MATERIA:

TALLER DE TRABAJO FINAL INTEGRADOR

TEMA:

INTEGRACIÓN DE LAS OPERACIONES DE GUERRA ELECTROMAGNÉTICA Y CIBERDEFENSA EN EL ÁMBITO PARA LA ACCIÓN MILITAR CONJUNTA.

TÍTULO:

HACIA LA CREACIÓN DE UNA FUERZA CIBERNÉTICA EN LA REPÚBLICA ARGENTINA.

AUTOR: MAYOR (EA) JUAN JOSÉ DELGADO.

TUTOR: TENIENTE CORONEL OIM (EA) CARLOS AMAYA.

Año 2022

Resumen

El ambiente ciberespacial de interés nacional requiere ser abordado de manera integral a nivel nacional para velar por los intereses de los argentinos, aunando los diferentes esfuerzos contra el accionar de actores indeseados que buscan afectar los sistemas e infraestructuras críticas usando especialmente el espectro electromagnético para el desarrollo de sus acciones.

Si bien en los últimos años se pueden observar importantes avances en este sentido, tales como la creación de organismos de coordinación y las acciones de los distintos ministerios y secretarías, las fuerzas armadas, comandadas por el jefe de estado, representan la última herramienta para asumir la defensa de la nación contra un enemigo militar externo. Expresado de otra manera, es un instrumento a disposición del estado para defender sus intereses vitales.

En el marco de una actitud estratégica defensiva, y tratando de proteger o brindar seguridad a las propias infraestructuras críticas, el Estado Argentino cuenta actualmente con un elemento al nivel conjunto, el Comando Conjunto de Ciberdefensa, y en el nivel específico, cada fuerza cuenta con su propia Dirección de Ciberdefensa, cada una de estas dependientes de su respectiva Dirección General.

Estas unidades mencionadas cuentan con un reducido grupo de especialistas para afrontar dicha responsabilidad, sin mencionar la poca interacción con otras áreas y/o agencias, necesarias para llevar adelante las acciones y reacciones correctas en el dominio del ciberespacio, entre ellas la ciberinteligencia o diferentes áreas como por ejemplo el Ministerio de Seguridad o el Comité de Ciberseguridad, el ciberdelito y cibercrimen, entre otras.

El presente trabajo de investigación busca analizar las ventajas y desventajas de crear una fuerza cibernética que integre las operaciones en el espectro electromagnético y la ciberdefensa para hacer frente tanto a los ciberataques que constantemente reciben las infraestructuras críticas de las fuerzas armadas o aquellos objetivos de valor estratégico que el poder ejecutivo determine para su protección, como así también los ciberataques que pretendan obstaculizar las operaciones del instrumento militar en caso de encontrarse en operaciones.

1.1. Palabras Clave.

Ciberdefensa – Cibernética - Ciberataques – Electrónica - Fuerza.

Índice General

Índice de Figuras

Introducción

En los últimos años se ha registrado un gran desarrollo tecnológico en el ambiente del ciberespacio, con el uso de las tecnologías de la información y de la comunicación, en la inteligencia artificial, que ha logrado importantes avances especialmente en el aprendizaje autónomo y que está presente de diferentes maneras en nuestra vida cotidiana. De acuerdo con lo mencionado precedentemente, se puede inferir que incluso hay un mayor empleo del espectro electromagnético para la transmisión y recepción de los datos. En su conjunto, esto nos revela un escenario en el que el intercambio de información, propio para que los sistemas continúen funcionando, conlleva serios riesgos y amenazas que pueden afectarlos.

Durante el desarrollo de las acciones bélicas en la actual guerra entre Rusia y Ucrania se observó claramente el volumen de actividades desarrolladas en el ciberespacio y la importancia del desarrollo de capacidades, especialmente para la protección de las infraestructuras críticas (IICC). Los distintos perfiles de atacantes que apoyan a ambos bandos explotan las vulnerabilidades tecnológicas del bando rival con objetivos claros como el de afectar los sistemas de comando y control, recabar información, sustraer activos de gran valor o amenazar servicios básicos, es decir, afectar de diferentes maneras a las infraestructuras.

La importancia del control y el dominio del ciberespacio está ocupando un lugar cada vez más importante en la agenda de temas estratégicos de los diferentes países, aspecto que claramente afecta también a las fuerzas armadas. Algunos países como los Estados Unidos de Norteamérica, la República Federal de Alemania y el Reino Unido de Gran Bretaña, inclusive han reestructurado sus fuerzas armadas, creando una fuerza ciber que integra desde las actividades de comando, control y comunicaciones, continuando con las operaciones electromagnéticas e incluyendo también actividades de información, inteligencia y contrainteligencia.

Relacionado con el planteo del problema, y como se expresó anteriormente en el resumen, el presente trabajo de investigación analizará en profundidad las ventajas y desventajas que trae aparejado el hecho de que el Estado Argentino cuente con una fuerza cibernética con la capacidad de integrar las operaciones de ciberdefensa y electromagnéticas para hacer frente tanto a los ciberataques que reciben las IICC de las fuerzas armadas como aquellos objetivos de valor estratégico (OVE) que el poder ejecutivo determine para su protección; del mismo modo, contrarrestar los ciberataques que pretendan obstaculizar las operaciones del instrumento militar en el caso de encontrarse en operaciones.

Tal es así que surge, entonces, el interrogante que da lugar al problema de la investigación, y se trata de: ¿Cuáles son las ventajas y desventajas de contar con una fuerza que integre las operaciones de ciberdefensa y electromagnéticas para el Estado Argentino?

En el desarrollo de esta nueva fuerza, se encuentran implícitas la evolución y el continuo desarrollo de las capacidades para accionar tanto en el ciberespacio como en el espectro electromagnético soberanos, ejercidas desde un comando único e independiente y adaptables a lo dispuesto por el jefe de estado para accionar también en los OVE que revistan importancia trascendente para el estado.

El objetivo general de la investigación es el de evaluar las ventajas y desventajas de una estructura organizacional unificada de ciberdefensa y operaciones en el espectro electromagnético para el Estado Argentino.

El primer objetivo particular es el de analizar las estructuras de ciberdefensa en los países de Estados Unidos, Alemania y Gran Bretaña y su adecuación a los cambios que impone el dominio del ciberespacio, identificando sus características distintivas como fuerzas independientes.

El segundo objetivo particular es el de determinar ventajas y desventajas de una estructura unificada que permitan establecer características de su diseño organizacional.

Como hipótesis, el Estado Argentino requiere que sus fuerzas armadas cuenten con una estructura unificada e independiente, capaz de integrar el trabajo de diferentes agencias que ejecutan operaciones desarrolladas en el espectro electromagnético y en el ciberespacio soberano nacional, para estar en capacidad de alerta permanente ante las diferentes amenazas en este dominio y poder contrarrestar los posibles ciberataques a las infraestructuras y sistemas críticos.

Para alcanzar el objetivo general y los objetivos particulares, se empleará el método de tipo descriptivo y deductivo, para ello se realizará el análisis de distintas fuentes abiertas y la descripción durante el desarrollo de cada capítulo a fin de obtener la conclusión general que permita dar respuesta al objetivo general planteado para la investigación.

Respecto del diseño de la misma, 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. Respecto a las fuentes bibliográficas principales empleadas, se basan particularmente en: leyes y derivados de índole nacional e internacional, doctrina conjunta y específica nacional y

extranjera; las fuentes secundarias serán sobre trabajos de investigación, informes y publicaciones y libros de investigación.

Cabe aclarar que en lo que respecta al enfoque doctrinario y en aquellos casos particulares donde la clasificación de seguridad lo imponga, se ve conveniente únicamente hacer mención de la existencia o proyectos futuros de la misma, pero no hacer referencias o citas que pongan en riesgo información clasificada. Sin embargo, se dará la opinión fundada de su alcance actual y en prospectiva.

Relacionado con el estado del arte, en el último quindenio, las fuerzas armadas a nivel internacional han incluido en sus diferentes procesos de planificación estratégica las acciones necesarias para actualizar y complementar sus propias doctrinas, el desarrollo orgánico y tecnológico en cuanto a la ciberdefensa, con la finalidad de obtener un conjunto de capacidades que le permitan operar en esta nueva dimensión presente tanto en los conflictos armados como en tiempos de paz.

Para los Estados Unidos de Norteamérica, el dominio ciberespacial posee características particulares que lo convierten en un dominio diferente a los cuatro estados (aire, mar, tierra y espacio), por ello es que se lo entiende como reciente e independiente, por lo tanto, requiere de una elevada especificidad ya que el adversario buscará obtener la ventaja estratégica en este nuevo escenario.

Como antecedentes se puede mencionar que las nuevas formas de hacer la guerra involucran un amplio uso del ciberespacio, además del desarrollo de capacidades de bajo costo o que materialicen la economía de fuerzas.

Es por estas razones que en el año 2009 se plantea la necesidad que los EEUU cuenten con una fuerza cibernética conjunta, que se dedique exclusivamente al dominio del ciberespacio, nace así el Cibercomando (USCYBERCOM).

Según Graham, M. (2016) las FFAA estadounidenses han acompañado el desarrollo del ciberespacio y lo referido a la guerra cibernética hasta conseguir que el departamento de defensa establezca el comando cibernético, el cual tiene un carácter conjunto para llevar adelante y organizar los esfuerzos del departamento en el ciberespacio. Agrega además que parte del presupuesto se asigna de manera directa a este comando y otros recursos provienen de las distintas fuerzas, es por ello que cada institución estableció un cuartel general de componente, similar a las direcciones de ciberdefensa argentinas, por ejemplo: el comando cibernético del ejército o el comando cibernético de la flota.

De acuerdo con Cañete, P.A. (2020), en el marco de la última reestructuración de las fuerzas armadas de la República Federal de Alemania, en abril del 2017 es creado el comando

del espacio de información y ciber (en adelante Kdo CIR), el cual cuenta con una acabada integración entre diferentes áreas técnicas para el comando y el control de las operaciones.

Uno de los aspectos que más llama la atención es el hecho que este Kdo CIR conduce al comando de inteligencia estratégica, el comando técnico de la información y el centro de geoinformación, es decir, materializa la integración antes mencionada entre las actividades de defensa del ciberespacio, del espectro electromagnético, las comunicaciones e información y las actividades de inteligencia estratégica.

En el marco de un creciente debate público sobre cuándo y cómo los gobiernos deben realizar operaciones ofensivas en el ciberespacio (contra terroristas, criminales y amenazas estatales), el Reino Unido de Gran Bretaña anunció recientemente una nueva inversión significativa en sus capacidades cibernéticas ofensivas.

Gran Bretaña lleva adelante el concepto de un poder cibernético democrático y responsable para enmarcar sus aspiraciones cibernéticas, pero hasta ahora este concepto y cómo se ejecutará se entienden solo en un esquema básico.

Al momento de estructurar el Sistema Nacional de Ciberdefensa en el Estado Argentino, se encuentra que la cabeza del mismo estaría a cargo del actual Comandante Conjunto de Ciberdefensa, quien depende en estrecha relación tanto del Jefe del Estado Mayor Conjunto como matricialmente del Subsecretario de Ciberdefensa, quien puede ejecutar control funcional.

En lo referente a la ciberseguridad, la jefatura de gabinete de ministros es la responsable de la misma, para lo cual cuenta, dentro de la Secretaría de Innovación Pública, con dependencia de la Subsecretaría de Tecnología de la Información y Comunicaciones, con la Dirección Nacional de Ciberseguridad. El Ministerio de Seguridad se encarga del ciberdelito, para lo cual se apoya en las Fuerzas de Seguridad y, finalmente, el Ministerio de Defensa se encarga de los aspectos referidos a la ciberdefensa protegiendo las infraestructuras críticas (IICC) del instrumento militar y aquellos objetivos de valor estratégico (OVE) que la jefatura de gabinete de ministros le asigne al ministerio de defensa para su protección (Ministerio de Defensa, 2014).

En cuanto a 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 son esenciales para la Nación, deben ser establecidas por el organismo responsable dependiente de la ciberseguridad. Como respuesta a esto, a nivel nacional se crea por Decreto N° 577 de fecha 28 de julio de 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 contra la seguridad de la información nacional (Presidencia de la Nación, 2017).

Desde el año 2017 a nivel nacional se trata de desarrollar una Estrategia Nacional de Ciberseguridad, con la intención de impulsar 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.

Con la implementación de la nueva Directiva de Política de Defensa Nacional (2021), se pone en marcha el proceso de planificación estratégico, 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).

Enmarcados en el ámbito del Ministerio de Defensa, la ciberdefensa se encuentra en un proceso de actualización y desarrollo doctrinario tanto específico, como en el ámbito conjunto; establece y da marco a las acciones que ejecutan las direcciones de ciberdefensa, favoreciendo el desarrollo de un programa de carrera, posgrados y cursos con el afán de desarrollar las capacidades necesarias para desenvolverse correctamente en este dominio que exige un elevado nivel de formación técnica y poder de resiliencia de los sistemas.

La presente investigación, además, tiene interés particular en el nivel estratégico operacional. En este sentido, y habiendo analizado el marco normativo de países que actualmente poseen tropas en diferentes conflictos, buscará determinar objetivamente cuáles son las principales ventajas y desventajas de contar con una fuerza capaz de operar de manera permanente en operaciones en el ciberespacio.

Asimismo, se pretende incluir el trabajo inter agencial de diferentes áreas necesarias para conformar esta nueva fuerza que deberá tener las competencias que le permitan el control y dominio del ciberespacio soberano nacional en todo momento, así como el ya mencionado poder de resiliencia de las estructuras básicas de telecomunicaciones afectadas.

Respecto de las limitaciones, se pueden mencionar, principalmente, la evolución permanente de la tecnología, lo que condicionará la eficiencia de las tropas pertenecientes a esta fuerza e inclusive su permanente actualización y capacitación y, finalmente, la evolución en cuanto al marco normativo nacional que limita las acciones en el dominio ciberespacial ya sea desde el punto de vista de la ciberdefensa o la ciberseguridad, según corresponda.

Desde el punto de vista estratégico operacional, el ciberespacio requiere un abordaje sinérgico de diferentes áreas, entre ellas las referidas a las operaciones electromagnéticas, la ciberinteligencia, la ciberdefensa y la ciberdisuasión, todas bajo una unidad de comando que permita optimizar los recursos y facilitando la eficiencia y eficacia en el cumplimiento de las misiones requeridas para la defensa de las infraestructuras críticas de las fuerzas y de los intereses de la nación en este nuevo y complejo dominio.

Capítulo 1

Estructuras de ciberdefensa en el marco internacional

Como se expresara en la introducción, en el presente capítulo se analizarán y compararán las estructuras de ciberdefensa en la República Federal de Alemania (RFA), Estados Unidos de América (EEUU) y el Reino Unido de Gran Bretaña (RUGB) con el objetivo de extraer conclusiones acerca de su adecuación a los cambios que impone el dominio del ciberespacio en la actualidad e identificar sus características distintivas como fuerzas independientes aplicables a la posible organización de una fuerza que integre las operaciones de ciberdefensa y electromagnéticas en el Estado Argentino.

Durante los últimos quince años las FFAA a nivel internacional han incluido en sus diferentes procesos de planificación estratégicos las acciones necesarias para adecuar la doctrina, el desarrollo orgánico y tecnológico de la ciberdefensa y las operaciones en el espectro electromagnético, para obtener un conjunto de capacidades que le permitan operar eficientemente en esta nueva dimensión en la que se desarrollan los conflictos armados y aquellas amenazas que se materializan por debajo del umbral de un conflicto armado.

En efecto, y como se podrá observar especialmente en las secciones referidas a EEUU y el RUGB, es opinión del autor del presente trabajo, unificar la terminología técnica considerando que el concepto de electromagnetismo en general abarca al de cibernética.

Algunos de los países que serán analizados muestran un avance constante y dinámico en lo que hace a las actividades a desarrollar en este ambiente complejo y transversal a los otros dominios, de alcance global, en el que existe una competencia constante por la ventaja operativa para el logro de los diferentes objetivos. En dos de ellos, las actividades en el ciberespacio y en el espectro electromagnético están unificadas ya que, como lo mencionan en sus respectivas doctrinas, están íntimamente relacionadas. En el otro, se podrá observar la trascendencia e importancia de las operaciones electromagnéticas al punto tal que forman parte de una organización mayor.

En el caso de la República Federal de Alemania, se puede observar el nacimiento de una nueva fuerza con la pericia necesaria para ejecutar operaciones ciberespaciales, junto con las electromagnéticas y el aporte de la inteligencia estratégica.

Para el caso de EEUU y RUGB, se evidencia una gran capacidad de adaptación a los cambios que producen la evolución constante y vertiginosa tanto de las TIC como de la actividad en este entorno operativo. En EEUU se termina de conformar el décimo comando conjunto combatiente en apoyo al resto de los comandos desplegados a lo largo del planeta, y

en el RUGB se pone de manifiesto la convergencia de las actividades cibernéticas y electromagnéticas (en adelante CEMA) en la fuerza cibernética nacional (FCN).

Sección 1

El Comando del Espacio de Información y Ciber de Alemania

De acuerdo con von der Leyen U. (2017), la seguridad cibernética en Alemania es el estado deseado de certeza y confiabilidad en el empleo de las TIC, en el que los riesgos que surgen del ciberespacio deben ser reducidos hasta un nivel mínimo y aceptable. La defensa, la ciberdefensa, la ciberseguridad y la política exterior son los medios para lograrlo.

Según el Libro Blanco (2016), es en pocas áreas, como ser el ciberespacio, en donde la seguridad tanto interna como externa coinciden. La situación plantea una amenaza que requiere una visión holística, mantener la seguridad y la defensa es, por tanto, una responsabilidad nacional que, además, requiere la protección conjunta de las IICC. La ciberseguridad es una tarea original del Ministerio Federal de Defensa (p. 38).

"Los innumerables ciberataques a servidores, redes y sistemas de control que se llevan a cabo contra Alemania, sus instituciones, empresas y ciudadanos están dirigidos a quedarse en el anonimato, lo más invisible posible" (Piedras angulares para el futuro de Alemania - MD, 2021, p. 4).

En abril del 2017, con Ursula von der Leyen como ministra de defensa, y atendiendo a lo planteado en la introducción de la presente sección, las FFAA alemanas ejecutaron una reestructuración de las mismas, dando origen a lo que se denominó como Comando del Espacio de Información y Ciber (Kdo CIR).

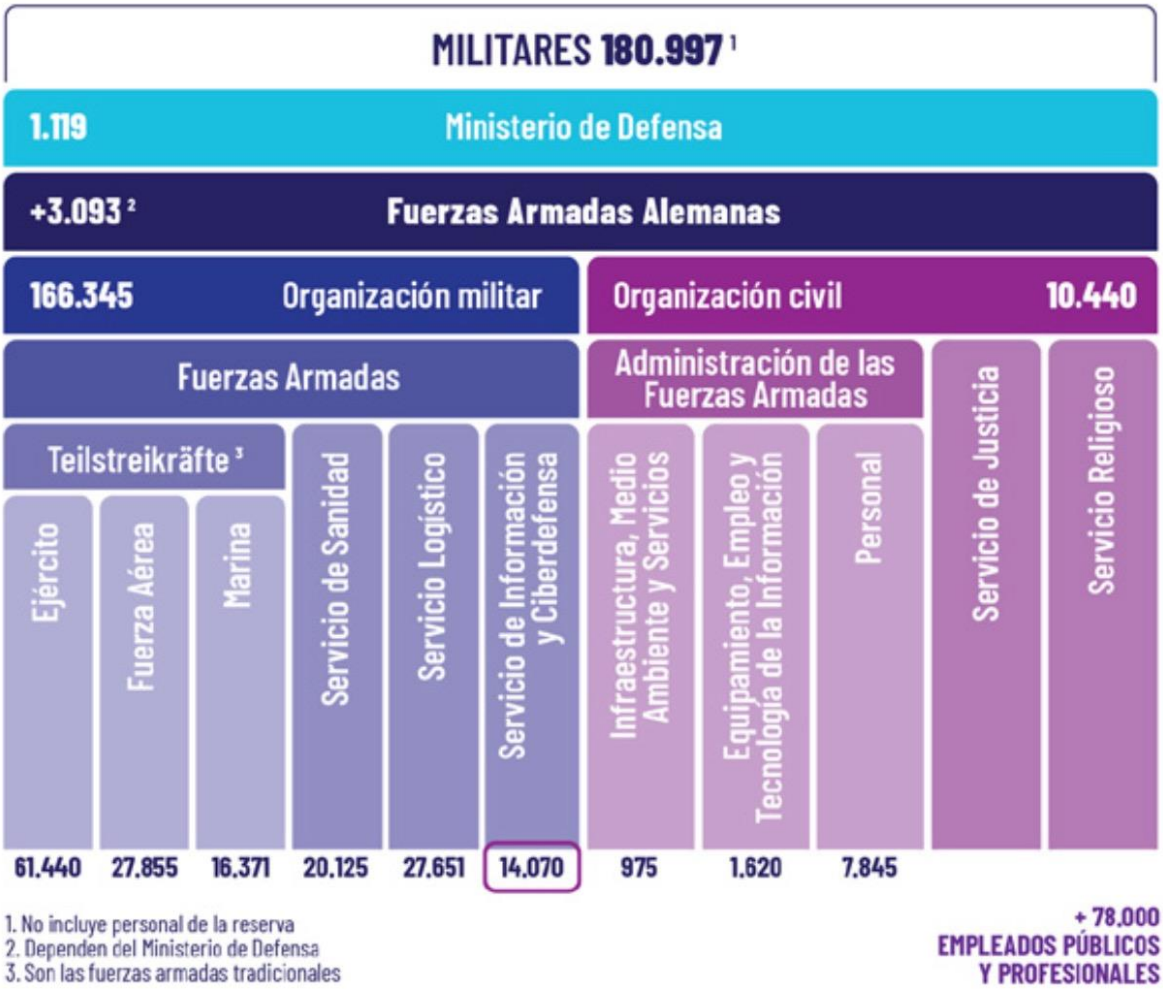
De acuerdo con lo publicado por Deutsche Welle (2020), el pasado 11 de agosto de 2020, Alemania ha puesto en marcha también su Ciberagentur, la ciberagencia encargada de estar al tanto de la seguridad informática y que debe garantizar el funcionamiento de la administración y la economía nacional, libre de interferencias. En la misma publicación se menciona que los ministros del interior y defensa indicaron que este hecho marca un "hito esencial del gobierno alemán para la protección de las ciudadanas y ciudadanos, la administración y la economía en el ciberespacio, y que supone un paso importante hacia la soberanía tecnológica de Alemania". (p. 1)

Con lo hasta aquí expresado, se puede inferir que la soberanía en el ambiente del ciberespacio revista una importancia superlativa en el gobierno alemán, lo que se materializa no sólo en la adecuación de su instrumento militar, sino también en la estructura del mismo

gobierno, asignando recursos humanos y materiales en la búsqueda de ese estado de seguridad en los diferentes dominios.

Figura 1

Estructura de las FFAA alemanas.



Nota. Detalle de la estructura de las FFAA alemanas. *Fuente*: Cañete P.A. (2020). El comando de ciberdefensa alemán, un claro ejemplo de integración. *Revista Visión Conjunta* (p.15). http://www.cefadigital.edu.ar/bitstream/1847939/1498/1/VC%2022-2020%20Caniete.pdf

Es importante aclarar, como detalla Cañete P. A. (2020), que la organización militar de las FFAA alemanas está estructurada en seis grandes fuerzas, de las cuales el ejército, la marina y la fuerza aérea forman un primer grupo llamado las *Teilstreikräfte*, y los servicios de sanidad, logístico y el Kdo CIR conforman el grupo llamado *Organizationsbereiche*, éstos últimos son de carácter conjunto, organizadas, equipadas e instruidas para apoyar a las FFAA.

Esto quiere decir que el comando de información y ciberdefensa, si bien no es una cuarta fuerza armada como las tradicionales, es más bien un comando conjunto responsable de brindar el apoyo de ciberdefensa a las otras fuerzas, es decir, es el responsable de manera

integral de la dimensión del ciberespacio y por lo tanto debe garantizar el funcionamiento y la protección del sistema de información tanto a nivel nacional como así también a los elementos que despliega en el exterior.

Como se puede observar en la Figura 1, a pesar de ser una organización nueva en constante actualización y desarrollo, posee sólo 2.301 efectivos menos que la armada, y en el presente año debe alcanzar los 15.000 efectivos, lo cual demuestra la seriedad y el grado de importancia que representa para el MD.

Organización del Comando del Espacio Cibernético y de la Información

Uno de los aspectos que más llama la atención es el hecho de que este Kdo CIR conduce el comando de inteligencia estratégica, el comando técnico de la información y el centro de geoinformación, que pueden observarse un poco más detalladamente en la Figura 2.

Figura 2

Organización del Kdo CIR

Nota. Detalle de cómo está estructurado el Kdo CIR alemán. *Fuente*: Cañete P.A. (2020). El comando de ciberdefensa alemán, un claro ejemplo de integración. *Revista Visión Conjunta* (p.16). http://www.cefadigital.edu.ar/bitstream/1847939/1498/1/VC%2022-2020%20Caniete.pdf

Comando de Inteligencia Estratégica

Además de proporcionar inteligencia, tiene la misión de dar el apoyo de guerra electrónica, ejecutar las operaciones psicológicas y la ciberdefensa, acciones que lleva adelante con las organizaciones detalladas en la Figura 2.

El tercer elemento de este comando, que es el centro de evaluación de guerra electrónica, es el responsable de analizar, identificar, evaluar y registrar toda la información relacionada a las actividades en el espectro electromagnético y de esta organización se desencadenan los cuatro batallones de guerra electrónica.

Asimismo, cada uno de estos cuatro batallones se diferencia de acuerdo a su misión. Algunos tienen capacidades ofensivas y defensivas electromagnéticas terrestres, navales o aéreos y otros tienen estaciones fijas para proteger el espectro electromagnético.

Centro de Geoinformación

La misión de este organismo es la de obtener, preparar, actualizar y proporcionar no solo los informes meteorológicos o las cartas topográficas sino también información en los campos de biología, etnología, teledetección, geodesia, geoinformática, hidroacústica, hidrografía, hidrología, cartografía, climatología, meteorología, ecología, oceanografía y fotogrametría.

Comando Técnico de Información

Este elemento es el responsable de brindar el apoyo de comunicaciones, informática y ciberoperaciones defensivas a las fuerzas armadas tradicionales, de acuerdo a como lo detallado la Figura 2 en la organización del Kdo CIR.

El segundo elemento de este comando, contando desde izquierda a derecha, es el Centro de Ciberseguridad de las FFAA, el cual lleva adelante las operaciones pasivas de ciberdefensa.

Como expresa Cañete P.A (2020), “En Alemania hay una verdadera concientización en lo que respecta a ciberseguridad, confían en la seguridad de su red y si hay que esperar porque el sistema operativo lo demanda, utiliza un refrán breve y contundente: hasta los comandantes esperan” (p. 18).

Sección 2

El Comando Cibernético de los Estados Unidos de Norteamérica

Si bien en el año 1972 el gobierno de EEUU reconoce la necesidad de una defensa integral que incluya la seguridad informática junto a los esfuerzos militares y la inteligencia; a lo largo de los años subsiguientes, el Departamento de Defensa (en adelante DDD), ha ido modificando sus estructuras, arribando en el 2009 al actual Comando Cibernético (USCYBERCOM) que, finalmente en el 2018 se transforma en Comando Combatiente Unificado (Reseña Histórica – USCYBERCOM, 2022, pp. 1-6, traducción propia).

Según la Estrategia Cibernética del DDD (2018), la prosperidad, la libertad y la seguridad de los estadounidenses dependen del acceso abierto y confiable a la información. La naturaleza abierta, transnacional y descentralizada de internet en esta era digital crea vulnerabilidades significativas que deben ser eliminadas o disminuidas tanto por las diferentes organizaciones del estado como también por el trabajo de los guerreros cibernéticos. (p. 1)

Para el DDD, el ciberespacio posee características diferentes a las de los dominios físicos, por lo tanto, requiere de especificidad ya que los diferentes estados buscarán obtener la ventaja en este nuevo entorno. Asimismo, el ciberespacio, cada vez más importante, se ha convertido en el centro vital de la seguridad nacional en donde, además, se desarrollan operaciones cibernéticas por debajo del nivel del conflicto armado.

De acuerdo con lo publicado en Cyber 1- Operaciones Electromagnéticas y en el Ciberespacio, las FFAA de los EEUU operan en un mundo cada vez más basado en redes. La proliferación de tecnologías de la información está cambiando la forma en que los humanos interactúan entre sí y con su entorno, incluidas las que se dan en las operaciones militares. Este amplio entorno operativo y que cambia rápidamente, requiere que las FFAA de hoy operen en el ciberespacio y aprovechen el espectro electromagnético, que cada vez es más competitivo, congestionado y disputado (2019, p. 4, traducción propia).

Las nuevas formas de hacer la guerra involucran un amplio uso del ciberespacio, además del desarrollo de diferentes capacidades de bajo costo o que materialicen la economía de fuerzas.

> El enfoque que se plantea con esta USCYBERCOM es que tal estructura planeará, coordinará, integrará, sincronizará y llevará a cabo las actividades para: liderar la defensa diaria y proteger las redes de información del Departamento de Defensa, coordinar las operaciones del Departamento de apoyo a las misiones militares, dirigir operaciones y defensa de redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una gran variedad de operaciones militares ciberespaciales. El comando se encarga de agrupar los recursos ciberespaciales existentes, creando una sinergia que no existe actualmente y sincronizando los efectos del combate para defender el entorno de la seguridad de la información. United States Strategic Command. (s.f.). *U. S. Cyber Command – misión.* https://web.archive.org/web/20100905140740/http://www.stratcom.mil:80/factsheets/cc.

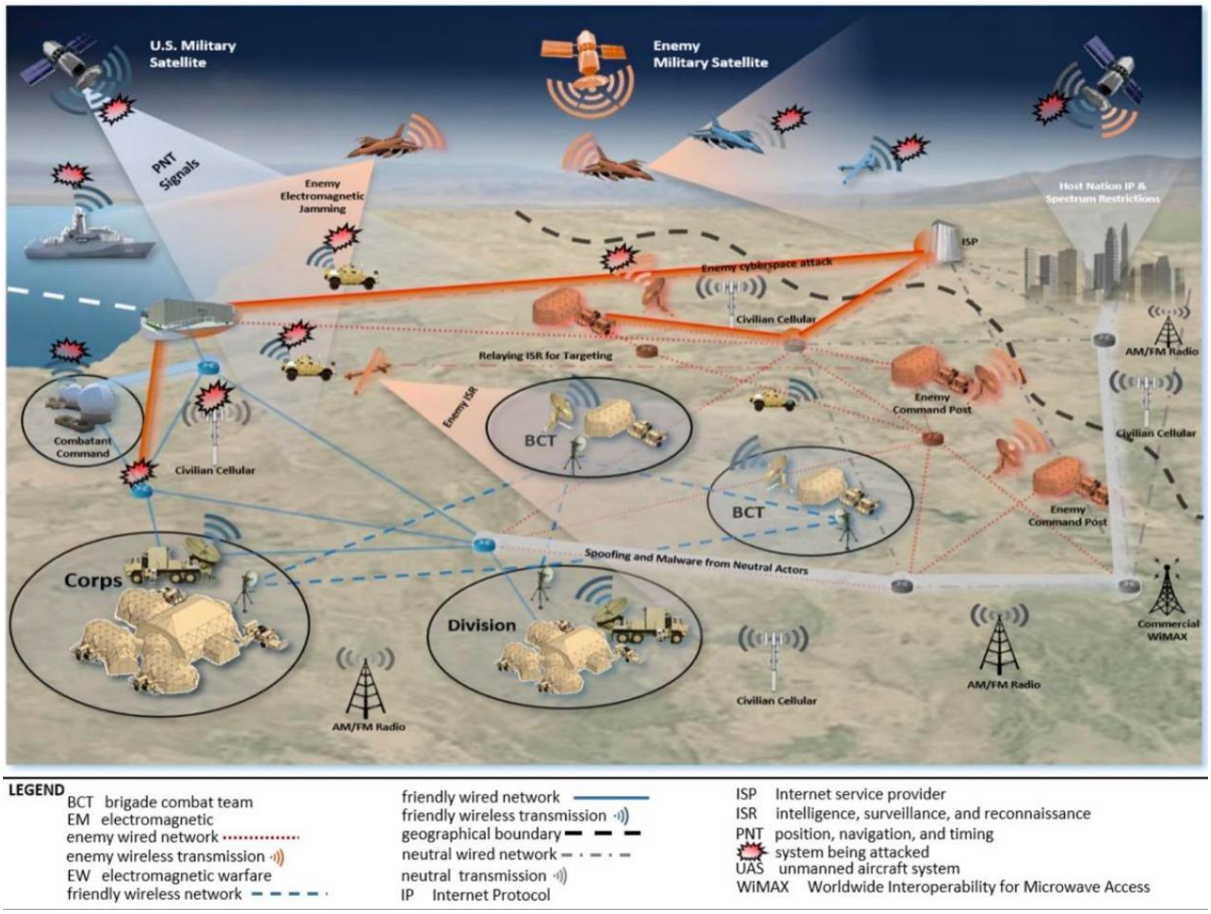
Según Graham, M (2016) las FFAA estadounidenses han acompañado el desarrollo del ciberespacio y lo referido a la guerra cibernética hasta conseguir que el departamento de

defensa establezca el comando cibernético de los estados unidos (USCYBERCOM), el cual tiene un carácter conjunto para llevar adelante y organizar los esfuerzos del departamento en el ciberespacio. Agrega además que parte del presupuesto se asigna de manera directa a este comando y otros recursos provienen de las distintas fuerzas. Es por ello que cada institución estableció un cuartel general de componente, similar a las propias DCD, por ejemplo: el comando cibernético del ejército o el comando cibernético de la flota.

Durante tiempos de guerra las fuerzas cibernéticas de EEUU estarán preparadas para operar junto con la fuerza aérea, la fuerza terrestre, la marítima y espacial para atacar las debilidades del adversario, compensar las fortalezas y amplificar la eficacia de otros elementos de la fuerza conjunta. En la Figura 3 se puede observar la disputa por el espectro electromagnético y el ciberespacio en un entorno operativo actualizado.

Figura 3

El ciberespacio y el espectro electromagnético en un entorno disputado.



Nota. Descripción gráfica de la disputa por el ciberespacio y el espectro electromagnético en un entorno operativo actualizado. *Fuente*: FM 3-12, *Operaciones ciberespaciales y guerra electromagnética* (2021). Departamento del Ejército – EEUU (p. 22).

El mundo depende cada vez más de la tecnología informática y de las redes, es por ello que el DDD debe explotar esta dependencia para obtener una ventaja militar, asimismo la fuerza conjunta empleará capacidades cibernéticas ofensivas y conceptos innovadores que permitan el uso de operaciones ciberespaciales en todo el espectro del conflicto.

Finalmente, el establecimiento de este nuevo comando ciber, es uno de los diez comandos unificados dependiente del departamento de defensa, es decir, tiene carácter conjunto, permitirá a EEUU prosperar en la capacitación de guerreros cibernéticos. Esto facilita el cumplimiento de las misiones de las otras fuerzas ya que les sustraería la responsabilidad operar en el ciberespacio; asimismo, protege los sistemas informáticos de EEUU y sus aliados brindando una respuesta inmediata frente a ciberataques o inclusive estará en capacidad de ejecutar operaciones en el ciberespacio para proteger sus intereses o permitir el desarrollo de otras operaciones militares.

Como corolario de esta sección, cabe destacar que el comandante del Comando Cibernético de los EEUU es, además, el director de la Agencia de Seguridad Nacional (ANS), lo que deja de manifiesto la estrecha colaboración entre el componente civil y militar, además del nivel en el que opera para poder apoyar eficientemente a los diferentes comandos y demás organizaciones del gobierno nacional que requieran sus servicios.

Sección 3

La Fuerza Cibernética Nacional del Reino Unido de Gran Bretaña

A diferencia de la RFA y los EEUU, para el Reino Unido, la seguridad en el ciberespacio es abordada al nivel estratégico nacional. El gobierno reconoce que el ciberespacio se está volviendo cada vez más importante en todas las áreas de la sociedad, la economía, la política exterior y la defensa misma.

Según describe Steve Barclay, “la nueva Estrategia Cibernética Nacional es nuestro plan para garantizar que el Reino Unido mantenga la confianza, la capacidad y la resiliencia en este mundo digital en rápida evolución; y que sigamos adaptándonos, innovando e invirtiendo para proteger y promover nuestros intereses en el ciberespacio”. (National Cyber Strategy 2022, p. 8, traducción propia)

En la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior (2021), el primer ministro en su Visión para el RUGB en el 2030 menciona que estarán a la vanguardia de la regulación global sobre tecnología, cibernética, digital y datos, para proteger su propia democracia y las de otros, para reforzar el estatus del RUGB como un centro global de servicios

digitales y de datos, maximizando las oportunidades comerciales y de empleo para los británicos. (p. 7, traducción propia).

En la Figura 4 se puede observar la evolución de la política del RUGB hacia sus objetivos estratégicos, en la que se muestra un ciberpoder responsable, democrático e integral para mantener su ventaja competitiva en este dominio de rápida evolución; pretenden construir un país digital, resistente y próspero, además de hacer un uso más integrado, creativo y rutinario del espectro al completo, incluidas las herramientas cibernéticas ofensivas de la FCN para detectar, interrumpir y disuadir a sus adversarios. (RISDDPE, 2021, p. 21, traducción propia)

Figura 4

Un Ciberpoder responsable y democrático como punto fuerte de la política del RUGB.

Nota. Descripción gráfica del ciberpoder responsable y democrático del RUGB. *Fuente*: Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior (2021). *HM Gobernment* (p.16), traducción de Google.

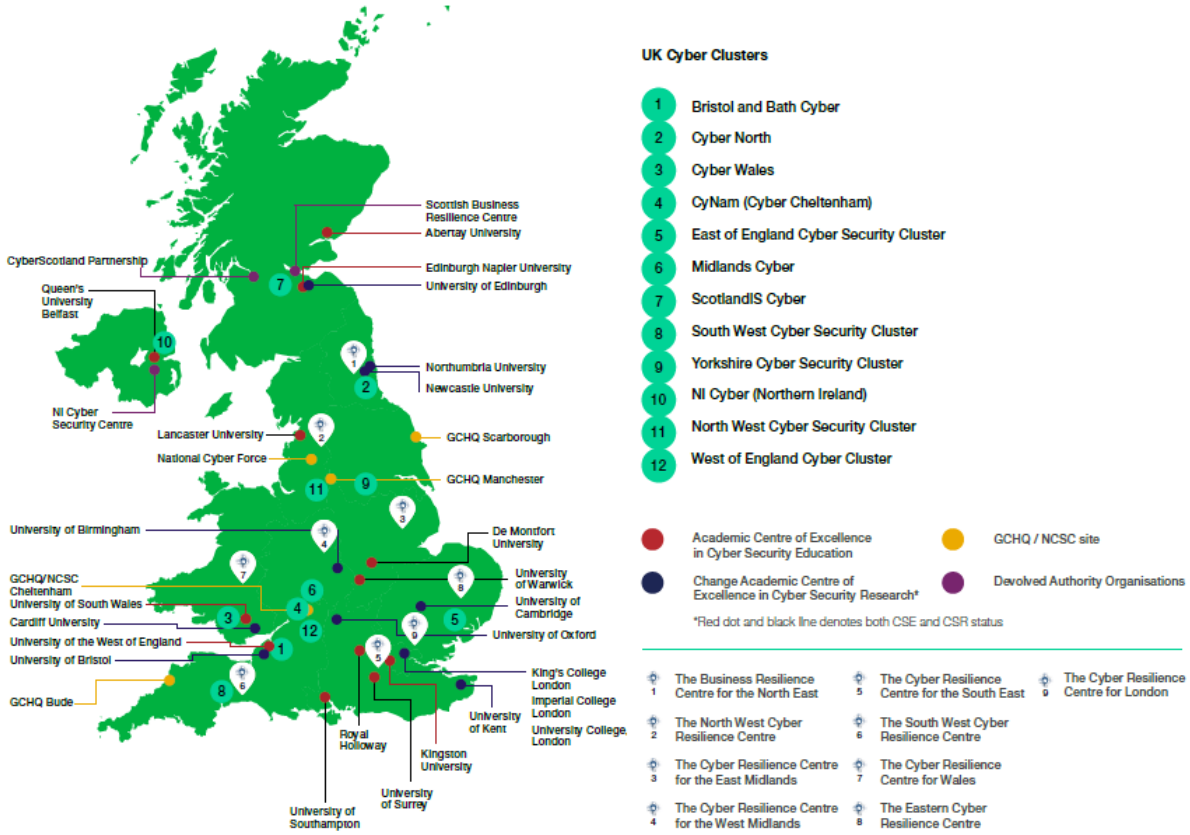
De acuerdo con la página oficial del gobierno del RUGB (2022), en el año 2020 se estableció la fuerza cibernética nacional, una asociación entre inteligencia y defensa. Esta fuerza es parte del Ministerio de Defensa (MD) y trabaja junto al laboratorio de ciencia y

tecnología de defensa, el servicio secreto de inteligencia y la sede de comunicaciones del gobierno (https://www.gov.uk/government/organisations/national-cyber-force/about).

Conforme a lo determinado por la Asociación y Defensa del RUGB, la FCN es responsable de operar en y a través del ciberespacio para contrarrestar las amenazas, perturbar y desafiar a aquellos que harían daño al RUGB y sus aliados y, de esta manera, mantener la seguridad en el país (2020, p. 1). Esta fuerza complementa el esfuerzo de las otras organizaciones detalladas en la Figura 5, que contribuyen a alcanzar los objetivos estratégicos del RUGB.

Figura 5

Organizaciones Cibernéticas en el RUGB.



Nota. Detalle de la ubicación y tipo de organizaciones cibernéticas en el RUGB. *Fuente*: Estrategia Cibernética Nacional (2022). *HM Gobernment* (p. 16, adaptación propia). https://www.gov.uk/government/publications/national-cyber-strategy-2022

Continuando nuevamente con lo descripto en la Estrategia Nacional de Ciberseguridad 2022 del RUGB, el gobierno ha invertido significativamente en sus capacidades cibernéticas ofensivas, en un principio, a través del Programa Cibernético Ofensivo Nacional y, más recientemente, mediante el establecimiento de la FCN, la que reúne personal de la Sede de Comunicaciones del Gobierno (GCHQ), el Ministerio de Defensa (MOD), el Servicio Secreto

de Inteligencia (SIS, también conocido como MI6) y el Laboratorio de Ciencia y Tecnología de Defensa, bajo un mando unificado por primera vez (p. 24, traducción propia).

La digitalización ha llevado a la convergencia de ciber y actividades de información hasta tal punto que la coordinación de CEMA en toda la fuerza conjunta será imprescindible para el éxito operativo. La libertad para usar de manera flexible o denegar, degradar o restringir el acceso del adversario al EME y partes del ciberespacio ofrecerá una ventaja operativa significativa.

De acuerdo con la Nota de Doctrina Conjunta 1/18 (JDN, 2018) la visión del CEMA es: "la sincronización y coordinación de las actividades cibernéticas y electromagnéticas, brindando una ventaja operativa que permite la libertad de movimiento y efectos, al mismo tiempo que niega y degrada el uso del entorno electromagnético y el ciberespacio por parte de los adversarios" (p. 3, traducción propia).

Haciendo referencia a lo publicado por esta doctrina conjunta, que analiza el uso por parte de Rusia, de las actividades cibernéticas y electromagnéticas y el cómo se han desarrollado, estableciendo paralelismos con las del RUGB, las operaciones rusas en el sureste y este de Europa destacaron la eficacia de sincronizar las CEMA con las actividades operativas convencionales para moldear la percepción internacional y la del adversario.

Sin embargo, dentro de la Organización del Tratado del Atlántico Norte (OTAN) y específicamente en la doctrina del Reino Unido, el desarrollo de la fuerza y la capacidad no ha seguido el mismo ritmo. La nota de concepto conjunto (JCN) 1/17, Future Force Concept identificó la necesidad de CEMA, mientras que esta JDN brinda aclaraciones al explorar cómo se implementa el concepto de CEMA para que pueda llevarse a cabo con una ventaja decisiva.

Lo descripto en este capítulo, especialmente lo desarrollado en EEUU y RUGB, lleva a inferir que hay una gran cantidad de áreas en donde las actividades cibernéticas y las actividades electromagnéticas se superponen, por lo tanto, es necesario definirlas. La naturaleza de CEMA es tal que permite la coordinación y sincronización en cualquiera o todas las actividades mencionadas en esas áreas.

La JDN 1/18 establece que, para brindar una ventaja operativa, un cuartel general desplegable deberá sincronizar y coordinar las operaciones electromagnéticas, la gestión del espectro, la inteligencia de señales y las actividades operativas cibernéticas con las actividades habilitadoras de CEMA y otras que son operativas no relacionadas con CEMA.

La lista a continuación indica algunas de las áreas a ser consideradas por una autoridad de sincronización y coordinación de CEMA:

a. Garantice la coherencia de la capacidad de CEMA en Defensa y la Sede de Comunicaciones del Gobierno (GCHQ) para las capacidades nuevas y existentes.

b. Informar y dar forma a la capacidad de CEMA en todas las líneas de desarrollo de Defensa, asegurando la coherencia entre los Comandos de servicio, Equipo y apoyo de defensa, Sistemas y servicios de información y Laboratorio de ciencia y tecnología de defensa.

c. Influir en la producción de la política y doctrina del CEMA.

d. Asegurarse de que el componente clave de CEMA y el personal del Comando de servicio reciban capacitación básica en los niveles táctico, operativo y estratégico.

e. Permitir que las actividades electromagnéticas (EMA) y las actividades cibernéticas se desarrollen de manera coherente bajo la estrategia CEMA.

f. Establezca relaciones con socios industriales de Defensa para problemas y vulnerabilidades de la cadena de suministro. (Joint Doctrine Note 1/18. *Cyber and Electromagnetic Activities*. 2018, pp 12-13, traducción propia)

Resumiendo, entonces, se deberían tener en cuenta los siguientes puntos clave:

1) Los bajos costos de entrada y la rápida adopción de tecnología de punta significan que los adversarios pueden estar igualmente o mejor posicionados para usar la información como un multiplicador de fuerza.

2) Existen desafíos entre el uso y la integración de la información al realizar operaciones conjuntas y de coalición.

3) Es clave sincronizar y coordinar las CEMA, con unidad de comando.

5) El entorno electromagnético y el ciberespacio son un recurso congestionado y las operaciones deben tener en cuenta a otros usuarios, tanto amigos como adversarios, de hecho, estas actividades se dan a menudo por debajo del umbral del conflicto.

6) Es importante aprender lecciones de operaciones pasadas como, por ejemplo, los eventos en Georgia, sobre la necesidad de sincronizar y coordinar las actividades cibernéticas y electromagnéticas.

Capítulo 2

La Ciberdefensa y las Operaciones Electromagnéticas del Estado Argentino en la Actualidad

Como se expresó en la introducción del presente trabajo, en este capítulo se describirá cómo se estructura y organiza la ciberdefensa desde la estrategia nacional hacia la militar y cuál es el enfoque de las operaciones en el espectro electromagnético, junto a la organización de los elementos que desarrollan operaciones electromagnéticas en las diferentes fuerzas.

De forma introductoria, corresponde recordar que las actividades a desarrollar tanto en el ciberespacio soberano nacional como en el espectro electromagnético están enmarcadas en la Ley de Defensa Nacional (LDN 23.557, 1.988) y la de Seguridad Interior (LSI 24.059, 1.991).

Asimismo, el Decreto Nro 577 publicado el 28 de julio de 2017 estipula la creación de un Comité de Ciberseguridad a nivel nacional y se establecen las tareas que el mismo debe desarrollar. En julio del 2019 se actualiza dicho decreto ampliando los integrantes del mismo.

De acuerdo con lo desarrollado anteriormente, se puede inferir que la ciberdefensa tiene un enfoque inicial en la estrategia nacional y militar, desde allí se desarrolla y estructura el sistema de ciberdefensa en el nivel operacional, cuyos elementos alcanzan el nivel táctico en las diferentes fuerzas.

Por otro lado, y de acuerdo con el Reglamento Conducción del Batallón de Operaciones Electromagnéticas y Ciberdefensa (Proyecto 2020), “las operaciones electromagnéticas, son el conjunto de acciones desarrolladas en el ámbito del espectro electromagnético que implica el el uso de la energía electromagnética o dirigida, con el objetivo de determinar y explotar la presencia de actividad enemiga en dicho espectro, neutralizar o reducir el uso de energía irradiada por el enemigo y asegurar la irradiada por los propios medios” (p. 7).

En las tres fuerzas, estas operaciones se conforman en los respectivos Subsistemas de Guerra Electrónica (SUGE) que, para el caso del Ejército Argentino, cuenta con dos estructuras: una territorial, con enfoque de nivel operacional, y otra de campaña, de nivel táctico.

Se puede inferir entonces, que la ciberdefensa tiene un enfoque inicial en el nivel operacional, desde allí se desarrolla y estructura el SUGE hacia los niveles tácticos de cada una de las diferentes fuerzas, aspecto claramente diferente a lo desarrollado en el capítulo 1 del presente trabajo.

Sección 1

La Estructura de Ciberdefensa y de las Operaciones Electromagnéticas

Continuando con lo descripto en la introducción del presente capítulo, en esta sección se describirán las estructuras de la ciberdefensa y la correspondiente a las operaciones en el espacio electromagnético, demostrando así, no solo el estado de las mismas, sino también las diferencias en cuanto al personal que las integra, su cadena de comando y formas de operar.

La Ciberdefensa en la Argentina

Coincidente también con la introducción del trabajo de investigación, a la hora de estructurar el Sistema Nacional de Ciberdefensa en el Estado Argentino, se encuentra que la cabeza del mismo está a cargo del actual Comandante Conjunto de Ciberdefensa, en estrecha relación con el Jefe del Estado Mayor Conjunto y con el Subsecretario de Ciberdefensa, quien puede ejecutar control funcional.

En paralelo a las actividades de ciberdefensa, el Comité de Ciberseguridad, en el cual participa el CCCD, es un órgano ad hoc con representantes de los diferentes ministerios y lo preside el jefe de gabinete de ministros.

Como queda expresado entonces, la jefatura de gabinete de ministros es la responsable de la ciberseguridad. Para ello cuenta, dentro de la Secretaría de Innovación Pública, con dependencia de la Subsecretaría de Tecnología de la Información y Comunicaciones, con la Dirección Nacional de Ciberseguridad. El ministerio de seguridad se encarga del ciberdelito, para lo cual se apoya en las Fuerzas de Seguridad y, finalmente, el ministerio de defensa se encarga de los aspectos referidos a la ciberdefensa, protegiendo las IICC del instrumento militar y aquellos objetivos de valor estratégico (OVE) que la jefatura de gabinete de ministros le asigne al MD para su protección.

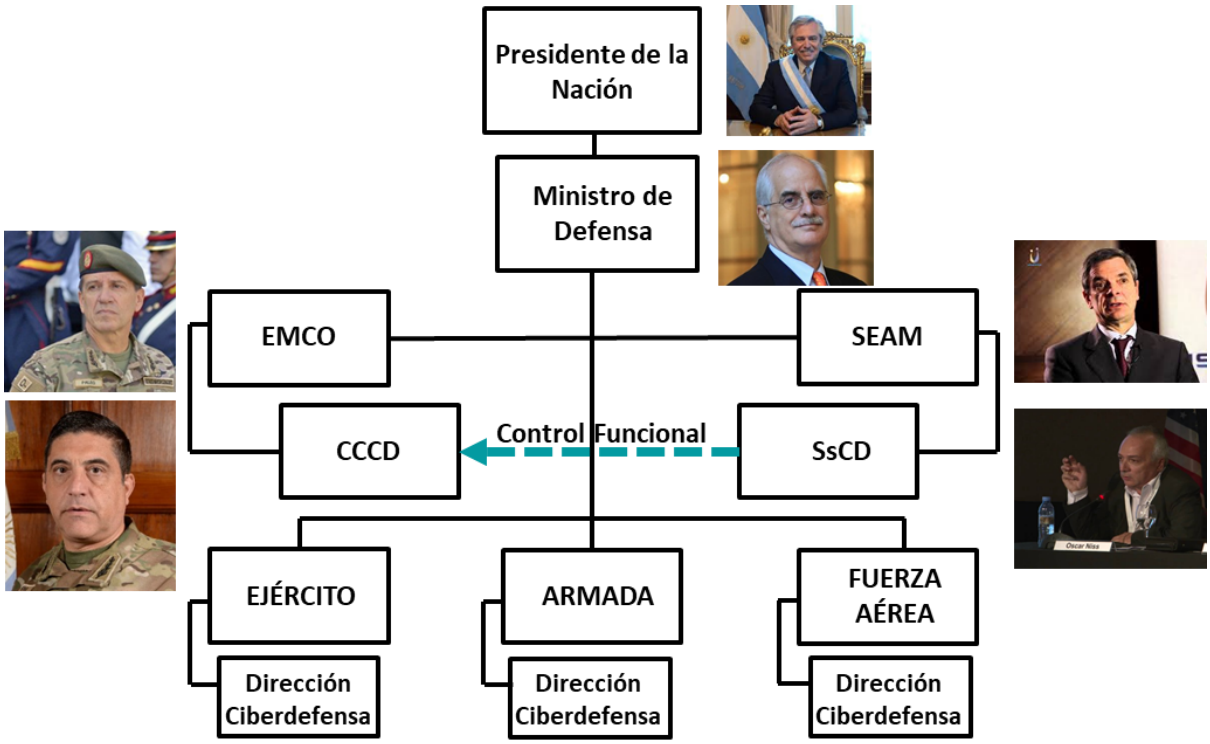
Cabe destacar que la ciberseguridad es una responsabilidad individual y de conjunto, pero la ciberdefensa sólo puede llevarse adelante por el MD ya que es el que único que tendría el marco legal para desarrollar capacidades ofensivas, y es a través de sus FFAA.

Continuando con el marco legal de la organización y avanzando hacia el sistema de ciberdefensa, se puede distinguir una rama política y una rama militar trabajando sobre esta temática. La cabeza del sistema se encuentra materializada en el ministro de defensa, para lo cual cuenta con la Secretaría de Estrategia de Asuntos Militares y ésta tiene la Subsecretaría de Ciberdefensa, la que ejerce el control funcional sobre el CCCD (Resol MD 343, 2014).

Este CCCD opera bajo la dependencia orgánica, funcional y operativa del EMCO, pero fuera del comando operacional. Asimismo, cada fuerza armada cuenta con una Dirección de Ciberdefensa (DCD), dependiente de las Direcciones de Comunicaciones e Informática, o Tecnologías de la Información, que pueden verse más claramente en la Figura 6. Ahora bien, existe una relación de control funcional entre el CCCD y las DCD, quienes materializan esta relación a través de reuniones de coordinación llevadas a cabo de manera mensual en el CCCDFFAA ya que cada DCD opera su Centro de Operaciones de Seguridad (SOC) en su fuerza respectiva.

Figura 6

Organización de la ciberdefensa en el Estado Argentino



Nota. La presente figura muestra cómo está organizado el sistema de ciberdefensa desde el nivel nacional al militar. *Fuente*: Intini, A.L. (2021). *Clase de ciberdefensa* [Diapositiva PowerPoint].

En continuidad con lo dispuesto por el Decreto Nro 684 (2019), el EMCFFAA opera el centro inteligente de operaciones de seguridad (en adelante iSOC), este trabaja de manera integrada con los centros de operaciones de control (SOC's) remotos de las distintas FFAA. En conjunto, los SOC's con el iSOC del EMCFFAA contribuyen a la planificación, desarrollo y establecimiento del equipo de respuesta ante emergencias informáticas en el MD (CIRST Defensa).

De acuerdo a lo expresado por el General de Brigada Aníbal Intini (Comandante Conjunto de Ciberdefensa) al diario digital Infobae, el CCCD tiene la responsabilidad de implementar la vigilancia y control de los sistemas cibernéticos de la jurisdicción de la defensa. Es desde este comando, y a través de los elementos de las tres fuerzas, que se puede monitorear el estado de las redes de las mismas, tanto de las que están expuestas a la internet como de las redes internas que cada fuerza opera. Este comando también está orientado a tener en claro cuáles son las IICC de la defensa, lugar medular para ejecutar el control y vigilancia del ciberespacio, ya que no todos los sistemas tienen la misma criticidad. (2022)

En la misma entrevista, el comandante conjunto de ciberdefensa también hace mención a que los recursos humanos asociados a la temática son altamente volátiles y se registra una escasez de personal con conocimientos y capacidades tan específicos. Por esta razón, el personal del CCCD es capacitado en universidades y centros de capacitación específicos, fuera de las fuerzas. También hace mención de la creación de la maestría en ciberdefensa en el Instituto de Ciberdefensa de las FFAA, inaugurado el presente año.

Continuando la entrevista y ya sobre el final, el general se refiere al concepto del ciberespacio. Lo define como nuevo dominio en el que las personas realizan actividades de todo tipo y, al mismo tiempo, porque el conflicto es inherente a la condición humana, es un dominio en constante disputa. Es en este ámbito que determinados actores intentan extraer información, alterar el normal funcionamiento de los sistemas y esto se convierte en lo que conocemos como incidentes que posteriormente pueden conformar los ciberataques.

En general, estos ciberataques están orientados a robar información, obstaculizar su acceso, alterar la función de los niveles, etc. Existen ataques con perfiles oportunistas, otros más profesionales y con un objetivo más claro y finalmente pueden ser atacantes provenientes de gobiernos y servicios de inteligencia de estados que claramente persiguen otros objetivos más estratégicos.

Las Operaciones en el Espectro Electromagnético

Mencionando la misma entrevista, el comandante conjunto de ciberdefensa expresó que la guerra electrónica, hoy llamada guerra electromagnética, nace mucho tiempo atrás cuando las transmisiones eran analógicas y aún no se pensaba montar una señal digital sobre la misma ya que aún no existía. Pero en la actualidad, se complementan al punto que se puede pensar que, al menos los elementos tácticos, podrían abarcar la temática de la ciberdefensa de una manera más dinámica y así obtener mejores resultados en sus despliegues.

La doctrina en el ámbito castrense menciona que las operaciones electromagnéticas se definen como cualquier acción que implica el uso de la energía electromagnética o dirigida para controlar el espectro electromagnético con la finalidad de determinar, explotar, reducir o prevenir el por parte de un actor hostil, o atacar al enemigo y mantener el propio uso efectivo del espectro.

Sección 2

Ventajas y Desventajas de contar con una Fuerza Cibernética Integrada a las Operaciones Electromagnéticas

Como corolario de la esta investigación y, conforme a lo desarrollado en la introducción con respecto a los objetivos de la misma, en esta sección se describirán las más destacadas ventajas y desventajas de contar con una fuerza específica que abarque e integre las operaciones en el ciberespacio y el espacio electromagnético.

Ventajas

1. La principal ventaja a la que se puede arribar es la unificación de la doctrina, aspecto que si bien, al momento, se encuentra en pleno desarrollo, facilitaría la concreción de las capacidades particulares a desarrollar por el instrumento militar abocado a este dominio.

2. Contar con unidad de comando, capaz de integrar ambas actividades, facilita el eficiente empleo de los recursos, tanto el humano como el material. En conjunto, esta fuerza contribuiría de manera significativa al resguardo de la información y, lo más importante, a la protección integral de las IICC de las FFAA.

Continuando en esta línea, y para matenerse como ventaja, esta unidad de comando centralizada debe permitir la ejecución descentralizada para facilitar la eficiencia de los elementos tácticos, lo cual, en su conjunto, facilita la ejecución de las operaciones de combate en un dominio seguro.

3. Desde el punto de vista de los recursos humanos, el hecho de contar con esta fuerza cibernética permite disponer de personal específico en su campo de trabajo, aspecto que al momento no se está dando de esta manera ya que, quienes hoy desarrollan las capacitaciones en ciberdefensa pertenecientes a las fuerzas armadas, podrían ser maquinistas de un buque o submarino, mecánicos de aviación, conductores tanquistas u oficiales que estando destinados en sus unidades ejercerían funciones de comando, entre otros más.

4. La reciente creación del Instituto de Ciberdefensa de las Fuerzas Armadas (ICDFFAA) es el núcleo de formación para la actual aptitud especial de ciberdefensa. Esta casa de altos estudios facilitaría la instalación, en el futuro, del homólogo a los colegios y escuelas militares de las otras fuerzas, constituyéndose en el instituto de formación de los oficiales, suboficiales y soldados que alimentarán las unidades pertenecientes a la fuerza cibernética.

5. Contar con esta fuerza específica e independiente y el ICDFFAA facilita la unificación de inversiones y presupuestos abocados a desarrollos propios de vanguardia relacionados a la temática.

Este aspecto, que esta mencionado en la DPDN 2021, permitiría también la exportación de tecnología, conforme a los objetivos estratégico del Estado Argentino, elevando la actual buena reputación de la nación y colocándola en una posible ubicación de privilegio en el Foro Iberoamericano de Ciberdefensa (FIC).

6. El hecho de continuar perteneciendo al FIC facilita la capacitación del recurso humano en los diferentes países que lo integran. Asimismo, permite los intercambios y el desarrollo de ejercicios y competencias que elevan el potencial nacional.

7. Desde el punto de vista logístico facilita la ejecución adquisiciones y mantenimiento de los recursos materiales que pueden ser centralizados al máximo nivel. De esta manera, también se optimizan los costos.

8. Al nivel estratégico militar, facilita el planeamiento y el lógico empleo de los elementos al nivel táctico, hecho que puede justificarse dadas las dimensiones territoriales y las hipótesis de conflicto.

9. Desde el punto de vista de los recursos humanos, al tratarse de elementos cuya capacitación es más bien técnica, intelectual o lógica, permite al personal perteneciente a las otras fuerzas que haya sufrido problemas médicos, accidentes o alguna disminución de su capacidad de combate, ejecutar los cursos de capacitación necesarios como para ocupar un lugar en la organización pese a su discapacidad.

Este aspecto materializa una nueva oportunidad al personal que, de otra manera, debiera ser retirado ya que deja de cumplir con los parámetros para ser un combatiente normal, pero que, en este dominio, puede convertirse en un cibercombatiente con la misma eficacia o “letalidad” que antes poseía ya que incluso puede emplear mandos a distancias, telecomando o comandos por voz en los diferentes desarrollos tecnológicos.

10. Desde el punto de vista logístico, esta autonomía e independencia le permite operar de manera permanente en la protección de las IICC y en la ejecución de respuestas inmediatas a los diferentes incidentes contribuyendo también a la resiliencia de los diferentes sistemas.

Desventajas

1. La principal desventaja a la que se puede arribar es la necesidad de nueva servidumbre logística, el hecho de requerir estados mayores y áreas abocadas a la administración del recurso humano y los recursos materiales dificulta el contar con la totalidad del personal especialista en los elementos que deben ejecutar el control y vigilancia del ciberespacio.

2. Siguiendo la línea del punto anterior, una nueva fuerza requiere también de infraestructura edilicia, medios de combates que, si no es cedido desde las otras tres fuerzas, deberá ser adquirido, lo cual conlleva implícito un gasto inicial de importancia, esto sin mencionar el mantenimiento de todo el material, tanto fijo como móvil.

3. Para los casos en los que la conducción de la fuerza sea centralizada, se pierde la posibilidad de reunión y procesamiento de información proveniente del nivel táctico, lo que dificulta la ejecución de respuestas inmediatas a los niveles inferiores del campo de combate.

Conforme a la dinámica actual en este dominio, la responsabilidad de la seguridad de la información debe estar en todos los niveles.

4. Las experiencias extraídas de los países analizados es aplicable sólo a aquellos en los que el marco legal, el presupuesto y la interrelación entre los factores de poder lo permite. Por ejemplo, el Kdo CIR alemán puede servir sólo para Alemania, cuya reestructuración de sus fuerzas está alineada con su extensión territorial y conectividad, entre otros aspectos que no son coincidentes con el Estado Argentino.

5. Desde el punto de vista del recurso humano, la idiosincrasia y el potencial adversario de Alemania, por ejemplo, dista de las características de los potenciales adversario que puede sufrir el Estado Argentino.

6. La centralización no consideraría la responsabilidad sobre los ataques electromagnéticos a las plataformas de guiado de los sistemas de armas (sistemas de defensa antiaérea, comunicaciones tácticas – por ejemplo, observador adelantado y centro de dirección de fuego – controles remotos de sistemas, etc).

7. El hecho de que la fuerza sea específica en el ciberespacio, aísla al ciberguerrero del compromiso operacional en el quinto dominio, es decir, las fuerzas se deben hacer cargo del resto de las funciones de combate. En otras palabras, a pesar de ser independiente, se trataría de una fuerza que mantiene el espíritu de “apoyo de combate”.

Al respecto se refuerza la necesidad de formar especialistas dentro de la estructura de todas las armas y especialidades vigentes en las FFAA argentinas (como especialistas, no como fuerzas independientes).

8. Se contrapone a uno de los principios de la conducción de la guerra como es la flexibilidad y respecto de los sistemas de transmisión de datos, el poder de resiliencia.

9. El hecho de formar profesionales con tan elevado nivel de tecnicismo dificulta la captura de talentos, ya que en el mercado laboral tanto nacional como internacional, un especialista de estos niveles suele ser blanco rentable para diferentes organizaciones y empresas que, lógicamente, no deberán invertir en su formación inicial, lo cual disminuye los costos de adquisición de personal pudiendo volcar estos montos a la oferta salarial, haciendo más tentadora la oferta de incorporación.

Conclusiones

De acuerdo a lo abordado por la presente investigación es menester la integración de las operaciones cibernéticas y electromagnéticas, conforme a la realidad actual de la evolución en este quinto dominio.

Como se puede observar en el primer capítulo, las experiencias extraídas de países extranjeros indica que la actividades cibernéticas y electromagnéticas deben integrarse también con otras agencias para obtener la eficiencia necesaria para conseguir la ventaja en este dominio. Tal es así que la inteligencia estratégica, la ciberinteligancia, los servicios secretos, la información geoespacial, las operaciones de información y la ciberdisuación están íntimamente relacionadas con los conceptos del CEMA descritos precedentemente.

La consideración de una fuerza cibernética independiente que integre también a las operaciones electromagnéticas se justificaría solamente para ser empleada desde el nivel estratégico nacional y con una legislación adaptada a tal fin. Es de esta manera que se potenciaría su eficiencia, elevando también la eficacia de los otros factores de poder.

Si bien en algún estado – nación se ha considerado la posibilidad de que ello exista, es conveniente esperar mayores resultados, ya que es demasiado pronto como para emitir un juicio de valor respecto de la efectividad o no de tal resolución, refiriendo específicamente al estudio de la experiencia internacional.

La experiencia que está dejando, por ejemplo, la guerra entre Rusia y Ucrania demuestra la importancia, a los mayores niveles, tanto del dominio del ciberespacio como el del espectro electromagnético. En el ciberespacio disputado por ambos adversarios hay actividad constante y, de hecho, ha contribuido a la eliminación de personalidades como comandantes, pero ninguno de estos países cuenta con una fuerza cibernética independiente que pueda constituir como ejemplo acabado para la investigación.

Los ejemplos a nivel internacional y de las grandes potencias sirven solamente como mera referencia, pero la solución al respecto debe ser absolutamente nacional, con recursos propios que se adapten a la idiosincrasia de los potenciales adversarios de la nación, de las propias características geográficas y de los objetivos geopolíticos perseguidos por el Estado Argentino.

Más allá de mencionar solo ventajas y desventajas de contar con una fuerza cibernética independiente, de acuerdo a lo estudiado, pese a ser necesaria, parece no ser acorde a la realidad socioeconómica de la nación, por todo lo que implica la creación de una nueva fuerza, sobre todo en lo que hace a la duplicación de funciones y logística.

La natural evolución tecnológica nacional y el desarrollo propio contribuirá de manera significativa al actual CCCD y las respectivas DCD, pero no estaría en capacidad de alimentar la logística requerida si fuera una fuerza independiente.

La capacidad alcanzada por el CCCD y la manera en cómo coordinan y comparten actividades e información los respectivos iSOC's y SOC's de las distintas fuerzas es superlativo, lo cual demuestra que, al menos en el corto y mediano plazo, es el elemento más acorde para ejecutar el apoyo a un eventual e hipotético teatro de operaciones.

La reciente creación del ICDFFAA, y de la "aptitud especial de ciberdefensa", es la principal fuente de perfeccionamiento para dotar de cibercombatientes a las distintas fuerzas.

Finalmente, y como aporte personal, se sugiere una investigación que evalúe las necesidades y las posibles modificaciones estructurales del actual CCCD y/o las respectivas DCD con vistas a convertirse recién en el largo plazo en una fuerza independiente abocada específicamente al quinto dominio.

Bibliografía

Anca, L. J. (2015). La Ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Argentina, pp. 6-16.

Cañete, P. A. (2020, Junio). *El comando de Ciberdefensa Alemán: un claro ejemplo de integración*. Visión Conjunta, volumen (22), pp. 14-20.

Casarino, P. y Ortiz, J. (2019). *La Ciberdefensa y la Ciberinteligencia Militar*. Visión Conjunta, Año 11, N° 21. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, pp. 43, 48 y 51.

CCCD (2019). *Ciberespacio, campo de operaciones del siglo XXI*. Revista del Suboficial, volumen (710/18), pp. 11-15.

La Prensa Relámpago. (2019). *Las operaciones del ciberespacio y guerra electromagnética*. Cyber 1, p. 4.

Decreto N° 457 de 2021 (Presidencia de la Nación). *Por el cual se actualiza la Directiva de Política de Defensa Nacional (DPDN) 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)". Instruir al Ministerio de Defensa en la elaboración de la Directiva de Política de Defensa Nacional en un lapso de CIENTO OCHENTA (180) días.* 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° 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° 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.

E.A. (2020). *Conducción del Batallón de Operaciones Electrónica y Ciberdefensa (Proyecto)*. 2020, pp. 7-11.

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.

FM 3-12 (2021, Agosto). *Operaciones ciberespaciales y Guerra Electromagnética*. Departamento del Ejército de los Estados Unidos de Norteamérica, pp. 13-25.

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

Gago, E. A. (2017, Mayo 29). *El enfoque argentino sobre ciberseguridad y ciberdefensa (Trabajo Final de Licenciatura)*. Facultad del Ejército – Escuela Superior de Guerra, Argentina, pp. 29-30 y 33-50.

H.M. Government (2022). *Estrategia Cibernética Nacional 2022: pioneros en un futuro cibernético con todo el Reino Unido*. Reino Unido de Gran Bretaña, pp. 8, 42-45, y 51-54.

JP3-12 (2018, Junio). *Operaciones del Ciberespacio*. Estado Mayor Conjunto, EEUU, pp. 9-17.

López Lio, R. (2016). *Ciberdefensa e Infraestructuras Críticas (Trabajo Final Integrador)*. Instituto de Inteligencia de las Fuerzas Armadas, Argentina, pp. 37-43 y 54-69.

Lucero, J. G. (2015, Diciembre). *Ciberdefensa: La dimensión desconocida*. Visión Conjunta, volumen (12), pp. 36-42.

MD, JDN 1/18 (2018). *Actividades cibernéticas y electromagnéticas*, Ministry of Defence, pp. 11-15 4.

MD (2021). *Piedras angulares para el futuro de Alemania*, p. 4.

Moyano, T. R. (2020, Junio). *La República Argentina y sus esfuerzos en ciberdefensa: el compromiso con las buenas prácticas como parte de su ideario*. Visión Conjunta, volumen (22), pp. 50-63.

NCF. (2021). *La asociación entre Defensa e Inteligencia.* National Cyber Force, pp. 1-2.

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.

Ortíz, M. H. (2015) *Análisis de las amenazas a la infraestructura crítica de un teatro de operaciones contemporáneo y maneras de combatirlas (Trabajo Final Integrador)*. Escuela Superior de Guerra de las Fuerzas Armadas, Argentina, pp. 12-18.

Primer Ministro (2021, Marzo) *Gran Bretaña Global en una era competitiva (Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior)*. Open Government License v3.0, Reino Unido, pp. 6, 8, 40.

Resolución N° 343 de 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 2014.

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° 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.