Instituto de Ciberdefensa
de las Fuerzas Armadas

TRABAJO FINAL INTEGRADOR

Título: "*Relación entre las Operaciones de Información y las Acciones en el Ciberespacio"*

Autores del TFI: Capitán JUAN CARLOS MAISONNAVE

Teniente de Navío MAXIMILIANO DANIEL GAMBOA

Suboficial Principal MARIO ALEJANDRO PUERTA.

Ciudad Autónoma de Buenos Aires, de noviembre de 2023.

Resumen

Las operaciones de información (OI) y las acciones en el ciberespacio están intrínsecamente entrelazadas en el ámbito de la cibernética. Las OI involucran la recopilación, procesamiento y distribución de datos para influir en la percepción, decisiones y comportamientos de los actores en un entorno específico. En el ciberespacio, estas operaciones se ejecutan a través de redes, sistemas y plataformas digitales.

Las acciones en el ciberespacio, por otro lado, abarcan una amplia gama de actividades que buscan manipular la información o los sistemas informáticos para alcanzar objetivos estratégicos, políticos o militares.

La relación entre ambas radica en cómo las OI pueden potenciar o contrarrestar las acciones en el ciberespacio. La manipulación de la información puede utilizarse como una táctica para influir en la percepción pública, desinformar a adversarios o fortalecer la posición en conflictos cibernéticos. Al mismo tiempo, las acciones en el ciberespacio pueden afectar directamente la capacidad de llevar a cabo OI al comprometer la integridad, confidencialidad o disponibilidad de los datos.

De esta manera la cibernética actúa como enlace que conecta las OI y las acciones en el ciberespacio, proporcionando el marco teórico y práctico para comprender y gestionar la interacción dinámica entre la información y la ciberseguridad.

La presente investigación buscará determinar cómo se relaciona estos conceptos para llegar a una conclusión de interés especialmente según el marco legal vigente en nuestro país.

Palabras Clave:

Operaciones de Información, Revolución Tecnológica, Ciberespacio,

Ciberdefensa, Estrategia.

Índice

Índice de Figuras

Introducción

Antecedentes y justificación

La concepción genérica sobre la guerra de información y las operaciones de información en general, apunta hacia la atención con respecto a la posesión y uso de la tecnología, en especial la tecnología informática e informativa identificados en el conjunto de accesorios de la computación y las comunicaciones.

Por tal motivo la presente investigación pondrá énfasis en estos aspectos para tomar consciencia de lo importante que es el control de la información.

Para esta investigación, teniendo en cuenta que nuestro país tiene varios vacíos de información y reglamentaciones referidas a este tipo de operaciones, tomaré de base una investigación realizada en la Universidad Piloto de Colombia, donde el autor recalca lo siguiente:

Es necesario dedicar tiempo y esfuerzo para que todos los poderes de la nación especialmente los comandantes de todos los niveles y los profesionales de la seguridad nacional, consideren estos conceptos en toda extensión, como una herramienta importante y clave para el cumplimiento de sus objetivos. (Andrade Rojas, Wilfredo, 11)

Para entender la importancia del valor que tiene la información, en las distintas estrategias que puede adoptar un Estado, la presente investigación tiene como objetivo detallar el ámbito de la información y sus dimensiones, para luego desarrollar las capacidades que tiene las OI y porque son tomas como ¨Operaciones¨ y ver las diferencias con la Guerra de Información.

Luego de profundizar sobre las OI, se describirá las particularidades de la Evolución Tecnológica en esta Era de la Información para luego llegar a conclusiones de interés sobre la relación que hay entre las llamadas OI y las Acciones que se pueden realizar en el Ciberespacio.

Hace unos años se analiza esta influencia de la revolución tecnológica, por ejemplo, Trama (2017) sostiene: ¨La diversa y amplia cantidad de agentes que utilizan o explotan esta revolución tecnológica plantean una grave amenaza a la infraestructura crítica de los Estados y a las Misiones Operacionales¨ (p.56)

Los conflictos en la actualidad nos demuestran a diario que con la evolución en la forma de hacer la guerra, debemos adaptar nuestras organizaciones y nuestros conceptos de empleo a la realidad que vivimos, en la cual debemos hablar de este tipo de operaciones complementarias que serán prioritarias y hasta en ocasiones serán determinantes para lograr nuestros objetivos.

Con respecto a esto, Agumosa Pila (2020) indicó en su artículo lo siguiente:

> Las caracteristicas del tipo de operaciones militares en el futuro, en donde el entorno Volatil, Incierto, Complejo y Ambiguo (VICA) y los cambio de era que vivimos en los terrenos de la seguridad, de la energía, de la biotecnología o de la tecnología de la informática, hacen oportuno preguntarse ¿cuáles son los diferentes tipos de operaciones que pueden aparecer en el nivel regional o el internacional mirando por ejemplo, al año 2035?
>
> De esta forma, se pueden preparar y adiestrar a las 3 Fuerzas Armadas para que puedan hacer frente a las nuevas amenazas, además de facilitar el diseño de la estructura orgánica, la adquisición de capacidades militares de alta tecnología y otras complementarias, junto con el personal que se necesitará para dichas operaciones. (p. 2)

En el análisis que realiza el autor, hace hincapié en la importancia de evolucionar lo más rápido posible para estar a la altura de las necesidades de los nuevos escenarios del conflicto. Esto involucra también una evolución en la cultura de la organización, lo cual no es tan sencillo de alcanzar.

Luego de analizar las citas de diferentes autores, se observa cómo evolucionan en nuestro país estos conceptos relacionados a las nuevas amenazas de la guerra moderna y como la mayoría de las variantes que influyen en este ambiente VICA, influyen de manera directa en los conflictos y en las intenciones que puedan tener otros agentes estatales o no estatales sobre otro Estado. El objetivo normalmente será la manipulación de las percepciones sociales con distintas herramientas informáticas (cabe destacar que las sociedades actualmente están sufriendo permanentemente la pérdida de la identidad cultural, debido a la globalización y a la permeabilidad de las fronteras).

Con respecto a los conceptos de Operaciones de Información se citarán distintos países donde estas acciones están más desarrolladas como así también la evolución de la ciberdefensa en nuestro país.

Formulación del Problema

¿Cuáles son los principales condicionantes en la Argentina, para controlar las acciones en el ciberespacio a fin de anticipar posibles OI?

Objetivos

Objetivo General

Proponer aspectos generales a tener en cuenta para garantizar el eficiente y eficaz control de las acciones en el ciberespacio para minimizar los efectos de las OI.

Objetivos Específicos

1. Analizar la influencia de la revolución tecnológica y su impacto en las OI.
2. Explicar los conceptos de las OI y el detalle de las acciones que se pueden realizar en el ciberespacio.
3. Establecer los principales aspectos en los que se relacionan las OI con las acciones en el dominio del ciberespacio y las normas que están vigentes en nuestro país sobre ambos conceptos.

Metodología a emplear

Explicación del Método

El método a emplear será deductivo.

Diseño de la Investigación

El diseño a utilizar será explicativo.

Técnicas de Validación

Las técnicas a emplear serán análisis bibliográfico, análisis documental y análisis lógico.

Capítulo 1

La influencia de la revolución tecnológica en las Operaciones de información

El propósito de este capítulo es analizar el impacto de las TIC en la evolución de las estrategias referidas a las OI.

Sección 1: La evolución tecnológica y la complejidad de la Era de la Información.

Para iniciar esta sección es importante explicar que las TIC son las nuevas Tecnologías de la Información y las Comunicaciones.

Estamos en la ¨Era de la Información¨ la cual está en pleno auge; esta ¨Era¨ está asociada a la revolución digital iniciada en la segunda mitad de siglo XX, en la que las innovaciones como la radio, la televisión y el teléfono revolucionaron la forma de comunicarnos.

Luego el avance de las comunicaciones pasó de lo analógico a lo digital, donde la capacidad de transmisión de la información era mayor y mucho más rápida.

En la década de los 50, en los avances en programas informáticos y redes de computadoras enlazadas con internet, dieron origen a los distintos protocolos que más adelante se utilizaron para el diseño de nuevas topologías de redes.

En la década de los 70 ya se modificó la manera de almacenar los datos, la digitalización de dispositivos comenzaba a surgir, pero recién en la década del 90 impactaron en la sociedad, obviamente este impacto fue inicialmente en países más desarrollados, los cuales comenzaron a incorporar nuevas tecnologías inmediatamente en el ámbito de la educación, la industrialización y particularmente en las empresas.

Este aspecto no es menor, porque surge una gran diferencia con respecto a la interacción que tuvieron a lo largo de la historia las necesidades militares y las revoluciones que se acontecieron.

Por ejemplo los conceptos de ¨Estrategia¨, ¨Organización¨ y ¨Logística¨, que en su esencia surgieron en el ámbito militar y luego en su evolución fueron empleados para el ámbito civil, especialmente en la producción y en lo empresarial.

Esta evolución en las tecnologías de información, tuvo un evento importante y reciente que fue el episodio mundial de la Pandemia (COVID- 19). Ante este nuevo escenario, la sociedad en su conjunto tuvo que adaptarse a lo virtual y esto obligó a todas las generaciones a amigarse de alguna manera con la tecnología para poder cumplir con sus obligaciones; desde los niños que aún no sabían leer ni escribir hasta nuestros abuelos que debían realizar sus trámites de manera virtual.

Esta emergencia sanitaria aceleró drásticamente los cambios de la TIC, obligó la creación de nuevas tecnologías que soporten gran magnitud de datos y permitan el acceso a todo tipo de información. Estos cambios abruptos también trajeron grandes inconvenientes especialmente en la falta de clasificación de la información y el tráfico de datos.

Como señala (Pedroza, 2021) ¨Se ha evidenciado que el exceso de información ha ocasionado que los seres humanos se sumerjan en ella. No sabiendo, de este modo, distinguir entre la realidad virtual del mundo real¨. (p.1)

Ante esta realidad, debemos entender que el entorno en el que vivimos realmente es complejo, mucho más complejo de lo que podemos comprender o imaginar, por lo tanto describiremos este tipo de ambiente particular en el que hoy en día están inmersos todo tipo de operaciones.

Lo describe en detalle Ministerio de Defensa de España (2019) dónde analiza los retos del entorno operativo para el año 2035, en el informe desarrolla los conceptos del entorno VICA e identifica la incertidumbre como una características constante que los Estados, de distintos actores no estatales y de la sociedad en general, plantea que la incertidumbre moldea y condiciona la forma en que los actores del sistema internacional planifican, actúan, responden

y se relacionan estratégicamente con el entorno, tanto a nivel internacional como doméstico.(p.19)

En cuanto a la volatilidad, se identifica esta cualidad en entornos que provocan cambios vertiginosos donde se dificulta la identificación de tendencias o patrones y afecta también la estabilidad de los procesos.

Estos cambios generalmente disruptivos, dificultan la capacidad de anticipar distintas amenazas y riesgos por lo cual es muy difícil la proyección de escenarios futuros deseados, esto afecta de esta manera en forma directa la metodología de la toma de decisiones.

Ésta es la razón por la cual el planeamiento debe ser la principal herramienta que nos permita la aproximación sistémica al análisis y síntesis de los problemas complejos, comprender la situación con pensamiento holístico, mente abierta y visión de futuro para poder visualizar la multiplicidad de causa y factores que están directamente relacionados con eventos o situaciones inesperadas.

Ante estos entornos cada vez más complejos es necesario evitar estereotipos o sesgos como también soluciones simples e inequívocas, porque si proponemos soluciones rápidas sin tener en cuenta este entorno VICA, nos llevará a cometer grandes errores.

Ante la ambigüedad de estos entornos, es muy difícil adoptar una solución completamente correcta, por lo cual es fundamental entender que debemos tener flexibilidad, agilidad y adaptabilidad ante este tipo de situaciones confusas.

Este tipo de entorno exige que las Fuerzas Armadas estén preparadas para nuevas amenazas o en su defecto, en capacidad de adaptarse rápidamente a los cambios que se presentan.

Obviamente estos entornos VICA se intensifican con el empleo de las nuevas tecnologías, es por ello que debemos pensar en la prioridad y urgencia de digitalización del campo de batalla.

Figura 1.

Entorno VICA

	Características	Efectos	Se requiere
Volatilidad	• Naturaleza del cambio • Velocidad del cambio • Dinámica del cambio	• Dificulta identificación de tendencias y patrones • Genera inestabilidad	VISIÓN
Incertidumbre	• Impredecibilidad • Desconocimiento de los resultados	Dificulta la anticipación de: • Riesgos y amenazas • Oportunidades	COMPRENSIÓN
Complejidad	• Multiplicidad de causas • Interrelación de factores	Dificulta la toma de decisiones	CLARIDAD
Ambigüedad	• Multiplicidad de interpretaciones	Desconocimiento de la situación	AGILIDAD

Nota. La figura resume lo citado del entorno VICA. Adaptado del Min Def España (p.19) por Ministerio de Defensa de España, 2019, Publicación de Defensa.

En el artículo sobre la evolución tecnológica de los sistemas de armas (Navarro, José Maria, 2018) indica lo siguiente:

> La tecnología tiene un papel predominante en los combates modernos, da lugar a conflictos que se caracterizarán por el dominio y control de la información y el empleo eficaz de nuevos dispositivos, donde los conceptos para la resolución del problema militar ya no aplican al empleo tradicional, sino que mutan a la prevalencia de la ciberguerra, la guerra de la información y la influencia que esto implica en la opinión pública internacional, busca en todo momento lograr su Efecto Final Deseado (EFD) con acciones no cinéticas.(p.1)

Luego de analizar los avances tecnológicos, el entorno actual y su influencia en el desarrollo de las estrategias y acciones, profundizaré sobre la definición del Dominio del Ciberespacio (el cual es un dominio transversal al reto de los dominios y ámbitos)

En cuanto a los Dominios es de interés destacar las características especiales por la cual el Ciberespacio, es considerado un ¨Dominio¨ según la Junta Interamericana de Defensa (2020):

- Requiere capacidades únicas para operar en ese ámbito.
- No está totalmente abarcado por ningún otro ámbito (tierra, mar, aire, espacio).

- Se caracteriza por una presencia compartida de capacidades aliadas y adversarias.
- Es capaz de ejercer control sobre un oponente a través de la influencia y el dominio.
- Brinda oportunidades de sinergia con otros ámbitos.
- Proporciona oportunidades asimétricas entre todos los ámbitos. (p.23)

En este documento citado anteriormente se desarrollan algunas características particulares de este dominio, que es necesario destacar, donde explica que es un entorno artificial, creado por el hombre y de la misma manera que lo ha creado, puede modificarlo a voluntad.

Se observa que este dominio va mutando como lo desarrolla la Junta Interamericana de Defensa (2020) ¨El ciberespacio adquiere una nueva dimensión a medida que se desarrollan nuevas tecnologías y servicios; a esta altura poco tiene que ver internet original de la web y el correo electrónico a la actual de las redes sociales¨(p.24).

Conclusiones parciales

A partir de las características expuestas anteriormente del entorno complejo en el que están inmersas las OI podemos inferir que es de suma importancia tener la capacidad de planificar e integrar de manera efectiva todos los elementos de poder del Estado para minimizar las condiciones del ambiente en el que se vive actualmente donde todas las personas somos altamente influenciables por distintos dispositivos móviles y canales de difusión.

Es necesario contar con medios respaldados por tecnología avanzada que permita la detección y neutralización de acciones adversarias mediante póliticas de estado y aspectos legales que nos garanticen el accionar, especialmente en el ámbito del ciberespacio.

No debemos dejar de lado que la percepción pública y la opinión nacional e internacional pueden afectar la legitimidad y el apoyo a las operaciones militares, lo que puede tener implicaciones políticas y estratégicas, para lo cual es muy importante, dentro de las fuerzas también contar con elementos específicos de OI que funcionen integrados

permanentemente con el sistema de Comando y Control en las operaciones y con acuerdos de cooperación con las distintas agencias con injerencia en este aspecto en todos los niveles.

Capítulo 2

Las Operaciones de Información y las acciones en el Ciberespacio.

Este capítulo tiene el propósito de desarrollar el concepto de OI y como se pueden llevar a cabo este tipo de operaciones gracias a las TIC mediante acciones en el dominio del ciberespacio.

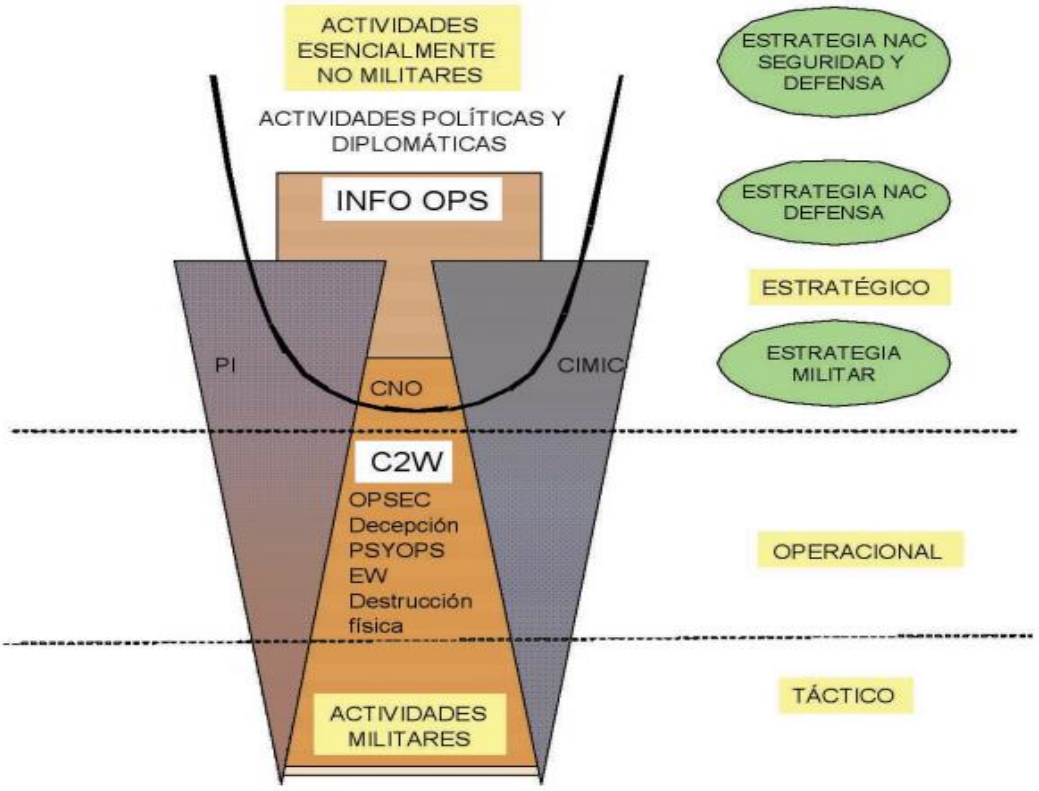
Sección 1: Operaciones de Información

Para iniciar con la temática, es necesario especificar las diferentes acciones de Información que pueden llevarse a cabo con propósito militar. Para ello es importante definir que constituye una Operación de Información, y sus alcances.

Inicialmente debemos entender las actividades que se realizan en los distintos niveles. (según la doctrina Española)

Figura 2

Actividades Militares y no Militares de las OI



Podemos citar también la doctrina militar conjunta de los Estados Unidos de América (a partir de ahora EEUU) la cual define a las OI como aquellas acciones planeadas para influir en la información y su entorno, de manera de favorecer la percepción, decisión y acción de actores específicos, de manera de negar, degradas, engañar o destruir la información del adversario, o su capacidad de que la misma circule (Joint Publication 3-13, Information Operations, 2019).

Para el presente trabajo, acotaremos el estudio de las OI basándonos en los efectos que las mismas persiguen, de acuerdo a lo establecido en la doctrina de EEUU.

Las mimas, buscan producir efectos de destrucción, interrupción, degradación, explotación, engaño e influencia, mientras que las defensivas se centran en producir los efectos de detección, restauración, protección, negación, y respuesta (U.S. DoD, 2016).

Los efectos explicitados anteriormente, se logran mediante el empleo de medios de diferente naturaleza, pero reduciremos el estudio a aquellos efectos que puedan implicar el uso de acciones en el ciberespacio para lograrlos, tales como:

- **Destrucción**: Consiste en dañar un sistema de forma tal, que no pueda realizar ninguna función o pueda ser restaurado a una condición utilizable. Desde el punto de vista OI, el logro de este efecto requiere del empleo de medios letales y no letales para inutilizar físicamente la información o sistema de información. Es más eficaz cuando se sincroniza para ocurrir justo antes de que el enemigo necesite ejecutar el C2 o cuando esté empeñado en un objetivo que le requiere el empleo intensivo de medios que son de difícil reconstrucción o reemplazo.
- **Interrupción:** Es la alteración del funcionamiento, proceso o tiempo de un sistema. Provoca que las fuerzas ejecuten prematuramente o fragmentada una operación. Dicho efecto se obtiene, mediante el empleo integrado de los fuegos

directos e indirectos, el terreno y los obstáculos. Interrumpir, en las OI, significa romper o interrumpir el flujo de información entre los nodos C2 seleccionados.

- **Influir**: Es hacer que el enemigo se comporte de una manera favorable a las fuerzas propias. Es el resultado de la aplicación de CRI sobre la gestión de la percepción para afectar las emociones, las motivaciones y el razonamiento. Es el efecto de mayor importancia, dadas las implicancias que involucra cuando logra su eficacia.
- **Detección**: Implica descubrir o discernir la existencia, presencia o hecho de intrusión en los sistemas de información. Es la identificación de los intentos del enemigo para acceder a la información y sistemas de información y comienza con los usuarios y administradores de éstos. La detección oportuna y la presentación de informes son las claves para iniciar la restauración y la respuesta. La detección electrónica ocurre en el perímetro digital interno.
- **Restauración**: Implica descubrir o discernir la existencia, presencia o hecho de intrusión en los sistemas de información. Es la identificación de los intentos del enemigo para acceder a la información y sistemas de información y comienza con los usuarios y administradores de éstos. La detección oportuna y la presentación de informes son las claves para iniciar la restauración y la respuesta. La detección electrónica ocurre en el perímetro digital interno.
- **Respuesta**: La respuesta en las OI es reaccionar rápidamente ante un ataque o intrusión de OI del enemigo. La identificación oportuna del mismo, la determinación de su intención y capacidades es la piedra angular para proporcionar una respuesta efectiva a las OI ofensivas enemigas.
- **Negación**: Implica impedir que el enemigo obtenga información sobre las capacidades e intenciones de las fuerzas propias, necesaria para una toma de decisiones efectiva y oportuna. Las Operaciones de Seguridad son el principal

medio no letal empleado para lograr este efecto, siendo ejecutadas en forma permanente.

- **Protección**: Son medidas que se adoptan para protegerse contra el espionaje o la captura de equipos e información sensibles. La protección se produce en el perímetro digital para controlar el acceso o mitigar los efectos del acceso del enemigo a los sistemas de información propios. Niega al enemigo, información acerca de las capacidades e intenciones propias mediante el control de los indicadores.

Los efectos mencionados, actúan las diferentes dimensiones del ambiente de la información, la física, informativa y cognitiva.

La dimensión física es aquella que se compone por los elementos tangibles que permiten el comando y control de las operaciones en los diferentes dominios.

La dimensión informativa es aquella que comprende a la información, su contenido y el flujo de esta a través de los sistemas de información destinados a su almacenamiento, procesamiento y diseminación.

La dimensión cognitiva centra su atención en las mentes humanas, elemento considerado clave para las acciones de influencia en la toma de decisión. Es en esta dimensión en la que se emplea la información para la influencia o falsas proyecciones para lograr toma de decisiones favorables a la situación propia. Principalmente, las acciones de las OI persiguen la influencia sobre normas, valores y creencias.

Sección 2: Acciones en el dominio del Ciberespacio.

Esta sección tiene el propósito de identificar a que nos referimos al hablar de acciones en el ciberespacio según la doctrina propia, y tomando como punto de comparación, lo

establecido en la doctrina de los EEUU, para finalizar con una conclusión referente a los alcances y limitaciones en el caso argentino.

El término “ciberespacio” no es un término en el cual haya una definición unánime, justamente por las características mencionadas en el capítulo anterior.

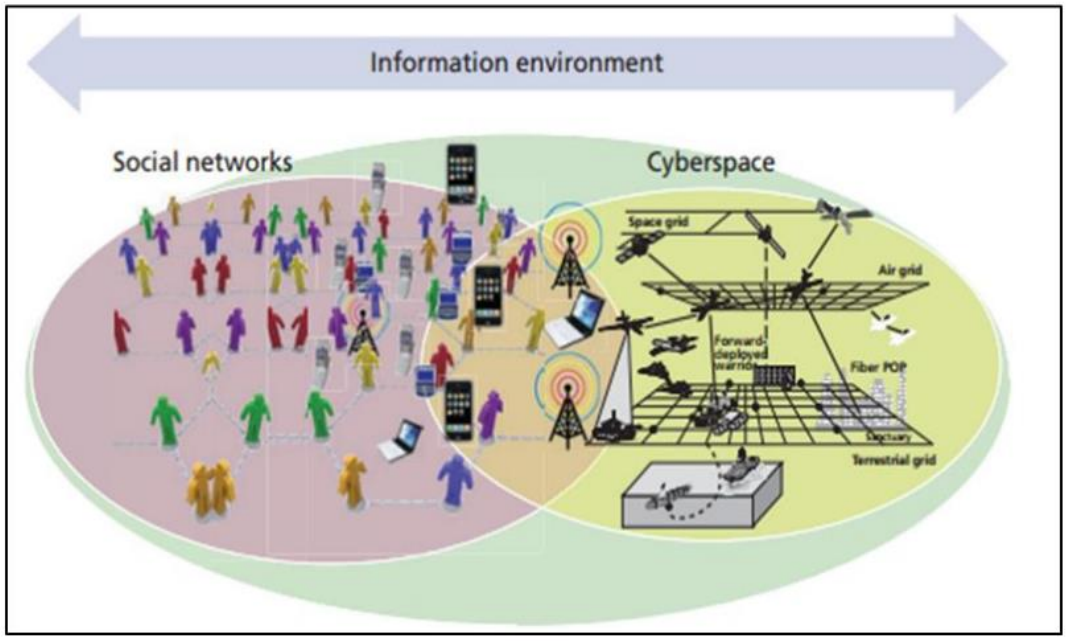
Muchos estudiosos de las acciones en el ciberespacio, concuerdan en que es un dominio que se caracteriza por poseer una dimensión física y una virtual, donde cuya interconexión permite el flujo de información entre usuarios en diferentes partes del globo.

En el ámbito militar, este flujo de la información resulta vital para el normal desarrollo de las operaciones, por ende, constituye un activo de gran valor para garantizar la libertad de acción en las mismas.

Es de interés entender el ambiente donde se desarrollan las OI y como se relacionan con las acciones en el ciberespacio, para ello se muestra en la siguiente imagen esta relación de manera gráfica.

Figura 3

Ambiente de las OI y la relación directa con el Ciberespacio.



Asimismo, cabe mencionar que para garantizar esta libertad de acción a la que se hace referencia, numerosos países del mundo están tendiendo a desarrollar elementos específicos con capacidades de garantizar la gobernanza de la información en los diferentes niveles de la guerra (entiéndase estratégico, operacional y táctico).

Ante lo mencionado, es importante destacar que la gobernanza de la información de combate sólo será posible si tengo el control de las redes de información por las cuales fluye la misma. Hay numerosas formas de lograr esto, pero a la que nos abocaremos será a las redes informáticas.

Son los componentes de las redes informáticas las que terminan configurando el ciberespacio, por ello es importante su protección y obtener la libertad de accionar en las redes propias y de un adversario. El conjunto de acciones destinadas a garantizar la libertad de acción propia, como a limitar la de un enemigo, son conocidas como acciones en el ciberespacio, entre las cuales encontramos las siguientes:

- **Operaciones Ofensivas:** Implican acciones destinadas a afectar adversarios a través de la manipulación, interrupción o degradación de sus sistemas y redes cibernéticas.
- **Operaciones Defensivas:** Incluyen medidas para proteger las redes y sistemas propios contra amenazas cibernéticas, como ataques informáticos, malware y intrusiones.
- **Operaciones de Influencia:** Esto se refiere a la capacidad de influir en la percepción y comportamiento de individuos, organizaciones o gobiernos mediante la manipulación de la información en línea, la propaganda y otras tácticas psicológicas.
- **Recolección de Inteligencia Cibernética:** Implica la recopilación de información a través de medios cibernéticos para comprender las capacidades y actividades de adversarios potenciales.
- **Operaciones de Red:** Incluyen la gestión y protección de las redes de comunicación, así como la identificación y mitigación de vulnerabilidades en dichas redes.

Cabe mencionar que el tipo de acciones referidas se corresponden con lo establecido en la doctrina conjunta de los EEUU (Departamento de Defensa de los Estados Unidos. (2018). Joint Publication 3-12, Cyberspace Operations).

Finalmente, en el caso del Instrumento Militar Argentino (a partir de ahora IMA) se cuenta con un Comando Conjunto de Ciberdefensa, cuya misión es la de brindar la protección cibernética a las redes informáticas de la defensa y, a orden, a las infraestructuras críticas que se le asignen, que permitan el normal desarrollo de las Operaciones Militares del IMA. Para ello, contempla entre sus tareas "La ejecución de las acciones necesarias y suficientes para operar en la eventualidad de un ambiente degradado desde el punto de vista cibernético y recuperar las capacidades afectadas por incidentes" (Comando Conjunto de Ciberdefensa), sin ahondar en los diferentes tipos de operaciones.

Por lo pronto, estos serán los puntos a tener en cuenta para el desarrollo posterior del trabajo.

Conclusiones parciales

De acuerdo a lo desarrollado, en este apartado, existen diferencias sustanciales entre los alcances de las acciones en el ciberespacio entre las doctrinas de los EEUU, España y los lineamientos otorgados al IM en el caso argentino.

Asimismo, la relación que existe entre las OI, y las Acciones en el Ciberespacio, ambas dos están concebidas para apoyar las acciones necesarias, lo cuál producirá que ambos tipos de dominios (Información y Ciberespacio) confluyan en beneficio de las la extensión de la política en todos los elementos de poder del Estado y especialmente influirán directamente en las operaciones militares y la libertad de acción de los elementos.

Capítulo 3

Aspectos vigentes en nuestro país sobre las Operaciones de Información y las acciones en el dominio del ciberespacio.

Este capítulo tiene el propósito de esclarecer la relación que existe entre las OI y las acciones en el ciberespacio, como unas apoyan a las otras, y como dentro de la doctrina en vigor se encuadran las mismas.

Sección 1: Relación entre las Operaciones de Información y las Operaciones en el Ciberespacio.

La relación entre las operaciones militares de información y las acciones en el ciberespacio es un tema de creciente importancia en el ámbito de la seguridad nacional y la defensa. En la era digital actual, donde la información y la tecnología desempeñan un papel crucial en todos los aspectos de la sociedad, las fuerzas armadas de todo el mundo han reconocido la necesidad de integrar estratégicamente las operaciones de información con las operaciones en el ciberespacio para lograr una ventaja competitiva en el campo de batalla contemporáneo, tal y como está siendo demostrado en los conflictos recientes de Ucrania e Israel.

Las operaciones militares de información se refieren a la recopilación, análisis y difusión de información con el objetivo de influir en las percepciones, decisiones y comportamientos de los adversarios, acciones que se dan en la dimensión cognitiva, tal y como se enunció en el capítulo anterior. De la misma forma, se busca proteger y fortalecer la propia posición en un conflicto. Este tipo de operaciones no se limita a la esfera física, sino que se extiende al ciberespacio, que como hemos visto, es un dominio transversal a los demás dominios, y donde la información fluye constantemente a través de redes digitales que se encuentran interconectadas.

En el ciberespacio, las acciones militares se llevan a cabo mediante operaciones cibernéticas, que pueden tener objetivos ofensivos o defensivos, tal y como fue expuesto en el capítulo anterior. Las operaciones ofensivas buscan comprometer la integridad, disponibilidad y confidencialidad de los sistemas de información del adversario, mientras que las operaciones defensivas buscan proteger los propios sistemas contra ataques cibernéticos. La relación entre las operaciones de información y las acciones en el ciberespacio es bidireccional y se manifiesta de varias maneras.

Para ser más específicos detallaremos como las acciones en el ciberespacio se relacionan con los efectos deseados de obtener por medio de las OI.

- Relación entre las OI y las acciones en el Ciberespacio para la destrucción/interrupción: En este aspecto, se vinculan por medio del uso de armas cibernéticas al emplear tácticas digitales para comprometer la integridad y funcionalidad de sistemas adversarios. Este enfoque busca causar daño significativo mediante intrusiones, manipulación de datos y desestabilización de infraestructuras críticas, fusionando habilidades cibernéticas con objetivos estratégicos de información y operaciones militares. El ejemplo más famoso de este tipo de acciones fue el empleo del arma “Stuxnet” en las plantas centrifugadoras iraníes en el año 2007.
- Relación entre las OI y las acciones en el Ciberespacio para la influencia: La manipulación de la información en línea, la difusión de desinformación y la realización de operaciones psicológicas en el ciberespacio son herramientas poderosas para moldear las percepciones y opiniones tanto a nivel nacional como internacional. Los actores estatales pueden aprovechar las redes sociales, los sitios web y otros canales en línea para difundir narrativas que respalden sus objetivos estratégicos y desacrediten a sus adversarios.

- Relación entre las OI defensivas y las acciones en el Ciberespacio: Este tipo de acciones se complementan permitiendo la negación de acceso del enemigo y la protección de activos digitales de gran valor para las operaciones propias.

  La negación de acceso implica la implementación de medidas cibernéticas para obstaculizar la capacidad del adversario para infiltrarse en sistemas críticos. Simultáneamente, la protección de activos digitales propios y sistemas de información se logra mediante estrategias de ciberseguridad, como firewalls, cifrado y sistemas de detección de intrusiones.

La negación y la protección, son dos efectos muy cercanos entre sí, por los cuales se busca salvaguardar la información de valor que fluye por medio de los sistemas propios. De esta forma, lo que se logra es prevenir la explotación de vulnerabilidades y mitigar posibles amenazas, asegurando la integridad y disponibilidad de la información.

Los efectos de restauración y respuesta están relacionados con las acciones tendientes a realizar ante la detección de una amenaza que daña total, o parcialmente, información propia. En este aspecto, las acciones relacionadas con el ciberespacio son aquellas que permiten la detección y mitigación de amenazas, como así también las medidas preventivas que permitan recuperar la información que se encontrase dañada. Tras la acción enemiga, y posterior a la identificación de la amenaza, prosiguen las acciones de respuesta, que poseen la misma naturaleza que persiguen las OI, pero en el dominio ciberespacial.

La efectiva coordinación de acciones en el ciberespacio con operaciones ofensivas y defensivas optimizan los efectos deseados por las mismas, y la integración de las OI y la tácticas de ciberdefensa fortalecen la capacidad de respuesta ante amenazas y la resiliencia de los sistemas de información en el ámbito digital.

Sección 2: Análisis de la Doctrina en vigor.

Por empezar, se debe destacar que no se cuenta en las Fuerzas Armadas con una doctrina que sirva de pilar para la comprensión, alcances y limitaciones de lo que son las operaciones de información. Lo mismo ocurre con las operaciones de ciberdefensa la cual está actualmente en revisión, tanto la conjunta como la específica.

Si bien hay extenso material bibliográfico disponible en línea para consulta, como doctrina de otros países, e incluso experiencias crecientes por el empleo de estas herramientas en los conflictos modernos, los mismos permiten seguir desarrollando y comprendiendo en forma diversa la naturaleza de estos tipos de operaciones.

La falta de una doctrina repercute en la comprensión de los contenidos consultados, dado que se suelen malinterpretar los conceptos de información, con inteligencia y con operaciones psicológicas.

Referente a estas últimas, las mismas se encuentran prohibidas para la acción militar por lo mencionado en la Ley de Inteligencia Nacional. No obstante, de los documentos consultados se infiere que las Operaciones Psicológicas están contenidas dentro de lo que son las Operaciones de Información, persiguiendo el objetivo de "influir". Este tipo de confusiones son las que afloran ante la falta de una doctrina.

Cabe destacar que, por lo expresado en la Ley de Defensa Nacional, la población civil no puede ser objetivo de ningún tipo de operación militar. Esta limitación afecta tanto a las Operaciones de información como a las Operaciones en el Ciberespacio. Esto exige un estudio minucioso, y claridad en los alcances de estos tipos de operaciones.

En el caso de las Operaciones en el Ciberespacio, se ha visto en esta Diplomatura, que los objetivos civiles constituyen un inconveniente en la planificación de las Operaciones Militares, por el hecho de que afectan tanto a los Sistemas enemigos, como a la población civil, y es esta dualidad la que termina imponiendo las limitaciones para el accionar del IM.

Asimismo, la Ciberdefensa en Argentina, tampoco posee una doctrina aprobada que sirva de orientación para la planificación de las operaciones, generando fallas en la interpretación de los alcance de este instrumento.

Conclusiones parciales

Bajo los aspectos desarrollados en el presente capitulo, se observa la necesidad con carácter de ¨Urgente¨ de contar con una doctrina y un marco legal que especifique los conceptos de empleo y respalde las acciones del IM en las operaciones que éste desarrolle. Asimismo, se deben considerar la complementariedad de los efectos producidos en los dominios de la información y del ciberespacio para lograr un uso eficiente de los medios disponibles para la AMC.

Asimismo es necesario que se revise la reglamentación en vigencia y que se vuelva a dar importancia a las Operaciones psicológicas las cuales son necesaria y complementarias para cualquier tipo de Operación.

Conclusiones finales

Dentro de los conceptos desarrollados en el primer capítulo de la presente investigación, se observa cómo las TIC surgen en esta evolución de la era de la información y obliga al Instrumento Militar a cambiar la manera de hacer la guerra, la cultura organizacional, tanto en el empleo de los distintos sistemas de armas como en el tipo de enlaces que se necesita para poder transmitir de manera instantánea y en tiempo real la información necesaria para la toma de decisiones, de esta forma favorecer el ciclo OODA (observación, orientación, decisión y acción) e irrumpir en el ciclo de decisión del enemigo.

Dentro de esta concepción es fundamental tener doctrina al respecto para poder desarrollar las OI o por lo menos poder previnir las acciones de otros actores estatales como no estatales, como lo hacen otros países vecinos.

Es fundamental tener políticas de Estado claras con respecto al accionar en los combates modernos, no podemos regirnos con reglamentaciones y normas legales que se aplican desde hace más de 20 años, debemos entender que la naturaleza de las necesidades de los Estados en plena ¨Era de la información¨ cambió la concepción de las formas tradicionales de imponer la propia voluntad ante intereses Políticos. Hoy en día hasta los conceptos más importantes de la Geopolítica Neoclásica quedan obsoletos ante el accionar en un dominio que no tiene límites y donde las reglas del juego van cambiando en función de la evolución de la Tecnología.

Bibliografía

Agumosa Pila. (21 de Noviembre de 2020). *Academia de las Ciencias y las Artes Militares.* Obtenido de Sección de Futuro de las Operaciones Militares: https://www.acami.es/publicacion/tipos-de-operaciones-militares-2035/

Andrade Rojas, Wilfredo. (02 de 11 de 11). *RE - PILO*. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/2444

EA (2023). *PC 00-02 Glosario para la Acción Militar Conjunta.* Buenos Aires: Publicaciones Militares.

EA (2023). *CCC*. Obtenido de Comando Conjunto de Ciberdefensa: https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/index.html

EMCO. (2023). Comando Conjunto FFAA. *Boletín Informativo Conjunto*. Buenos Aires, Argentina: EMCFFAA.

Junta Interamericana de Defensa. (2020). Ciberdefensa. *Guia de Ciberdefensa,* 113.

Min Def España. (2019). *Entornos Operativos 2035.* España: Publicaciones de Defensa del Gobierno de España.

Navarro, José Maria. (24 de Junio de 2018). *Defensa.com* . Obtenido de La evolucion tecnológica de los sistemas de armas: https://www.defensa.com/reportajes/evolucion-tecnologica-sistemas-armas

Pedroza, S. (28 de 08 de 2021). *La era de la información* . Obtenido de https://muytecnologicos.com/historia/era-de-la-informacion

Rossi, A. O. (2015). *Libro Blanco de la Defensa.* Obtenido de Mindef: www.libroblanco.mindef.gov.ar

Sain, G. R. (19 de 02 de 2021). *Jefatura de Gabinete de Ministros Direccion Nacional de Ciberseguridad.* Obtenido de boletinoficial.gob.ar: https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222

Trama, G. A. (2017). Operaciones Ciberneticas. *Vision Conjunta, 9*(17), 57.