MATERIA: TRABAJO FINAL INTEGRADOR

TEMA:

El Sistema de Comando y Control del Nivel Operacional

TÍTULO:

Estructura del Sistema de Comando y Control en el Nivel Operacional y los desafíos del siglo XXI

AUTOR: My BAIGORRIA, Francisco Javier

PROFESOR: DANISA RIERA.

Año 2019

RESUMEN

El comando y control puede definirse como el conjunto de medios humanos, equipos y materiales que, de manera integrada y estructurada, le permiten al Comandante y a su Estado Mayor, conducir, asesorar y controlar las fuerzas casi en tiempo real. Este sistema se encuentra en permanente evolución, producto de los avances tecnológicos y del surgimiento de nuevas exigencias característicos de esta época, cumulo de información, ampliación de los dominios y demás.

El sistema de comando y control en el nivel operacional en Argentina se ha actualizado, buscando poder hacer frente a estos nuevos desafíos. A pesar de ello, la constante evolución técnica que atraviesan los subsistemas que lo componen exige una permanente revisión y actualización de su estructura. Como así también contemplar y evaluar las necesidades de los sistemas particulares de cada una de las Fuerzas. Estas tienen su propia idiosincrasia, características, y responden a problemáticas, que en ocasiones son distintas entre ellas. Este punto es importante, ya que, en este nivel el trabajo de las tres Fuerzas debe ser caracterizado por la conjuntez.

Se debe tener en cuenta también, las exigencias que surgen de la ampliación de los dominios tradicionales –pasando de los tres, mar, aire, y tierra a cinco, agregándose el espacio y el ciberespacio– y de la integración del trabajo interagencial, necesarios para afrontar los desafíos de éste nuevo milenio.

El objetivo de esta investigación es intentar fijar los lineamientos básicos que debe contener el Sistema de comando y control del nivel operacional de la República Argentina que le permita afrontar los desafíos del siglo XXI en un Teatro de Operaciones Operacional.

Se determinaron los siguientes lineamientos: El Sistema de comando y control se debe estructurar de la siguiente manera: Subsistemas: Comando, control, comunicaciones, computación, vigilancia y reconocimiento, podría agregarse ciberdefensa o estar inmerso dentro del Subsistema computación. Con las siguientes características: Integrado, flexible, móvil, resiliente, interoperable, con capacidad de soportar la tecnología de Inteligencia Artificial.

Palabras clave: *C*omando y control, Comunicaciones e informática, Inteligencia, Vigilancia, Reconocimiento.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

INTRODUCCCIÓN

El presente trabajo está relacionado con el sistema de comando y control empleado en el nivel operacional. Particularmente, lo que se investiga y analiza, son los lineamientos básicos sobre los que se debe apoyar dicho sistema, para facilitar la conducción del comandante, y el asesoramiento y asistencia por parte del Estado Mayor, para la conducción de las operaciones militares.

Este es tan antiguo como las guerras mismas, y fue evolucionando en cada momento histórico producto de diversos factores circunstanciales, tales como los tecnológicos, organizacionales, entre otros. La necesidad de los Comandantes de poder dirigir sus fuerzas, fue lo que origino su creación. (ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, 2016, págs. I-5). Dicho sistema no siempre fue así, en un principio era simple, se basaba en la observación, generalmente desde una altura para obtener la información, la cual era procesada por el líder, y luego se la transmitía en forma de órdenes a viva voz o por señales. Este sistema fue empleado hasta no hace mucho tiempo por distintos Comandantes, siempre y cuando el campo de batalla le permitiera observar desde una altura que le facilitara la evaluación y análisis de la situación que se sucedía. Sin embargo, medida que crecían los volúmenes de las fuerzas y se expandían los espacios donde se desarrollaban los conflictos, este sistema iba quedando obsoleto. Ya no les permitía a los conductores adoptar decisiones, dado que no podían ver la evolución de la situación. Es así que se comenzaron a emplear mapas y maquetas representativas de los diferentes escenarios. Estos eran recorridos por estafetas para la transmisión de las órdenes y la obtención de información de las posiciones de las tropas. Consecuentemente, esta modalidad trajo aparejada el peligro de que dichos mensajeros fueran interceptados y se les robara la información; por lo cual debieron emplearse códigos para encriptar los mensajes. Esto dio como resultado, un sistema rígido y poco flexible de comando y control, donde todo se centraba en el comandante y anulaba la iniciativa de sus subordinados (Cubeiro Cabello, 2001, pág. 38).

Lo mismo que sucedía en tierra, se vivía en el mar, donde todo pasaba por la observación y la transmisión de órdenes, las cuales se generaban en el buque insignia. Este proceso se realizaba a través de banderas y naves que transmitían partes. Traía como consecuencia que el enemigo identificara dicho buque y centrara sus fuegos sobre éste, lo que ocasionaba que los Comandantes estuvieran más preocupados por su seguridad, que por el desarrollo de la batalla en sí (Cubeiro Cabello, 2001, pág. 38)

En 1840, la tecnología hizo un salto cualitativo que influyó en el desarrollo de los conflictos. Se trató de la invención del telégrafo, el cual facilitó el ejercicio del mando en el combate, a

lo largo de grandes distancias acortando los tiempos. Este instrumento fue empleado en todos los conflictos importantes, incluso hasta la Primera Guerra Mundial. El inconveniente que presentaba, era que se encontraba anclado a la instalación física de postes e hilos conductores, los cuales eran costosos, lentos de instalar, y muy susceptibles a las actividades del enemigo (Cubeiro Cabello, 2001, pág. 39).

Con posterioridad surgió el teléfono, el cual, al ser transmisión de voz en forma directa, permitió el traspaso de un mayor volumen de información en menor tiempo. No obstante, al igual que el telégrafo, siguió teniendo una servidumbre de estructura y continuó siendo afectado por las acciones del adversario.

Recién con la aparición de la radio se volvió a producir un cambio sustancial que permitió una evolución en la manera de ejercer el Comando y el Control. Su fase de prueba por excelencia fue la Segunda Guerra Mundial, donde pudo demostrar sus bondades. Se comprobó la facilidad para impartir ordenes en tiempo real, obtener información de manera instantánea y, apenas adoptadas las resoluciones, poderlas transmitir de forma pertinente. Dotó a las fuerzas de la flexibilidad y descentralización, de la cual se habían privado hasta el momento (Cubeiro Cabello, 2001, pág. 39).

A partir de allí, se inició una carrera en el mejoramiento del subsistema de comunicaciones, haciéndolo cada vez más adaptable, flexible, ligero, extendiendo su alcance. Recién con la aparición de los primeros procesadores, se produjo un nuevo salto tecnológico. Esto permitió, a medida que iban evolucionando, se agregaran los subsistemas de radares, nuevas armas, satélites, sonares, etcétera, dándole al Comandante y a su Estado Mayor infinidad de información. Éste cúmulo de datos producía en ciertas ocasiones, una suerte de parálisis por análisis, ya que tornaba imposible su evaluación de manera integral, limitando a los escalones decisorios en lo que respecta a la adopción de resoluciones.

Dados éstos inconvenientes, los Sistemas de Comando y Control debieron adaptarse y buscar nuevas formas de solucionar tal situación. Esto dio lugar al desarrollo de redes, banco de datos, simuladores, entrenadores gráficos, y demás. Sin embargo, estos dispositivos en ocasiones brindaron resultados favorables y en otras fueron más parte del problema que de la solución. Evolucionaron, modificaron sus capacidades C2, C3, C3 I2, C2TI, y así sucesivamente, en la búsqueda de solucionar y facilitar la conducción por parte del Comandante y el asesoramiento de su Estado Mayor. (ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, 2016, págs. I - 6)

El presente trabajo de investigación pretende determinar los lineamientos básicos, tanto funcionales como estructurales, que debe contener un sistema de comando y control. Esto a

fin de facilitar la integración, no solo de los tres Sistemas particulares de las Fuerzas Armadas Argentinas, sino también para afrontar las necesidades surgidas de las exigencias actuales.

Relacionar dicho Sistema de Comando y Control con tres nuevas exigencias, ciberdefensa, inteligencia artificial y armas de impulso electromagnético. Ésta última fue seleccionada por su capacidad de afectación sobre los distintos Subsistemas, principalmente, el de comunicaciones e informática, el cual constituye la columna vertebral del Sistema de Comando y Control. Si bien éstos no son los únicos desafíos de ésta época, son representativos de la influencia e impacto que tendrán las guerras modernas sobre dicho Sistema.

A fin de afrontar lo anteriormente descripto, surge el siguiente interrogante que guía esta investigación: ¿Qué lineamientos se deben tener en cuenta en la composición de la estructura de un Sistema de Comando y Control tipo, que permita afrontar los desafíos del siglo XXI en un Teatro de Operaciones?

La investigación seguirá un proceso metodológico descriptivo en el que se realizará análisis documental y bibliográfico de autores que hayan trabajado el tema, con un enfoque cualitativo. El trabajo se apoyará sobre conceptos básicos y esenciales de la composición de la estructura de un Sistema de Comando y Control tipo que facilite la conducción en el nivel operacional.

Para la elaboración del trabajo se analizarán en forma inicial los reglamentos relacionado con el tema, existentes en el nivel conjunto, y los correspondientes a cada Fuerza Armada. También integrarán el análisis los reglamentos y publicaciones de actualidad e interés a nivel mundial relacionados al tema, los cuales son en general de acceso público y se encuentran en los diferentes medios digitales.

Esto a fin de dar cumplimiento al objetivo general de determinar los lineamientos básicos que debe contener el sistema de comando y control del nivel operacional de la República Argentina que le permita afrontar los desafíos del Siglo XXI en un Teatro de Operaciones. Los objetivos específicos, el primero de describir la necesidad del Sistema de comando y control, como lo estructura cada una de las Fuerzas Armadas, y como es el empleado por Estados Unidos. El segundo de describir las características funcionales y estructura de un Sistema de comando y control, y los desafíos que debe afrontar en el Siglo XXI en el Teatro de Operaciones.

A partir de que las guerras actuales –con características híbridas y no trinitarias como menciona Martin Van Creveld en su libro La Transformación de la Guerra– exigen un Sistema de Comando y Control confiable, flexible, expandible, entre otras características.

Éste Mantiene una capacidad de resiliencia para soportar los distintos ataques y poder seguir funcionando para permitir la conducción en el nivel operacional del Teatro de Operaciones.
Por ello, se deberá tener en cuenta en su estructura la integración de los siguientes Subsistemas: el comando, el control, la inteligencia, las comunicaciones e informática, la vigilancia, sensores, medios agresivos para la defensa, reconocimiento, ANT. Todos ellos integrados y en capacidad de funcionar en forma permanente e ininterrumpida. Dicho Sistema deberá basarse en una estructura expandible, integrado, distribuido y con la capacidad de multifunción que le permita asistir a todas las funciones del Comando y con la resiliencia anteriormente mencionada.
Este trabajo buscará dar respuesta a los interrogantes planteados sobre cuáles deben ser los lineamientos básicos a tener en cuenta en la estructura de un Sistema de comando y control tipo, que le permita afrontar las exigencias del Siglo XXI. Y a la verificación o no de la hipótesis, en la cual se expresa la necesidad de integrar los siguientes Subsistemas: Comando, control, comunicaciones, inteligencia, informática, vigilancia, sensores, medios agresivos para la defensa, reconocimiento, ANT. Todos ellos integrados y en capacidad de funcionar en forma permanente e ininterrumpida, con una estructura expandible, integrado, distribuido, y con la capacidad de multifunción que le permita asistir a todas las funciones del comando y con la resiliencia que le facilite su supervivencia. Será desarrollado a través de dos capítulos. El primero abarca tres desafíos del siglo XXI, la inteligencia artificial, la ciberdefensa y las armas de pulso electromagnético. Si bien existen un mayor número de desafíos característicos de ésta época, el solo hecho de expresar su existencia y su explicación, merecerían la realización de un trabajo de investigación particular, y ésta no es la finalidad del presente trabajo. Estos tres desafíos han sido seleccionados considerando el impacto y la influencia que generaran en el sistema, obligando su revisión.
El segundo capítulo se divide en cuatro apartados. El primero desarrolla los Sistemas empleados por cada una de las Fuerzas Armadas Argentinas. El segundo la descripción del Sistema de comando y control en el nivel operacional, empleado en la República Argentina. El tercero describe el sistema C4ISR, empleado por Estados Unidos, al solo efecto de ver las características de un sistema probado en combate. Y el cuarto marca los lineamientos básicos que debería tener un sistema de comando y control, que le permita afrontar las exigencias del nivel operacional y los desafíos mencionados en el capítulo I.
Ésta investigación abarcará la descripción básica y conceptual de los factores que deberán ser tenidos en cuenta para la composición de un Sistema de comando y control en el nivel operacional del Teatro de Operaciones. Se tendrá en cuenta las necesidades de las Fuerzas

Armadas Argentinas. Y esto no limita que en el futuro pueda sufrir modificaciones, debido a la evolución constante del contexto mundial, servirá como punto de partida para futura mejoras.

Además, se hará una explicación del Sistema empleado por Estados Unidos, el C4ISR, y será a solo efecto de tomarlo como parámetro de máxima, sin bien el mundo afronta los desafíos de este Siglo, cada país tiene distintas capacidades y exigencias impuestas para sus Fuerzas, por lo tanto, éste aspecto será a solo efecto de mostrar un sistema más desarrollado que el empleado en Argentina. Y como desafíos de éste siglo en lo que respecta al Comando y Control, solo se abordarán tres temas a modo ejemplificador para exponer las exigencias que deberán afrontar dicho Sistema, el primero será la Ciberdefensa, el segundo la Inteligencia Artificial y el tercero dentro del concepto de las nuevas armas, las de Pulso Electromagnético. De los tres temas anteriormente mencionados, me limitare a detallar su conceptualización y manera de afectación de los Sistemas de comando y control.

El presente trabajo de investigación pretende constituir un aporte importante a la doctrina Conjunta, actualizando la misma en el nivel operacional principalmente del Teatro de Operaciones, poniendo de manifiesto las nuevas características tanto funcionales como estructurales, que permitan el desarrollo de un adecuado Sistema de Comando y Control que facilite la integración no solo de los tres Sistemas particulares de las Fuerzas Armadas Argentinas, sino también las necesidades surgidas de las exigencias actuales.

Pretende servir de base sólida no solo para el presente empleo, sino también para futuras actualizaciones del Sistema que pudieren surgir a futuro producto de los cambios en la naturaleza subjetiva de la guerra, que seguramente impactaran en forma directa sobre el mismo, exigiendo una expansión en sus capacidades.

Brindará aporte en los distintos Subsistemas que lo conformarán, entre otros el Subsistema de Comando, el de Control, el de Inteligencia, de comunicaciones, el de informática, vigilancia, etc. Como así también los medios y los aspectos básicos y mínimos que se deberán tener en cuenta para el adecuado funcionamiento del mismo.

Relacionará dicho Sistema de Comando y Control con tres nuevas exigencias, Ciberdefensa, Inteligencia Artificial y Armas de Impulso Electromágnetico - ésta última fue seleccionada por su capacidad de afectación sobre los distintos Subsistemas, principalmente el de comunicaciones e informática, el cual constituye la columna vertebral del Sistema de comando y control- si bien éstos no son los únicos desafíos de ésta época, son representativos de la influencia e impacto que tendrán las guerras modernas sobre dicho Sistema.

CAPÍTULO 1. Desafíos del siglo XXI

1.1 La inteligencia artificial

En la actualidad no hay un concepto único consensuado por la comunidad científica para definir la Inteligencia Artificial. Sin embargo, esta puede ser descripta como una rama de la informática, la cual, mediante la combinación de algoritmos, le permite a un procesador ser inteligente. Es decir que puede imitar las acciones cognitivas de los seres humanos, como ser la resolución de problemas a partir de una cierta base de datos o parámetros, aprender, etcétera.

(Cespedes D, Hernandez w, 2017, pág. 6)

Los primeros trabajos relacionados a la Inteligencia Artificial se los pueden atribuir al matemático inglés Alan Touring, quien en 1950 publicó un artículo, Computing Machinery and intelligence -Maquinaria informática e inteligencia-. En él exponía que si una maquina podía actuar como un humano, entonces era una maquina inteligente. Para demostrar su teoría, dispuso que si un ser humano, podía mantener una conversación mediante el empleo de un terminal con otro ser humano o una computadora que se encontrara en una habitación contigua, y luego de la conversación, no pudiera distinguir si lo hizo con un humano o una máquina, entonces lo que se encontraba en la habitación contigua era un humano o una maquina inteligente. Si bien han pasado muchos años desde el planteo de este concepto, aún hoy en día mantiene su importancia, ya que sostiene ciertos parámetros que debe poseer una máquina para ser considerada inteligente. Ellos son: reconocimiento del lenguaje natural, razonamiento, aprendizaje y representación del conocimiento. (Garcia Serrano, 2012)

Dentro de la Inteligencia Artificial hay varias clasificaciones, dependiendo del autor que se utilice. Por ejemplo, Arend Hintze, profesor asistente de biología integrativa e informática e ingeniería de la Universidad de Michigan, Estados Unidos, la clasifica en cuatro tipos. El primero, la maquina reactiva es considerada la más básica, ya que ella no puede almacenar recuerdos, tomar decisiones. El segundo son las máquinas con memoria limitada que emplean experiencias guardadas para poder ser utilizadas en la toma de decisiones. El tercero son las máquinas con una teoría de la mente, es decir, las que poseen a capacidad de entender y expresar las ideas, emociones, intenciones, que afectan a la toma de decisiones. Por último, las máquinas con conciencia propias: Estas son capaces de analizar el entorno y poseen conciencia, serían la máxima expresión de la Inteligencia Artificial. Pero aún no han sido desarrolladas. (Hintze, 2016)

Otra clasificación es la que ofrece la que describe el Capitán George Galdorisi en su artículo *La Marina necesita la IA, simplemente no está seguro por qué* donde hace referencia a la inteligencia artificial general (AGI), conocida también como inteligencia artificial fuerte o completa. Esta Inteligencia se describe como la capacidad que puede tener una máquina para ejecutar distintos tipos de acciones en general. Ésta busca de cierta manera compararse con la inteligencia humana. También hace referencia a la inteligencia estrecha artificial (ANI) que es la que se aboca a tareas más específicas; es más limitada en cuanto a la ejecución de acciones. El autor considera que ésta última sería la más apta en colaboración con el combatiente, ya que éstos podrían emplear dicha tecnología para hacer más eficiente su trabajo. Pero a la vez el autor se pregunta, si no sería mejor, si la Marina definiera qué tipo de tecnología de inteligencia estrecha artificial necesita para contribuir en su toma de decisiones, es decir, en el sentido de poder resolverse más rápido que su adversario. (Galdorisi, 2019, pág. 2).

La última clasificación realizada por Galdorisi - inteligencia estrecha artificial-, de poder ser delimitada y establecida, simplificaría la actividad de la toma de decisiones en todos los niveles de la conducción, en particular, en el nivel operacional que es donde se da la conjunción de las tres Fuerzas Armadas, sumado a el trabajo interagencial que se debe desarrollar en el mismo, como por ejemplo, con Gendarmería Nacional, Policía Federal, Policía Provincial, Organizaciones no estatales, y demás, como así también todos los factores del ambiente operacional:

- La influencia de la política y la estrategia Nacional y militar.
- El ambiente geográfico, los factores militares.
- Las características de la lucha.
- Los sistemas de armas que pueden emplearse.
- Los factores sociales.
- Los medios de información y su influencia en la opinión pública.

sumado a la conjunción de los mismos, ya que éstos rara vez actuarán en forma aislada o independiente, darán origen a:

- Limitaciones y restricciones impuestas en el uso de la fuerza.
- Las características de las operaciones que desarrolla el CTTO.
- La magnitud de las fuerzas que podrán ser empleadas

- La composición y el tipo de las Fuerzas.

- La proporción entre las armas, tropas técnicas, tropas para operaciones especiales y servicios.

- La estructura orgánica y de comando más apropiada.

- La necesidad de equipos especiales.

- Los medios para proporcionar movilidad y rapidez a las Fuerzas.

- Medios especiales para la comunicación social y el control de la población. (Ejército Argentino, 2015, págs. I - 6).

Antiguamente los Jefes se veían limitados en sus decisiones debido a la falta de medios de obtención de información y, por ende, la ausencia o escasa cantidad de la misma. Por lo tanto, sus respuestas estaban limitadas a los datos disponibles, debiendo acudir a su experiencia, intuición e incluso muchas veces al azar.

En la actualidad el factor tecnológico ha ampliado el espectro y el alcance para la obtención de la información, haciendo que el Comandante de éste nivel cuente con un excesivo cumulo de datos. Dentro de la cual se dificulta su clasificación entre aquella que es realmente útil, de aquella que no lo es abarcando un mayor espacio temporal para su análisis, para obtener un resultado tal que le permita al Jefe adoptar la mejor resolución para afrontar un problema militar.

Por estas razones, se considera que el poder desarrollar y aplicar la inteligencia artificial, es un nuevo desafío que le va permitir al Comandante operacional determinar qué información buscar. Por ende, hacer un mejor análisis de ella, una integración más detallada y minuciosa de los distintos datos obtenidos, reducir los tiempos, actuar más rápido que el enemigo. Lo que le brinda la posibilidad de meterlo dentro de su ciclo OODA – Observación, Orientación. Decisión, Acción- y arribar a la mejor respuesta a la problemática planteada, con un menor grado de error.

Además, éste tipo de tecnología permite su combinación con otras tales como el Aprendizaje Autónomo y el *Big data*, las que brindan una mayor capacidad y velocidad de respuesta. Para entender ésta afirmación es preciso describir cada una de ellas. El Aprendizaje Autónomo es una rama de la inteligencia artificial, la cual le permite aprender a una máquina, de manera automática a partir del empleo de técnicas. Así, aprende a través de la inserción repetitiva de patrones. Ejemplo de esto serían los buscadores de internet o los reconocimientos faciales o

de voz. Se diferencia de la inteligencia artificial anteriormente descripta en que ésta se basa en una programación algorítmica y no en la inserción repetitiva de ejemplos. (Movetia, 2018)

Por su parte, *el Big Data* hace referencia al conjunto de datos y combinación de ellos, sin especificar cantidades, ya que se habla de petabytes (1.000.000.000.000.000 bytes) y exabytes (1.000.000.000.000.000.000 bytes), los cuales, debido a su volumen, variabilidad y velocidad, son difíciles de analizar. (IBM, 2012). Si se toma en cuenta que la inteligencia artificial se nutre de datos para poder desarrollar algoritmos, entender el entorno e interactuar con él, esta se transforma en una combinación perfecta para alcanzar un mayor grado de eficiencia. Lo cual permite obtener respuestas en menor lapso temporal, y contribuyendo con el desarrollo de nuevos algoritmos que amplíen las capacidades de ésta.

Países como Estados Unidos y China ya están tratando de implementar estos avances a sus Fuerzas Armadas. Las aplicaciones son diversas, van desde el empleo en vehículos no tripuladas, hasta sistemas de defensas antiaéreos, sistemas de GPS y otros. En este trabajo la aplicación que interesa es la empleada sobre el sistema de comando y control, más específicamente para la toma de decisiones del Comandante del nivel operacional. El Capitán George Galdorisi, en el artículo ya mencionado anteriormente, explica que "la ANI no toma la decisión, ni debería hacerlo, pero le brinda al Comandante suficiente información bien curada, para que él pueda tomar la mejor decisión y más rápido". (Galdorisi, 2019, pág. 4). Luego afirma que la Marina de los Estados Unidos debe aprovechar el *Big Data*, el aprendizaje autónomo y la Inteligencia Artificial para que, mediante ésta combinación, sus Fuerzas obtengan una ventaja respecto del enemigo. También menciona, que la Armada solicitó que se incluya en el presupuesto de este año (2019) 60 millones de dólares para que sean empleados en el desarrollo científico, de prototipos y compras de Inteligencia Artificial y aprendizaje autónomo. (Galdorisi, 2019, pág. 4).

Una posible combinación a futuro sería la Inteligencia Artificial con la Computación Cuántica, ésta última al usar cúbits –sistema cuántico que posee dos estados- en vez de bits, permite alcanzar nuevos algoritmos y analizar un gran volumen de datos en menor tiempo. Éste puede ser empleado para realizar una nueva manera de aprendizaje automático, teniendo un impacto directo sobre la primera. De darse ésta situación, potenciaría la Singularidad –las maquinas superen a la inteligencia humana. (Knight, 2017)

Un aspecto controversial que ha desatado foros e infinidad de opiniones, es el factor ético, ya que se plantea que una maquina no posee sentido común, valores ni necesidades humanas.

Entonces surgen algunos interrogantes tales como la prudencia y fiabilidad en la toma de decisiones, rendición de cuentas, y el lugar que ocupa el ser humano entre otras. Además, hay que tener en cuenta que la ética no es igual en todas las culturas por ende la postura ante ésta nueva tecnología varía dependiendo de las mismas. (López de Mántaras, 2017)

Resumiendo, se puede ver como la Inteligencia Artificial, que hasta hace unos años se creía que no iba a tener aplicación práctica y casi cae en descarte, ha recobrado en este nuevo mileño un auge sin precedentes. Si bien aún se encuentra en desarrollo y todavía no se sabe cuál va a ser su límite, si es que los tiene, y con qué otras tecnologías podría combinarse, si se puede vislumbrar el uso aplicativo a la toma de decisiones que facilitaría el comando y control en el ambiente operacional por parte del Comandante, ofreciéndole una ventaja sustancial respecto del oponente, logrando que éste entre en su ciclo OODA.

1.2 La ciberdefensa

A los dominios clásicos, mar, aire y tierra, en los últimos años se le han sumado otros más, como ser el espacio, el ciberespacio. Este último ha recibido varias definiciones, depende del autor que se utilice a tal fin. Según Adrianna Llongueras Vicente, autora del libro *La guerra inexistente*, la ciberguerra toma lo expresado por el Departamento de Defensa de Estados Unidos, el cual caracteriza al ciberespacio como "caracterizado por el uso de la electrónica y el espectro electromagnético para guardar, modificar, intercambiar información a través de los sistemas de redes de la información y las infraestructuras físicas". Como así también la de la Directiva Presidencial sobre Seguridad Nacional (NSDP 54), la cual lo define como "un dominio global dentro del medio de la información compuesto por las interdependientes infraestructuras y redes de información, incluyendo internet, las redes de telecomunicaciones, sistemas de computadoras, así como procesadores y controladores". (Llongueras Vicente, 2011, pág. 18)

Éste dominio fue creado artificialmente por el hombre, por ende, es sintético; ésta es una de las principales diferencias que tiene con los medios tradicionales. En él se apoyan todas las estructuras Estatales y no Estatales, independientemente de que las actividades sean licitas o ilícitas y todos aquellos que emplean las técnicas de la informática y comunicación. Ejemplo de ello son todos servicios que tiene un país asociado al empleo de éste dominio, sistemas bancarios, administrativos, energéticos y demás.

Otra gran diferencia es que, al día de hoy, no hay internacionalmente un marco jurídico legal que lo regule. Por lo tanto, es permeable de la ejecución de actividades ilícitas, normalmente realizada por personas o entidades a las que se las denomina *hackers* "Persona experta en el manejo de computadoras, - o también - persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta" (Real Academia Española, 2019). Los *hackers* pueden trabajar para sí mismos, para organizaciones o para Estados, con un variado número de objetivos.

El ciberespacio permite la interacción social, a través de varias redes -facebook, instagram y demás-, y es el lugar donde confluyen el común de los usuarios virtuales, los *hackers* y la información. Convirtiendo este dominio, en un atractivo sitio para la ejecución de actividades prohibidas - reclutamiento terrorista, comercio en el mercado negro, ataques contra instituciones, países, como así también actividades licitas como ser comercio, actividades de esparcimiento, y otras-. Los distintos Estados tienen la necesidad de proteger sus sistemas de estas actividades realizadas por los ya mencionados *hackers*, para lo cual hacen empleo de la ciberdenfensa y la ciberseguridad. Muchas son las definiciones respecto de estos dos conceptos, tantas como autores que escriben sobre ellas. La autora Adrianna Llongueras Vicente define Ciberseguridad como la que se encarga de "…identificar que se debe proteger, como proteger, contra qué o quién, y con qué medios se debe proteger" (Llongueras Vicente, 2011, pág. 23). Mientras que la ciberdefensa es definida como "…además de prevenir los ataques como hace la ciberseguridad, da respuesta a los mismos con nuevos ataques con el fin de salvaguardar la seguridad" (Llongueras Vicente, 2011, pág. 23). Hoy en día en los medios de comunicación se habla de ciberguerra, la cual es definida por Sandra Camila Rojas en su trabajo Ciberdefensa y ciberseguridad: Una nueva prioridad para las naciones, de la siguiente manera:

> …una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el método empleado no sería la violencia física, sino un ataque informático… (Valencia Rojas, 2014, pág. 6)

Ejemplo de la aplicación de ésta definición es el ataque Ruso contra Ucrania -comenzaron el 27 de junio de 2017-, en la cual le produjeron cortes de energía, desaparición de registros digitales de organismos nacionales, fallas en los cajeros automáticos, afectación de las

computadoras que controlaban la central nuclear de Chernobyl, y otras fallas más. (Infobae, 2019)

Como se puede ver en lo descripto anteriormente, esta nueva amenaza no tiene fronteras, puede ser empleada desde un individuo con intereses personales, organizaciones y Estados. Puede atacar indistintamente cualquier nivel de la conducción y es transversal a todos los dominios. Por ello, el Sistema de comando y control que apoya al Comandante del nivel operacional, es un blanco perfecto para el desarrollo de este tipo de actividades por parte del enemigo. Su afectación podría dejar paralizado a todo el comando y sus medios desplegados en cada uno de los dominios que le son pertinentes. Por eso debe tener la competencia suficiente para poder hacer frente a este peligro existente, detectarlo oportunamente, anticiparse a sus acciones y tener la capacidad de reaccionar y hacer las acciones ofensivas necesarias que contribuyan a su protección y afectación de los sistemas del oponente. Debe estar preparado para hacer un uso intensivo de la ciberdefensa y ciberseguridad en este marco de ciberguerra que se desarrolla en nuestros días.

1.3 Las armas de pulso electromagnético

Éste tipo de armas son propias de ésta era, pero basados en experimentaciones del siglo pasado, las cuales han encontrado su punto de aplicación, a pesar de aún estar atravesando etapas de desarrollo, en los campos de batalla modernos. Se las puede clasificar como armas de avanzadas o armas no letales, ya que solo afectan a dispositivos eléctricos u electrónicos. Si se quiere entender que es este tipo de armamento, hay que comenzar por definir que es un pulso electromagnético. Éste se comprende como un pulso de breve duración temporal de energía electromagnética, el cual puede ser generado por distintas fuentes, desde una fuente natural como el sol, o una maquina destinada a tal fin.

Antes del lanzamiento de las primeras bombas nucleares en la Segunda Guerra Mundial -Little Boy y Fat Boy-, el físico italiano Enrico Fermi, concluyó que - ante un evento de violenta liberación de energía, se produciría una potente emisión de radiofrecuencia de un gran ancho de banda-. A pesar de ello, recién en el año 1962 se llevaron a cabo las primeras pruebas, haciendo explosiones nucleares en altura, logrando afectar a los equipos eléctricos y electrónicos. Dichos descubrimientos motivaron el interés para su aplicación en el campo militar. El continuo estudio de esta tecnología permitió lograr los mismos efectos, pero ya sin la necesidad de emplear el factor nuclear. (Grunschlager, 2016)

La utilización de este armamento en los campos de batallas actuales, dejaría a todos los dispositivos eléctricos y electrónicos fuera de servicio. Imaginando esta situación, se

observaría a un Comandante sin su sistema de comunicaciones, columna vertebral de su sistema de comando y control. Los sistemas de vigilancia, reconocimientos, posicionamiento, armamentos, vehículos, sistemas sanitarios, todo lo que emplee algún tipo de energía quedaría fuera de servicio, llegando al colapso casi la totalidad del sistema. Se volvería tal vez, a combatir como en el siglo XIX, navegando con brújula, haciendo los reconocimientos como en la guerra de Zapa para el cruce de los Andes. La tracción empleada sería a sangre y se volvería al uso de las armas convencionales; los campos de batallas actuales pasarían a ser una suerte de conflictos de guerras napoleónicas.

El Pentágono ya ha tomado conciencia de ésta amenaza, temiendo el empleo de las mismas sobre sus centrales nucleares, las cuales, de ser afectadas, podrían detener sus circuitos enfriadores. Dicha situación derivaría en la explosión de sus reactores y crearía una nube radioactiva que afectaría a millones de habitantes. El Ministerio de Defensa reconoce que aún no están preparados para afrontar este tipo de acontecimientos. Su Presidente, Donald Trump, firmó una orden en el mes de marzo de 2019, que estableció el trabajo conjunto de distintos Departamentos de Estado, en la búsqueda de formas de prevención ante un posible ataque de éstas características. (Hispantv, 2019)

Los temores de Washington no son infundados ya que otros Estados, no alineados bajo su órbita, tales como Rusia, Corea del Norte e Irán, se encuentran en continua investigación y producción de armamento de pulso electromagnético. Contando éstos con vectores, vehículos y otros medios en capacidad de disparar este tipo de energía, amenazando al Sistema de defensa norteamericano.

En el año 2001, Rusia presento su primer vehículo el Ránez-E, con capacidad de dirigir ataques de pulso electromagnético contra aeronaves, logrando el apagado total de estas. Ese fue el puntapié inicial a partir del cual fue perfeccionándolo para su empleo militar.

Así como se invierten millones en la producción de armas con estas características, también se destinan inversiones en medidas defensivas. Éstas existen actualmente y sirven para la protección de aquellos medios que pueden ser afectados, el inconveniente que presentan, es que tienen un costo sumamente elevado y su duración es limitada, ya que se van degradando con el tiempo, exigiendo un nuevo tratamiento para alcanzar sus capacidades defensivas óptimas.

Ya en el año 2010 la OTAN, en su Revisión del Concepto Estratégico, estableció en su punto 14 lo que sigue:

Un número de tendencias significativas relacionadas con la tecnología incluyendo el desarrollo de armas láser, guerra electrónica y tecnologías que impiden el acceso al espacio, parecen prontas para causar importantes efectos globales que impactarán en la planificación y operaciones militares de la OTAN. (Grunschlager, 2016).

Esto indica como este tipo de avances, cuyas verdaderas capacidades se desconocen, podrían llegar a afectar en un futuro no muy lejano. Por lo cual la OTAN deberá contar con ésta clase de armamento, dando la pauta de la importancia que le asignan a esta tecnología las principales potencias mundiales.

Conclusiones

Los nuevos desafíos detallados en el presente capítulo no son los únicos que son representativos de éste siglo XXI, se podrían numerar muchos más, a modo de ejemplo, armas laser, robótica, desarrollo de exoesqueletos, armas cuánticas. Se tomó estas debido a lo avanzado que se encuentran en su desarrollo y aplicación como así también en el impacto directo que tienen y tendrán sobre el sistema de comando y control en el nivel operacional.

Estas tecnologías obligaran a dicho sistema a perfeccionarse, y actualizarse permanentemente, para poder continuar siendo eficientes y permitirle al comandante conducir sus medios en el campo de batalla. A su vez, impondrá tanto al Comandante del nivel operacional como a su Estado Mayor la necesidad de capacitarse y adaptarse a estos cambios. Ya que nada sirve tener un sistema de comando y control del siglo XXI, con conductores de del siglo XIX, que no están a la altura de su empleo, desperdiciando las capacidades de éste, ofreciéndole así grandes ventajas al enemigo.

La delantera en lo operacional la tendrá aquel que mejor entienda de estos nuevos desafíos, haga un eficiente empleo de los medios que disponga, afecte todos los dominios de manera transversal, y evolucione en una conjunción hombre – tecnología, sumado a la experiencia y conocimientos.

CAPÍTULO 2. El Sistema de Comando y Control

2.1 El Sistema de comando y control en el Ejército Argentino

El Sistema de comando y control empleado en el Ejército, ha atravesado a lo largo de su historia variadas modificaciones, pasando desde C3I -comando, control, comunicaciones e inteligencia-, C2TI -comando, control, teleinformática e inteligencia-, llegando hasta su denominación actual C3I2- comando, control, comunicaciones, inteligencia e informática. Éste es definido como:

> Un conjunto de medios humanos, equipos y materiales de alta tecnología que, integrados y estructurados en forma automatizada y por medio de procedimientos normalizados, posibilitará al Comandante/Jefe y a su órgano de asesoramiento, ordenar, controlar, comunicarse, conocer la situación de otras fuerzas amigas, las condiciones del terreno, las condiciones meteorológicas y al enemigo y sus acciones, cuasi en tiempo real. (ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, 2016, págs. I-6)

Éste está integrado por una serie de Subsistemas:

a. Subsistema de comando: Compuesto por el personal integrante del Puesto Comando: Comandante/Jefe, su/s Estado Mayor/es y auxiliares, medios y procedimientos.
b. Subsistema de control: Integrado por el personal mencionado en el punto anterior, sumado los conjuntos de sensores, procedimientos y mecanismos de empleo de los mismos.
c. Subsistema de inteligencia: Integrado por el personal y tropa técnica de inteligencia, sus medios, procedimientos y los productos elaborados por éstos.
e. Subsistema de comunicaciones e Informática: Es la columna vertebral del sistema de comando y control, se compone por el personal de comunicaciones y del sistema de cómputo de datos, como así también por los medios y procedimientos de empleo de los mismos. (ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, 2016, págs. I-6)

En lo referente a su funcionamiento contempla no solo su empleo interno para el Ejército, sino que prevé su integración con las otras Fuerzas Nacionales, la Fuerza Aérea y la Armada Argentina, como así también con las de países aliados. Es importante destacar éste aspecto, ya que, en la actualidad los despliegues para afrontar misiones de paz, acciones bélicas, ayudas humanitarias, y demás, se realizan mediante coaliciones entre dos o más países. Esto trae implícito la compatibilidad e interoperabilidad de los sistemas de apoyo a las operaciones. Estas no son las únicas características que contempla el mismo, le asigna otras,

agrupándolas en Generales: Auxiliar, ya que debe aportar la información necesaria al Comandante para la toma de decisiones y a su Estado Mayor para brindar el asesoramiento necesario. Adaptable, debe tener la capacidad de apoyar a todos los niveles de comando.Funcionales/Operativas: Confiable, asegurando la ininterrupción del servicio, con alta capacidad de supervivencia a los ataques de Guerra Electrónica, de superficie, aéreos, y de ciberataques. Amigable al usuario, debe ser intuitivo, permitiendo que cualquier operador del sistema pueda comprenderlo y operarlo de manera sencilla y simple. Seguro, procesando la información, evitando que el enemigo o personal no autorizado tenga acceso a ella. Potente, para procesar la mayor parte del trabajo, facilitando la función del Comandante y su Estado Mayor. Flexible, permitiendo su adaptación a los distintos tipos de situaciones que se presenten, por ejemplo, estar apoyando una operación ofensiva y pasar rápidamente a apoyar una defensiva, sin que los usuarios sufran la interrupción o parcialización del funcionamiento del sistema. Móvil, debe poseer el mismo grado de movilidad que el del elemento al cual brinda apoyo. Estructurales: Expandible, pudiendo ampliar sus capacidades. Integrado, que permita la interrelación entre los distintos subsistemas. Multifunción, que le facilite la asistencia al Comandante en aquellas funciones que éste requiera. Distribuido, éste aspecto apunta a que su ubicación en el terreno mantenga la dispersión necesaria tal que evite su afectación por parte de los medios aéreos y/o de artillería del enemigo, y que dicho posicionamiento contribuya con la operación del sistema. (ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, 2016, págs. I-8)

Esta estructura, con sus respectivas características fue plasmada en la doctrina y puestas en funcionamiento dentro del Ejército en el año 2016. Por ende, los desafíos descriptos en el Capítulo I del presente trabajo no han sido tenidos en cuenta en su totalidad. Si bien éstos existen desde hace ya bastante tiempo, el único que se ha contemplado fue la Ciberdefensa, la cual es referenciada de forma general en varios puntos del reglamento ROD-05-01. Lo más destacable para resaltar es, dentro de sus aspectos a tener en cuenta, la mención de operar en ambientes hostiles de guerra electrónica y de ataques cibernéticos, evaluar los sistemas enemigos que ejercen esas acciones. Como así también de disponer de su propio sistema eficiente de Guerra Electrónica y Ciberdefensa. Más allá de todas estas expresiones, no especifica en ninguna parte de la doctrina, la manera o forma de realizar dichas actividades.

Respecto a la inteligencia artificial, no se contempla en ninguno de sus capítulos. La actualización de la doctrina fue un salto importante para la fuerza, pero aún requiere actualizaciones, forzadas por la evolución permanente del factor tecnológico.

2.2 El Sistema de comando y control en la Fuerza Aérea Argentina

La Fuerza Aérea define al comando y control como: “Son aquellas acciones destinadas a la planificación, dirección, coordinación y supervisión de las operaciones y las fuerzas asignadas, que contribuyen al logro de los objetivos de una Campaña Aérea.”

Comprende procedimientos tales como: Comando y Control en Vuelo, Comando y Control en Tierra. (Fuerza Aére Argentina, 2010, pág. 9)

Básicamente dicho Sistema se apoya sobre un Subsistema de comunicaciones, un Subsistema integrado por los medios aéreos y un Subsistema de sensores.

Define al Subsistema de comunicaciones de la siguiente manera:

Son aquellas acciones destinadas a asegurar el Comando y Control de las Operaciones Aéreas mediante enlaces confiables, rápidos y seguros y apoyar la navegación aérea de los medios aéreos propios. Comprende procedimientos tales como: Comunicaciones Radioeléctricas, Control de Emisiones, Enlace de Datos, Contra Medidas Electrónicas, Contra Contra Medidas Electrónicas, Balizamiento Radioeléctrico. (Fuerza Aére Argentina, 2010, pág. 9)

El Subsistema de sensores puede ser definido como aquel que tiene la capacidad de detectar una aeronave en vuelo a través del aeroespacial, y envía la información capturada a un puesto comando en tiempo real, para que la misma sea procesada, permitiendo la obtención de datos necesarios, que faciliten la toma de decisiones del Comandante/Jefe, o el asesoramiento de su Estado Mayor. Los medios empleados no solo abarcan al material de radares de la Fuerza, sino que se pueden incluir otros tales como aeronaves no tripuladas con capacidad de captar y enviar información en forma instantánea, sensores de patrullas terrestres también con capacidad de transmisión de información y radares de buques. (Cap Miranda, 2013, pág. 11)

Las principales características en la que se debe apoyar éste Sistema son:

Confiabilidad garantizando su funcionamiento operativo, siendo robusto para evitar fallas en el mismo. La seguridad en el manejo de la información restringiendo el acceso a la misma por parte de personal no autorizado. Resistencia a las acciones de Guerra Electrónica del enemigo. Interoperabilidad es decir que pueda integrarse a los sistemas de otras Fuerzas.

Como se puede observar, éstas características son coincidentes con algunas de las ya expresadas en el Sistema de comando y control del Ejército. Donde es de resaltar la

importancia que se le da a la supervivencia del sistema -confiabilidad, resistencia-, al manejo de la información -seguridad-, y a la integración y compatibilidad que debe haber entre los Sistemas de las Fuerzas –interoperabilidad-. Ésta última es la que va a permitir un rápido flujo de la información, dando el dinamismo necesario que impone el manejo de los datos, para su análisis, procesamiento, y finalmente brindarle al Comandante la herramienta necesaria que apoye su decisión. También destaca la Unidad de comando, la planificación centralizada del mismo y su funcionamiento descentralizado, de manera que le dé la flexibilidad requerida al Sistema, para enlazar desde el nivel estratégico hasta el táctico, permitiendo la consecución de los objetivos estipulados por el Comandante.

La fuerza se destaca por darle gran importancia y preponderancia a la vigilancia aeroespacial. Si bien éste trabajo integrador es específico del nivel operacional, se considera que hay que tener en cuenta una de las normativas que rige el funcionamiento de ésta para entender cómo estructura su Sistema de comando y control. Dicho documento es el Decreto 1407/04, el cual determina lo que sigue: como deberá organizarse el sistema de control aeroespacial, tanto en la ubicación de los sensores como en los vínculos de comunicaciones que debe poseer, lo que en grandes rasgos definiría la estructura donde deberá asentarse el sistema de comando y control del país… (Cap Miranda, 2013, pág. 4). Más allá del despliegue de medios que requiera la actividad operacional a desarrollar, lo expresado en el Decreto anterior da la pauta de la distribución de éstos en tiempo de paz, los cuales teniendo en cuenta dicha ubicación, podrán ser empleados en apoyo al nivel operacional, para la obtención de datos adecuados y oportunos, necesarios para apoyar a ese comando.

2.3 El Sistema de comando y control en la Armada Argentina

La Armada Argentina no presenta dentro de su doctrina una definición que tipifique el Sistema de comando y control. Si bien en su Reglamento el PCN – 3 hace mención a cómo debe ser el Subsistema de comunicaciones y su relación de estructura con respecto a éste, para facilitar la función del Comandante, no detalla lineamientos, ni pautas a seguir o respetar para su establecimiento.

Esto se debe a que la Armada presenta tres particularidades que surgen del análisis de su forma de empleo. La primera de ellas es que ésta abarca a más de un dominio tradicional, ya que se prevé su despliegue tanto en el mar, tierra y aire de manera simultánea, o particular a

uno de ellos, y de forma individual o conjunta. La segunda es que su estructura funcional está dividida en cuatro componentes: -de superficie – medios que se desplazan sobre el mar-, submarino -compuesto por éstos medios propiamente dicho y su sistema de mantenimiento-, aeronaval - medios aéreos, aviones, y helicópteros-, y terrestre - integrado por la Infantería de Marina y medios logísticos. Finalmente, la tercera es que, si bien tienen elementos orgánicos, éstos se configuran de acuerdo a una misión específica, es decir no existe un elemento superior que los agrupe, por lo tanto, su conformación, o designación de elementos se realizará a orden para dar cumplimiento a una tarea operacional determinada.

Dadas las características detalladas anteriormente, ésta Fuerza emplea un Sistema de comando y control para cada uno de sus componentes. Dependiendo de la operación que deban cumplir, instalará un Sistema superior que le permita su funcionamiento de manera coordinada e integrada para facilitar el comando por parte del Comandante.

Se infiere que dicho sistema es interoperable, ya que debe permitirle a la Armada integrarse a las otras dos Fuerzas Armadas de la Nación para el desarrollo de operaciones conjuntas tanto en tiempo de paz como de guerra. Claros ejemplos de esto fueron, tanto la operación Rosario –realizada de manera conjunta con el Ejército, donde se desplegaron tres Fuerzas de Tarea, FTN40 -anfibia-, FTN 20 -apoyo-, y la FTAe, las cuales actuaron de manera sincronizadas y coordinadas, lo cual hubiera sido casi imposible de realizar sin un acorde Sistema de comando y control, como las operaciones desarrolladas en el marco del Conflicto Armado del Atlántico Sur, donde por similitud a la anterior, se debió contar con un Sistema que permitiera la conducción de las distintas acciones.

También se puede determinar que es un Sistema confiable y flexible, debido a que debe estar en capacidad de adaptarse a las distintas configuraciones que la Fuerza adopte y a las diversas situaciones y cambios de que éstas presenten, permitiendo su funcionamiento operacional bajo todo tipo de circunstancias.

2.4 El Sistema de comando y control en el Nivel Operacional

Si se quiere definir el Sistema de comando y control del nivel operacional, es preciso establecer primeramente que es el nivel operacional, dicha definición se puede encontrar en el Reglamento del Estado Mayor Conjunto de las Fuerzas Armadas, PC-20-01 Planeamiento para la acción militar conjunta, nivel operacional, el cual establece:

> …es el nivel que enlaza o conecta al Nivel Estratégico con el táctico. Desde la paz y hasta la resolución de un conflicto se concentra en el planeamiento y ejecución de maniobras operacionales y

apoyos logísticos de los recursos militares asignados a un teatro de operaciones, para colocarlos en la mejor situación para contribuir al logro del EFO. Es el nivel en el que se llevan a cabo las campañas. Todas las actividades militares incluidas en un plan de campaña, se traducen en un diseño operacional particular.

Este nivel es en esencia conjunto, puesto que en él participan dos o más Fuerzas Armadas bajo el comando unificado de un Comandante de nivel operacional designado, que asegura la acción militar conjunta y la unidad de esfuerzo en pos del objetivo… (Estado Mayor Conjunto de las Fuerzas Armadas, 2017, pág. 4)

Como se puede apreciar este es el nivel del trabajo conjunto por excelencia, por ende, independientemente del Sistema de comando y control adoptado por cada una de las Fuerza, es aquí donde deberá emplearse un Sistema superior, capaz de integrar a los tres anteriormente mencionados, para brindarle al Comandante Operacional y su Estado Mayor las herramientas necesarias para cumplir con lo expresado en el párrafo reglamentario precedente.

Además de lo establecido en la doctrina ya mencionada, la Directiva de Política de Defensa Nacional (DPDN) del -2018- en su *Capítulo III Prioridades y lineamientos para la reforma del Sistema de Defensa Nacional, en el punto II. Instrucciones para la Reforma del Sistema de Defensa Nacional, 2. Accionar militar conjunto*, le impone al Estado Mayor Conjunto de las Fuerzas Armadas la elevación al Ministerio de Defensa, de los planes que den cumplimiento a diferentes objetivos, entre ellos:

a. Fortalecimiento de la arquitectura del Sistema de comando y control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento (C4ISR) de los niveles Estratégico Militar, **Operacional** y táctico.

d. Fortalecimiento de las capacidades de anticipación, disuasión, vigilancia y control de la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional. (Ministerio de Defensa, 2018, pág. 33)

Se puede apreciar cómo la DPDN ya adopta la sigla C4ISR, lo cual trae implícito las exigencias y características del Sistema de comando y control que desea para sus Fuerzas de defensa, adoptando por similitud la establecida por las Fuerzas Armadas norteamericanas. Si bien es un planteo para el Estado Mayor Conjunto, indefectiblemente influirá no solo en lo operacional sino en los otros dos niveles. También como marca el punto d., la importancia que hace ésta sobre la seguridad cibernética, la cual aparece en varios puntos de la directiva,

como así también la ciberseguridad, dando la pauta del significado que es éste desafío para el Gobierno Nacional, y por consiguiente en el presente nivel. Ejemplo de ello es la transcripción del siguiente párrafo:

…utilización del ciberespacio con fines militares. La consolidación del ciberespacio como un ambiente operacional militar configura una amenaza de interés estratégico para la Defensa Nacional. El desarrollo de las nuevas tecnologías de información y comunicaciones, junto con la extensión global de la conectividad, han convertido al ciberespacio en un ámbito en el que los Estados despliegan operaciones de agresión e influencia sobre las naciones adversarias. La tendencia hacia una mayor competencia estratégica internacional en el ciberespacio ha llevado a numerosos países a desarrollar capacidades cibernéticas de vanguardia, a fin de garantizar la seguridad de sus infraestructuras informáticas críticas o estratégicas.

La REPÚBLICA ARGENTINA debe adecuar sus organizaciones militares al impacto que emerge de estos nuevos riesgos. La política de ciberdefensa debe orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional… (Defensa, 2018, pág. 18)

En Estado Mayor Conjunto de las FFAA ya han tomado nota de éstos lineamientos, plasmándolo en un documento sobre la *Reconversión del Instrumento Militar -2019-*, en el cual se expresa lo siguiente:

El Sistema de Investigación y Desarrollo de la Defensa, integrado al esfuerzo del Sistema de Investigación y Desarrollo Nacional, privilegiará aquellos desarrollos tecnológicos multiplicadores de las aptitudes operacionales del Instrumento Militar, conforme las operaciones previstas, en las áreas de ciberdefensa, alerta estratégica y Sistema de comando y control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento (C4ISR). (FFAA, 2019, pág. 16)

Se observa un direccionamiento del esfuerzo de sectores del potencial nacional, para la producción e implementación de un Sistema de comando y control orientado más a un modelo C4ISR y a un factor muy importante como es la ciberdefensa.

Las exigencias desarrolladas en los párrafos precedentes deben ser tenidas en cuenta para la determinación correcta de un eficiente Sistema de comando y control. El elemento responsable de concretar estas directivas es la Compañía de Comunicaciones Conjunta, la cual guarda relación de dependencia con el Estado Mayor Conjunto de las Fuerzas Armadas. Es la encargada de enlazar a éste último con el nivel operacional del Teatro de Operaciones.

Al día la de hoy, la Compañia todavía no ha adoptado el Sistema C4ISR, ya que dado lo reciente de la orden recibida, necesita el tiempo y los medios para poder dar cumplimiento a lo establecido. Como así también los acuerdos necesarios entre las distintas Fuerzas, para lograr uno de los factores imprescindibles ya mencionados, como es la interoperabilidad. Hasta el momento cuenta con un desarrollado Subsistema de comunicaciones que le permite la realización de transmisiones de manera analógica y digital, con capacidad de integrar voz, datos, video en tiempo real, contando a su vez con tecnología satelital. Aunque los equipos que conforman dicho Subsistema no cuentan con ninguna norma de protección contra Guerra Electrónica, como por ejemplo las *TEMPEST* –concepto desarrollado más adelante-. Sin embargo, tanto esto como la futura implementación de desarrollo de Inteligencia Artificial, son aspectos que están siendo evaluados para su futura implementación, dependiendo siempre de factores económicos. La mutación hacia el Sistema C4ISR está en proceso, pero es un lento camino por el cual están transitando, encontrándose en la etapa de planeamientos y acuerdos, y aún queda mucho camino por recorrer.

2.5 El Sistema C4ISR

Dentro del Departamento de Defensa de Estados Unidos se encuentra el Comando Estratégico de Estados Unidos. Éste es el responsable, entre otras funciones, de suministrar al resto de los Comandos encargados de realizar operaciones militares las capacidades de comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento, comúnmente conocido como C4ISR. (Command, 2009)

Hasta no hace muchos años, las Fuerzas Armadas de Estados Unidos presentaban una debilidad importante en su Sistema de comando el control, el cual dificultaba a sus conductores tomar decisiones acertadas de manera rápida y segura. Dicha situación se daba debido a que seguían manteniendo una gran dependencia de los sistemas manuales, tales como transmisión de ordenes en forma manual o personal, en ocasiones a través de la radio o el teléfono, en soporte papel, y demás. Todo ello ralentizaba el proceso, desde que la información era obtenida, procesada y diseminada a su legítimo usuario, el cual, en la mayoría de las veces, podía encontrarse a miles de kilómetros del lugar donde todo esto se originaba. Ya para cuando la persona contaba con la información en su poder para adoptar una decisión, ella había perdido su valor, o era inoportuna debido al cambio de la situación, por lo cual se debía esperar nuevos datos para decidir.

A esto se le sumó, en estos últimos tiempos una serie de nuevas exigencias, despliegue de pequeños grupos de trabajo, operaciones en ambientes urbanos, dificultad de identificar al enemigo, presencia de civiles y muchas otras más, lo que obligó al comando y control a reconfigurarse para poder afrontar éstos cambios.

Basándose en lo detallado anteriormente se llegó a la conclusión de que debían hacer un aprovechamiento de las tecnologías de la información la cual aumentaría la velocidad en el proceso de obtención, análisis y distribución de la información/inteligencia. Como así en el desarrollo de interfaces que permitieran los enlaces entre los distintos sistemas, ya que esa era una dificultad que restringía las comunicaciones entre los mismos, aún más si tenemos en cuenta que ya no solo había que interconectar los tres dominios conocidos -mar, aire, tierra- sino que ahora también se agregaban el espacio y el ciberespacio. Además, se impuso la exigencia que esa interconexión sea viable en todos los niveles, por ejemplo, que el soldado combatiente tuviera acceso a los sensores que le fueran útiles para el cumplimiento de su misión, o que un Jefe de nivel superior pudiera tener contacto con un soldado de primera línea.

Es así que se decidió trabajar bajo el concepto *Network Enabled Capability -capacidad habilitada por la red-*, conocida por su sigla en inglés NEC. Esto significa el aprovechamiento de los distintos sensores y sistemas de armas, para apoyar la toma de decisiones mediante la consigna de información necesaria y correcta, en el momento y lugar correctos. (SITE, 2001) La ventaja de trabajar bajo el paradigma anteriormente mencionado, es que se adapta a cualquier situación, pudiendo dar soporte desde una misión de paz hasta las últimas operaciones militares llevadas a cabo en Siria. Como se observa la base para que ésta tecnología pueda funcionar es la interoperabilidad, no solo de los Subsistemas internos de cada Fuerza, sino entre ellas y con los Sistemas Federales, dando la pauta incluso de un trabajo interagencial donde confluye todo el potencial nacional.

Otro aspecto muy importante que se tuvo en cuenta al momento de su proceso de formación –del Sistema- fue la seguridad, y hoy más que nunca desde la óptica de la ciberseguridad. Dado que, al ser un Sistema interconectado e interoperable, hay un sin número de ventanas que pueden ser aprovechadas por los *hackers*, para el robo de información, despliegue de malware, etcétera. Ejemplo de ello se vio en el Ministerio de Defensa de España del -2019- el cual funcionó con un virus en sus servidores durante dos meses, sin que sus usuarios se dieran cuenta. Aún están tratando de determinar si hubo robo de información y que otros subsistemas fueron afectados. Como se aprecia, la afectación de un nodo puede llevar a la infección del resto nodos y de sus respectivos usuarios.

El C4ISR no es cerrado, permite la incorporación de software y actualizaciones para la mejora de su funcionamiento. A modo ejemplificador podría verse la integración del Sistema *MAJIIC* -para vigilancia y reconocimiento-, el *TALOS -para apoyo de fuego de artillería, morteros y naval-, DSC2S –para las tropas a pie-* y otros más. (Edefa.SA, 2019)

Las Fuerzas Armadas norteamericanas se encuentran enmarcadas en la guerra contra el terrorismo -*GWOT*- y para lograr una mayor eficiencia en la misma, tiene planificadas mejoras en su C4ISR. Entre ellas se puede mencionar la incorporación de satélites Gapfiller de banda ancha, lo que le brindara un salto cuántico en lo que respecta a las comunicaciones, uso de comunicación laser, troncales satelitales –para bajar los tiempos de transmisión de la información- incorporación de la mejora en la inteligencia de imágenes que aumente la capacidad de recolección de éstas, aumento del sistema de radarización, incremento de los *UAV -unmanned aerial vehicle-* tanto aéreos como submarinos, y actualizaciones de los sistemas existentes. Finalmente, se prevé el establecimiento del Global Information Grid –este Sistema permitirá la máxima explotación de las comunicaciones, independientemente del lugar del planeta donde se encuentre, obteniendo, analizando, y diseminando información a requerimiento de los usuarios- (Pacus, 2006) (Magazine, 2017).

Se puede observar que el C4ISR es un Sistema probado en combate, el cual ha ofrecido y ofrece una gran variedad de capacidades para todos sus integrantes, permitiendo la máxima explotación de la información y las comunicaciones, acelerando el proceso de asesoramiento, asistencia y toma de decisiones. No es un sistema cerrado ni ha finalizado su etapa de mejoras. Por el contrario, está abierto a la integración hacia todos los niveles, y hacia la incorporación de nuevos softwares y hardware que mejoren su rendimiento. Se encuentra en un continuo proceso evolutivo conforme se van presentando los desafíos. Todo ello agrupado bajo el paraguas de seguridad e interoperabilidad, base primordial del éxito del correcto funcionamiento del Sistema.

2.6 Lineamientos básicos del Sistema de comando y control

En base a los desafíos analizados en el Cap 1, y los temas desarrollados en el Cap 2, y teniendo en cuenta principalmente la exigencia que determina la DPDN, la cual impone la adopción de un Sistema C4ISR, se pudo arribar a una serie de aspectos a ser considerados para la determinación de los lineamientos básicos para el desarrollo de un Sistema de comando y control para el nivel operacional:

Debe contener un Subsistema comando, el cual será integrado por el Comandante, su Estado Mayor/Plana Mayor, Estado Mayor Especial y eventualmente su Estado Mayor Personal, los auxiliares de las áreas y el personal necesario para la operación y funcionamiento del mismo.
Subsistema control integrado por similitud al Subsistema comando, sumado a los sistemas de sensores y procedimientos de empleo que faciliten el funcionamiento del mismo. Subsistema Comunicaciones integrado por el personal del Arma de Comunicaciones, sus medios/equipos y procedimientos, que conformarán la columna vertebral del Sistema de comando y control del nivel operacional, permitiendo los enlaces necesarios entre los distintos niveles de manera integral. Subsistema computación integrado por el personal del servicio del Sistema de Computación de Datos, informática y comunicaciones designados a tal fin, sumado a los medios/equipos y procedimientos necesarios para su funcionamiento. Subsistema inteligencia integrado por el personal de la especialidad de inteligencia y los medios/equipos y procedimientos destinados a tal fin. Subsistema vigilancia compuesto por el personal, medios/equipos y procedimientos, requeridos para realizar las acciones que permitan determinar la presencia de vehículos aeroespaciales, su condición sobre un área, para el control aéreo y necesidad del empleo de los propios medios. Subsistema reconocimiento compuesto por el personal, medios/equipos y procedimientos necesarios para la obtención de información en los distintos dominios.
Estos Subsistema a su vez deben ser integrados, debiendo haber una interrelación entre ellos.
El Sistema de comando y control del nivel operacional, como ya se ha mencionado, se caracteriza por abarcar a las tres Fuerzas Armadas, por lo cual debe tener la capacidad de soportar las particularidades y exigencias de cada una de ellas de manera individual y conjunta. Es así que deberá ser flexible, lo que le permitirá adaptarse a las estructuras propias de las Fuerzas, como así también a los distintos cambios de situación, que será lo normal en los escenarios actuales. Eso se facilitará a través de una estructura modular con circuitos redundantes.
Asimismo, deberá ser móvil, permitiendo al Comandante y a su Estado Mayor los desplazamientos dentro del Teatro de Operaciones, otorgándoles las mismas facilidades como si estuvieran en el Puesto Comando.
La resiliencia del Sistema será esencial ya que le permitirá su supervivencia ante las acciones de Guerra Electrónica del enemigo, los ataques desde los distintos dominios, y evitar su localización. El factor fundamental para que pueda darse será la redundancia de medios y el empleo de equipos con normas adecuadas para la protección electrónicas, como por ejemplo equipos con normas *TEMPEST – Telecomunications Electronics Material Protected From*

Emanating Spurius Transissions, estas normas están destinadas a evitar o disminuir las emisiones que realizan los distintos circuitos, computadoras, chips, cables, y demás. Estas, al operar de manera aisladas, no representan un gran riesgo, pero al estar agrupados en centros de comunicaciones, o lugares físicos para conformar los distintos Subsistemas, irradian energía, de tal manera que generan un campo electromagnético, susceptible de ser detectado por el enemigo, lo que le permitiría a éste, la reconstrucción y análisis de la señal detectada. La incorporación de medios que contengan este tipo de normas eleva considerablemente su costo, pero es una de las medidas necesarias para alcanzar la resiliencia buscada. Otro aspecto a tener en cuenta, es el desarrollado precedentemente sobre las armas de pulso electromagnético. Existen, hoy en día, equipos que están preparados para soportar dichos ataques, pero su valor en el mercado es también elevado. Si se tiene en cuenta las limitaciones económicas de nuestro país, la adquisición de dicho material es un tanto incierta. Por lo cual, para contribuir con la resiliencia, se debe mantener de forma paralela el sistema manual, tal que permita el almacenamiento de datos en formato papel, como así también el mantenimiento de personal destinados a la transmisión de información de manera personal.

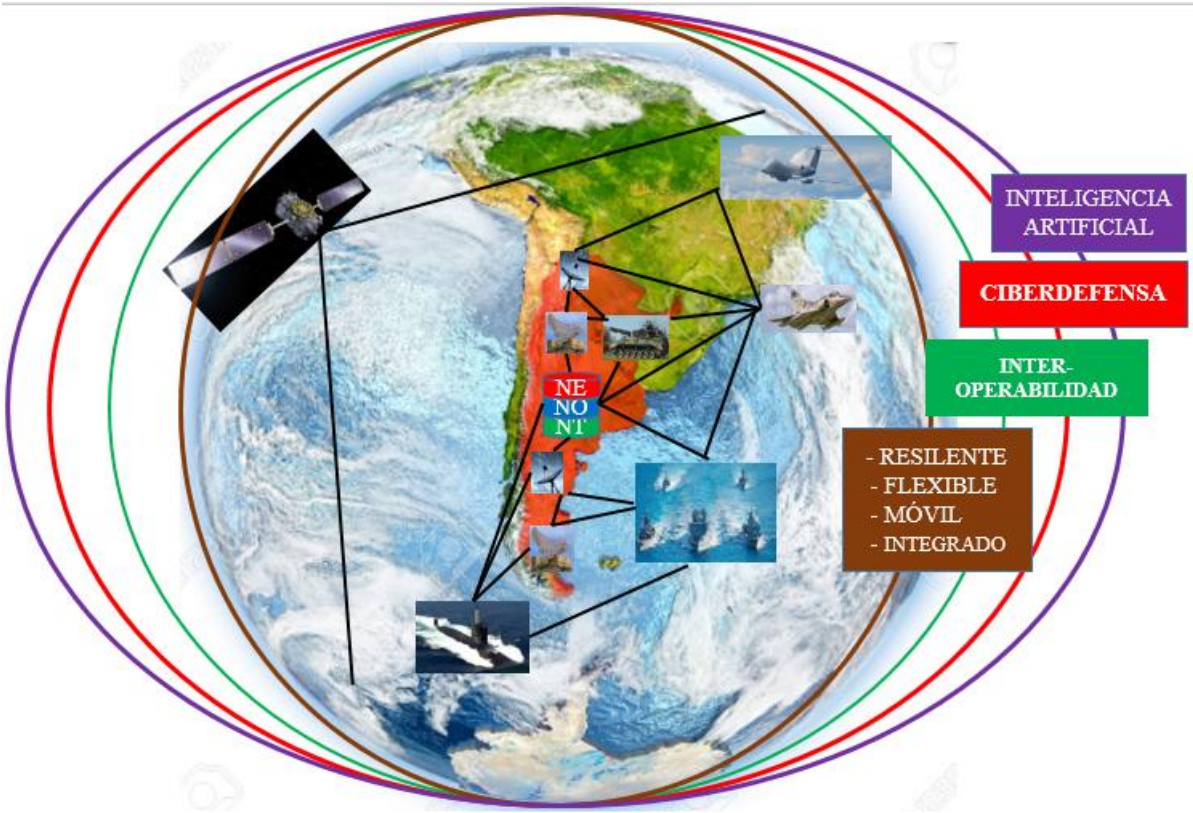
La interoperabilidad será fundamental en éste nivel de trabajo, no solo entre las tres Fuerzas, sino entre los distintos niveles con los que debe interactuar –nivel estratégico y nivel táctico- y con las distintas agencias con las que normalmente deberá relacionarse. Por ejemplo, con el Comando Conjunto de Ciberdefensa, con la Agencia Federal de Inteligencia, y otros. Dicha interoperabilidad se podrá alcanzar empleando *software y hardware* compatibles con implementación de una estructura abierta que permita la integración de otros Subsistemas, incluyendo la de Fuerzas de países amigos. Esto amplía las facilidades del Sistema, evitando las limitaciones por incompatibilidad que ralentizan y dificultan su funcionamiento y eficiencia.

Como se expuso en el capítulo 1, la ciberdefensa es un factor fundamental en el desarrollo del Sistema de comando y control, por ende, el nivel operacional debe tener un Subsistema destinado a este tipo de actividad o el Subsistema computación debe asumir dicha responsabilidad. Esta determinación dependerá de la cantidad de presupuesto, personal, medios disponibles y una decisión organizacional. Independientemente de cómo se organice, deberá estar integrado de manera directa con el Comando Conjunto de Ciberdefensa, el cual deberá bajarle los lineamientos pertinentes, habiendo un flujo continuo de información que permitan la protección del propio Sistema y dé respuesta sus necesidades. También deberá estar conectado con el nivel inferior para canalizar las medidas determinadas a su función.

La Inteligencia Artificial es otro punto a considerar, ya que como se ha descripto, es una herramienta que de manera individual o en conjunto con el *Big data*, el Aprendizaje Autónomo, o las futuras computadoras cuánticas, explotará al máximo el mundo de la información, su almacenamiento, análisis, flujo y por ende la toma de decisiones. Es fundamental trabajar en conjunto con los centros de investigación y desarrollo del potencial nacional, para la producción de ésta tecnología y su implementación en los Sistemas de comando y control, no solo del nivel operacional, sino también en el estratégico y el táctico. Siempre teniendo en cuenta la premisa de que su empleo será para facilitar a los Comandantes/Jefes la adopción de resoluciones, y no que éstos se conviertan en meros transmisores de información y las maquinas sean las que adopten las decisiones. En el mundo ya se trabaja para implementar cada vez más la inteligencia artificial, desde celulares, autos con conducción autónoma, pasando a drones, UAV, tanques no tripulados, y otros. Negarse a su implementación sería igual a rechazar o no querer mirar hacia adelante. Por ello, si bien ahora no se dispone en forma efectiva de ésta herramienta, debe contemplarse su futura aplicación. Para lo cual, el desarrollo de los distintos Subsistemas debe estar preparados para soportar su implementación, y capacitación por parte del personal operador y auxiliar.

En resumen, de lo anteriormente descripto, los lineamientos básicos que debe tener un Sistema de comando y control en éste nivel, serán los siguientes: Subsistemas Comando, control, comunicaciones, computación, vigilancia y reconocimiento, podría agregarse ciberdefensa o estar inmerso dentro del Subsistema computación. Con las siguientes características: Integrado, flexible, móvil, resiliente, interoperable y con capacidad de soportar la tecnología de inteligencia artificial.

Sistema C4ISR del Nivel Operacional



Fuente: Elaboración propia

Se pudo observar en este capítulo, cómo cada una de las Fuerzas Armadas que componen el Sistema de Defensa de la República Argentina, tiene sus propias características en lo referente a su Sistema de comando y control, poniendo el foco en aspectos bien diferenciados una de otras. Así se plasmó como la Fuerza Aérea prepondera la vigilancia y el reconocimiento, mientras que la Armada conforma su Sistema prácticamente *ad hoc*, y que el Ejército se apoya con más preponderancia en su Subsistema de comunicaciones. Esto no quiere decir que se desentiendan del resto de los Subsistemas, sino que simplemente adaptan el Sistema a sus propias exigencias.

El nivel estratégico ha tomado una decisión respecto del tipo de Sistema de Comando y Control a adoptar para sus niveles dependientes, bajando los lineamientos pertinentes a través de la DPDN. El Estado Mayor Conjunto de las Fuerzas Armadas tradujo estas órdenes mediante un documento: *Reconversión del Instrumento Militar* -2019, en el cual adopta el Sistema C4ISR. Si bien la orden es muy reciente, y aún no se ha implementado, se están dirigiendo los esfuerzos en esa dirección para poder cumplir con lo delimitado.

Los lineamientos determinados son los básicos que debería comprender un Sistema de comando y control que pretenda estar a la altura de las exigencias en un Teatro de Operaciones de este siglo. No son los únicos puntos a tener en cuenta los determinados en éste capítulo, habría muchos más para agregar, conforme avanza la tecnología, los dominios, la manera de hacer la guerra y los distintos aspectos del ambiente operacional. Los establecidos permiten la ampliación, integración, e interoperabilidad del sistema, dándole la resiliencia necesaria para sobrevivir y poder ser la herramienta útil en la toma de decisiones de un Comandante y como instrumento para el asesoramiento y asistencia por parte de un Estado Mayor.

CONCLUSIONES

Esta investigación trata sobre el Sistema de comando y control del nivel operacional, así el objetivo que se plantea es determinar los factores que se deben tener en cuenta en la composición de la estructura de un Sistema de Comando y Control tipo, que permita afrontar los desafíos del siglo XXI en un Teatro de Operaciones. De éste se desprenden dos objetivos específicos, el primero describir la estructura del Sistema de Comando y Control de cada una de las Fuerzas Armadas de Argentina, y la del empleado por Estados Unidos. El segundo describir las características funcionales, operativas y subsistemas de un Sistema de Comando y Control, que le permitan ser resiliente a los nuevos desafíos.

Relacionado con el primer objetivo específico, se pudo comprobar como dicho Sistema ha evolucionado a lo largo del tiempo, y como continua en un cambio constante, influenciado por factores tecnológicos, modos de hacer la guerra, el ambiente operacional, y otros. Ha pasado por numerosas modificaciones estructurales, como por ejemplo de C2, C3I, C3I2, C2TI, hasta llegar a lo establecido en la DPDN 2018 y plasmado en documento de *Reconversión del Instrumento Militar* 2019 –Estado Mayor Conjunto-, que es la orden de adopción del Sistema C4ISR, similar estructura base al empleado por Estados Unidos. Esto conlleva un gran desafío, dado que, al ser establecido en el nivel operacional, implicará un cambio en los otros dos niveles también. Como así, una revisión de los Sistemas de comando y control propios de cada Fuerza, los cuales, sin descuidar y preponderar sus exigencias particulares, deberán hacer los esfuerzos necesarios para lograr la integración con el Sistema superior, con sus elementos paralelos y dependientes.

La adopción del Sistema C4ISR, trae aparejado implícitamente la ampliación, o como mínimo, cambios estructurales dentro de cada una de las Fuerzas. Poder estar en capacidad de lograr estas modificaciones demandará tiempo, costos económicos, reestructuración de personal y medios, cambios de doctrina, acuerdos y coordinaciones entre las Fuerzas y los distintos niveles de la conducción, entre otros. Es por ello que el proceso no será en el corto plazo, conllevará pruebas y errores hasta lograr su implementación y correcto funcionamiento.

Con respecto al segundo objetivo específico, luego del desarrollo del presente trabajo se pudo extraer lo siguiente: Lo ordenado por la DPDN establece la adopción de los siguientes subsistemas: Comando, control comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento. Se determinaron las consecuentes características estructurales: Integrado y expandible. Las funcionales: Resiliente, Flexible, Móvil, Interoperable y Confiable. Estos son los requisitos mínimos, como ya fue mencionado, que permiten que el Sistema pueda operar frente a los nuevos desafíos. Esto no quiere decir que a futuro no deban ser reevaluados o modificados, ya que, como se ha explicado a lo largo del trabajo, con el tiempo van surgiendo nuevos elementos que exigen la adaptación de lo ya establecido para poder seguir superviviendo y cumpliendo las misiones del nivel.

Los tres desafíos seleccionados – Inteligencia Artificial, Ciberdefensa y Armas de Pulso Electromagnético – permitieron vislumbrar y cimentar los lineamientos necesarios para el Sistema de comando y control y poder dar respuesta al objetivo general. La llegada e implementación de la inteligencia artificial de manera particular o en conjunción con otras herramientas –*Big Data*, Aprendizaje Autónomo, etcétera – será sin duda un salto cualitativo tanto en el proceso de toma de decisiones, como para arribar al asesoramiento y asistencia por parte de los distintos Estado Mayores. Proveerá gran caudal de información en tiempo cuasi real, y prácticamente procesada, pero hay que tener presente que no deja de ser una –herramienta–, y nunca debe reemplazar a la decisión final, la cual debe ser adoptada por el Comandante.

La aparición del ciberespacio ha modificado las reglas de juegos en todos los niveles y escenarios conocidos. Hoy se puede recibir un ataque, robo u manipulación de información, sin darse cuenta, e incluso sin poder determinar quién fue el responsable. Se rompió la

barrera física y temporal, la agresión puede ser ejecutada desde miles de kilómetros de distancia, he incluso pudo haber sido lanzado horas, días o meses antes de que se produzca. Por lo detallado anteriormente sería inconcebible el desarrollo de un Sistema de comando y control sin tener en cuenta la Ciberdefensa. Por ello, se aprecia la necesidad de agregar ésta responsabilidad al Subsistema computación, para hacer frente a ésta nueva exigencia, de manera tal que éste en capacidad de proteger al Sistema, como así también adoptar medidas en caso de que se le sea requerido. En su defecto la incorporación de un nuevo Subsistema llamado de Ciberdefensa, ya que la peligrosidad que representa ésta amenaza amerita la adopción de medidas reales y concretas, en un trabajo coordinado con el Comando Conjunto de Ciberdefensa e interagencial con otras entidades Nacionales.

Son de destacar dos factores muy importantes para que el Sistema funcione, la interoperabilidad, ya mencionada anteriormente, y la resiliencia. La primera permitirá expandir las fronteras y capacidades, haciendo que el Sistema funcione de manera armónica facilitando las coordinaciones, sincronizaciones y el tráfico de datos, y contribuirá con la segunda. La resiliencia permitirá su supervivencia, necesaria para la conducción dentro del Teatro de Operaciones.

Todo lo descripto y establecido en el presente documento sobre los lineamientos básicos que debe tener el Sistema de comando y control deberá ser acompañado de la capacitación del personal en su totalidad, ya que la adopción del Sistema C4ISR requerirá reestructuraciones, y la implementación de futuras nuevas tecnologías. Por ende, exigirá al personal la preparación necesaria para poder llevar adelante los procedimientos y operación de los distintos Subsistemas. De nada servirá tener el mejor Sistema con equipos modernos si su personal no puede explotar al máximo sus facilidades. Independientemente del tiempo que conlleve el desarrollo y establecimiento final del Sistema, el factor humano debe continuar con su preparación para que, llegado el momento, se pueda producir el armonioso funcionamiento de todo el conjunto.

Bibliografía

Cap Miranda, S. (2013). *Comando y control, necesidades para la vigilancia y control aeroespacial del territorio nacional.* CABA.

Cespedes D, Hernandez w. (2017). *Inteligencia Artificial.* Obtenido de https://es.calameo.com/read/0051074327b779c4a67ad

Cubeiro Cabello, E. (2001). *Dialnet.* Obtenido de file:///C:/Users/baigo/Downloads/Dialnet-LosSistemasDeMandoYControl-4602258%20(3).pdf

Defensa, M. d. (30 de Julio de 2018). *Directiva Particular de Defensa Nacional.* CABA: Ministerio de Defensa.

Edefa.SA. (11 de Octubre de 2019). *Defensa.com.* Obtenido de https://www.defensa.com/reportajes/innovacion-clave-sistemas-mando-control-defensa

Ejército Argentino. (2015). *ROB-00-01 Conducción para las Fuerzas Terrestres-II.* Buenos Aires: Ejército Argentino.

Escuela de Altos Estudios de la Defensa. (2014). *Documento de Seguridad y Defensa. Estrategia de la Información y Ciberdefensa.* Ministerio de Defensa del Reino de España.

Estado Mayor Conjunto de las Fuerzas Armadas. (2012). *PC 00-01 Doctrina Básica para la Acción Militar Conjunta.* Buenos Aires: EMCFFAA.

Estado Mayor Conjunto de las Fuerzas Armadas. (2017). *PC 20-01 Planeamiento para la Acción Militar Conjunta - Nivel Operacional - Proyecto.* Buenos Aires: EMCFFAA.

Estado Mayor Conjunto de las Fuerzas Armadas. (2018). *PC 00-02 Glosario de Términos para la Acción Militar Conjunta - Proyecto.* Buenos Aires: EMCFFAA.

Estado Mayor General del Ejército. (2015). *ROB 00-01 Conducción de las Fuerzas Terrestres.* Buenos Aires: Instituto Geográfico Nacional.

FFAA, E. M. (2019). *http://www.fuerzas-armadas.mil.ar.* Obtenido de http://www.fuerzas-armadas.mil.ar/Noticias/Noticia-2019-07-26-jemco-reconversion-instrumento-militar/Publicacion-JEMCO-RECONVERSION.pdf

Fuerza Aére Argentina. (2010). *RAC-3 Reglamento de Conducción Operacional.* Fuerza Aerea Argentina.

Galdorisi, G. (2019). La Marina necesita IA, simplemente no esta segura por qué. *El Observtorio*.

Garcia Serrano, A. (2012). *Inteligencia Artificial. Fundamentos, práctica y aplicaciones.* Madrid: RC Libros.

Grunschlager, G. (diciembre de 2016). Armas de Energía. El futuro a la vuelta de la esquina. *Revista de la Escuela de Guerra Naval*, 177-190. Obtenido de http://190.12.101.91/bitstream/123456789/758/1/RESGN-62_Armas_de_energia.pdf

Hintze, A. (13 de noviembre de 2016). *http://theconversation.com.* Obtenido de http://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

Hispantv. (27 de marzo de 2019). *Hispantv.* Obtenido de https://www.hispantv.com/noticias/ee-uu-/424544/ataque-electromagnetico-trump-sistemas-defensivos

IBM. (18 de Junio de 2012). *IBM.com.* Obtenido de https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

Infobae. (11 de Septiembre de 2019). *Infobae*. Obtenido de https://www.infobae.com/america/tecno/2019/09/11/el-arma-perfecta-que-vladimir-putin-ya-uso-contra-ucrania-y-amenaza-con-expandir-a-otros-paises/

Knight, W. (29 de Diciembre de 2017). *MIT Technology Review*. Obtenido de https://www.technologyreview.es/s/9871/el-nuevo-romance-de-la-computacion-cuantica-y-la-inteligencia-artificial

Llongueras Vicente, A. (2011). *Academia.* Obtenido de https://www.academia.edu/6182513/La_Ciberguerra_la_guerra_inexistente

López de Mántaras, R. (1 de Agosto de 2017). *Investigación y ciencia*. Obtenido de https://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/el-multiverso-cuntico-711/tica-en-la-inteligencia-artificial-15492

Magazine, G. M. (Enero de 2017). *satelliteevolutiongroup.com.* Obtenido de http://www.satelliteevolutiongroup.com/articles/C4ISR.pdf

Ministerio de Defensa. (31 de Julio de 2018). Directiva Política de Defensa Nacional. *Decreto 703/2018*. Buenos Aires, Ciudad Autónoma de Buenos Aires, Argentina: Boletín Oficial.

Movetia. (2 de Febrero de 2018). *A Medium Corporation (US).* Obtenido de https://medium.com/@Movetia/inteligencia-artificial-aprendizaje-autom%C3%A1tico-y-aprendizaje-profundo-4f09802353bd

Pacus, A. (2006). *Impacto del C4ISR/Digitalización y fuerza conjunta, capacidad de conducir la guerra global contra el terror.* Kansas: Comando del Ejército de los Estados Unidos.

Real Academia Española. (2019). *Diccionario de la lengua española.* Madrid: Real Academia.

ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, I. y. (2016).

Valencia Rojas, S. (2014). *repository.unimilitar.edu.co.* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/12937/CIBERDEFENSA%20Y%20CIBERSGURIDAD.pdf?sequence=1&isAllowed=y

van Creveld, M. (2007). *La transformación de la guerra.* Buenos Aires: José Luis Uceda Editor.