.

En el ámbito del Ministerio de Defensa, la presente temática se encuentra en desarrollo doctrinario tanto específico y como en el ámbito conjunto; establece y da marco a las acciones que ejecutan las Direcciones de Ciberdefensa y el Comando Conjunto de Ciberdefensa, favoreciendo así al desarrollo de un programa de carrera, posgrados y cursos, sobre la normativa vigente de ciberseguridad y ciberdefensa dentro del ámbito del Ministerio de Defensa.

Internacionalmente, poco se puede mencionar respecto a legislaciones específicos y particulares que hayan adoptado estados para el control del ciberespacio, la implementación de políticas de ciberseguridad y principalmente las acciones a ejecutar durante el desarrollo de operaciones en el dominio del ciberespacio, van modificándose de acuerdo a los nuevos conflictos y, resulta dificultoso dar parámetros de empleo al empleo de medios, principalmente por el inconveniente del desconocimiento de las atribuciones del incidente.

Sin embargo países como España, Brasil, Estados Unidos, Gran Bretaña y otros integrantes de la OTAN, realizan adaptaciones normativas a la Carta de las Naciones Unidas, y al Derecho Internacional de los Conflictos Armados (DICA), que han servido para ordenar y humanizar, dentro de las posibilidades, el control o conducta de las hostilidades de los conflictos; si bien estas normas de *ius ad bellum* y el *ius in bello*, han cumplido su función con limitaciones, previniendo y evitando vulnerar derechos y tratar de ordenar el desarrollo de los mismos, permite enmarcar estas acciones del ciberespacio protegiendo a los individuos, sus derechos y su privacidad, incluyendo a los estados y organizaciones públicas y privadas que se vean afectadas.

Por otro lado y gracias a la actualización del año 2017 del Manual de *Tallin* 2.0, presenta al día de la fecha el análisis más completo existente en legislación sobre operaciones en el ciberespacio y añade un análisis jurídico sobre los incidentes más comunes y por los cuales no es necesario el uso de la fuerza o de un conflicto armado (p. 19). A esto podemos sumar el informe de la Comité Internacional de la Cruz Roja (CIRC) que aborda la temática del derecho internacional y su relación con el empleo de nuevas tecnologías de la información y comunicación, inteligencia artificial, sistemas de armas autónomos. Cuya finalidad es "reseñar algunos de los desafíos que los conflictos armados contemporáneos plantean al derecho internacional humanitario (DIH), incitar a la reflexión sobre esos desafíos y hacer una síntesis de la acción, posición e interés actuales o futuros del CICR" (Comité Internacional de la Cruz Roja, 2019).

El presente trabajo de investigación trata de la importancia de tener a nivel nacional y en concordancia con el marco regional e internacional, una normativa actualizada y acorde a las características que impone a las fuerzas armadas la guerra moderna y la transversalidad del ciberespacio y las acciones que se desarrollan en él, que se adecúe y permita reducir los riesgos e incertidumbres de situaciones que no contempladas durante el proceso de planeamiento o ejecución de operaciones, para poder facilitar las acciones preventivas o reactivas, y que las mismas estén dentro de los límites que establece la legislación.

De acá surge entonces el interrogante que da lugar al problema de la investigación de ¿cómo influye el marco legal de la República Argentina en el planeamiento y ejecución de las operaciones en el ciberespacio desde una perspectiva del nivel operacional? La respuesta permitirá optimizar procedimientos en el planeamiento y en la ejecución de ciberoperaciones.

El problema planteado, establece alcances y limitaciones que influyen en el desarrollo de la investigación tiene interés particular en el nivel operacional, en tal sentido, y realizando un análisis del marco normativo internacional, nacional, y la propia doctrina sobre la temática en cuestión, buscará determinar las principales exigencias y limitaciones que los aspectos legales imponen a las operaciones en el ciberespacio.

El estudio incluirá, por lo tanto, y dentro del contexto, definir el alcance de las competencias del Estado en el ciberespacio y en establecer los mecanismos o herramientas operativas y eficaces que den solución a los conflictos de competencias jurídicas que puedan surgir y que afecten o influyan en el novel operacional.

Relacionado a las limitaciones que se pueden mencionar, principalmente, marcada por la evolución permanente de la tecnología que incide directamente sobre métodos, doctrinas y leyes obsoletas que regulan el ciberespacio o intentan hacerlo, más allá de esto, el estado y configuración actual, preservará información que pueda resultar de carácter sensible o que sea intención de alguna fuerza armada publicar.

Respecto a los aportes teóricos y/o prácticos al campo disciplinar, el actual marco doctrinario específico y conjunto se encuentra en constante revisión, es un aspecto a destacar dentro del Ciclo de Planeamiento de la Defensa iniciado en el año 2021, continuando con lo establecido en el Decreto Nro 1729/2007 sobre los aspectos a desarrollar en el mencionado ciclo; y con relevancia dentro de la Directiva de Política de Defensa Nacional vigente según el Decreto Nro 457/2021; aún no se han publicado por parte de las Fuerza Armadas de Argentina o del Estado Mayor Conjunto publicaciones militares y/o reglamentos que efectúen un análisis de los procedimientos a realizar tanto en el marco nacional como en el marco internacional, formando parte de acciones conjuntas o combinadas de ciberdefensa o interagencial, abarcando legislación nacional, regional o mundial en cuestiones puntuales o exigencias particulares.

Desde el punto de vista operacional, el nuevo ambiente es una realidad diferente, el ciberespacio como parte del mismo es una realidad capacitada para alterar la naturaleza y el normal funcionamiento de una no virtual del estado, sus fuerzas armadas y de seguridad, dentro y fuera del territorio. Dado esto por las recientes operaciones multidominio, la extensión geográfica nacional, la virtualidad y transversalidad del ciberespacio, la no linealidad de las operaciones, la velocidad de las acciones y la necesidad de una flexibilidad imperante en los sistemas y decisores, imponen nuevas exigencias a satisfacer, las cuales por el avance tecnológico y el cambio en los intereses de los estados, requiere estar a la altura de las circunstancias, y buscar alcanzar en el corto y mediano plazo los medios y capacitación, y proyectar en el largo plazo el completamiento y repotenciación tanto de material como personal especializado en lo técnico y legal sobre el accionar en el ciberespacio.

Así entonces la relevancia de la investigación recae en el estudio de una actualización y reorganización de un modelo jurídico para ordenar la realidad difícilmente comprensible por los esquemas tradicionales de organización del derecho en torno al Estado, es decir, va más allá

de la traslación de aquellas normas que rigen en los espacios físicos; tierra, mar, aire, aire/espacio; sino también aquellos que conforman el ciberespacio y el espectro electromagnético, creando una norma específica que dé garantías y competencias reglamentadas, y que ofrezcan mecanismos para la posible solución de los conflictos antes, durante y después de las ciberoperaciones.

El valor del presente estudio estará dado en el planteamiento del objetivo general de investigación que busca evaluar la situación y probable evolución de la normativa vigente de ciberseguridad y ciberdefensa para el nivel operacional y su adecuación a las restricciones del derecho nacional e internacional. Determinando en dos objetivos particulares los cuales permitirán como primera mención, analizar el plexo normativo general internacional y nacional, y su adecuación a los cambios que impone el ciberespacio; y posteriormente poder Analizar el marco jurídico nacional y la doctrina vigente; las adaptaciones necesarias y las limitaciones implícitas para las operaciones en el ciberespacio.

En tal sentido, la hipótesis queda planteada que si el ciberespacio por sus características de transversalidad y virtualidad, requiere un marco jurídico específico para poder reducir los riesgos e incertidumbres ante aquellas situaciones que no están contempladas durante el proceso de planeamiento o las que se contemplaron parcialmente, con la finalidad de facilitar las acciones preventivas o reactivas durante el desarrollo de operaciones en este dominio por parte del nivel operacional.

La metodología a emplear para el cumplimiento de los objetivos general y particulares propuestos será del tipo deductivo, para ello se realizará el análisis de distintas fuentes y la descripción durante el desarrollo de cada capítulo a fin de obtener las conclusión general que permita dar respuesta al objetivo general planteado para la investigación.

Respecto al diseño de la investigación, el método será de tipo explicativo, no solo se describirá el problema, sino que se establecerán relaciones entre distintos conceptos para dar respuestas a las causas que los originan. Las técnicas de validación empleadas son el análisis bibliográfico, documental y lógico; esta metodología se puede apreciar gráficamente en el Anexo 1. Respecto a las fuentes bibliográficas principales empleada, se basan particularmente en: leyes y derivados de índole nacional e internacional, doctrina conjunta y específica, doctrina extranjera; las fuentes secundarias, serán sobre trabajos de investigación, informes y publicaciones y libros de investigación.

Capítulo 1

Adecuación del marco legal internacional y nacional al ciberespacio.

El análisis actualizado del marco normativo tanto nacional como internacional, respecto del uso del ciberespacio con fines militares, dentro de su consideración como nuevo dominio militar, es necesario para poder determinar aquellas limitaciones que poseen las fuerzas armadas argentinas en operaciones, para el control del ciberespacio y de las actividades a realizar en el plano de la ciberdefensa.

El presente capítulo hará referencia a las normas existentes en el derecho internacional, su aplicación e interpretación, en un contexto mundial, los casos de políticas aplicadas por el Estado Argentino en relación a uno de los factores que ha impuesto la globalización respecto a la proliferación de las Tecnologías de la Información y Comunicación (TICs), y aquellas que han surgido de los avances tecnológicos, de la innovación armamentística sobre el ciberespacio, y del profundo desarrollo de la ciencia y tecnología sobre el aumento del uso de la internet en todos los privados y públicos.

Conociendo que estos cambios han complejizado y alcanzado los escenarios de conflictos militares, han traído como consecuencia, criterios particulares que implican adoptar políticas y asumir responsabilidades sobre el uso del ciberespacio antes, durante y posterior a los conflictos armados, con las limitaciones que el derecho establece actualmente y sus dificultades de adaptación e implementación. Respecto a estos criterios, se puede mencionar que el procesamiento de información y su interconexión ha aumentado en gran volumen, exigiendo una rápida selección de lo realmente útil y qué lo descartable sea tenido en cuenta o no, requiriendo la necesidad de analistas de información más capacitados y entrenados en las nuevas Tecnologías de la Información y Comunicación (TICs). Tal vez el incremento tecnológico trae aparejado un aumento en los riesgos de la seguridad de la información propia pública y privada, llevando a circunscribir nuevas responsabilidades para las organizaciones que se ocupan del control y protección de este dominio, como es el caso de las fuerzas armadas.

Las consecuencias de estos aspectos se remiten a la velocidad que necesita la organización de ciberdefensa del nivel operacional, tanto en el proceso de selección de información y detección de vulnerabilidades, como en la forma de contrarrestar las mismas. Esto exige estar operando dentro del marco legal adecuado para poder discernir entre lo correcto, determinar los procesos y establecer los límites durante la ejecución de operaciones dentro del ciberespacio.

Asegurar la supervivencia de las infraestructuras críticas de información, implica asumir riesgos en otros dominios debido a la transversalidad del espacio cibernético y el alcance de sus

acciones, ya que una intromisión dentro del sistema defensivo, afecta y pone en riesgo diversos factores del Poder Nacional.

Basado en estos se deben analizar e interpretar las legislaciones y las políticas necesarias para que los factores del Poder Nacional se sirvan de herramientas necesarias para mitigar las intromisiones y coadyuven a la protección de la territorialidad, la soberanía, la seguridad nacional, la protección de sus habitantes, y sus datos e información privada y sensible.

Ciberseguridad y derecho internacional.

Desde el punto de vista del derecho internacional, tomamos como referencia organismos supraestatales de injerencia mundial, como el caso de la Organización de las Naciones Unidas (ONU), para poder inferir en las decisiones que atañen a tratados y convenciones orientadas a regular los conflictos armados, y sus diferentes aristas dentro de una región o zona de influencia y su entorno. De esta manera es importante resaltar que el uso y búsqueda de control del ciberespacio trae riesgos actuales y futuros, y como el Derecho Internacional Humanitario (DIH) o conocido también como Derecho Internacional de los Conflictos Armados (DICA), pueden contribuir a mitigar el daño.

El Comité Internacional de la Cruz Roja (CICR) en sus informes destaca la relevancia de estos hechos en los conflictos actuales y vigentes, por su afección y amenazas sobre la población civil exenta del conflicto. Cito en el informe último del año 2019, y respecto a las operaciones cibernéticas establece que "pueden permitir que las fuerzas armadas alcancen sus objetivos sin provocar daños civiles ni causar daño físico permanente a la infraestructura civil", sin embargo las operaciones en el ciberespacio recientes, que se realizaron fuera de un conflicto armado "muestran que los actores con mayor sofisticación tecnológica han desarrollado la capacidad de interrumpir el suministro de servicios esenciales para la población civil" (Comité Internacional de la Cruz Roja, 2019); lo que dificulta la aplicación del DICA ya que no se puede contextualizar el mismo.

Aclara el mencionado informe que para los Estados firmantes de la Carta de las Naciones Unidas y los convenios y tratados internacionales, las Naciones Unidas establece que, tanto en el desarrollo como en la adquisición de armas o medios de guerra, son responsables de garantizar que los mismos sean empleados en cumplimiento de lo ordenado por el Derecho Internacional Humanitario/Derecho Internacional de los Conflictos Armados (p. 26). Esto se aplica "al desarrollo y al uso de nuevos armamentos y nuevas tecnologías en la guerra si implican: cibertecnología; sistemas de armas autónomos; inteligencia artificial y aprendizaje automático;

o el espacio exterior" (Comité Internacional de la Cruz Roja, 2019). Otro dato destacable expuesto por el Comité Internacional de la Cruz Roja (2019), es que "celebra el hecho de que un número creciente de Estados y organizaciones internacionales estén reconociendo que el Derecho Internacional Humanitario se aplica a las operaciones cibernéticas en situaciones de conflicto armado" (p. 27). Referido a ello los beligerantes deben respetar y hacer respetar la protección de las infraestructuras críticas de los Estados cuya afección o amenaza vaya en contra de las leyes de la guerra y no cumpla con los principios de los principios de distinción, proporcionalidad y precaución y protección de los civiles; y ponga en riesgo cualquier infraestructura que "el Derecho Internacional Humanitario prohíbe específicamente atacar, destruir, sustraer o inutilizar bienes indispensables para la supervivencia de la población civil" (p. 27).

Por consiguiente los ataques cibernéticos no pueden ser deliberados o desproporcionados, incluso si los mismos son parte de un objetivo militar o se convierte en uno. A sabiendas de esto, sólo se puede afectar la parte determinada como objetivo y reducir al máximo el posible daño colateral que pueda acaecer sobre el objetivo o infraestructura vital. En conclusión a esto, "establece que las partes en conflicto, cuando lanzan un ciberataque, deben tomar todas las precauciones viables para impedir, o al menos minimizar, los daños incidentales a personas civiles y a bienes de carácter civil" (Comité Internacional de la Cruz Roja, 2019).

La Carta de las Naciones Unidad (1945) hace referencia en sus propósitos que cualquier recurso de empleo de la fuerza por parte de los beligerantes, sea cinético o cibernético, está regido primero por la Carta de las Naciones Unidas y las normas del derecho internacional consuetudinario, y que el Derecho Internacional Humanitario es una herramienta más que confiere un nivel de protección adicional contra las hostilidades y sus efectos. (p. 13).

Si en el Derecho Internacional Humanitario y el derecho consuetudinario, observamos que los Estados poseen capacidades de ejecutar acciones cibernéticas por medio de sus fuerzas armadas en el ciberespacio, los ataques que afecten infraestructuras y soberanía, y no cumplan con los mismos serán considerados violaciones al derecho internacional.

Las distancias geográficas y las fronteras ya son irrelevantes para este dominio, un ciberataque puede provenir de cualquier extremo del mundo en cuestión de segundos. El inconveniente principal es el anonimato o desconocimiento de la atribución, pudiendo afectar tanto en la paz como en la guerra y causar grandes daños a un Estado con capacidad militar convencional muy superior. Actualmente este aspecto ha sido tenido en cuenta en el marco regional, a cargo de la Organización de Estado Americanos (OEA) y realizado por el Comité Jurídico Interamericano (CJI), donde se han establecido objetivos, referidos a acciones en el ciberespacio; que afectan no sólo a objetivos militares sino también a infraestructuras de un Estado antes y

durante un conflicto. Dificultando por sus características quienes son combatientes y quienes civiles, o si es proporcional utilizar fuerza cinética sobre blancos cibernéticos.

Plantea este quinto informe, la falta de normas y estándares a medida, la ausencia de tratados y medidas a tomar; refiere a lo expuesto en el Convenio de Budapest sobre la protección de la información de las personas y su privacidad. Haciendo hincapié en que "a nivel mundial no existe un consenso universal entre los Estados sobre qué normas internacionales generales vigentes se aplican a las operaciones cibernéticas" (Comité Jurídico Interamericano, 2020). En base a proyectos de las Naciones Unidas y de otros organismos internacionales, propuestas de aplicación e interpretación del derecho internacional consuetudinario y el blanqueo de medios y acciones actuales, para facilitar y retroalimentar el derecho.

En forma similar la Organización de Estados Americanos ha realizado lo que según Segura Serrano (2017) en su trabajo, sobre Ciberseguridad y derecho internacional, la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN) han establecido la primera estrategia de ciberseguridad en el 2013 como cooperación internacional sobre la temática con gran avance futuro y actualizable (p. 296).

Una primera consideración desde el punto de vista del marco internacional, es que todo el cuerpo legal internacional vigente en la actualidad, se ve referido prácticamente a la geografía y soberanía de los territorios, es decir, a la relación entre el ámbito terrestre, marítimo y aéreo; en este contexto, el concepto de soberanía territorial ya no se ajusta tanto al nuevo concepto de ciberespacio y su transversalidad. Pero tampoco existe un acuerdo internacional donde se pueda reconocer si un ciberataque es considerado o no, por sus características, en las mismas condiciones de un ataque no cinético. Cuando surgen los problemas, se debe clarificar si se emplearán medidas defensivas u ofensivas; por consiguiente es acá donde los Estados y sus niveles ejecutivos, particularmente el nivel operacional, se encuentran en constante revisión de los procedimientos, que inicialmente, todos están de acuerdo en que los poderes nacionales defiendan sus infraestructuras críticas de acciones cinéticas y no cinéticas.

Legislación nacional.

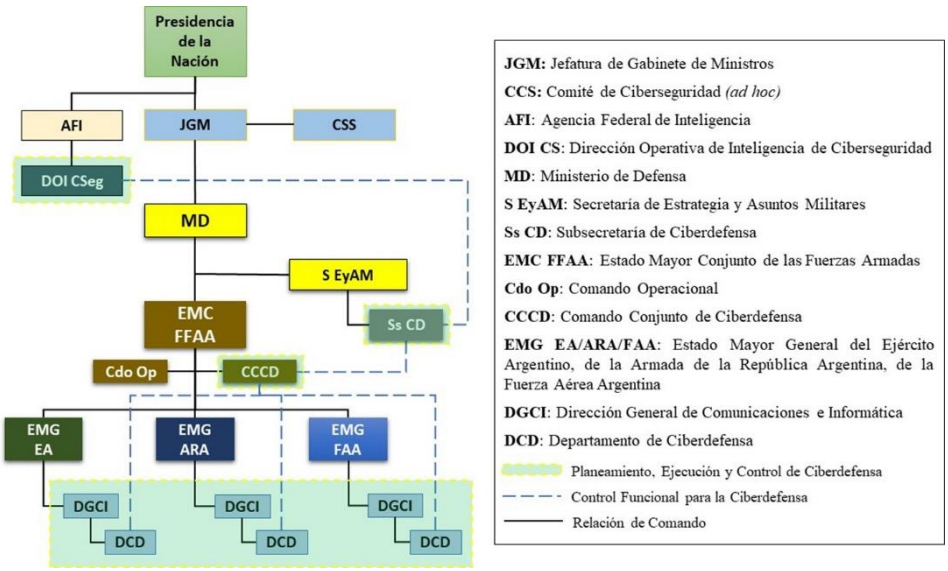
Cuando nos referimos al marco legal nacional del ciberespacio, y su relación con el empleo en el ámbito castrense, y en particular en el nivel operacional, debemos conocer donde se encuentra enmarcado el mismo dentro de la regulación del ciberespacio. Así observamos que en la República Argentina la evolución y el actual desarrollo de una serie de políticas y la necesidad de creación de organizaciones tendientes a acompañar estas políticas de ciberseguridad,

y la regulación de los efectos y las acciones en la ciberdefensa, se basan en una estructura ministerial acorde a las circunstancias actuales, que requieren un sistema jerárquico representado en la Figura 1 en la cual se muestra a nivel ministerial y dentro del Ministerio de Defensa, la Secretaría de Estrategia y Asuntos Militares, dependiente de la Subsecretaría de Ciberdefensa, y con control funcional sobre el Comando Conjunto de Ciberdefensa y las Direcciones de Ciberdefensa de cada Fuerza Armada. Eso permite que cada fuerza adopte propias políticas y las establecidas por los niveles superiores para llevar a cabo las acciones ordenadas.

Si bien todos los elementos que operan en el ciberespacio a nivel nacional, son responsables del planeamiento y ejecución, dependiendo de la autorización; de acciones en redes, sistemas de información y telecomunicaciones del Instrumento Militar o de aquellas que imponga como prioridad el Nivel Estratégico Militar o Nacional para el resguardo por parte de las fuerzas armadas, y responder ante amenazas contra la Defensa Nacional.

Figura 1.

Relaciones de la ciberdefensa en el marco nacional.



Nota. Adaptado de "Dirección Nacional de Diseño Organizacional", 2021. Fuente: https://mapadelestado.jefatura.gob.ar/organigramas/autoridadesapn.pdf

En el análisis primario de la Ley N° 23554 que instituye, que la defensa nacional está integrada y coordinada por todas las fuerzas de la nación, con la finalidad de solucionar los conflictos, empleando las Fuerzas Armadas en forma disuasiva o efectiva, para generar las garantías para la nación y sus habitantes (Honorable Congreso de la Nación, 1988); pero para cumplir con ello y en este marco, es donde se establece el nivel operacional, que limitado por el Decreto N° 683/2018, donde concierta de manera similar al artículo 2 de la Ley de Defensa Nacional respecto a la forma disuasiva y efectiva de las fuerzas armadas ante agresiones sólo de origen externo y marca las particularidad de aquellas excepciones que establece la Ley de

Seguridad Interior y aquellas formas de agresión que sin ser de origen externo vaya en contra de la Carta de las Naciones Unidad o sea incompatible (Presidencia de la Nación, 2018).

En materia de las circunscripciones de la ciberinteligencia, queda claramente definido en la Ley N° 25520, y modificada por la Ley N° 27126 donde dispone que "es la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior de la Nación" (Honorable Congreso de la Nación, 2015). Marcando con esto el claro límite de aplicación de la seguridad interior para asuntos criminales, y para el sistema de defensa, la producción de inteligencia referida a las áreas de responsabilidad del Instrumento Militar.

Si bien a partir del año 2013 la inteligencia se incumbe en el análisis de ciberamenazas, la puesta en funciones de la Ley N° 27126 y el Decreto N° 1311/2015, conllevaron a la producción de inteligencia referente a ciberseguridad y la ciberdefensa, deliberando escenarios definidos y priorizando asuntos establecidos en la Estrategia Nacional de Ciberdefensa; por consiguiente a esto y dentro del marco legal se conciben acciones de producción de inteligencia en el empleo del ciberespacio con fines militares (Presidencia de la Nación, 2015).

La existencia de otras normas han permitido y/o limitado el control del ciberespacio, y que tiene injerencia en el accionar de las fuerzas armadas, las acciones a tomar y darle marco a esta problemática actual y en constante cambio; por ejemplo, la Resolución N° 580/2011 crea el Programa de Infraestructuras Críticas de la Información y de la Comunicación, que adopta el marco jurídico regulatorio, permitiendo identificar y proteger aquellas infraestructuras estratégicas y críticas del Sector Público Nacional cuya posible afectación atente contra la seguridad nacional (Jefatura de Gabinete de Ministros, 2011).

Hacemos referencia a otras normas que actúan sinérgicamente en la temática de ciberseguridad y ciberdefensa, tanto en la protección, obtención, como en el manejo de la información, tal como la Resolución N° 13/2014 de la Comisión Argentina de Políticas de Internet, que busca articular la participación de los distintos actores en el diseño de una estrategia nacional sobre el gobierno de la Internet (Secretaría de Comunicaciones). La Ley N° 27411 que establece el convenio sobre el ciberdelito del año 2017, y ratifica el Convenio de Budapest del año 2001 (Honorable Congreso de la Nación, 2017).

Otro ejemplo es la Decisión Administrativa N° 669/2004 sobre las políticas de seguridad de la información, establece a los organismos del Sector Público Nacional (Jefatura de Gabinete de Ministros, 2011); también se encuentra la Resolución N° 69/2016 que pauta el programa nacional contra la criminalidad informática e incorpora los nuevos tipos de delitos vinculados

con la criminalidad informática, esta resolución exige la participación activa del Comando Conjunto de Ciberdefensa y las Direcciones Generales de Ciberdefensa de cada Fuerza Armada, a responder y accionar ante posibles incidentes en forma legal, sobre aquellos que realicen este tipo de actividad que principalmente busquen obtener información o afectar las infraestructuras críticas a defender (Ministerio de Justicia y Derechos Humanos, 2016).

La volatilidad de los límites del ciberespacio, condicionan el concepto de soberanía territorial y su marco legal nacional por afuera y dentro del ámbito militar, dificulta las actividades de un dominio transversal, con límites difusos y muy complejo, que debe controlar el nivel operacional, y detectar amenazas, atribuciones individuales o grupales, ya sean de carácter estatal o internas, la necesidad de aumentar la resiliencia, detectando las propias vulnerabilidades; todo esto ocasionado por la discordancia entre las leyes, resoluciones y decretos vigentes y desactualizados en algunos casos. Dado que la legislación nacional marca una línea incisiva de los límites entre la defensa nacional y la seguridad interior, sumado a esto, los aspectos de ambas, circunscriptos en la ley de inteligencia; limitan así al Instrumento Militar a actuar sólo en caso de agresiones de carácter de guerra convencional entre Estados.

Capítulo 2

La ciberdefensa en el nivel operacional y sus limitaciones legales y doctrinarias.

La ciberdefensa en este nivel deberá, entender, intervenir y participar de diferentes acciones como parte de sus funciones particulares y generales; que enmarcadas en la doctrina conjunta y específica y dentro de la legislación nacional, permita la ejecución de acciones para el logro de efectos y alcanzar los objetivos operacionales previstos.

Analizando los riesgos, explotando sus capacidades, la protección de las infraestructuras críticas de la defensa, como sistemas de comando y control, sistemas de armas con componentes informáticos, electrónicos y/o de comunicaciones; a fin de proteger la información almacenada, procesada y su intercambio; y para con el oponente, obtener su información, debilitar, negar el uso y/o destruir sus propios sistemas.

Para esto en el nivel operacional, el planeamiento debe adaptarse y saber interpretar las limitaciones que la ley impone en el desarrollo de operaciones. Este análisis bibliográfico, documental y lógico será el lineamiento de este capítulo para poder abordar las conclusiones y dar respuesta al problema planteado.

La comprensión del ciberespacio y su definición, favorece el empleo de los elementos de nivel operacional para operar y, si bien en la actualidad existen diferentes concepciones y puntos de vista, como cantidad de autores, en nuestra legislación, la Resolución N° 1523/2019, lo ha definido expreso en su Anexo 2, como “el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas Tecnologías de la Información y Comunicación” (Secretaría de Gobierno de Modernización, 2019).

El reglamento de Glosario de Términos de Empleo Militar para la Acción Militar Conjunta (2014) lo define como el ámbito virtual en el cual redes interdependientes están interconectadas, software, firmware, desarrollan actividades relacionadas con información y empleando tecnologías de la información y comunicación, con las cuales procesan, almacenan, explotan esa información disponible y obtenida para sacar provecho o protección (p. 42).

Estas definiciones, y el momento de su establecimiento, no han considerado conceptos que engloben la totalidad actual de lo que significa el espacio cibernético y, haciendo una referencia realizada por profesionales de las fuerzas armadas, han realizado una semejanza mayor a la realidad de su significado y concepción; así lo expuesto en su obra, de Vergara y Trama (2017), aludiendo a Feliú Ortega, observan al ciberespacio como algo superior a sólo la Internet,

abarcando no sólo sistemas, equipos, hardware, software, usuarios; afirman que es algo novedoso y propio en sí mismo, que incluye leyes físicas, pero principalmente que fue una creación del hombre para su servicio (p. 28).

Los mencionados autores añaden, que la visión sistémica de esto, configura el conjunto de sistemas de información, conectados en tiempo, dicho de otra manera, todos los integrantes del ciberespacio y la información que circula se transforma en el tiempo; y que los mismos usuarios, nodos, conexiones son los que interactúan con estos sistemas, pudiendo ocurrir cambios radicales en poco tiempo y afectar o beneficiar, según la posición o nivel donde se encuentre el usuario o el sistema (p. 29).

El llamado quinto dominio, posee características distintivas y pueden apreciarse que sus efectos alcanzan todos los niveles de la conducción, e incluye diferentes actores, ya sean civiles públicas y privadas, militares, gubernamentales, económicos, y sobre todos genera influencia a través de las operaciones cibernéticas, en consecuencia, podemos dividir el ciberespacio en una realidad de capas. Referenciando nuevamente a de Vergara y Trama (2017) infieren que según el informe generado para el período 2016-2028 del Centro de Integración de Capacidades Militares del Ejército de Estados Unidos, se establecen una capa física, una lógica y una humana.

En la capa física fluyen los datos que genera el componente ciber-persona, vista como esa porción del componente persona presente en la red en ese momento y que transmite información en forma de datos a través de conexiones lógicas; esta capa lógica es la que permite y facilita el intercambio independientemente de lo físico y de los individuos; esto se realiza sobre el componente geográfico distribuido, siendo este cualquiera de los otros dominios. Consecuentemente lo social, la gente, la persona, la información, las redes, hacen del ciberespacio un ambiente dinámico, interactivo y global.

Por ello y desde el punto de vista de la ciberdefensa, este dominio es cada vez más utilizado para controlar sistemas de comando y control, sistemas de armas, sistemas de inteligencia y coadyuva, por las características que posee de alcance, a apoyo de operaciones de información, de engaño y velo, seguridad y guerra electrónica.

La influencia de los conflictos cibernéticos en el nivel operacional.

En el nivel operacional, el desarrollo de operaciones militares, lleva implícito el análisis y estudio del ambiente operacional donde se van a desarrollar las mismas; asimismo se tendrán en cuenta aquellos factores que serán afectados y los que podrán condicionar las operaciones en su preparación, ejecución y finalización. Respecto de la ciberdefensa, podrá tenerse en cuenta en el planeamiento como una operación contribuyente o una particular conformándose

como una línea de operaciones debido a las características de los puntos decisivos a afectar o protección del propio centro de gravedad.

Siguiendo con el análisis del ambiente operacional, la actualidad generada por los avances estrepitosos de la tecnología e información, implican un planeamiento en un contexto complejo que no sólo abarca los dominios tradicionales de un conflicto armado, sino que es mucho más amplio, y que el mismo posee gran cantidad de aristas donde el desarrollo de ciberoperaciones podrá contribuir con afectar alguno de ellos y lograr los efectos buscados o favorecer otra operación como parte constitutiva de una operación de contribución.

En forma holística los dominios tradicionales del aire, aeroespacio, mar, tierra, espectro electromagnético/ciberespacio; incluyen diferentes sistemas y subsistemas del entorno operacional, que según la Figura 2 podemos traducirlo como sub-ambientes o partes de un todo, con generación de planeamientos o conformación de células para afectar alguno determinado dentro de una capacidad crítica como una vulnerabilidad de infraestructuras de información.

Figura 2.

El ambiente operacional e informacional – Visión holística.

Nota: Adaptado de "JP-0-5 *Joint Planning". Department of Defense, Joint Chiefs of Staff*, 2017. Fuente: *FM 3-12 Cyberspace and Electronic Warfare Operations.*

Así también, el planteamiento de las acciones podrán basarse sobre el desarrollo de defensa por capas o multicapa dentro de un contexto de multidominio, sobre la base de un despliegue de medios en diferentes niveles, pero conducidos a nivel operacional, generando una sinergia en las acciones previstas dentro del teatro de operaciones.

Esto se logrará a través de la explotación de sus capacidades dentro del ciberespacio; creando la libertad de acción adecuada, y que favorezcan a acciones a desarrollar en los otros dominios, creando efectos dentro y a través del ciberespacio, conociendo que cada efecto por sí solo, o la integración de todos puede ser decisivo.

Estos efectos buscados por las operaciones en el espacio cibernético podrán ser de: neutralización, interrupción, denegación, degradación sobre los sistemas de comando y control, de armas, de redes informáticas, de información, y aquellos que operan a base de tecnologías de información y comunicación.

Basado en estas características de los efectos, es necesario contar con un sistema de ciberdefensa que permita la operación interdisciplinaria e independiente en los distintos niveles, es decir conformarse una fuerza adaptable y versátil que opere en todo momento y con alcance global. Este enfoque del nivel operacional, versátil y adaptable, otorgará las posiciones favorables en los otros dominios, asegurando los sistemas y protegiéndolos.

Al impartirse la Directiva Estratégica Militar, el nivel operacional debe planificar las operaciones, y sobre la estructura del sistema nacional, podrá determinar que Activos Críticos de Información (ACI), Objetivos de Valor Estratégicos (OVE) e Infraestructuras Críticas de la Información y Comunicación (ICIC) de la Defensa Nacional, y del Estado deben preservarse; cuáles vulnerabilidades críticas han sido detectadas en los requerimientos y/o capacidades críticas que posee el oponente, que contribuirá su afectación a hacer caer el centro de gravedad.

Enmarcada en el nivel operacional, la ciberdefensa, debe desarrollar capacidades para el logro de los efectos requeridos sobre el sistema oponente; sumado al control, relativo/parcial, del ciberespacio, buscando alcanzar una superioridad y poder proteger los sistemas propios.

Las operaciones en el ciberespacio deben producir efectos que se traduzcan principalmente en ventajas estratégicas, y también operacionales y tácticas, según Anca (2017); paralelamente a esto, la defensa nacional requiere desarrollar sistemas capaces de proporcionar velo y engaño sobre las propias vulnerabilidades críticas, en consecuencia, el sistema de ciberdefensa, debe poseer principalmente una característica transversal a todos los niveles; del estratégico nacional al táctico; que es la resiliencia cibernética (pp. 33-34)

Para desarrollar un sistema ciber-resiliente, que recupere su capacidad o igual estado inicial luego de haber sido afectado, es decir, “concepto regenerador de capacidades, luego que el sistema haya recibido una afectación por acciones cibernéticas del enemigo” (Gómez, 2017). Además determina que este nivel es el responsable de la seguridad, su ciclo de vida y del diseño de la implementación de aquellas medidas técnicas que aplicadas reducen los riesgos definidos por el Nivel Estratégico, además de la supervisión, auditorías y diseño de mejoras (p. 7-8).

El sistema de ciberdefensa del nivel operacional y sus restricciones legales.

En el nivel operacional, el sistema de ciberdefensa posee una estructura jerárquica vertical; como muestra la figura 1, relaciones de la ciberdefensa en el marco nacional, citada en el

capítulo 1 (p. 15); de quien dependen del Comando Conjunto de Ciberdefensa las direcciones de cada fuerza, quienes se pondrán a disposición en el caso de un conflicto que atente contra las infraestructuras críticas de la información de defensa. Por tal motivo relevante se constituye como un nuevo sistema de armas transversal a los dominios, pero presenta limitaciones para poder detectar, en oportunidad, el origen de las amenazas, agresiones y ataques; si bien evoluciona a la par de la tecnología o lo más próximo a ella; debe reducir la afectación, prioritariamente, al comando y control, y el empleo oportuno de aquellos sistemas de armas integrados por componentes críticos de naturaleza electrónica, informática o de comunicaciones.

Particularmente el marco legal internacional y nacional sobre esta temática, impacta en forma directa en la producción de doctrina conjunta y específica, la misma, aún en revisión y basada en proyectos, es de carácter secreto por las implicancias en sus procedimientos y datos sobre las infraestructuras críticas de la información, por consiguiente se ha hecho un análisis de las mismas; pero sin desconocer que se dificulta por la falta de precisión en la regulación nacional. Todavía no se pueden comparar cuáles son y cómo afectan, los efectos indirectos o directos de las operaciones convencionales con los ciberataques, directos, en lo que respecta a las pérdidas de vidas, los daños materiales totales o parciales; e indirectos de un ataque cibernético dirigidos y ejecutados contra un país en forma sorpresiva y masiva que busquen interrumpir planes estratégicos o detengan acciones gubernamentales, o el desempeño normal de la vida de los habitantes y sus actividades cotidianas por un tiempo determinado o permanente.

En el actual entorno complejo donde se desarrollan las operaciones militares, el teatro se conforma en un ambiente operacional que posee diferentes características, dentro de las cuales se encuentran aquellas que refieren al ciberespacio. Las operaciones que ejecuta la ciberdefensa en el desarrollo de operaciones militares, pueden denominarse como defensivas, directas o de protección; estas acciones serán contribuyentes a la seguridad informática y a las operaciones principales y secundarias; interactuarán en todos los dominios y podrán afectar a uno o todos, como así también a los diferentes factores del poder nacional de un Estado.

Sobre esto hace referencia el Derecho Internacional de los Conflictos Armados en el manual del Ministerio de Defensa (2010), donde establece entre algunos crímenes de guerra, el ataque contra la población civil en forma intencional contra instalaciones sanitarias o protegidas, o aquellos que afectan o ponen en riesgo la vida, como plantas nucleares, represas y que puedan infligir grandes sufrimientos contra la integridad física o a la salud; el empleo indebido de tácticas, técnicas o estrategias de guerra que sean prohibidas por sus formas (pp. 88-92).

Todo Comandante de Nivel Operacional (CNO), podrá emplear el sistema de ciberdefensa de su nivel como una herramienta principal, constituido como un sistema de armas, ya

sea para el desarrollo de operaciones defensivas en profundidad multicapa, que le permitirá integrar los medios puestos a disposición con los estados finales requeridos, y que le permitirán desgastar al oponente. Debido a la no linealidad del empleo conjunto que atañe al comandante, tiene la implicancia del combate no clásico, por esta razón y por la transversalidad del ciberespacio, estas operaciones cibernéticas permitirán degradar al oponente y sus sistemas de comando y control, comunicaciones, inteligencia, adquisición de blancos y reconocimiento. Buscando con los efectos la paralización y colapso del enemigo.

En el marco de operaciones militares, se ejecutan sólo a orden, aquellas ofensivas, como consecuencia de la detección dificultosa de la atribución del ataque; por tal motivo, se sincronizarán dentro del diseño operacional para restituir los sistemas propios y afectar los del oponente, dentro de la operación principal y/o las operaciones secundarias o contribuyentes, aquellos efectos para alcanzar el logro de los objetivos operacionales asignados por la estrategia militar que refieren a infraestructuras críticas de la información de defensa.

Durante la paz se realizarán únicamente acciones pasivas con efectos de proteger, prevenir, preservar y restituir los sistemas. Pero con estos efectos inician las limitaciones durante la paz para poder contrarrestar u obtener capacidad de resiliencia cibernética, debido a que las operaciones de exploración; con efectos de identificar, vigilar, que destacan a la ciberinteligencia particularmente y en el caso de una acción fuera de una operación, también restringe a las operaciones ofensivas, indirectas o de ataque, y de aquellas que tendrán por objetivo efectos de interrumpir, degradar, neutralizar, denegar los sistemas de la atribución detectada.

Por lo tanto la ciberdefensa ofrece como herramienta diferentes posibilidades, pero a la vez limitaciones distintivas presentes en este dominio; para el Instrumento Militar en su planeamiento y supervisión de la acción, da ventajas en la conducción, que favorecerán a concretar o coadyuvar al objetivo operacional, y cooperar con órganos externos del Sistema de Defensa Nacional; lograr la sorpresa explotando vulnerabilidades de las capacidades críticas de los sistemas enemigos; y también poder reducir costos integrando operaciones de guerra electrónica en esta teoría de multicapas.

En base a esto, el Comandante, deberá planificar sus operaciones en el ciberespacio teniendo en cuenta que hay limitaciones ejercidas por el marco legal, que reducen el empleo en diferentes ámbitos, ya sea para obtener información previo a las operaciones, en su fase preparación, como así también en el durante de las mismas. Por consiguiente analizada la legislación nacional, uno de los puntos que queda expresamente establecido en la reglamentación, es que el sistema de defensa nacional, no puede contemplar situaciones pertenecientes al ámbito de la seguridad interior, conforme la delimitación establecida en la Ley de Seguridad Interior N°

24059. Este estudio especifica e identifica entonces, que el concepto de ciberdefensa de la República Argentina, en el marco de la normativa, sólo rige dentro del sistema de defensa nacional, siguiendo un modelo de carácter defensivo y orientado al desarrollo de capacidades.

En la actualización de la Directiva de Política de Defensa Nacional, por Decreto N° 457/2021, existe en la legislación argentina una definición específica de ciberdefensa que se incluye en esta directiva; asimismo en el capítulo I, realiza el diagnóstico y apreciación de los escenarios global y regional de defensa, y articula a la defensa nacional con la política exterior para el cumplimiento de sus misiones de paz regional y vigencia del derecho internacional, a fin de proteger los intereses vitales y estratégicos nacionales. Ejerce limitación en la acción, porque excluye en este ciclo, la guerra contra el terrorismo, la concepción de nuevas amenazas y guerra asimétrica, como todo lo que conlleva sobre capacitación, doctrina, organización, planeamiento y equipamiento, confirmando y ratificando lo que establece la Ley N° 23554 sobre el empleo de las fuerzas armadas en acciones contra actores externos con fuerzas regulares (Presidencia de la Nación, 2021).

Pero a su vez resalta la necesidad de permanecer en la línea del planeamiento de ciberdefensa, ya que a través del aumento tecnológico y de la transmisión de datos e información sensible, implica el desarrollo de políticas de planeamiento, coordinación, dirección, ejecución y control y supervisión del ciberespacio para tener presencia en el control de los medios de transmisión y almacenamiento de datos. Dando con esto un amplio marco de control en el momento de asignarse infraestructuras críticas al Comando Operacional.

La Directiva de Política de Defensa Nacional, es dentro del marco legal del nivel estratégico militar y operacional, un determinante en lo que respecta a las limitaciones y obligaciones que puede ejercer la ciberdefensa. Por consiguiente, es indispensable tomar una perspectiva soberana en este dominio y reorientar los esfuerzos y recursos a este ámbito. En operaciones es una obligación para este nivel tener el control más allá de los límites del teatro. Debe ser considerado en el planeamiento de las operaciones cibernéticas.

En el marco regional principalmente en la presencia ilegal del Reino Unido de Gran Bretaña e Irlanda del Norte en las Islas Malvinas, Georgias del Sur Sándwich del Sur, espacios marítimos e insulares, Territorio Nacional Antártico, exige a los efectos de garantizar los intereses vitales, debe le Instrumento Militar el control, la vigilancia, el reconocimiento y la producción de inteligencia militar estratégica de los espacios aeroespaciales, terrestres, marítimos, insulares y ciberespaciales; para generar disuasión razonable y efectivo, a fin de afianzar el derecho sobre el mencionado territorio.

En el nivel operacional, 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 (Ministerio de Defensa, 2021). Así permite aumentar la posibilidad de generar efectos militares nuevos, de forma combinada entre lo convencional y lo innovador, basados en nuevas tecnologías y lograr así ventajas operacionales y estratégicas acordes a los objetivos operacionales y estados finales deseados.

Considerando que la directiva otorga al Ministerio de Defensa la posibilidad de ordenar el establecimiento de un dispositivo de defensa militar para proteger uno o varios objetos de valor estratégicos a través del despliegue de una capacidad militar para prevenir o conjurar un eventual ataque contra un objeto de valor estratégico, a partir de la disposición de la correspondiente alerta temprana estratégica; o bien como resultado de la necesidad de contar con un dispositivo de defensa militar ante un evento de naturaleza estratégica, siendo este despliegue de carácter no permanente y que no se pueda ejecutar por la Seguridad Interior, abre las posibilidades de intervenir en diferentes marcos.

El relevamiento del marco legal nacional y particularmente de defensa, permite observar que, se ha producido un aumento significativo en las regulaciones sobre la ciberseguridad, ciberdefensa y ciberdelito; provenientes del uso masivo de las tecnologías de información y comunicación, que trajeron como consecuencia la existencia de nuevas amenazas. Pero dicho crecimiento normativo, no está exento de ambigüedades e interpretaciones; lo que afecta el desarrollo de doctrina; para de Vergara y Trama (2017), establecen respecto al desarrollo de doctrina sobre ciberdefensa, que la misma debe reducir a los comandantes los riesgos y favorecer la defensa como actividad principal, que provean adecuadas capacidades en el ejercicio del comando y control, resiliencia ante afecciones y alertas tempranas; y expresan que “el propósito común de las doctrinas militares en materia de ciberdefensa es alcanzar la superioridad informativa antes y durante el desarrollo de las acciones en el Teatro de Operaciones, reteniendo la libertad de acción en el espacio cibernético” (p. 160).

Dentro del análisis, las políticas de ciberdefensa establecidas por el Decreto N° 1380/2019, conceptualiza al ciberespacio como “un espacio soberano y la misión encomendada al Ministerio de Defensa de anticipar y prevenir ciberataques que pudieran comprometer la disponibilidad de los sistemas y redes de la Defensa” (Ministerio de Defensa, 2019) y determina los objetivos en materia de Ciberespacio; esto lleva a un planeamiento con dos focos para lograr los objetivos planteados; un plan de adecuación de las organizaciones militares y otro plan nacional de infraestructuras críticas de la defensa nacional; así otorga herramientas para contener

acciones dentro del marco legal nacional y facilitar el empleo de medios descentralizados en caso de ser necesario o aquellos que se requieran en otros ámbitos del Estado.

Por consiguiente para el Comandante, cualquier acto que afecte al Estado, lo habilita a responder con contramedidas proporcionales, incluyendo medidas cibernéticas, contra el agresor; pero sabiendo que cualquier operación en el ciberespacio va a constituir el uso de la fuerza, aun cuando la escalada y/o los efectos sean comparables con operaciones cinéticas. Existiendo la posibilidad de realizar acciones preventivas, basadas en el derecho de usar la fuerza en defensa propia, y neutralizar la fuente de dicha agresión basado en lo determinado por nuestra Ley de Defensa Nacional.

Otra herramienta legal para actuar, que posee el comandante en el nivel operacional es la Resolución N° 154-E/2017, que establece que la zona militar para ejercer competencias propias y poder repeler con sus medios cualquier delito que atente contra la seguridad de las instalaciones o aquello que tenga relación directa con la misma zona; así poder equiparse, capacitarse y actuar en cualquier dominio que se realice la afectación, y permitir el desarrollo de reglas de empeñamiento acordes para cada caso particular o la previsión de estos (Ministerio de Defensa, 2017).

Por tal motivo, el diseño de operaciones cibernéticas del nivel operacional, no pueden evaluarse por separado, es decir, el sistema de armas a emplear con el método a utilizar. La licitud del sistema no depende de su diseño o finalidad de empleo, sino que influye el cómo se va a utilizar y las circunstancias para su aplicación; esto dará a conocer las consecuencias legales o no que traiga el mismo. En tal sentido y durante las operaciones militares, dentro del teatro se encontrarán los objetivos de valor estratégicos y aquellas infraestructuras críticas de la información de la defensa nacional que haya determinado el nivel estratégico nacional y militar. Esto traerá diferentes vinculaciones con otros actores que podrán estar o no dentro del teatro de operaciones, pero que tendrán influencia en el planeamiento y adopción de medidas de protección y resiliencia cibernética de estos objetivos e infraestructuras y que deberán ser considerados para su análisis y coordinaciones.

Cabe destacar que la transición del planeamiento a la ejecución, es una gran limitación a las operaciones, por el cambio y adaptación que requerirán los planes y aquellos procedimientos que permitirán actuar dentro del ciberespacio; algunos ejemplos de aspectos a considerar para poder ejecutar las acciones en este nivel puede ser la actualización de los sistemas informáticos en relación a los cambios en el ambiente operacional, la actualización de la inteligencia y ciberinteligencia obtenida y capacidades, requerimientos y vulnerabilidades críticas en el ci-

berambiente de interés, previsión de planes de alternativa o correcciones progresivas; determinación de los agentes intervinientes (militares o civiles), a disposición (gobierno, sectores económicos y de servicios) y de aquellos necesarios fuera del nivel operacional (estratégicos nacionales o internacionales), entre otros; como lo establece el reglamento de Planeamiento para la Acción Militar Conjunta (2019).

Hasta el momento, el planeamiento y conducción de la ciberdefensa del nivel operacional, presentan una serie de limitaciones legales impuestas por la doctrina, el Estado y el derecho internacional; por lo que exigirá una mayor capacitación y conocimiento de la norma y doctrina, para poder confrontar las amenazas y encontrar la eficacia de las acciones, a través de una actuación colaborativa de las diferentes agencias que se encuentren en el teatro de operaciones, de índole pública o privada; interactuando para obtener datos e información; con la finalidad de facilitar las acciones derivadas de una evolución hacia situaciones de crisis o conflictos en el ciberespacio; asegurando su uso efectivo, impidiendo o dificultando su uso contra los intereses de la defensa nacional. Generando con esto, una facilidad más para el comandante de mantener un cierto grado de libertad de acción del instrumento militar que le depende, a través del logro de una disuasión real en el ciberespacio de interés integrando todos los sensores y alertas que operen en el mismo.

Conclusiones finales

En el presente trabajo, se ha realizado la lectura analítica de las leyes de defensa nacional, seguridad interior e inteligencia, sumado a los decretos presidenciales, ministeriales y secretariales concernientes al ciberespacio; y en el marco internacional, los tratados y convenios relacionados con la ciberseguridad a los cuales el Estado adhiere. Y dentro del marco de la defensa, de los proyectos de doctrina y en vigencia, preservando su clasificación de seguridad.

Esto favorece el arribo a las conclusiones finales; que serán relevantes para dar respuesta al problema planteado y al contexto donde se desarrollan las operaciones de ciberdefensa del nivel operacional. Asimismo y teniendo en cuenta la profundidad de los tecnicismos del derecho, y principalmente la interpretación del mismo; se ha considerado desde una perspectiva nacional y desde una posición de defensa y concernientes al ciberespacio en su empleo y explotación con fines únicamente militares.

En el nivel operacional, el comandante, se encuentra en una posición con una división claramente marcada entre las áreas de seguridad y defensa, basada en un criterio geográfico, el cual no es de aplicación, particularmente, en el ciberespacio debido a su naturaleza no especial, y al criterio de atribución de la acción. Es relevante la problemática de la atribución, y la determinación fehaciente del origen de un ataque, siendo un reto en la asignación de objetivos o puntos decisivos; especialmente cuando los actores elaboran sus intrusiones para confundir a la búsqueda de quién es el responsable.

En base a esto, uno de los problemas y restricciones más importantes que tiene la ciberdefensa desde lo legal y en la paz o conflicto; cuando el origen de un ataque se puede localizar dentro de un Estado en particular, sería difícil determinar si el atacante estaba actuando de manera individual, o en nombre de una organización criminal, el gobierno o las fuerzas armadas. De aquí surgen las limitaciones analizadas de la Ley N° 23554 de Defensa Nacional y la Ley Nº 24059 de Seguridad Interior. Ambas son taxativas respecto a los límites y qué puede hacer cada parte en las circunstancias determinadas.

La división genera un inconveniente en el proceso de planeamiento de las ciberoperaciones, como en su evolución, al no poder contar con la ciberinteligencia previa para conocer capacidades y vulnerabilidades del oponente o aquellos puntos de accesos propios, y poder generar posibles respuestas ante intromisiones. Esta limitación de la inteligencia militar dada por el marco legal y el doctrinario para el nivel operacional, dificultan la anticipación frente a la constitución de potenciales amenazas cibernéticas cualquiera sea su origen.

Las limitaciones también están circunscriptas en resoluciones, en las cuales determinan restricciones al momento de detectar una afectación de las infraestructuras críticas, debiendo

realizar el análisis de aquellas fronteras territoriales, marítimas o espaciales de la nación que se vulneren y cuál es el impacto sobre la soberanía nacional, cuando mediante la afectación de un sistema informático se cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio de nacional. Lo cual, para el comandante, será un factor determinante, para el planeamiento y ejecución de acciones para el logro de efectos de protección de los sistemas propios y proteger o mantener una disponibilidad del ciberespacio como espacio soberano.

De los reglamentos militares y de la Directiva de Política de Defensa Nacional vigente, se destaca que el espacio se encuentra definido con límites geográficos; si bien es necesario para poder determinar la soberanía y territorialidad del Estado; en el nivel operacional, el establecimiento de un teatro de operaciones deja circunscripto el ciberespacio a límites que son imposibles de contemplar, quitando flexibilidad y limitando el accionar de los elementos asignados para ciberdefensa. Esto da como resultado la carencia de la flexibilidad necesaria para neutralizar los efectos en oportunidad, dado que surge la dificultad para identificar la autoría, objetivos e interés del oponente.

Se aprecia que el establecimiento de un teatro de operaciones, particularmente para el ciberespacio, es un aspecto doctrinario poco flexible, quita integración, limita el intercambio de información con organismos adyacentes de interés o aquellas infraestructuras críticas que pueden vulnerar las que se encuentran dentro del mismo, disminuye la capacidad de trabajar interagencialmente, reducida ya por la Ley de Seguridad Interior y decretos relativos; impidiendo hacer frente eficientemente a efectos generados a través del ambiente ciber, que afectará al ambiente operacional contextualizado.

Se puede decir que aun existiendo un principio de legítima defensa, el uso de la fuerza, incluida la fuerza letal, debe basarse en los criterios de necesidad y proporcionalidad. Pueden surgir ciertas ambigüedades jurídicas con respecto a la legítima defensa nacional, aunque tanto el derecho internacional como el derecho nacional dejan claro que éste se deriva de las facultades conferidas por la Carta de las Naciones Unidas. Pero resultan dos aspectos importantes, uno sobre lo que permite que un Estado use la fuerza antes de una agresión real que, de llevarse a cabo, podría tener consecuencias devastadoras para ese Estado, como un ciberataque sobre lugares vitales. Por otro lado, basado en la agresión externa, de la Directiva de Política de Defensa Nacional, donde el uso de la fuerza armada por uno o más países contra los intereses esenciales de la nación, y sobre qué actos pueden ser considerados agresión armada o externa y de dónde debe provenir un ataque armado, en este caso cibernético.

El estudio concluye que el ordenamiento jurídico argentino aún no cuenta con una codificación general y sistemática de las ciberdefensa. Una sistematización del marco legal y regulatorio, y definir mejor los objetivos, poderes y funciones de las diversas agencias gubernamentales puede ser muy útil y ayudar a lograr algunas metas estratégicas que contribuyan al nivel operacional.

Tanto como el desarrollo entre otras cosas del diseño de tecnologías digitales destinadas a salvaguardar los intereses nacionales y participación regional e internacional, la priorización de los procesos legislativos destinados a regular las actividades críticas tanto del sector público como del privado sobre la ciberseguridad y que responsabilidades otorgar a las fuerzas, y mejorar las regulaciones entre la seguridad interior y la defensa nacional. Claramente esto supera al nivel operacional, pero no quita que el comandante durante el ejercicio de su comando pueda solicitar al nivel estratégico propuestas para otorgarle mayor libertad de acción y respuesta.

Finalmente, las conclusiones expuestas, y en consonancia con los objetivos particulares planteados, permiten considerar que el objetivo general ha sido alcanzado satisfactoriamente; en consecuencia, los capítulos desarrollados dan respuesta al problema de investigación planteado de cómo influye el marco legal de la República Argentina en el planeamiento y ejecución de las operaciones en el ciberespacio desde una perspectiva del nivel operacional.

Y en virtud de las conclusiones a las que se ha arribado; como aporte profesional a esta investigación, surge la necesidad de complementar la investigación, orientada a abordar la misma desde el punto de vista al que se enfrenta el derecho tradicional, ya al ser un instrumento de ordenamiento jurídico, debe actualizarse, principalmente por la propia costumbre; adaptando los parámetros específicos que la guerra actual impone en acciones en el ciberambiente. Se aprecia también que es recomendable tener una visión actual más amplia al menos en materia de ciberdefensa, pero enfocada en la permeabilización de la distinción entre seguridad y defensa, problemática no puede ser enmarcada en el nivel operacional, pero sí que desde este nivel surgen las propuestas por la continua operación de estos sistemas y suma de experiencias.

Claramente este nivel es quien debe enfocarse en la propia doctrina, siendo el principal elemento a realizarlo, considerando esto como otra área de investigación complementaria. En este contexto, se podrán determinar los alcances que pueda tener o no el comandante operacional y sus competencias para poder establecer reglas de empeñamiento y mecanismos técnico-operativos más eficaces para la resolución del conflicto.

Referencias.

Anca, J. (2017). *La conducción de las operaciones de ciberdefensa: Principios básicos en el campo de combate moderno.* Escuela Superior de Guerra, pp. 33-34.

Baretto, J. (2017). *La defensa nacional y la estrategia militar de seguridad cibernética*. Escuela Superior de Guerra Conjunta, p. 10.

Casarino, P. y Ortiz, J. (2019). *La Ciberdefensa y la Ciberinteligencia Militar*. Visión Conjunta, Año 11, N° 21. Escuela Superior de Guerra Conjunta, p. 51.

Comité Internacional de la Cruz Roja (CIRC) (2019). *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, pp. 2 y 26-28. https://www.icrc.org/es/publication/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados.

Comité Jurídico Interamericano (1 de noviembre de 2020). *Derecho Internacional y Operaciones Cibernéticas del Estado*, Washington DC, Estados Unidos, pp. 3-7.

Convenio de Budapest (23 de noviembre de 2001). *Convenio sobre la Ciberdelincuencia*. Consejo de Europa, Budapest, p. 2.

De Vergara, E. y Trama, G. (2017). *Operaciones Militares Cibernéticas. Planeamiento y Ejecución en el Nivel Operacional*. Editorial Visión Conjunta, pp. 8-29 y 160.

Decisión Administrativa N° 669 de 2004 (Jefatura de Gabinete de Ministros). *Por la cual se establecen las Políticas de Seguridad de la Información para el Sector Público Nacional.* 20 de diciembre de 2004.

Decreto N° 457 de 2021 (Presidencia de la Nación). *Por el cual se actualiza la Directiva de Política de Defensa Nacional como anexo del presente decreto*. 14 de julio de 2021.

Decreto N° 571 de 2020 (Presidencia de la Nación). *Por el cual se establece la derogación de los Decretos N° 683 del 23 de julio de 2018 y N° 703 del 30 de julio de 2018; restablecer la vigencia de los Decretos N° 727 del 12 de junio de 2006 y N° 1691 del 22 de noviembre de 2006; restablecer la vigencia de los Decretos N° 1714 del 10 de noviembre de 2009 por el que se aprobara la "Directiva de Política de Defensa Nacional" y su actualización aprobada por el Decreto N° 2645 del 30 de diciembre de 2014 "Directiva de Política de Defensa Nacional (DPDN 2014)"*. 26 de junio de 2020.

Decreto N° 577 de 2017 (Presidencia de la Nación). *Por la cual se establece la creación del Comité de Ciberseguridad en la órbita del Ministerio de Modernización*. 28 de julio de 2017.

Decreto N° 683 de 2018 (Presidencia de la Nación). *Por el cual se deroga el Decreto 727/2006*. 24 de julio de 2018.

Decreto N° 703 de 2018 (Ministerio de Defensa). *Por el cual se establece la Directiva de Política de Defensa Nacional y deroga los Decretos N° 1714 del 10 de noviembre de 2009 y N° 2645 del 30 de diciembre de 2014*. 30 de julio de 2018.

Decreto N° 1311 de 2015 (Presidencia de la Nación). *Por el cual se establece la nueva doctrina de Inteligencia Nacional y su Anexo 1 que forma parte del mismo*. 06 de julio de 2015.

Decreto N° 1380 de 2019 (Ministerio de Defensa). *Por la cual se establecen las Políticas de Ciberdefensa y creación de organismos dependientes del Ministerio de Defensa en materia de Ciberdefensa.* 29 de octubre de 2019.

Decreto N° 1729 de 2007 (Presidencia de la Nación). *Por el cual se aprueba el Ciclo de Planeamiento de la Defensa Nacional*. 27 de noviembre de 2007.

Eissa, S., Gastaldi S., Poczynok, I. y Zacarías Di Tullio, E. (2014). *El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino*. Revista de Ciencias Sociales de la Universidad Nacional de Quilmes Número 25, pp. 181-197.

Estado Mayor Conjunto (2014). *PC-00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta*. Estado Mayor Conjunto de las Fuerzas Armadas, p. 42.

Estado Mayor Conjunto (2019). *PC-20-01 Planeamiento para la Acción Militar Conjunta - Nivel Operacional*. Estado Mayor Conjunto de las Fuerzas Armadas, pp. 85-87.

Fonseca, J. y Ansorena Gratacos, M. (2017). *La Defensa Cibernética: Alcances estratégicos, proyecciones doctrinarias y educativas*. Escuela Superior de Guerra, p. 35.

Gómez, M. (2017). *La resiliencia aplicada al nivel operacional en el ambiente cibernético.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, pp. 3-8.

Jefatura de Gabinete de Ministros, Dirección Nacional de Diseño Organizacional, Coordinación Mapa del Estado. (09 de septiembre de 2021). *Administración Pública Nacional. Administración Central y Organismos Desconcentrados. Autoridades Superiores*. https://mapadelestado.jefatura.gob.ar/organigramas/autoridadesapn.pdf.

Ley N° 23554. *Ley de Defensa Nacional*. 13 de abril de 1988.

Ley Nº 24059. *Ley de Seguridad Interior*. 18 de diciembre de 1991.

Ley N° 25520. *Ley de Inteligencia Nacional*. 27 de noviembre de 2001.

Ley N° 27126. *Agencia Federal de Inteligencia*. 03 de marzo de 2015.

Ley N° 27411. *Convenio sobre Ciberdelito*. 15 de diciembre de 2017.

Ministerio de Defensa (2010). *Manual de Derecho Internacional de los Conflictos Armados.* 1ra Edición, Buenos Aires, Ministerio de Defensa, pp. 89-92.

Organización de las Naciones Unidas (26 de junio de 1945). *Carta de las Naciones Unidas*, United Nation, pp. 13 y 16.

Organización del Tratado del Atlántico Norte (2013). *Tallinn Manual 1.0. Tallinn Manual on the International Law Applicable to Cyber Operations*. Cambridge University, p. 54.

Organización del Tratado del Atlántico Norte (2017). *Tallinn Manual 2.0. Tallinn Manual on the International Law Applicable to Cyber Operations*. Cambridge University, p. 19.

Resolución N° 13 de 2014 (Secretaría de Comunicaciones). *Por la cual se establece la creación de la Comisión Argentina de Políticas de Internet.* 23 de abril de 2014.

Resolución N° 69 de 2016 (Ministerio de Justicia y Derechos Humanos). *Por la cual se establece el Programa Nacional contra la Criminalidad Informática*. 11 de marzo de 2016.

Resolución N° 154-E/2017 (Ministerio de Defensa). *Por la cual se establecen los principios para ser aplicados ante hechos delictivos contra la Zona Militar.* 21 de febrero de 2017.

Resolución N° 343/2014 (Ministerio de Defensa). *Por la cual se establece la creación de la Unidad de Coordinación Cibernética; y las Direcciones de Ciberdefensa del Ejército Argentino, de la Armada de la República Argentina y de la Fuerza Aérea Argentina*. 14 de mayo de 2014.

Resolución N° 364 de 2006 (Ministerio de Defensa). *Por la cual se establece la creación del Comité de Seguridad de la Información del Ministerio de Defensa*. 12 de abril de 2016.

Resolución N° 385 de 2013 (Ministerio de Defensa). *Por la cual se establece la creación de las Direcciones de Ciberdefensa de las Fuerzas Armadas*. 22 de octubre de 2013.

Resolución N° 580 de 2011 (Jefatura de Gabinete de Ministros). *Por la cual se crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*. 28 de julio de 2011.

Resolución N° 829 de 2019 (Secretaría de Gobierno de Modernización). *Por la cual se establece la Estrategia Nacional de Ciberseguridad*. 24 de mayo de 2019.

Resolución N° 1523 de 2019 (Secretaría de Gobierno de Modernización). *Por la cual se establece la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.* 12 de septiembre de 2019.

Segura Serrano, A. (junio-diciembre 2017). *Ciberseguridad y derecho internacional.* Revista Española de Derecho Internacional. Volumen 69/2. Madrid, p. 296.

Spretz, N. (2018). *Las operaciones de información de nivel operacional y su influencia en el ambiente informacional.* Escuela Superior de Guerra, p. 10.

United States Army (Abril de 2017). FM 3-12 Cyberspace and Electronic Warfare Operations. Headquarters – Department of the Army, pp. III 8.

Anexo 1.

Esquema gráfico – metodológico.

<table>
<tr><td colspan="2">Tema del trabajo final de investigación.
Implicancias legales en la ejecución de operaciones militares (conjuntas y combinadas) en el ciberespacio.</td></tr>
<tr><td colspan="2">Formulación del problema del trabajo final de investigación.
¿Cómo influye el marco legal de la República Argentina en el planeamiento y ejecución de las operaciones en el ciberespacio desde una perspectiva del nivel operacional?</td></tr>
<tr><td colspan="2">Objetivo general del trabajo final de investigación.
Evaluar la situación y probable evolución de la normativa vigente de ciberseguridad y ciberdefensa para el nivel operacional y su adecuación a las restricciones del derecho nacional e internacional.</td></tr>
<tr><td>Capítulo I.
Adecuación del marco legal internacional y nacional al ciberespacio.</td><td>Capítulo II.
La ciberdefensa en el nivel operacional y sus limitaciones legales y doctrinarias.</td></tr>
<tr><td>Objetivo particular Nro 1.
Analizar el plexo normativo general internacional y nacional, y su adecuación a los cambios que impone el ciberespacio.</td><td>Objetivo particular Nro 2.
Analizar el marco jurídico nacional y la doctrina vigente; las adaptaciones necesarias y las limitaciones implícitas para las operaciones en el ciberespacio.</td></tr>
<tr><td>Leyes Nacionales, Decretos, Normas, Directivas de índole Nacional e Internacional, Trabajos de Investigación.</td><td>Doctrina Conjunta, Específica, Doctrina Fuerzas Armadas Extranjeras, Trabajos de Investigación, Informes, Libros de Investigación.</td></tr>
<tr><td>Análisis bibliográfico, análisis documental y análisis lógico.</td><td>Análisis bibliográfico, análisis documental y análisis lógico.</td></tr>
<tr><td colspan="2">Conclusiones finales.</td></tr>
</table>