VISIÓN CONJUNTA

ESCUELA SUPERIOR DE GUERRA CONJUNTA DE LAS FUERZAS ARMADAS DE LA REPÚBLICA ARGENTINA

Año 12 . Nº 22
Junio 2020

ISSN: 1852-8619

HISTORIA

BELGRANO Y LAS VIRTUDES MILITARES

Por CY **Gabriel Anibal Camilli**

CIBERESPACIO

El Conflicto Futuro
Por BM Alejandro Aníbal Moresi

CIBERESPACIO

El comando de ciberdefensa alemán un claro ejemplo de integración
Por MY Pablo Alejandro Cañete

DEFENSA Y SEGURIDAD

El factor militar como medio de prevención pacífica de conflictos
Por CR (R) Eduardo Cundins

UNDEF
Universidad de la Defensa Nacional

STAFF

EDITOR Y PROPIETARIO
Escuela Superior de Guerra Conjunta
de las Fuerzas Armadas

Registro DNDA: 16005854 / ISSN: 1852-8619

www.facebook.com/esgcpaginaoficial
vision-conjunta@fuerzas-armadas.mil.ar

NUESTRO ÍCONO

Es el conocido Cubo de Rubik, ornamentado con los colores de la bandera argentina y con el escudo que identifica al Estado Mayor Conjunto de las Fuerzas Armadas Argentinas. La elección de este ingenioso mecanismo para nuestra revista se debe a que éste es la representación visual de la complejidad del accionar conjunto.

La imagen simboliza el desafío de combinar armónicamente los elementos constitutivos de las Fuerzas Armadas para lograr el eficiente empleo del instrumento militar.

La adecuada utilización de las fuerzas permite configurar, en un mismo plano, el escudo del Estado Mayor Conjunto, que presupone un proceso mental para combinar variables en un escenario sumamente complejo.

Para obtener el éxito en la resolución de la situación planteada se necesita un esquema mental de gran amplitud que permita tener la percepción general del objetivo a lograr; esto define la “visión conjunta”.

CONTENIDOS

EDITORIAL

CY **GABRIEL ANIBAL CAMILLI**

La presentación del Nº 22 de nuestra revista Visión Conjunta se produce en circunstancias excepcionales, en el marco de una pandemia de alcance global, que no registra antecedentes en la última centuria, si consideramos como referencia la "gripe española" de 1918.

Esta situación crítica, devuelve al primer plano la vigencia de la Incertidumbre como un rasgo distintivo de la estrategia. En tal sentido, la Escuela Superior de Guerra Conjunta de las FFAA estimula y sostiene el pensamiento estratégico, con lo cual este escenario sirve de base para una reflexión serena, ante el problema que nos interpela como sociedad, sobre nuestro papel como casa de altos estudios.

En consonancia con lo anterior, dicha Incertidumbre nos conduce a la Seguridad como condición imprescindible para preservar los intereses vitales de la República, expresados en nuestra Constitución. La protección y el bienestar de los habitantes de nuestro suelo, adquiere características dramáticas por la situación creada por la pandemia, y demanda el esfuerzo integrado y sin fisuras de la sociedad.

Es por ello que la cabal comprensión del escenario, la identificación de los objetivos estratégicos y la correcta determinación de las prioridades -en cuanto a las acciones a ejecutar-, constituyen los pasos fundamentales para mitigar los daños provocados por la crisis en lo inmediato, y de esa forma revertir sus consecuencias en el futuro. No es momento para falsas dicotomías, tales como salud o economía, ni para especulaciones de cualquier naturaleza.

En el contexto de emergencia, cabe para la comunidad educativa de la Escuela Superior de Guerra Conjunta una consideración especial referida a los pilares de su proyecto pedagógico, que promueve el enfoque estratégico, la innovación, la creatividad, y el desarrollo de las competencias necesarias para analizar contextos desafiantes como el actual y elaborar respuestas aptas para enfrentar la crisis. Los momentos que vivimos, indican la pertinencia de la herramientas que brindamos a quienes transitan por nuestras aulas.

Como director, pero fundamentalmente con la experiencia de los años en el ejercicio de la profesión, invito a los alumnos a reflexionar sobre el *ethos* que define nuestra formación; las situaciones tensas y angustiosas que se viven, que guardan una lejana semejanza con las imperantes en cualquier contienda armada, invocan los fundamentos espirituales, éticos y morales que dan solidez a quien eligió la carrera de las armas. Las Fuerzas Armadas argentinas efectúan un despliegue inédito desde la Guerra de Malvinas en 1982, en apoyo de la comunidad a la que pertenecen y a la que juraron defender.

En este año 2020, tan especial en la memoria colectiva nacional y global, nos conmueven los 250 años del nacimiento del general Manuel Belgrano y el bicentenario de su paso a la inmortalidad; en consecuencia, se impone el deber cívico de honrar y recordar a este prócer nacional. Su aporte en las etapas fundacionales de nuestra Nación, se agiganta a medida que contemplamos, con la amplitud que permiten las dos centurias transcurridas, la dimensión de lo realizado por este insigne argentino. Sirva la memoria y el empeño del General Don Manuel José Joaquín del Corazón de Jesús Belgrano, arquetipo de la Patria, como sostén de todos los argentinos en estas horas inciertas.

Finalmente, convoco a todas las personas a cuyas manos llegue esta publicación académica a mirar con esperanza y optimismo el futuro, estrechando lazos como seres humanos, con la íntima convicción de que sabremos superar las dificultades del presente, y que un mejor porvenir nos espera. Se lo debemos a quienes nos precedieron, pero fundamentalmente a las generaciones que vendrán.

BELGRANO Y LAS VIRTUDES MILITARES

Por CY **GABRIEL ANIBAL CAMILLI**

Palabras Clave:
> Virtudes militares
> Vida del General Belgrano
> Arquetipo de la Patria

Ni la virtud ni los talentos tienen precio, ni pueden compensarse con dinero sin degradarlos.

General Manuel Belgrano

Fue Pedro Calderón de la Barca quien glosó aquello de que "fama, honor y vida son caudal de pobres soldados; que en buena o mala fortuna, la milicia no es más que una religión de hombres honrados".

Sin duda el General Manuel Belgrano en su paso por la Universidad de Salamanca, 170 años después que Calderón de la Barca, habría conocido los versos de uno de los últimos grandes poetas del siglo de Oro español, que de este modo definen claramente al Ejército.

Una religión de hombres honrados que se hermanan para defender a nuestro pueblo, así lo entendía el prócer, con la única recompensa de la satisfacción del deber cumplido.

Un militar, al servicio de la patria

Nuestros militares son hijos de nuestra Patria y son hijos de nuestro pueblo.

Los militares cultivan las virtudes cardinales, valores altos y nobles: lealtad, sacrificio, humildad, generosidad, alegría, liderazgo, compañerismo, obediencia, cuidado de las tradiciones y el recuerdo a los caídos en acto de servicio, que descansan en el seno de Dios.

Valores castrenses que se perfeccionan en nuestras academias y escuelas: quienes entran en ellas como jóvenes del mundo, salen como soldados defensores de la Patria.

En 2020, año del Bicentenario del paso a la inmortalidad del General Manuel Belgrano, creemos conveniente destacarlo como arquetipo y como modelo por sus virtudes militares. Lo haremos con claros e inobjetables momentos de su vida militar como fiel reflejo de esas virtudes.

Es interesante destacar las palabras de Guillermo Furlong: "Belgrano fue extraordinario en las virtudes ordinarias y fue ordinario en las virtudes extraordinarias"[1].

Creemos que hay dos virtudes militares esenciales que constituían el eje coordinador del espíritu militar de Manuel Belgrano: el patriotismo y la valentía, la primera sería la virtud motora y la segunda, la virtud instrumental.

Los conceptos de soberanía nacional y de integridad territorial constituyen para Belgrano dos factores indisolubles que hacen a la grandeza nacional. Sin dudas, Belgrano fue mucho más que el creador de la bandera, aunque ese hecho es el que lo sintetiza. La bandera es tan importante si la entendemos como soberanía, como Nación y como la unión de todos los argentinos; es la síntesis de lo que fue Belgrano. De las ideas de libertad e independencia que él pregonaba y por las que tanto luchó.

El 25 de mayo de 1812, estando en Jujuy y al cumplirse el segundo aniversario de la Revolución de Mayo, Belgrano hizo bendecir y jurar a la bandera. En su arenga, sostiene que tenían el honor de "estar viendo la bandera nacional y que la distinguiría de los otros países del globo".

Cuando Belgrano acepta la profesión militar entiende que es algo mucho más allá que un instrumento de poder; Ortega y Gasset decía al respecto: *"Medítese un poco sobre la cantidad de fervores, de altísimas virtudes, de genialidad, de vital energía que es preciso aumentar para poner en pie un ejército [...]. La fuerza de las armas, ciertamente, no es fuerza de la razón, pero la razón no circunscribe la espiritualidad. Más profundas que ésta fluyen en el espíritu otras potencias y entre ellas las que actúan en la bélica operación. Así el influjo de las armas, bien analizado, manifiesta, como todo lo espiritual su carácter predominante persuasivo"* [2]. Así nuestro prócer va a hacer gala de estas altísimas virtudes al armar ejércitos de la nada para marchar al Paraguay o al Alto Perú, para mostrar su gran sentido de la persuasión y el ejemplo personal ante sus oficiales y tropa, con sus paisanos y aun hasta con sus enemigos u oponentes.

El General Manuel Belgrano poseía una serie de competencias de liderazgo que ayudan a los demás a adaptarse o recuperarse de la adversidad. Fue, sin duda, el catalizador que inspiró a su tropa para alcanzar metas que no podrían haber logrado por sí solos.

Virtudes del general

Nuestro líder muestra grandeza frente a la mezquindad. Es capaz de darse y dar sin pedir nada a cambio: es así que ya el gobierno a través de instrucciones reservadas, le sugería una retirada en el Norte con el fin de evitar el enfrentamiento contra un adversario varias veces superior. Es entonces cuando Belgrano decide ponerse al frente de una de las hazañas más asombrosas de la historia patria: el éxodo jujeño. Hemos de señalar que su decisión no fue mirada con buenos ojos por gran parte de la población que habitaba las provincias del Norte, pues a través del bando expedido el 19 de julio de 1812, las órdenes que emanaban de dicho documento eran estrictas y debían ser cumplidas en forma inmediata. Esas órdenes consistían en el abandono de las viviendas, de los animales, en la quema de los campos y productos pertenecientes a los labradores, a los hacendados y a los comerciantes, y de todo aquello que pudiera ser de utilidad para el ejército realista, que se hallaba cada vez más cerca de su objetivo. Es cierto que el polémico bando dirigido a los pueblos de Salta y de Jujuy –pues hay que remarcar que formaban una sola– era de un rigor tal que despertó entre sus habitantes un indisimulable terror, pues el castigo que se iba a aplicar en caso de desobediencia era la pena de muerte. Así, sin más, no había posibilidad de apelación ni de clemencia alguna. La orden, además, debía ser cumplida en el acto. Bernardo Frías, un duro crítico del bando expedido por el jefe del ejército, sostenía que las disposiciones que de allí emanaban eran inhumanas pues iban en contra de los intereses de los norteños, ya que los hería en su fuero interno. A nadie favorecía, más bien aumentaba el odio, pues nadie ama a quien lo hiere y le hace daño. Expresa el investigador salteño que tanto el Cabildo de Salta como el de Jujuy elevaron su súplica en nombre de los vecinos, ya que al tomar el pueblo conocimiento del bando, solo se oían penas y lamentos por todas partes; y con el fin de evitar medidas tan rigurosas y llegar a un acuerdo satisfactorio para todos, se le ofreció a Belgrano hacer aportes voluntarios, ofrecimiento que el jefe del Ejército del Norte rechazó de plano. Nada fue suficiente para torcer la voluntad del General, pues consideraba que lo que estaba en juego era el futuro de la Patria y a ella había que someterse.

En defensa de su firme posición, el prócer señala: *"no busco plata con mis providencias: busco el bien de la Patria. Yo no oigo clamores de particulares, sino el bien general. Los que no quieran sufrir esos perjuicios, anímense a defender la provincia, y no por conservar unos ganados, que serían para el enemigo, permanezcan fríos espectadores de las desgracias de la Patria".* Las palabras de don Manuel eran sinceras, le nacían desde el fondo de su corazón y estaba convencido de que procedía correctamente porque para él no había acto más grande y noble que ponerse al servicio de la Patria en espíritu y alma.

Magnanimidad, grandeza de alma

Luego de enterrar a los fallecidos del 20 de febrero de 1813, el General Manuel Belgrano colocó una humilde cruz con la leyenda "A los Vencedores y Vencidos", iniciaba así una larga tradición nacional. Las magnánimas condiciones impuestas a los derrotados fueron ejemplo de su virtud. La generosidad del General tenía su sentido. El 8 de marzo de 1813, la Asamblea Constituyente dispuso premiar a Belgrano con 40.000 pesos y un sable con guarnición de oro por el brillante triunfo obtenido; el prócer declinó el obsequio y, al hacerlo, comprometió para siempre la gratitud de Tarija, Jujuy, Tucumán y Salta, para quienes dispuso, con ese dinero, la creación de cuatro escuelas.

1. Furlong , Guillermo. *Belgrano, el santo de la espada y de la pluma*, Ed. Club de Lectores. Bs. As., 1974, página 9.
2. Salas López, Fernando de. *La utopía de la guerra y la paz y el terror de la guerra*, colección ADALID, página 101.

Belgrano se niega a que el Norte sea tomado por el enemigo y entiende que presentar batalla era la única solución, aunque era consciente del riesgo que corría su decisión. Se jugaba el todo por el todo: su vida, su destino, su futuro.

Austeridad y sobriedad de Soldado

Al ser nombrado Jefe del Regimiento de Patricios, dijo: "ofrezco a V.E. la mitad del sueldo que me corresponde, siéndome sensible no poder hacer demostración mayor, pues mis facultades son ningunas, y mi subsistencia pende de aquel, pero en todo evento sabré reducirme a la ración de soldado [...]"[3].

El arrojo frente a la timidez o cobardía, hace obrar al hombre en los momentos del combate por el valor. Ejemplo de ello está en la prueba que Belgrano da en reiteradas oportunidades durante la dura Campaña al Paraguay de 1810-1811. En el combate de Tacuarí, ante la situación que se mostraba desfavorable porque el enemigo tenía amplia superioridad numérica, el General se puso al frente de sus hombres y desenvainó su espada para encabezar la carga. Belgrano comentó a uno de sus soldados: *"aún confío que se nos ha de abrir un camino que nos saque con honor de este apuro; y de no, al fin lo mismo es morir de 40 años que de 60".*

El General Belgrano a lo largo de su vida demostró valor físico, mental y moral ante la adversidad. El Coronel Blas Pico nos refiere: *"se lo vio siempre incansable en el bufete expidiendo órdenes concernientes, las más de las veces, de su puño y letra para dar a los negocios el mayor impulso, corría a todas horas por los cuarteles, campos de instrucción, hospitales... hasta mirar el rancho de sus soldados"*[4].

Siempre se mostró valiente pero no temerario, compartió el riesgo, soportó dificultades y enfrentó el peligro. Mostró coraje en moderación, incluso cuando hacerlo supuso correr un riesgo personal. Altivez contra el servilismo, lo vemos en las horas de la entrega máxima. Luego de la derrota de Vilcapugio, la campaña militar pasaba por su hora más oscura; sin embargo, el jefe patriota no quería ceder a los caprichos del destino; por lo tanto iba a insistir con su objetivo de proseguir en la lucha con el fin de obtener la victoria definitiva. El ánimo del prócer no declinaba; su espíritu no iba a dejarse dominar por la desazón y por la desesperanza. Finalizada la batalla de Vilcapugio, don Manuel Belgrano tomando el mástil de la bandera nacional, dijo a viva voz: *"¡Soldados!: hemos perdido la batalla después de tanto pelear. La victoria nos ha traicionado, pasándose a las filas enemigas en medio de nuestro triunfo. ¡No importa! Aún flamea en nuestras manos la bandera de la Patria".* Se dice que, al día siguiente, luego de rezar el Rosario con la tropa, el prócer dio una arenga a sus hombres para finalizar diciendo que si lo abandonaban estaba dispuesto a morir por el honor del ejército, a lo que al unísono sus soldados respondieron: *"¡Todos moriremos al lado de nuestro general!".* Estas palabras calaron hondo en el espíritu de Belgrano, dándole la fuerza suficiente para proseguir adelante con el duro y sinuoso camino que se había trazado: liberar a su Patria de las garras del enemigo realista.

Todo por la patria

En estas tres situaciones, el prócer antepone el interés supremo de la Patria a cualquier resquemor formalista.

La intrépida decisión de Belgrano de hacer caso omiso de las órdenes del Gobierno de replegarse hacia Córdoba, pues se niega a que el Norte sea tomado por el enemigo. Presentar batalla era la única solución aunque era consciente del riesgo que corría su decisión. Se jugaba el todo por el todo: su vida, su destino, su futuro.

En su esquema de ideas, y en su escala de valores, la Nación está por encima de cualquier otro interés individual o sectorial. A ella cabe, como deber, brindarle los mejores esfuerzos y aún consagrarle la vida. Se convierte así, la Nación misma, en la ley suprema ante la cual cede cualquier argumentación en contrario.

3. Furlong , Guillermo. *Belgrano, el santo de la espada y de la pluma*, Ed. Club de Lectores. Bs. As., 1974, página 15.
4. Bruno, Cayetano. *Creo en la vida eterna: el ocaso cristiano de los próceres*. Ed. Didascalia. Rosario, 1982, página 28.

El verdadero líder tendrá más pálpito que cálculo, si la causa es justa y el deber militar se lo impone, él mantendrá firme el objetivo. Por ello, en la heroica y arriesgada expedición auxiliadora por la libertad del Paraguay, él mismo nos dirá en sus *Memorias: "llegamos al Río Corrientes, al paso ya referido y sólo encontramos dos muy malas canoas que nos habían de servir de balsa para pasar la tropa, artillería y municiones: felizmente, la mayor parte de la gente sabía nadar y hacer uso de lo que llamamos "pelota" y aun así tuvimos dos ahogados y algunas municiones perdidas por la falta de una balsa. Tardamos tres días en este paso, no obstante la mayor actividad y diligencia y el gran trabajo de los nadadores que pasaron la mayor parte de las carretas dando vuelcos. El río tendría una cuadra de ancho y lo más de él a nado".*

La férrea y verdadera humildad del líder hace obrar con certeza a su tropa, forjada en el sacrificio y la austeridad del trabajo diario silencioso y constante, así lo demuestra este párrafo por él escrito que describe con humildad y respeto la victoria en Campichuelo: *"por lo que hace a la acción, toda la gloria corresponde a los oficiales ya nombrados y siento no tener los nombres de los siete soldados para apuntarlos, pero en medio de esto son dignos de elogio por sólo el atrevido paso del Paraná en el modo que lo hicieron, así oficiales como soldados, y espero que algún día llegará en que se cuente esta acción heroica de un modo digno de eternizarla, y que se mire como cosa de poco más, o menos, porque mis enemigos empezaban a pulular y miraban con odio a los beneméritos que me acompañaban y los débiles gobernantes que los necesitaban para sus intrigas trataban de adularlos".*

El General Manuel Belgrano poseía una serie de competencias de liderazgo que ayudan a los

CV

GABRIEL ANIBAL CAMILLI

Coronel Mayor del Ejército Argentino. Magister en Política de la Universidad del Norte "Santo Tomas de Aquino". Magister en Historia de la Guerra del IESE. Magister en Defensa Nacional. Se desempeñó como agregado de la Defensa Militar Naval y Aeronáutica en Alemania, Austria y Suecia. Actualmente es el Director de la Escuela Superior de Guerra Conjunta y Decano de la Facultad Militar Conjunta.

demás a adaptarse o recuperarse de la adversidad. Fue, sin duda, el catalizador que inspiró a su tropa alcanzar metas que no podrían haber logrado por sí solos. La adversidad supone la verdadera prueba del liderazgo. Muchas de las lecciones más valiosas que nos ofrece la vida surgen de ella. Hay un ejemplo en este caso: luego de la fatal derrota en Vilcapugio, el 5 de octubre de 1813, Belgrano y sus hombres se dirigen a Macha. Apenas instalado allí, intenta reorganizar al maltrecho ejército a su mando. De inmediato puso manos a la obra, pues no había un minuto que perder. Comenzó por pedir ayuda de todo tipo a los gobernadores con los cuales tenía contacto. Solicitaba la pronta remisión de armamento, soldados, pertrechos, vestimenta, alimentos y todo aquello que fuera útil para enfrentar con posibilidades de triunfo al enemigo. Uno de los militares que respondió a su llamado fue Ortiz de Ocampo, gobernador de Charcas, luego de una carta que recibiera del mismo Belgrano el 7 de octubre de ese año. En ella, el prócer le escribe: *"fortaleza, ánimo, constancia y esfuerzo (no de los comunes) son los que necesita la Patria. Ella será libre e independiente si no nos amilanamos. Si en este pueblo hay cobardes, que vengan a Macha, y sepan que no hemos de abandonar el puesto, sino cuando sea imposible sostenerlo. Aún hay sol en las bardas y hay un Dios que nos protege".* Resultan admirables estas palabras del creador de la bandera, quien no se deja intimidar por las dificultades ni por un destino que se le presentaba incierto y oscuro.

Ciertamente, Belgrano era respetuoso de las tradiciones, de la jerarquía, del principio de autoridad y amante del orden.

La religiosidad del prócer

El sentido trascendente de la vida se halla presente en nuestro líder militar. El mejor ejército que poseía Belgrano fue la sólida Fe por sobre todo. Le quedaría bien aquel axioma criollo: "en Dios confiando y con el mazo dando". Porque esa profunda Fe queda demostrada en varios documentos y cartas a lo largo de su vida, y entre varios, este: *"la Divina Providencia nos abra un camino para mejorar de suerte, y que la Patria se vea libre de tantos apuros que la rodean". "Soy verdadero cristiano, católico, apostólico, romano".* El 24 de septiembre se celebra la Fiesta de Nuestra Señora de la Merced, Patrona del Ejército Argentino. El General Belgrano durante la batalla de Tucumán, el 24 de septiembre de 1812, puso toda su confianza en Dios y en Nuestra Señora de la Merced. En el parte de guerra que envía al gobierno, dice: *"la Patria puede gloriarse de la victoria que han obtenido sus armas el 24 del corriente, día de Nuestra Señora de la Merced, bajo cuya protección nos pusimos".* Conmovido por el triunfo, nombra a la Virgen de la Merced Generala del Ejército Argentino y en solemne ceremonia le entrega su bastón de mando. En 1912, al cumplirse el centenario de la Batalla de Tucumán, la imagen de Nuestra Señora de la Merced, que se venera en San Miguel de Tucumán, fue coronada solemnemente en nombre del papa San Pío X.

Una de la virtudes más característica del General Belgrano, sin duda ha sido la fortaleza de carácter o de espíritu, que destaca a un buen conductor militar, en el sentido que relata von Clausewitz[5]. En el caso de nuestro prócer, por supuesto, nada tiene que ver con la exhibición vehemente de sentimientos o con el temperamento apasionado con los que quizás podría asociarse. La fortaleza de carácter se expresa en Belgrano en la capacidad para conservar la cabeza en momentos de tensión excepcional y emociones violentas en innumerables circunstancias de su vida. ¿Podría derivar esta facultad solo de su fuerza intelectual? Lo dudamos. Creemos que se acercaría más a la verdad suponer que la facultad conocida como *autocontrol* -la virtud de conservar la calma incluso en situaciones de tensión enorme-, hunde sus raíces en el temperamento de este hombre singular. Se destaca por demostrar una emoción que sirve para equilibrar los sentimientos apasionados propios de un carácter fuerte sin destruirlos, y es solo este equilibrio el que garantizó el dominio del intelecto. Este contrapeso que equilibró su acción fue sencillamente el sentido que poseía de la dignidad humana, el orgullo más noble y la necesidad más profunda: el anhelo de actuar racionalmente en todo momento. Por lo tanto, podemos argumentar que su carácter fuerte fue tal porque no se dejó desequilibrar por las emociones más poderosas.

El legado belgraniano

El General Manuel Belgrano conocía acabadamente el valor de los

símbolos como medio de cohesión de un Ejército y de una comunidad. Sabía perfectamente que la bandera ha sido un instrumento militar, que se llevaba al combate con una triple finalidad:

> **Ceremonial:** dice a los demás quién es quién.
> **Práctica:** dice dónde estamos a nosotros mismos, marca la posición del jefe y sirve de referencia para realizar las maniobras en el combate.
> **Espiritual:** en la tela se representan los símbolos de aquello que se quiere defender, la razón de ser de esa fuerza.

Antonio Vallecillo dice en sus *Comentarios Históricos: "como prenda de juramento, como señal de formación, como guía del combate, como punto de reunión y como llamada a reclutas..."*[6]. Asimismo, Alfonso X "el Sabio", (1221-1284), en su *Libro de las siete partidas,* define de este modo el valor de los símbolos: *"señales conocidas pusieron antiguamente, que traxesen los grandes homnes en sus fechos, i mayormente en los de guerra, porque es fecho de gran peligro en que conviene que hayan los homnes mayor acabdillamiento, ca no tan solamente se han de acabdillar por palabra o mandamiento de los cabdillos, más aun por señales".*

Entendiendo cabalmente esto, el general le encargó a María Catalina Echeverría, una vecina de Rosario, que confeccionase una bandera con los colores de la Escarapela.

El sentido del Sacrificio y el llevar los padecimientos dignamente, sin duda son muestras de fortaleza y carácter de un verdadero soldado. En los primeros días de noviembre de 1819, regresó a Tucumán luego de haber estado

En el año del Bicentenario del paso a la inmortalidad del General Manuel Belgrano, lo destacamos como arquetipo y como modelo por sus virtudes militares.

allí en 1812 cuando había asumido como Jefe del Ejército del Norte y vencido en la batalla de Tucumán; y también en 1816 cuando concurrió al Congreso para que declarara la Independencia. Pues bien, el 11 de noviembre de 1819 estalla en la provincia norteña un movimiento encabezado por Bernabé Aráoz y un capitán llamado Abraham González, quien intentó apresar al prócer, a pesar de que se encontraba postrado en cama. González ordenó a uno de sus subordinados que le pusiera una barra de grillos, de modo tal que la humillación fuera absoluta. Ante esa actitud, reaccionó el Dr. Joseph Redhead, un destacado médico que sentía un profundo afecto por el ilustre enfermo. Levantó las sábanas de la cama donde reposaba Belgrano y tras mostrarles la brutal hinchazón que tenía en sus piernas, el mediocre González desistió en aplicar el cruel castigo. Por lo tanto, debido a la valiosa intervención de Redhead, que auxilió a Belgrano en sus últimas horas, el prócer no fue engrillado, pero sí detenido en sus aposentos y con un centinela que lo vigilaba durante todo el día. Finalmente, por presión del Congreso, el gobernador Bernabé Aráoz dispuso su libertad. Desilusionado por la ingratitud de Tucumán, Belgrano decidió partir a Buenos Aires. No podía hacerlo sin medios que no poseía y eso lo movió a solicitarle al gobernador tucumano la suma de dos mil pesos para poder trasladarse. Aráoz se los negó y le hizo saber que el estado tucumano no estaba en condiciones de soportar ese gasto.

"Fueron días de una gran tristeza para el héroe, pues en esos difíciles momentos ningún funcionario acudió en su ayuda; muy por el contrario, se le negó todo subsidio para poder cumplir con el viaje como ya se pudo ver. Una actitud propia de la gente sin principios, pues a pesar de los servicios que había prestado a la patria –muchas veces en pésimas condiciones de salud– ninguna de las personas que ostentaban el poder movió un pelo para borrar esa injusticia de la que don Manuel Belgrano fue víctima. Quien le dio plata para que pudiera dirigirse a Buenos Aires fue su gran amigo José Celedonio Balbín. Pocos días después, el prócer emprendía su viaje a la capital acompañado del Dr. Redhead. Allí pasará sus últimos días, abandonado y condenado a un cruel olvido por todos aquellos que en los momentos de gloria lo adularon... La soledad y la ingratitud de los hombres serían las encargadas de darle al ilustre general la estocada final"[7].

La ingratitud de los hombres es lo que quisimos reparar con estas líneas que quieren, no solo hacer justicia con un hombre grande, sino mostrar esa grandeza reflejada en las virtudes que adornaron su vida y que son ejemplo para quienes nos formamos a su sombra.

5. Von Clausewitz, Carl, *De la Guerra;* Libro I Capítulo III: "El genio militar".
6. Antonio Vallecillo Luján (1807-1880), que alcanzó el grado de coronel y fue un prestigioso erudito y autor de numerosas obras compilatorias de los códigos históricos del ejército español.
7. Libro de Belgrano.

EL CONFLICTO FUTURO

Por BM **ALEJANDRO ANÍBAL MORESI**

Palabras Clave:
> Conflicto
> Estrategia
> Singularidad

ARTÍCULO CON REFERATO

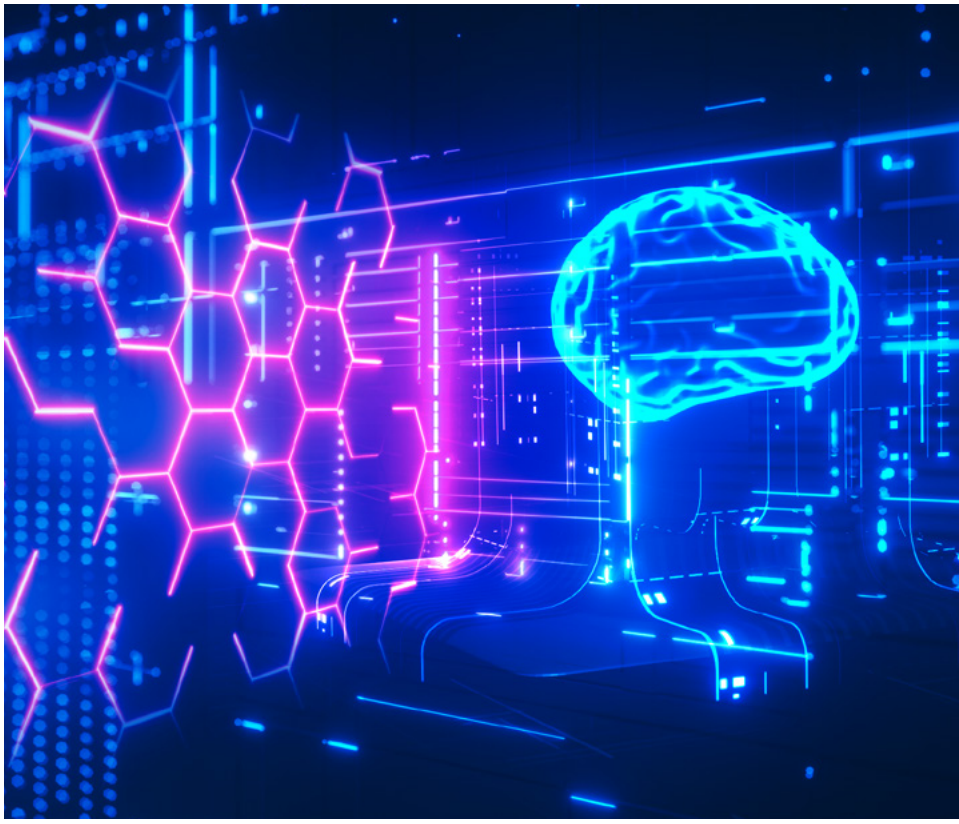
La virtualidad es parte de la vida humana, desde la invención de la radio (podemos citar el programa de Orson Welles "La guerra de los mundos", como un ejemplo de control de masas desde la virtualidad, en este caso empleando solo las ondas hertzianas), hasta nuestros días. El tiempo que dedicamos al mundo real y al virtual ha ido creciendo y mucho más dramáticamente a partir del advenimiento del ciberespacio como un ámbito de vida, donde prácticamente todas las actividades del mundo real pueden ser replicadas en el mundo virtual, donde el tiempo humano en el mismo se incrementa dramáticamente.

El problema de ello es que en cada ámbito en que desarrollamos la actividad humana tenemos un proceso de aprendizaje. Por eso, antes de salir al mundo terrestre aprendemos a caminar, nos enseñan a cruzar la calle, nos advierten ante el peligro de tratar con desconocidos. Antes de ir al mar, aprendemos a nadar, nos informan de sus reglas y riesgos. Ni hablemos de los que pretenden desenvolver su actividad en el aire, donde ya no resulta posible hacerlo sin una preparación física, intelectual y las certificaciones correspondientes; y mucho más exigente aún es la actividad espacial. Sin embargo, para acceder al ciberespacio, un mundo creado por nosotros basado en un manifiesto[1] anárquico en su naturaleza, accedemos a él sin ninguna preparación ni precaución, es más, entregamos la llave (un smartphone) de ese universo desconocido a nuestros hijos sin advertirle que nosotros tampoco conocemos cuáles son los riesgos y peligros que entraña y cómo son las reglas y procedimientos para movernos con él.

Esto nos sucede porque la tecnología se ha movido más rápido que nuestra adaptación a ella. Todo el material que en la década del '80

requería una oficina (PC, agendas, archiveros, teléfono, fax, máquina de escribir, máquina de fotos, fotocopiadora, etc.), hoy está en nuestro bolsillo, con muchas más capacidades, a través de un teléfono inteligente.

Ni las leyes, ni nuestras mentes, ni el sistema de aprendizaje se han adaptado al cambio y ya estamos en la próxima estación: la inteligencia artificial (IA), estos cambios usan a nuestro cerebro como campo de batalla de las actuales guerras y será el ambiente donde se desarrollará el conflicto futuro, sin embargo, no nos estamos preparando para ello.



La visión estratégica del conflicto actual

Si bien la naturaleza de la guerra no ha cambiado, desde el principio de los tiempos hasta hoy, podemos citar a Sun Tzu, Clausewitz, Mao, Warden, Eikmeier, no importa a quién, siempre el problema es quebrar la voluntad del enemigo al menor esfuerzo posible. La realidad es que el ambiente ciberespacial introduce un cambio de paradigma en cómo hacer la guerra y qué debe analizarse, esto consiste en:

1. El campo de batalla se ha movido del mundo real a través del ámbito virtual a la mente de las personas, no importa cuál es la realidad, sino lo que la gente cree que la realidad es, más allá de los hechos que se muestren.
2. La realidad que prima es lo que la sociedad cree que es, más allá de la realidad fáctica del hecho en cuestión, ello se refleja en la decisión política consecuente.
3. El tiempo de permanencia en el ciberespacio se incrementa dramáticamente día a día.

Corolario de esta situación

Napoleón había dicho: "la infantería es la reina de las batallas", y todos los grandes estrategas lo habían aceptado porque sin duda, hasta que los infantes no ocupen el terreno no se puede hablar de victoria. El problema es que el campo principal de batalla en el siglo XXI es la mente de la sociedad, por ende el rol de la infantería será ocupado por una nueva clase de guerreros: los guerreros del ciberespacio, que serán los reyes de las mentes.

Aquí es donde radica el problema estratégico de este ambiente operacional (el ciberespacio), ya que la esencia de la guerra no ha cambiado, pero este modo que siempre existió (velo, engaño, guerra de la información, etc.), que las Tecnologías de la Información y de la comunicación (TICs) han potenciado a niveles difíciles de ponderar, ha llevado a la guerra a un nivel de implementación que me gusta llamarlo como la estrategia del demonio (si haces todo bien de algún modo caes al infierno; y si lo haces mal ya estás en el infierno, pero no importa lo que hagas siempre el demonio gana).

¿Cómo se implementa esto en el ciberespacio? Es aquí donde aparecen las nuevas hipótesis de conflicto, que son etéreas, cosas difíciles de dimensionar, sin embargo, nos introducen en un estado de cuasi guerra, cuasi total (no desde la perspectiva de Clausewitz, sino desde la perspectiva del hombre común que pierde el concepto esencial de seguridad).

Hemos pasado de la batalla aeroterrestre, cuyo zenit se encontró en "Tormenta del Desierto", a la batalla multidominio donde fuerzas terrestres, aire, mar, espacio y ciberespacio conjugan sus esfuerzos en el logro de objetivos. Sin embargo, han mostrado una eficacia relativa frente al conflicto planteado en *"escenarios híbridos"*[2] y *"guerra irrestricta"*[3], donde el ciberespacio ha adquirido

1. John Perry Barlow, "Electronic Frontier Foundation" http://homes.eff.org/~barlow/Declaration-Final.html, feb 1996.
2. Molly K. Mckew, *Gerasimov doctrine*, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia- foreign-policy-215538, sep/oct 2017.
3. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999.

un valor trascendental. Cada uno de estos ambientes a su vez es considerado desde diferentes dimensiones (tiempo, información, inteligencia, ayuda humanitaria, medio ambiente, asuntos civiles, asuntos militares, infraestructura, economía, ambiente psicosocial, criminal, financiero biológico etc.). Una primera aproximación la ha dado Naciones Unidas (ONU) con las *"High-Level Independent Panel on Peace Operations"*(HIPPO)[4]. Todos estos intentos fueron para tratar de alcanzar una doctrina que permita efectivizar el enfrentamiento en el campo de batalla futuro, que finalmente se dará en tres grandes ámbitos: 1) la REALIDAD, 2) el VIRTUAL y 3) de la INFORMACIÓN.

En el ciberespacio también podríamos establecer tres niveles a considerar, el de la **seguridad Informática** (los *firewall*, antivirus, concientización, etc.), el de la **Ciberdefensa** (protección de las infraestructuras críticas, ya sea mediante operaciones ofensivas, defensivas o de exploración) y el de la **Información** que coincide con el tercer ámbito de la batalla futura.

El lugar donde las acciones se llevan a cabo es común en ambos: **el cerebro humano,** allí es donde se dirime gran parte del conflicto actual y también el futuro, más allá de las acciones en el campo real y en el virtual, las decisivas serán en el de la información: el cerebro humano es el objetivo de los conflictos actuales.

El problema es que cuando hablamos de Ciberdefensa, Occidente se centra de manera exclusiva en las problemáticas de los dos primeros niveles: la seguridad informática y la Ciberdefensa (protección de las infraestructuras críticas), pero nunca se protege al hombre común en el nivel de la información, (perspectiva ciberespacial o como ámbito de guerra) porque Occidente respeta la libertad del Individuo, sin embargo, es allí donde se producen las agresiones.

¿Cuál es Conflicto Futuro?

El conflicto futuro[5] viene de la mano de la "singularidad", una promesa de bienestar y progreso para toda la humanidad, similar a la que en las décadas de 1980 y 1990 surgió con la "globalización", que trajo beneficios a la humanidad, pero con ella llegó la WEB profunda, el ciber-terrorismo, el ciber-crimen, las guerras híbridas, solo por citar algunos problemas que no visualizamos entonces.

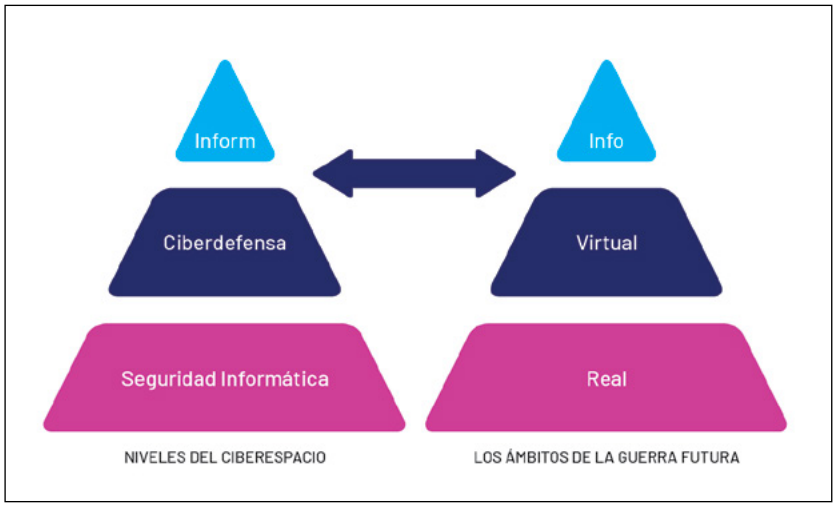
¿Qué nos promete la singularidad?, el mundo para el 2050 nos va a encontrar compitiendo con la racionalidad perfecta, máquinas con capacidades iguales a las del ser humano, pero con la ventaja de un conocimiento cuasi infinito ya que ella dispondrá de toda la ***big data*** a la hora de responder. La punta del iceberg la mostró el caso Cambridge Analítica. Hoy se podría hablar de una nueva clase de ***"dios",*** que puede dedicarse a cada uno de nosotros de manera individual, pero que a diferencia del Dios espiritual, que pugna por el libre albedrío, este busca esclavizar nuestras mentes y quitarnos la capacidad de autodeterminación, ¿y quién nos defiende de esto?

¿Cómo competimos contra la racionalidad perfecta?, mientras que nosotros solo dispondremos de nuestro puñado de conocimientos para afrontar cada situación, la inteligencia artificial dispondrá casi instantáneamente de la totalidad del conocimiento humano para resolver la misma pregunta. ¿Podrán las reglas de Isaac Asimov[6] permitirnos sobrevivir?, y de hacerlo ¿a qué se limitarán nuestras vidas?

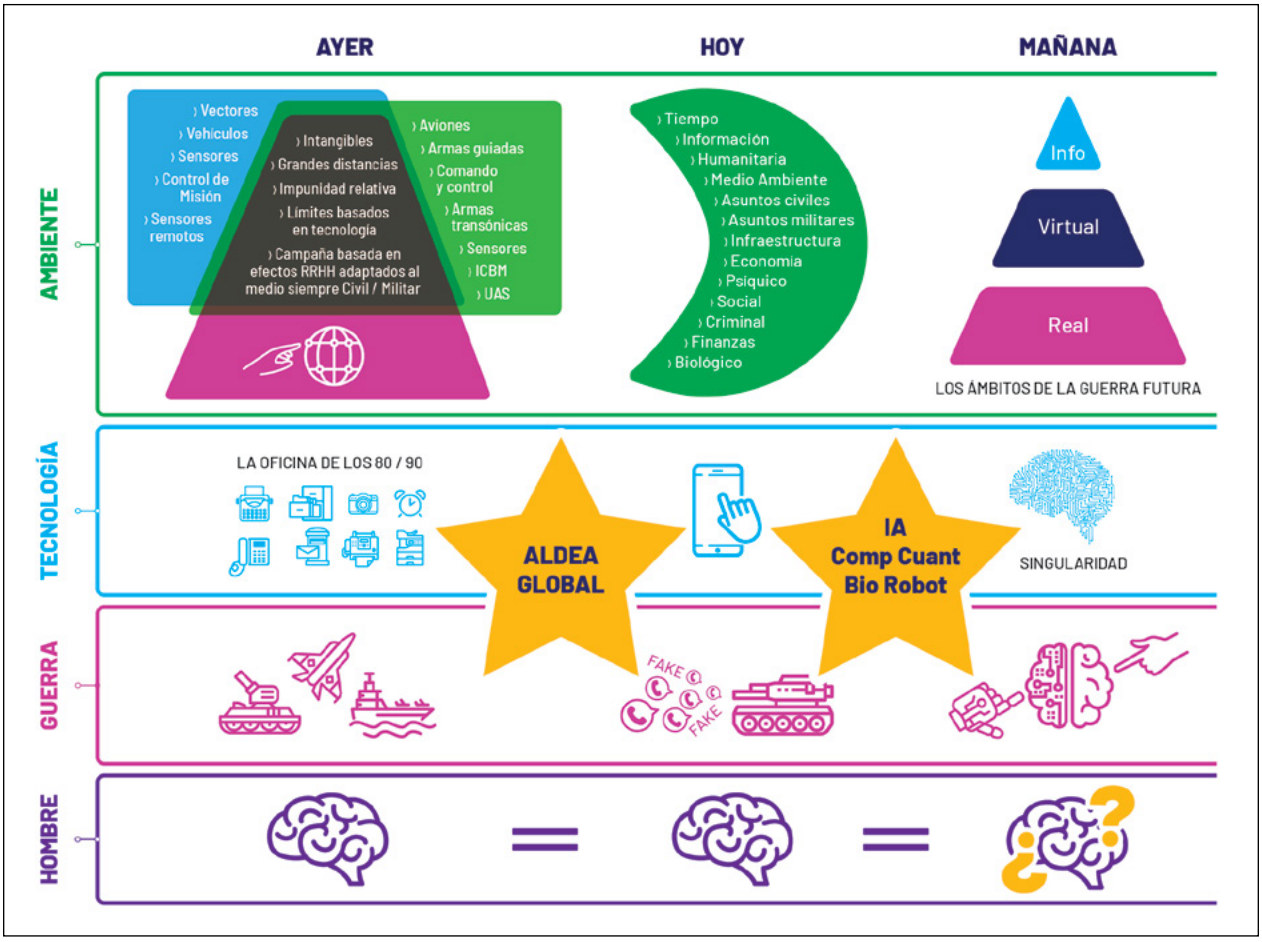
Llevamos aproximadamente 2500 años (desde que los grandes filósofos griegos definieron al *"hombre como un animal racional"*), educando nuestro cerebro en el desarrollo de la racionalidad, cuando en realidad nuestro cerebro tiene otras potencialidades, como es la intuición (capacidad de ver la respuesta de manera directa), cualidad que asignamos a los artistas y a los genios, ¿acaso Einstein no introdujo la teoría de la relatividad y luego la demostró? Pero si nos auto observamos, notaríamos que en general las decisiones cruciales o trascendentales son aquellas que implican cuestiones de vida o muerte, que no proceden de un proceso racional, sino que son decisiones tomadas en el campo emotivo.

En la década del '60, descubrimos que teníamos la capacidad de

RELACIÓN ENTRE ÁMBITOS DE CONFLICTO Y LOS NIVELES DEL CIBERESPACIO



4. https://www.un.org/pga/70/wp-content/uploads/sites/10/2016/01/PolicyBrief2015_5_-Implementing_the_HIPPO_Alexander-Ilitchev.pdf
5. Se aplica este concepto al dominio de tierra, agua, aire, espacio y ciberespacio
6. Asimov, Isaac (1989). «Círculo vicioso». *Los robots.* trad. Domingo Santos. Barcelona:Martínez Roca. ISBN 84-270-0906-2.



advertir en una película, más de 30 cuadros por segundo, que algunos de ellos tienen información que es procesada en nuestro inconsciente y nos hace adoptar determinadas conductas, (mensajes subliminales). Esto lo hemos empleado para incrementar el consumo pero nunca trabajamos para cultivar nuestro cerebro y poder traer cosas del inconsciente al consciente.

El gran desafío de los próximos 30 años es lograr un diferencial importante con la futura inteligencia artificial, un diferencial que nos permita seguir siendo la especie que domine este planeta. El potencial lo tenemos entre nuestras orejas y las neurociencias, que han abierto las puertas del conocimiento de nuestro cerebro. El desafío es crear una nueva cultura de aprendizaje. Ello requiere inicialmente comprender y conocer los desafíos que impone el ciberespacio para impedir ser dominados a través de él.

La confrontación de hoy ya no conoce de seguridad interior o nacional, no distingue entre soldados y civiles, el campo de batalla somos cada uno de nosotros, desarrollar una cultura común y una forma de pensar propia, pero con una base cultural común es la que nos permitirá afrontar con éxito las crisis y conflictos del presente y prepararnos para la segunda etapa del proceso, que es aprender a desarrollar nuevas capacidades cerebrales, para así poder enfrentar el conflicto futuro: la competencia con la Inteligencia Artificial (IA).

CV

ALEJANDRO ANÍBAL MORESI

Brigadier Mayor en situación de Retiro. Master en Dirección de Empresas; Master en Dirección de Recursos Humanos; Licenciado en Sistema Aéreos y Espaciales; Postgrado en Gestión de Proyectos; Administración de la Calidad, Curso de Derecho Bélico y Derecho Internacional Humanitario (INDAE). Fue Director General de Planes Programas y Presupuestos de la FAA; Director General de Investigación y Desarrollo de la FAA, entre otros. Actualmente se desempeña como Director del proyecto Observatorio Argentino de Ciberespacio.

EL COMANDO DE CIBERDEFENSA ALEMÁN
UN CLARO EJEMPLO DE INTEGRACIÓN

Por MY **PABLO ALEJANDRO CAÑETE**

ARTÍCULO CON REFERATO

En el marco de la reestructuración de las Fuerzas Armadas alemanas, el 5 de abril de 2017 la ministra de Defensa, Ursula von der Leyen creó el Comando del Espacio de Información y Ciber (Kdo CIR)[1]. A partir de ese momento, innumerables artículos y redacciones en el mundo no han dejado pasar ese evento para destacar la conformación de este significativo elemento de ciberdefensa en la República Federal Alemana.

Sin embargo, muchas preguntas hay detrás de esta nueva organización. Entre mujeres y varones, el personal supera las 14.000 personas, es decir solo 2.000 efectivos menos que la Armada alemana. ¿Es la cuarta Fuerza Armada en Alemania? ¿Cuál es su misión? ¿Cómo está organizado? ¿Qué capacidades posee? En mayo de 2019, he tenido la oportunidad de realizar una pasantía en el mencionado comando, lo que me permite responder a los interrogantes. La finalidad del

Palabras Clave:
> Comando
> Ciberdefensa
> Ciberseguridad
> Integración
> Inteligencia estratégica

El Comando del Espacio de Información y Ciber alemán no es una fuerza armada, sino que es un comando conjunto que proporciona apoyo de ciberdefensa a sus fuerzas armadas.

presente trabajo es proporcionar información sobre la misión, las funciones, la organización y las capacidades del Kdo CIR.

¿La cuarta fuerza armada alemana?
Las Fuerzas Armadas alemanas (FFAAA) están conformadas por dos grandes organizaciones: civil y militar, que a modo de fácil comprensión se esboza en la figura 1 con sus respectivos efectivos.

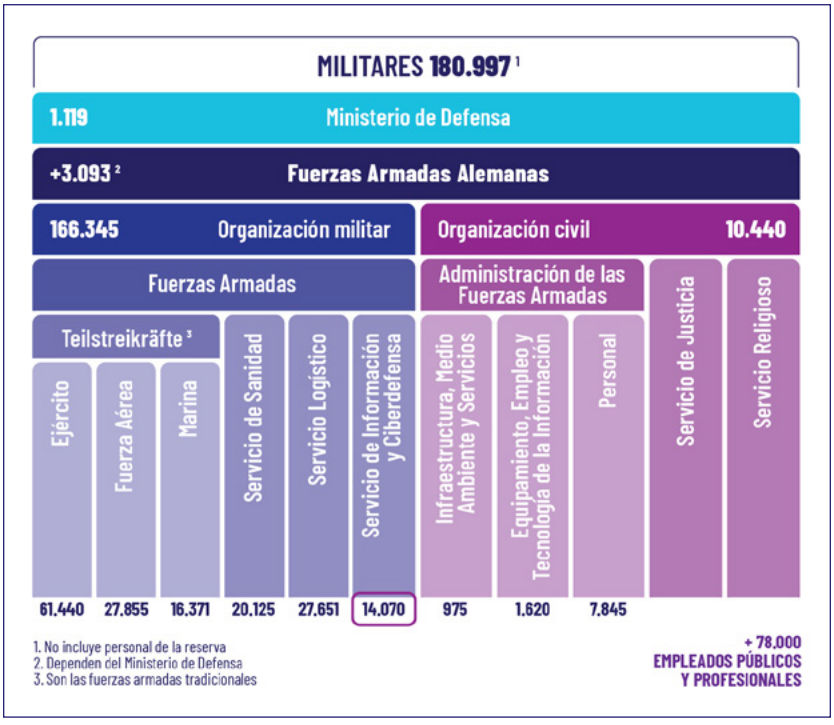
La organización civil normalmente no está relacionada con la parte operacional de las Fuerzas Armadas y en su estructura forman parte las siguientes organizaciones: Infraestructura, Medio Ambiente y Servicios, Equipamiento, Empleo y Tecnología de la Información, Servicio de Personal, Servicio de Justicia y el Servicio Religioso.

La organización militar está estructurada en 6 grandes fuerzas. Las *Teilstreitkräfte* son las Fuerzas Armadas tradicionales, tales como Ejército, Marina y Fuerza Aérea. Poseen además otras 3 organizaciones que los militares alemanes denominan *Organisationsbereiche*. Estas son organizaciones conjuntas, organizadas, equipadas e instruidas para proporcionar apoyo a las FFAAA y comprenden los Servicios de Sanidad, de Logística y el Kdo CIR. Cada fuerza tiene un comandante y depende directamente del Comandante Conjunto de las FFAAA.

Haciendo referencia al primer interrogante, el Kdo CIR no es una Fuerza Armada, sino que es un comando conjunto que proporciona apoyo de ciberdefensa a sus Fuerzas Armadas.

¿El Kdo CIR proporciona sólo apoyo de Ciberdefensa?
La respuesta se obtiene al analizar la misión del Kdo CIR y sus funciones. El Kdo CIR (2019) sostiene que: "así como el Ejército, la Fuerza Aérea y la Marina son responsables de las dimensiones de la tierra, el aire y el mar, también son responsables de manera integral de la dimensión del espacio cibernético y

FIGURA 1. ESTRUCTURA DE LAS FUERZAS ARMADAS ALEMANAS
En el resaltado se visualiza el efectivo del Kdo CIR



Fuente: Bundesministerium der Verteidigung. Recuperado de https://www.bmvg.de (03/05/2019).

1. Kdo CIR: Kommando Cyber- und Informationsraum (Comando del Espacio de Información y Ciber).
2. *Bundeswehr (2019). Servicios del Espacio Cibernético y de la Información.* Recuperado de https://cir.bundeswehr.de/portal

de información [...]"[2]. Además, establece que el mencionado comando garantizará el funcionamiento y la protección del sistema de información de las FFAAA, tanto a nivel nacional como en sus contingentes desplegados en el exterior.

Haciendo referencia a sus funciones, dentro del espacio cibernético y de la información, el Kdo CIR es la máxima autoridad conjunta de comando y control, proporciona además un centro de situación conjunta de información y ciberdefensa a sus Fuerzas Armadas y garantiza la cooperación de organismos nacionales e internacionales en temas relacionados con la quinta dimensión.

Uno de los aspectos más relevantes del mencionado comando es que conduce 3 elementos, como puede verse en la Figura 2. El primer elemento es el Comando de Inteligencia Estratégica, que proporciona apoyo de inteligencia, guerra electrónica, operaciones psicológicas y ciberoperaciones activas. El segundo elemento es el Comando Técnico de la Información que proporciona apoyo de comunicaciones, informática y ciberoperaciones pasivas. El tercer elemento es el Centro de Geoinformación, que proporciona apoyo de información a las ciencias y disciplinas de biología, etnología, teledetección, geodesia, geoinformática, geología, geofísica, geopolítica, hidroacústica, hidrografía, hidrología, cartografía, climatología, meteorología, ecología, oceanografía y fotogrametría.

Entonces, la respuesta a la pregunta inicial es un rotundo no. El Kdo CIR es un elemento conjunto, que integra capacidades de comunicaciones, informática, guerra electrónica, inteligencia, ciberdefensa, operaciones psicológicas e información de diferentes ciencias y disciplinas para proporcionar apoyo a sus Fuerzas Armadas, dentro y fuera del país.

En síntesis, el Kdo CIR funciona como un sistema conjunto que a través de la interoperabilidad de sus medios (personal y material) proporciona capacidades de C4I2SR[3] a sus Fuerzas Armadas desplegadas dentro o fuera de Alemania, tales como misiones de la Organización del Tratado Atlántico Norte (OTAN), de la Unión Europea (UE) y de la Organización de las Naciones Unidas (ONU).

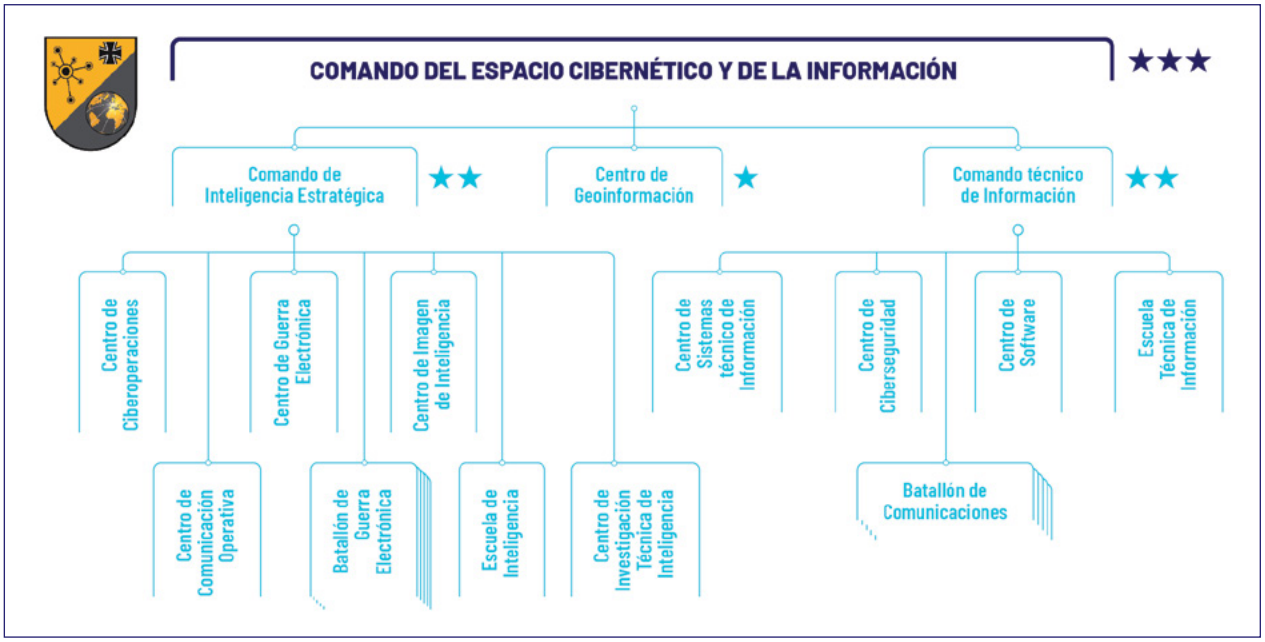
Organización del Kdo CIR

El Kdo CIR tiene a cargo 3 elementos. Su comandante es un general de 3 estrellas. A continuación, se describen la misión de cada uno de ellos y una breve descripción de sus capacidades.

Comando de Inteligencia Estratégica

Tiene la misión de proporcionar apoyo de inteligencia, guerra electrónica, operaciones psicológicas y ciberdefensa a sus Fuerzas Armadas. De izquierda a derecha en la Figura 2, se visualizan sus organizaciones dependientes. El Centro de Ciberoperaciones tiene la capacidad de ejecutar ciberoperaciones activas y el Centro de Comunicación Operativa proporciona apoyo de operaciones psicológicas. Este último Centro conduce la radio y televisión de las FFAAA para personal en el exterior. La radio se llama *Andernach*[4]. Además planifica y conduce medios masivos de comunicación

FIGURA 2 . ORGANIZACIÓN DEL COMANDO DEL ESPACIO DE INFORMACIÓN Y CIBERDEFENSA



Fuente: Das Führungsunterstützungskommando der Bundeswehr 2013-2017 (p.290)

Uno de los aspectos más relevantes del comando es que conduce 3 elementos, el primero es el Comando de Inteligencia Estratégica, el segundo es el Comando Técnico de la Información y finalmente el tercer elemento es el Centro de Geoinformación.

compuesto por personal autóctono de Afganistán, como es la multimedia Bayan Shamal Mediencenter in Mazar-e Sharif[5].

El tercer elemento del Comando de Inteligencia Estratégica es el Centro de Evaluación de Guerra Electrónica. Esta organización es responsable de analizar, identificar, evaluar y registrar toda información relacionada con el espectro electromagnético. Además, tiene como tarea el control técnico sobre los 4 batallones de guerra electrónica. Con respecto a los mencionados batallones, su misión es proporcionar apoyo de guerra electrónica. Sin embargo, cada uno difiere conforme a su misión. Algunos tienen capacidades ofensivas y defensivas de guerra electrónica, tanto en el espectro electromagnético terrestre, naval o aéreo. Otros batallones poseen estaciones fijas de guerra electrónica y todos tienen elementos móviles de guerra electrónica.

Otro elemento perteneciente al Comando de Inteligencia Estratégica es el Centro de Imagen de Inteligencia. Esta organización debería formar parte del Centro de Información de las FFAAA, pero la diferencia radica en que no solo produce información de imágenes satelitales sino que es un centro de interpretación de imágenes. Emplea medios como el radar de reconocimiento SAR-Lupe[6] de las FFAAA, el sistema francés Helios II y productos satelitales del Centro Europeo de Satélites.

La siguiente organización es la Escuela de Inteligencia Estratégica de las Fuerzas Armadas, cuya misión es la formación y perfeccionamiento de los soldados alemanes en el área inteligencia. El último elemento es el Centro de Investigación de Inteligencia Técnica cuya competencia es desarrollar nuevas capacidades técnicas en el espectro electromagnético.

Centro de Geoinformación

Este organismo tiene más de 50 años de experiencia. Su misión es obtener, preparar, actualizar y proporcionar no solamente informes meteorológicos o cartas topográficas a las Fuerzas Armadas, sino también información en los campos de biología, etnología, teledetección, geodesia, geoinformática, geología, geofísica, geopolítica, hidroacústica, hidrografía, hidrología, cartografía, climatología, meteorología, ecolo-

3. Command, Control, Communications, Computers, Intelligence, Information, Surveillance, and Reconnaissance (comando, control, comunicaciones, computación, inteligencia, información, vigilancia y reconocimiento).
4. https://www.radio-andernach.bundeswehr.de/
5. https://www.facebook.com/Bundeswehr/posts/731725646892030
6. https://cir.bundeswehr.de/portal/a/cir/start/dienststellen/ksa/zabbaufkl
7. https://cir.bundeswehr.de/portal/a/cir/start/dienststellen/zgeobw

cv

PABLO ALEJANDRO CAÑETE

El Mayor Pablo Alejandro Cañete egresó como Subteniente del Arma de Comunicaciones en el año 1999 y pertenece a la promoción 130 del CMN. Es Oficial de Estado Mayor y Licenciado en Matemática Aplicada. Posee la Aptitud Especial de Capacitación Antártica. Realizó el Curso de Capacitación del Espectro Electromagnético en Francia (Paris). Actualmente está cursando la Escuela de Guerra en la República Federal de Alemania (Hamburgo).

En Alemania hay una verdadera concientización en lo que respecta a ciberseguridad, confían en la seguridad de su red y si hay que esperar porque el sistema operativo lo demanda, utilizan un refrán breve y contundente: "hasta los comandantes esperan".

gía, oceanografía y fotogrametría[7]. Este Centro trabaja conjuntamente con el Servicio Meteorológico Alemán y su comandante es un general de 1 estrella.

Comando Técnico de Información

Su misión es proporcionar apoyo de comunicaciones, informática y ciberoperaciones defensivas a las FFAAA. Su comandante es un general de 2 estrellas y posee 5 organizaciones.

En la Figura 2, de izquierda a derecha, se visualiza en primer lugar al Centro de Sistemas Técnico de Información. Este administra todas las facilidades de comunicaciones e informática de las FFAAA. Es el nexo directo entre los proveedores de tecnología de información y comunicación (TIC) privados y las Fuerzas armadas. Además, gestiona la asignación de frecuencias y anchos de banda para los enlaces satelitales requeridos en cada operación, asigna frecuencias en las bandas militares a todos los elementos de las FFAAA. Con respecto a los proveedores privados TIC, estos conforman una sociedad privada llamada BWi[8]. Esta empresa es la proveedora directa de servicios TIC para las FFAAA y está compuesta por empresas relevantes tales como Siemens, IBM y Telecom, entre otras. El mencionado Centro de Sistemas administra también los telepuertos satelitales y monitoriza los satélites militares Satcom Bw-1 y Satcom Bw-2 que poseen las FFAAA.

El segundo elemento que forma parte de este comando es el Centro de Ciberseguridad de las Fuerzas Armadas. Su misión es ejecutar operaciones de ciberdefensa pasivas. El Centro de Ciberseguridad posee 2 departamentos y 3 grupos, como puede verse en la Figura 3. El departamento de operaciones planifica y conduce las operaciones de ciberdefensa pasivas de las FFAAA. El departamento *Cyber Security Operations Center* (CSOC) ejecuta la vigilancia, observación, analiza los riesgos de las ciberamenazas y conduce el *Computer Security Incident Response Team* (CSIRT) de las FFAAA.

El Grupo Protección y Prevención realizan actividades y tareas para fomentar la concientización de la seguridad a los usuarios de las redes informáticas de las FFAAA, y es el responsable de estandarizar las técnicas de ciberdefensa y protege los sistemas de armas de las Fuerzas Armadas.

En este punto es necesario destacar algunos aspectos cuya relevancia contribuye a la ciberseguridad de una gran organización como son las Fuerzas Armadas.

En primer lugar, el sistema operativo que emplean las FFAAA es Windows de Microsoft. La herramienta que usan es *Office*. Todos los software son originales y han adquirido la licencia para su uso. Además, está prohibido el empleo

FIGURA 3 . ORGANIZACIÓN DEL CENTRO DE CIBERSEGURIDAD DE LAS FUERZAS ARMADAS ALEMANAS

en los puestos de trabajo de computadoras personales. Las mismas son provistas por las Fuerzas Armadas y solo pueden ser instalado *software* y aplicaciones autorizados. Está terminantemente prohibido el uso de memoria externa tipo USB (*pendrive*) o el empleo de discos duros externos. En los puestos de trabajo, la conexión a intranet o Internet es a través de conexión alámbrica, o sea por cable UTP/STP *(Unshielded Twisted Pair)/(Shielded Twisted Pair)*[9]. Además, en lugares como sala de reuniones, aulas u oficinas con clasificación de seguridad relevante, existen inhibidores de señal de telefonía celular.

En efecto, hay una verdadera concientización en lo que respecta a ciberseguridad. Se imparten innumerables instrucciones y presentaciones en unidades militares y particularmente en la Escuela de Guerra alemana. No se pueden detectar civiles, soldados, suboficiales, oficiales ni siquiera comandantes de más de 1 estrella que vulneren por ejemplo la seguridad a través del uso de un *pendrive*. Todos sus trabajos o presentaciones están en intranet. Confían en la seguridad de su red y si hay que esperar porque el sistema operativo necesita reiniciarse o porque la red está un poco lenta para bajar una presentación de *power point* por ejemplo, el *slogan* es breve y contundente: "hasta los comandantes esperan". Ordenadores provistos, licencia de *software* adquirida, conectividad alámbrica, prohibición de *pendrive* o discos duros externos, inhibidores de señal de telefonía celular en áreas sensibles de información y, por sobre todas las cosas, concientización sobre la seguridad informática. Esas son las bases de la ciberseguridad.

El Grupo Seguridad y Acreditación forman parte también del Centro de Ciberseguridad. Esta pequeña organización es responsable de acreditar y asesorar en lo concerniente a seguridad informática y proyectos TICs. Es el organismo nexo entre las FFAAA y las industrias TICs en materia de seguridad informática. Por último, el Grupo Control y Apoyo ejecuta pruebas de penetración y da seguridad en las redes.

El Comando Técnico de Información conduce 7 batallones de Comunicaciones, de los cuales 6 son conjuntos y 1 combinado en apoyo a las fuerzas de la OTAN. Los mencionados elementos proporcionan apoyo de comunicaciones e informática a los elementos desplegados fuera del territorio de Alemania, por ejemplo contingentes de la OTAN, la UE u ONU. Eventualmente, podrá proporcionar apoyo a las divisiones del ejército alemán o a otros elementos de otras Fuerzas Armadas. Es necesario resaltar que las 3 divisiones del ejército alemán tienen su elemento de comunicaciones dentro de sus formaciones y además, cada brigada posee en su orgánica una compañía de comunicaciones. Otro aspecto relevante es que los mencionados batallones son conducidos por el segundo comandante del Comando Técnico de Información y no por su comandante.

En nuestra estadía, hemos visitado el batallón de Comunicaciones 282 ubicado en Kastellaun (Renania del Norte) y el batallón de Comunicaciones 293 situado en Murnau (Baviera). Los batallones normalmente están organizados por 5 compañías. Difieren mínimamente en su estructura, pero en general cuentan con una compañía de redes locales, de comunicaciones satelitales, radioeléctrica, de comunicaciones troncalizadora (facilidad radioeléctrica de *trunking*) y una compañía comando y servicios que no posee elementos de sanidad porque lo proporciona el Servicio de Sanidad de las FFAAA, tal como se explica en la Figura 1. En general las mencionadas compañías tienen similares misiones, funciones, actividades y tareas de acuerdo a lo especificado en la doctrina de la OTAN.

Con respecto a la cultura de la organización, es importante resaltar que los batallones están compuestos por personal de las 3 Fuerzas Armadas. Por ejemplo, el jefe de batallón puede ser del Ejército y su segundo jefe o el oficial de operaciones (S-3) de la Fuerza Aérea o de la Armada. La integración del personal culturalmente está totalmente asimilada.

El Centro *Software* de las FFAAA es otra organización del comando técnico de información. Este elemento desarrolla, prueba, controla e integra *software* de gestión, operación y simulación de las Fuerzas Armadas. Trabaja en conjunto con el organismo federal de equipamiento, tecnología e información y empleo para las FFAAA, en proyectos como HaFis (*Harmonisierung der Führungsinformationssysteme*). Es un proyecto para integrar el sistema C4I2SR de las FFAAA que sea a la vez interoperable con el sistema de la OTAN y con algunos sistemas para misiones de la UE y de la ONU. El centro Software trabaja con la licencia del *Virtual Battle Space,* que es una simulación con armamentos y procedimientos de la FFAAA, ambientado en escenarios reales tales como Afganistán (misión de la OTAN) o MALI (misión de la ONU). El Centro certifica además todos los *Software* que emplean las FFAAA.

La última organización del comando es la Escuela Técnica de Información. Es el centro de capacitación del personal de las Fuerzas Armadas relacionado con comunicaciones, informática, ciberdefensa y guerra electrónica. Actualmente, está emplazada en Feldafing, pero el siguiente año será trasladado a sus nuevas y modernas instalaciones en Pöcking. Ambas ciudades se sitúan en Baviera.

El Kdo CIR, a través de escuela de formación y perfeccionamiento, ha

8. https://www.bwi.de
9. Par trenzado apantallado/Par trenzado blindado.

Es necesario resaltar que las tres divisiones del ejército alemán tienen su elemento de comunicaciones dentro de sus formaciones y además, cada brigada posee en su orgánica una compañía de comunicaciones.

realizado acuerdos con firmas privadas de TICs para que el personal de suboficiales y soldados realice un curso de especialización en TICs en solo 21 meses. Al término del curso, los suboficiales son certificados para trabajar en cualquier empresa de TICs cuando finalicen su carrera militar. Es importante resaltar este aspecto porque la capacitación técnica en Alemania dura normalmente 3 años. Es una buena motivación para el ingreso de personal a las FFAAA. La escuela recibe anualmente un promedio de 7.000 cursantes de las FFAAA y dictan, aproximadamente 170 cursos.

Conclusiones finales

El Kdo CIR no es una Fuerza Armada, sino un comando conjunto que posee innumerables capacidades, una de ellas es la ciberdefensa. El comando cuenta actualmente con un efectivo de más de 14.000 militares y civiles y prevé arribar al año 2022 con alrededor de 15.000, o sea aproximadamente la misma cantidad de efectivos que la Armada alemana.

El Kdo CIR planifica, organiza y conduce los apoyos de comunicaciones, informática, guerra electrónica, inteligencia, ciberdefensa (operaciones defensivas y ofensivas), operaciones psicológicas y geoinformación de las Fuerzas Armadas alemanas para proporcionar capacidades de C4I2SR a las misiones en el exterior (OTAN, EU u ONU) o ante la necesidad particular de alguna Fuerza Armada en la República Federal de Alemania.

En lo concerniente a educación, este comando es responsable de la capacitación no solo del área de ciberdefensa sino también de comunicaciones, informática, inteligencia y guerra electrónica de las FFAAA. Con respecto a la cultura de la organización, la integración del personal de las tres Fuerzas Armadas lo tiene totalmente asimilado.

El Kdo CIR es un claro ejemplo del principio de la conducción denominado integración, permite lograr la mayor interoperabilidad de sus medios (personal y material) a través de la integración de las capacidades de comunicaciones, informática, inteligencia, guerra electrónica, ciberdefensa, operaciones psicológicas y geoinformación en sus Fuerzas Armadas. Mientras que en algunas Fuerzas Armadas de otros países continúan aun debatiendo si las operaciones de ciberdefensa son de la competencia de comunicaciones, de informática o inteligencia, sin embargo, el Kdo CIR las ha integrado.

En las guerras actuales, las Fuerzas militares se caracterizan por contar con elementos pequeños, rápidos, autosostenibles e interoperables con un moderno sistema C4I2SR. El Kdo CIR ha cumplido con uno de esos requisitos y es por ello un claro ejemplo de integración. ▮

AGRADECIMIENTOS

General de División (R)
Evergisto de Vergara
–
Brigadier Mayor
Alejandro Moresi
–
Teniente Coronel
Jürgen Nehring
–
Teniente Coronel
Jan Wilheine
–
Mayor (R)
Alejandro Corletti
–
Mayor
Oscar Gómez

EL FACTOR MILITAR COMO MEDIO DE PREVENCIÓN PACÍFICA DE CONFLICTOS

Por **CR (R) EDUARDO CUNDINS**

Palabras Clave:
> Cooperación
> Controversia
> Paz
> ONU
> Guerra
> Disuasión

Resumen
El autor propone una perspectiva paradójica para analizar la evolución del fenómeno bélico que afectó al sistema global en el siglo XX y que alcanzó su paroxismo en la incapacidad de revertir la lógica guerrera como único modo para la solución de diferendos.

Los dilemas y debates de las Relaciones Internacionales entre el realismo más beligerante y el cooperativismo más kantiano descubrieron en el instrumento militar el medio de acercamiento y la confianza que refuerzan las políticas exteriores y de defensa.

Introducción
El hoy habitual apretón de manos que simboliza cercanía o amistad, (*shaking hands* en inglés) proviene de un gesto inequívoco de "indefensión deliberada" ofrecido mutuamente como prenda de cercanía, en el cual dos personas construyen un entendimiento. Reconocido como el rito social por excelencia, poco haría suponer que su origen hunde sus raíces en el hecho bélico.

Si bien 4.000 años nos acercan al gesto de los monarcas babilónicos para con su dios Marduk (idolatrada escultura) en señal de sumisión, el acto fue seguido por asirios y romanos, pero fundamentalmente por los griegos, que dieron al "uso de la daga"[1] el accesorio inseparable de viajeros; el arma añadía seguridad a las travesías solitarias en tan desoladas vastedades.

Ofrecer la mano desarmada, la que empuña la daga o la espada, induciendo a esa reciprocidad al desconocido para parlamentar, daba lugar a la palabra que simboliza confianza y, por tanto, ausencia de agresión. Suponía la asunción de un riesgo que, una vez superado, permitía construir cercanía, afinidad, acuerdo... eventualmente alianza[2].

Esta vinculación física gestual fue una primera aproximación para concretar la finalidad y no el objetivo de las disputas por la

1. OLIVER, A. Anfrix. Disponible en: *https://www.anfrix.com/2006/09/la-curiosa-historia-de-saludar-con-un-apreton-de-manos/*
2. Imágenes de Atenas y Hera (Hera and Athene (5th c. BC, Acropolis Museum, Athens). Obtenida en *https://alison-morton.com/2015/04/22/roman-forearm-handshake-true-gesture-or-hollywood-codswallop/*
(The 'Roman' handshake - Photo courtesy of Caroline Lawrence's Pinterest account).

ARTÍCULO CON REFERATO

La construcción de paz puede iniciarse a partir de gestos en el terreno orientados a la implementación de acercamientos, entendimientos y confianza recíproca, sobre todo por parte de las organizaciones a las que les corresponde encabezar la disputa y dirimir los diferendos y las controversias.

vía de la violencia: la definitiva convivencia en paz, en amistad y en armonía que debiera definir la coexistencia entre los pueblos. Le sucederá "el parlamento", la palabra que acuerde los entendimientos en una gimnasia de aproximaciones sucesivas, respeto, renuncias y reclamo de intereses. Un jurista argentino (Mariano Grondona)[3] afirma que existe justicia cuando ninguna de las partes se halla plenamente satisfecha con el fallo alcanzado. La justeza del reparto[4] (en sentido goldschmidtiano) debe superar esa prueba.

La guerra es un hecho político definido en su decisión de inicio y en los acuerdos ulteriores de rendición, armisticio o convenio que sella la suerte de las armas.

La convenida disputa para dirimir los intereses contrapuestos con costo de sangre y sacrificios superlativos puede, muchas veces, acotarse a soluciones inesperadas; burbujas culturales, entrópicas y viciadas de prejuicios que solo atinaron a encontrar en el duelo mortal del fallo definitivo. Un reduccionismo belicoso inconducente.

Si bien el objetivo de la guerra, ese duelo clausewitziano, supone imponer la voluntad a un enemigo "cooperativo"[5] en el que ambos apelan a una violencia formalizada, acordada y protocolizada, su finalidad última no es otra que la de acceder a un estadio de no beligerancia ulterior honrosa y plausible, es decir, mutuamente beneficiosa. Claro está que los umbrales de tolerancia y asimilación de una "paz honrosa" no ha sido la norma en el siglo de las Guerras[6], ante la también patológica inclinación a la guerra permanente como condición "excelsa" de una virtud de valores ultramontanos. Este umbral será definido por la política.

El paroxismo de las conflagraciones como verdadero "flagelo para las generaciones futuras", que resalta el artículo primero de la carta de las Naciones Unidas (ONU), desnudó la supina incapacidad humana para desembarazarse de la lógica bélica que signó el siglo XX.

Desde el fracaso de la Sociedad de las Naciones hasta la fracasada imposición de la "impracticabilidad de la guerra" o, la inaceptabilidad del uso de la fuerza que reclama el artículo 42 de la Carta de San Francisco de 1945, opera en un sentido restrictivo cuando los países, fundamentalmente periféricos, intentaron recurrir al empleo del medio militar para dirimir sus contenciosos que maduraron en "la conquista del poder a través del conflicto armado"[7], librado en la periferia global que aliviaba el peso conflagratorio de las potencias amenazadas por la propia lógica de la destrucción mutua asegurada (MAD por sus siglas en inglés) nuclear. Un mundo dividido.

De ello se desprende que la construcción de paz no provenga indefectiblemente de un fallo político adoptado en el ápice de la decisión estratégica estatal, el de la conducción política del poder central, sino que también puede iniciarse a partir de gestos (*en el terreno*) orientados a la implementación de acercamientos, entendimientos y confianza

3. Grondona Mariano. (1993) "Hora Clave" a Programa Televisivo (Canal 9) Min 52:27 a 55:24 Disponible en https://www.youtube.com/watch?v=GyOBP-J2yaM Consultado 30/06/2020 07:57 p.m.

4. Goldschmidt, Werner (2005) *"Introducción filosófica al Derecho"* ISBN: 9789875920088. Editorial: LexisNexis S.A. Buenos Aires. Pág.: 27

5. Bartolomè, Mariano (2009). *"Los conflictos intraestatales y el empleo de la fuerza"*. Disponible en *http://old.revistas.unlp.edu.ar/RRII-IRI/article/view/1332/1295*

6. Kolko, Gabriel. (2005). *El siglo de las guerras: política, conflictos y sociedad desde 1914*, Paidós Ibérica, 2005.

7. Brieva Felgueras, Viacava. 2004 *"La trinidad de Clausewitz en la Guerra Revolucionaria"*, Roberto Brieba, Juan Carlos Felgueras, José Francisco Viacava. Disponible en *https://revistamarina.cl/revistas/2004/6/brieba.pdf*

8. Tandurella, Alberto. Extracto de la clase dada el 16 de marzo de 2004 por el profesor Tandurella en la Maestría en Defensa Nacional de la Escuela de Defensa Nacional, Argentina.

9. Morin, Edgar (1994) *"Introducción al pensamiento complejo"*. Ed Gedisa. Pag 168

10. Llanos Villanueva, Luz Amparo. "Las Operaciones de Paz de Naciones Unidas. Una mirada desde el realismo político de las relaciones internacionales. Las políticas de defensa y exteriores de Argentina, Chile y Perú en la misión de las Naciones Unidas en Haití". Tesis Doctoral no publicada. Universidad de Santiago de Chile. Instituto de Estudios Avanzados Facultad de Humanidades. Santiago de Chile, 2012.

recíproca, sobre todo por parte de las organizaciones a las que les corresponde encabezar la disputa y dirimir los diferendos y las controversias. Tributarios e imbuidos por los objetivos dictados por la conducción política, la finalidad perseguida converge en la construcción de puentes de convivencia aunque respaldados por organizaciones concebidas para la disputa. Cooperación en la competencia. Unidad en la diversidad. Entendimiento en la diferencia sumando identidad entre los factores de la trinidad clausewitziana: pueblo, gobierno y milicia.

Poderíos y convivencias afectadas. Sucesivos paradigmas

A lo largo de los períodos históricos, el poder y la riqueza de las naciones fueron identificados por factores cuya valoración y preponderancia era generada por el interés específico del Estado de acuerdo al paradigma prevalente. Especialmente, a partir de 1648 con Westfalia en el que los estados nacionales comienzan a definir sus fronteras y dominios, diferenciando el régimen gubernativo y las rivalidades ante el roce de intereses superpuestos con sus pares estatales.

En el siglo XVI fueron los metales preciosos el factor predominante que, según la corriente mercantilista, identificaban la riqueza y el poderío de las naciones. Ya en el siglo XVIII fue la posesión de minerales, la agricultura y la pesca (los recursos naturales en general) que suplantaron la piedra de toque anterior. De esta matriz productiva devino que la magnitud del territorio constituía un aspecto trascendental para una mayor disponibilidad de recursos, lo cual resultó un asunto de Estado.

Con la Revolución Industrial se dieron las condiciones para la explotación de materias primas y la demanda de productos primarios o *commodities*, que incitaron a aventuras militares de conquista en el mundo periférico: el ajeno a los poderes centrales del hemisferio norte.

Posteriormente, sobrevendrían "activos" (fortalezas, valores) más "blandos" como lo son la capacidad tecnológica y el *knowfare* que suplantaron la fórmula de poder que respondía a una ecuación algebraica de factores tangibles, entre otros, población, superficie y desarrollo industrial, para brindar una resultante del poder[8] de la nación. Del hardware al software y de este al *knowfare*.

Claro está que el choque de intereses generaba disrupciones que inducían su consecución mediante el empleo de los medios militares, aspecto que cobró su máxima expresión en el pasado siglo con las conflagraciones mundiales que llevaron a la humanidad al escarnio y al flagelo de guerras de gran magnitud. Cabe también destacar que además se suscitaron vinculaciones, afinidades, alineamientos, o directamente, alianzas y acuerdos que procuraron la obtención de objetivos compartidos mediante la construcción de mecanismos de asociación o trabajo por afinidad. El **neofuncionalismo** sostenido por Immanuel Wallerstein alienta con algunas semejanzas, a la interdependencia compleja de Robert Kehoanne y Joseph Nye y la experiencia europea de la integración compleja, la descripción que la relación interestatal no es una simple conexión de tipo neuronal, sino múltiple y compleja (en términos de Morin)[9], una interdependencia multilateral en planos superpuestos y simultáneos. Dos Estados pueden tener fuerte relaciones comerciales aunque severas diferencias políticas, alentar acuerdos migratorios divergentes y asociarse en foros culturales regionales.

Por neofuncionalismo se entiende una escisión del institucionalismo liberal que aboga por concretar procesos de integración cuya finalidad última no es otra que el mantenimiento de la paz entre los Estados: principal objetivo de la Disciplina de las Relaciones Internacionales. Esta visión, aparentemente irreconciliable (integración y cooperación por un lado, y competencia y antagonismo por otro), encuentra en el trabajo de la doctora Amparo

Llanos Villanueva un nuevo giro sorprendente, pues sostiene en su tesis[10] que la participación nacional en misiones de mantenimiento de la paz responde a la vertiente realista de las relaciones internacionales dado que apela a la herramienta militar en procura de satisfacer sus intereses nacionales, sintagma que podría ser refrendado por autores del más puro pensamiento realista como Hans Morgenthau[11] que asocia interés nacional con poder, Kenneth Waltz[12] o el propio John Mearshheimer[13] defensor del "realismo ofensivo". La cita sorprende dado que toda la vertiente de los autores realistas de las Relaciones Internacionales asocia la noción de poder a la del empleo agresivo y ofensivo de la herramienta militar estatal (en un mundo anárquico y sin orden) que es diametralmente opuesta a la de una visión liberal y cooperativista (¿kantiana?), no competitiva, que (naturalmente) identifican a las misiones humanitarias de paz.

Claro está que este postulado se da de bruces con la visión contrapuesta de Mearshheimer que sostiene un realismo basado en el poder militar por el cual no existiría posibilidad alguna de convivencia que no sea competitiva y, por lo tanto, el tablero internacional debiera ser interpretado como un campo de batalla en el que la anarquía y los intereses nacionales solo quedarían atenuados por el juego de competencias que, a la vez que proyecten poder, beneficiaran la "salud del Estado" por sobre los restantes rivales, para concluir (en la página 138) que "el poder militar tiene una base económica"[14]. Una síntesis superadora de estas dos visiones -liberal y realista-, es conjugada por la Escuela Inglesa de Martin Wight, que orienta sus investigaciones en una saludable convergencia que atenúa las expresiones extremas mutuamente excluyentes.

Fue así que ese "Siglo de Guerra Total" que imprimió cambios en las estructuras sociales y, por ende, alteró las formas de vida tradicionales[15] en las matrices productivas, conllevó al seno de las sociedades el conflicto interno con un enemigo conviviente.

El propio Pacto de la Sociedad de las Naciones de 1919, sus precedentes y los posteriores acuerdos remitían a la inevitabilidad de la beligerancia y, en su defecto, postulaban cómo paliar o contrarrestar los efectos devastadores de las acciones bélicas, el propio ejercicio del gobierno en las zonas sometidas a control militar (tras una invasión) y cómo contrarrestar la suerte de los combatientes; como se puede apreciar era la imposibilidad, la impracticabilidad de la paz; una grave burbuja cultural que no supo concebir otra solución para el arreglo de las controversias interestatales. Sobrevendrían, pues, la Cruz Roja Internacional y sus sucedáneas, los convenios de

El llamado "Siglo de Guerra Total" imprimió cambios en las estructuras sociales y, por ende, alteró las formas de vida tradicionales en las matrices productivas, conllevó al seno de las sociedades el conflicto interno con un enemigo conviviente.

Ginebra de 1949 y, paralelamente, las acciones que intentaban morigerar los efectos, aunque no las causas de las conflagraciones.

El caso argentino

La República Argentina ha sido pionera en iniciativas de paz; en particular, en el período de entreguerras del siglo XX. La experiencia sufrida en el desmoronamiento de los 14 puntos kantianos del presidente Wilson asumiendo que la propia potencia victoriosa no respaldará a su presidente sumado a la inacción e inefectividad de la Sociedad de las Naciones -constituida más como un tribunal inquisidor europeo, administrador de puniciones a los injuriados y menoscabados derrotados- contribuyó con la cimiente dada en llamar la continuación de la Primera Guerra Mundial. "Europa se suicidó por medio de una guerra dividida en dos"[16], frase adjudicada al español, Juan Slava Galán, quien aseguraba que "la Segunda Guerra Mundial fue una continuación de la primera".

Esa actitud precursora desde "el fin del mundo" (al decir de S.S. Francisco) se concretó en iniciativas galardonadas con la presea de la Paz en 1936 y en 1980. El canciller argentino, Carlos Saavedra Lamas condujo con sagacidad y astucia la acción de "pinzas", una maniobra de doble modalidad que aseguró el éxito consumado en la firma de la paz de los estados beligerantes hermanos: Paraguay y Bolivia. Esa maniobra "envolvente" apeló al empleo de la diplomacia en los foros, y simultáneamente, al factor militar en el terreno de las operaciones, asegurando la efectiva conjunción del pensamiento y la acción que Bergson completaría con su exquisita frase[17]: "Pensar como hombres de acción y actuar como hombres de pensamiento".

Sin las conferencias panamericanas simultáneas y las concebidas para reforzar el seguimiento e imponer el interés internacional de los países involucrados nada podría haberse logrado si no se hubiera contado con el concurso de la Comisión Militar Neutral, que en el terreno de Villamonte convalidara y respaldara las decisiones sobre la diplomacia adoptaba en salones y conferencias.

La "Comisión Internacional de Mediación" integrada por Brasil, Chile, Perú, Uruguay y Estados Unidos, que garantizó el armisticio del 12 de junio de 1935, puso fin a la Guerra del Chaco". Se concretó en Buenos Aires mediante la firma del Protocolo de Paz entre Paraguay y Bolivia", el 9 de junio del mismo año.

Fue así que el 14 de junio de 1935 arribó a Villamontes, en el corazón del Teatro de las Operaciones, la "Comisión Militar Neutral" integrada por los mismos países, pero con el concurso de ejecutivos militares se aseguraba el definitivo cese de las hostilidades.

En honor a la verdad, la recepción de un Segundo Premio Nobel de la Paz[18] no hace más que confirmar la mutación antes descripta y hoy confirmada sobre la naturaleza de

10. Llanos Villanueva, Luz Amparo. "Las Operaciones de Paz de Naciones Unidas. Una mirada desde el realismo político de las relaciones internacionales. Las políticas de defensa y exteriores de Argentina, Chile y Perú en la misión de las Naciones Unidas en Haití". Tesis Doctoral no publicada. Universidad de Santiago de Chile. Instituto de Estudios Avanzados Facultad de Humanidades. Santiago de Chile, 2012.

11. Morgenthau, Hans. *Política entre las Naciones. La lucha por el poder y la paz,* Edit. GEL, traducción de Heber Olivera. Buenos Aires, 1986.

12. Waltz, Kenneth. *El hombre, el estado y la Guerra.* Ed. Nova, Buenos Aires, páginas 93-138, 177-206 y 247-262, 1970.

13. Mearsheimer, John, *The Tragedy of Great Power Politics,* W. W. Norton & Co. Nueva York, 2001.

14. Mearshheimer. Op. Cit., 2001.

15. Aron, Raymond. *Un Siglo de Guerra Total.* Editorial Rioplatense, traducción capitán (RE) L. E. Pérez Roldán, Buenos Aires, página 126, 1973.

16. Slava Galán, Juan. "Testimonios". Disponible en: *https://ejercitotierra.wordpress.com/2014/10/23/juan-eslava-galan-escritor/ Subido por Blog Oficial del Ejército de Tierra Español. Fecha de la Consulta 2014*

17. Rovira-Reich, Ricardo (2011) "El buen gobernante en la antigüedad clásica Indagación de un enfoque sapiencial en Plutarco" Extracto de la Tesis Doctoral presentada en la Facultad Eclesiástica de Filosofía de la Universidad de Navarra Pamplona Recuperado en https://www.academia.edu/5496528/EL_BUEN_GOBERNANTE_EN_LOS_MORALIA_POL%C3%8DTICOS_DE_PLUTARCO

18. En la persona de Adolfo Pérez Esquivel.

La participación en misiones de paz constituye un factor importante en la consecución de los objetivos perseguidos por las políticas de Defensa y de Exterior de los países que poseen bajos presupuestos de defensa.

CV

EDUARDO CUNDINS

Doctor en Relaciones Internacionales (USAL). Licenciado en Estrategia y Organización. Magíster en Estrategia y Geopolítica. Director del Centro de Estudios de la Defensa y la Integración Regional y Columnista del IEERI del Círculo de Legisladores de la Nación. Graduado 2014 del Curso SDP del CHDS. (Washington D.C.-Estados Unidos). Miembro del CARI (ISIAE). Director del Programa de Radio/multimedio "Cascos Azules. Argentinos por el mundo" Observador en el Sahara Occidental (1991) MINURSO, Jefe del Departamento Humanitario en la Misión de las NNUU en Chipre (98-99) UNFICYP, Jefe del Equipo de Negociación ante ONU por el despliegue inicial de la Contribución Argentina en Haití 2004 (MINUSTAH). Actualmente se desempeña como Jefe de Departamento de Cursos Extensión Universitaria del CEFFAA.

conflictos que abandonarán la esfera internacional para instalarse en la intraestatalidad o la No-Estatalidad, flagelo que se ha materializado en un crecimiento de los conflictos armados de la segunda mitad del siglo XX. Una nota más simbólica lo constituye la participación junto con otros 34 países en la presea de la paz recibida por el peruano Pérez de Cuellar, secretario General de la ONU en 1988 en nombre "Del Personal de Paz de las Naciones Unidas" en la cual, Argentina, también le cupo participar.

Ingeniería inversa

Se desprende que nadie mejor para intervenir en la guerra que el soldado, aún a la hora de evitarla o atenuar sus consecuencias. De ello surge que el desafío es inclusive mayor, pues su matriz de actuación depende de una iniciativa cedida de antemano y, por lo tanto, concretada en la acción paliativa de su mitigación o en las instancias posteriores al advenimiento de la crisis: el posconflicto. Un sinnúmero de doctrinas (como la Capstone), aportes, informes (como el Brahimi del año 2000), la sistematización de lecciones aprendidas y mejores prácticas, iniciativas (como las *New Horizon* de 2010 y 2011) y reformas o recomendaciones como la reciente HIPPO (*High-level Independent Panel on Peace Operations*) han procurado articular y mejorar la calidad de las respuestas no siempre exitosas, como lo fueron los fracasos de Ruanda en 1994 y Sebrenika en 1995.

Argentina fue pionera en la construcción de afinidades o acercamientos a partir de contribuciones que permitieron, para mediados de la década del 90, desplegar contingentes en misiones de paz (al amparo de la ONU). Este empleo del instrumento militar obedecía al consenso generalizado de las transiciones democráticas sudamericanas no dispuestas a tolerar la acción pendular de interrupciones autoritarias al decurso democrático.

Dilema que admite semejanzas con las que ha debido afrontar España en su transición del régimen franquista, en 1975, y el cierre de contenciosos territoriales que podrían haber alentado el protagonismo del rol militar en su nueva instancia con los vestigios del irresuelto asunto del Sahara Occidental[19].

Con el incremento exponencial de las Misiones de Paz auspiciadas por las Naciones Unidas a partir de 1991, un renovado ímpetu de desmantelamiento de litigiosidad iluminó el terreno de las relaciones internacionales en la región. Aportaciones individuales u orgánicas de Brasil, Uruguay, Perú, Chile y Paraguay se sucedieron en una amalgama de identificaciones, afinidades y problemas o temas semejantes.

Surgía un nuevo desafío que permitiría la inserción comprometida de un Estado en el tablero mundial merced a sus aportes en esta globa-

lización y cercanía de los conflictos mundiales. Por entonces, se discutía que la "Argentina no es irrelevante estratégicamente por su ubicación geográfica, sino por su actitud hacia los desafíos que el mundo actual impone, se percibe a sí misma como un país aislado de los principales acontecimientos mundiales y por lo tanto se considera ajena a los hechos que a nivel internacional más preocupan, aunque simultáneamente, busca obtener de los principales países de occidente apoyo para superar su crisis económico-financiera. Al mismo tiempo, la condición de aliado extra OTAN que la Argentina logró en los años '90 como fruto directo de su más que ponderable participación en las fuerzas de paz de las Naciones Unidas... El Estado argentino, al demostrarse absolutamente incapaz de ejecutar políticas que accionen de alguna manera contra estos aspectos, hace que Estados Unidos orienten su interés por naciones que le parezcan más dispuestas a tomar políticas que contribuyan a crear un ambiente de seguridad en la región"[20].

Ese protagonismo del rol militar concebido como única solución para librar la disputa y para "librar" al político de la toma de decisiones medulosas fue reconvirtiéndose en nuevas orgánicas, magnitudes y funciones que apelaban a una suerte de ingeniería inversa, en herramientas de integración a lo internacional sin por ello, abandonar definitivamente sus capacidades disuasivas y letales para encarar operaciones militares.

Luciana Micha[21], ex funcionaria ministerial del área, sostiene que en las misiones de paz convergen una función disuasiva y cooperativa dado que al militar que le toca desenvolverse en roles de cargos ejecutivos y de asesoramiento en los *staff* internacionales, compite en una suerte de "soft disuasión" y, simultáneamente, colabora con sus pares en el ejercicio del mandato humanitario que, al decir del papa Francisco, consisten las "Misiones Humanitarias de Paz y Reconciliación".

Existe una causalidad no-lineal en estos acercamientos. En algún caso, producto de dificultades taxativas como lo fue la crisis argentina de 2001, que puso en riesgo el compromiso de sostener la contribución nacional ante las Naciones Unidas para solventar los costos de los contingentes nacionales desplegados y,

19. NdA: percíbase la connotación de tan delicado tema, toda vez que el desafío del Presidente del Gobierno Adolfo Suárez a partir de 1976 y del Presidente Argentino Raúl Alfonsín que debieron transitar la transición de regímenes autocráticos a la "era democrática" suponía desmantelar o minimizar el rol de los militares en uno y otro estado.

20. Fraga, Rosendo, *"Argentina y la irrelevancia estratégica"*. Editorial Oct-09-02. Comisión de Defensa del Centro de Estudios Nueva Mayoría. Disponible en: *http://www.nuevamayoria.com/ES/INVESTIGACIONES/defensa/021009.html 2002*

21. MICHA, Luciana. Cuaderno "La participación argentina en misiones de paz - Lecciones aprendidas". La Experiencia Argentina en Misiones de Paz. Una Visión Integrada. Número 3-2004 CARI. 2004.

por ello, se optó por el ofrecimiento bajo el aspecto de una apertura inducida a países de la región para robustecer las políticas de fortalecimiento de las medidas de confianza mutua, de aproximación y mecanismos de integración regional que se gestaban en la región. No obstante, existen antecedentes de otros países que poseían menos experiencia en estas misiones y que, de algún modo, el ofrecimiento del *"laboratorio Chipre" (UNFICYP)* se constituyó en virtual escuela, en la que fueron integrándose países tales como Uruguay, Chile, El Salvador (luego suspendido), Perú, Paraguay y hasta se estuvo a punto de concretarlo con el Reino de España.

Otro sólido intento de acercamiento extra continental lo constituyó el "Grupo de Trabajo Multinacional Iberoamericano" que, a iniciativa del Ministerio de la Defensa de España convocó a representantes del país anfitrión, Uruguay, Chile y Argentina para mayo de 2003. Contemporáneo al encuentro, se desencadenaban las operaciones de retaliación encabezadas por Estados Unidos y una coalición de países bajo el amparo preliminar de la resolución 1386 del Consejo de Seguridad de las Naciones Unidas de diciembre de 2001. Con el concurso de la OTAN (Organización del Tratado del Atlántico Norte) se constituyó la Fuerza Internacional de Asistencia para la Seguridad (ISAF por sus siglas en inglés: *International Security Assistance Force*). Sería imposible eludir lo acaecido entonces y conocido como **"el mayor accidente en la historia del Ejército Español",** con un saldo de 62 muertos, el traslado del primer batallón al mando del teniente coronel José Ramón Solar Ferro. Por entonces, producida la "reconciliación" de las potencias en el G8 y durante la reunión del 15 de marzo de 2003, de los máximos mandatarios de Estados Unidos (George W. Bush), Reino Unido (Tony Blair) y España (José María Aznar) en la Cumbre de las Azores, que luego se alegaría como causa del ataque del 11M en Atocha un año después[22]. Uruguay alistaba un batallón completo que desplegaría en Bunia, República Democrática del Congo en la que continúa siendo la misión desplegada de mayor magnitud: MONUSCO.

Los acontecimientos derivaron en la participación de España en Afganistán al amparo de la OTAN con el concurso de Honduras, Guatemala y El Salvador, que arrojó disímiles respuestas desde los países participantes y ajenos. Argentina finalizó un enriquecedor período de participación en la Misión de la OTAN KFOR[23], emanada del mandato de la UNMIK hasta que en 2006 por decisión unilateral del Ministerio de Relaciones Exteriores se decidió discontinuar.

Ha quedado demostrado que la participación en misiones de paz constituye un factor importante en la consecución de los objetivos perseguidos por las políticas de Defensa y de Exterior de los países que poseen bajos presupuestos de defensa[24].

La máxima expresión de integración puede ser considerada con el advenimiento de los mecanismos de interconsulta en los niveles

El desafío que afronta el actual profesional militar es superar los paradigmas de sucesivos espirales de violencia inédita, que lo impulsen a descubrir horizontes de participación continuamente superados, estimulándolo con renovada creatividad.

ministeriales que acompañaron el despliegue de los países miembros del MERCOSUR en Haití. En efecto, las convocatorias que, en mayo de 2005, condujeron a la "Reunión de Viceministros de Defensa de Argentina, Brasil, Chile y Uruguay sobre Haití "(2x4)" constituyeron la cimiente de una sólida conformación de lo que luego sería la UNASUR. La expresión "2 x 4" respondía a la identificación de "2 ministerios de 4 países". Sucesivamente, los representantes de Cancillerías y Ministerios de Defensa de los 4 países Latinoamericanos "Contribuyentes de Tropas a MINUSTAH (Haití)" generaban una agenda de trabajo que incluía, según Mendelson Forman (en Resdal 2007: 308), un sólido basamento de entendimiento "a la sombra" de los contingentes militares desplegados en el Caribe. Tales mecanismos, aumentados y perfeccionados llegaron a involucrar a 9 países (la base sustantiva de la UNASUR y Guatemala) de los 3 ministerios o carteras que atendían la gestión relaciones exteriores, defensa y seguridad: "3x9".

Conclusiones

Resta interrogarse qué prioridad se le adjudica a la paz, en la propia escala de valores de la sociedad argentina. Contradictorio o provocador, cabe la misma pregunta que excede lo meramente vocacional al profesional de la violencia en el universo conceptual militar. La propia "latencia"[25] de la función militar según Cruces, lleva consigo el deseo de evitabilidad de la guerra, el erróneo "anhelo" que sea su ocurrencia la que convalide y justifique aquella decisión que ha comprometido toda su vida, la vida del soldado magníficamente descripta por Calderón de la Barca[26]. La tentación antitética de alentarla desacreditaría la propia honorabilidad del soldado de todas las jerarquías, de todas las fuerzas, de todas las Patrias. Así como el filósofo de la guerra por excelencia advierte que "El supremo Arte de la Guerra es someter al enemigo sin luchar"[27], el desafío que afronta el actual profesional militar es superar los paradigmas de sucesivos espirales de violencia inédita, que lo impulsen a descubrir horizontes de participación continuamente superados, estimulándolo, con renovada creatividad, a superar los caminos transitados con el vertiginoso devenir de escenarios confusos, cambiantes e inciertos. ¿Quién sino el soldado deberá afrontar los riesgos?

Mientras tanto, el factor militar en los países centrales, en los que aún se manifiesta una "saludable" y equilibrada integridad de sus activos sociales, económicos, tecnológicos e industriales, convive aportando los respaldos que las políticas de Estado requieran. Sería redundante advertir la prevalencia que regímenes totalitarios y aun democráticos otorgan al sostenimiento de su andamiaje militar. Renovadas demostraciones misilísticas de alcance intercontinental, sumado a paradas militares (desfiles) imponentes, recurrencia profesional en emergencias catastróficas e inclusive desbordes de criminalidad inusitada, encuentran al uniformado atento siempre a nuevas demandas. Superar encuadramientos teóricos, ideológicos o atávicos no debiera demorar el necesario aggiornamiento a los nuevos

22. *http://www.elmundo.es/elmundo/2004/04/18/espana/1082310065.html*
23. *https://www.lanacion.com.ar/9912-los-argentinos-que-trabajan-por-la-paz-en-kosovo*
24. CUNDINS, Eduardo. Tesis "La participación militar en operaciones de mantenimiento de paz de Naciones Unidas y su relación con la política exterior y de defensa. Caso: Argentina en Haití período 2004-2014". Universidad del Salvador. Director de Tesis Dr. Mariano Bartolomé. Buenos Aires, 2017.
25. Cruces, Néstor: *Hacia otro ejército posible,* Sudamericana Planeta Editores, Buenos Aires, página 25, 1988.
26. Palau, José (2014) "Nacimiento de Pedro Calderón de la Barca, soldado e insigne escritor 17 de enero de 1600. "Aquí, la más principal hazaña es obedecer…" Publicado en *One Magazine* el 17 de febrero de 2014, Disponible en http://www.onemagazine.es/noticia/1473/historia/17-de-enero-de-1600.-aqui-la-mas-principal-hazana-es-obedecer tambien en *https://gradualhaterecords.bandcamp.com/track/los-soldados-del-rey*
27. González Camacho, Enrique Javier. *"El Arte de la Guerra"* de Sun Tzu. *http://www.gibralfaro.uma.es/criticalit/pag_1987.htm,* julio-septiembre 2015.

La guerra es un hecho político definido en su decisión de inicio y en los acuerdos ulteriores de rendición, armisticio o convenio que sella la suerte de las armas.

imperativos que el soldado de todas las guerras, de todas las épocas ha debido enfrentar sobreponiéndose a los esquemas prevalentes.

Un reciente suceso acaecido a principios de 2018, en el norte de Israel, en la localidad de Acre encontró al ya *habitual atentado jihadista* con vehículo ("Intifada de la embestida")[28] hiriendo a tres servidores israelíes: dos militares (soldados) y un policía. Tal episodio podría no concitar más atención a la debida por su desenlace no letal (lamentablemente tan habitual en Levante) aunque sí por su connotación subliminal: son **dos fuerzas de funciones diversas y finalidades diferentes** que se ven afectadas por un mismo vector de agresión violenta. Tal simbiosis que encuentra su correlato "latino" en el empleo de "Fuerzas Intermedias" o de "Policía Militar" como en las favelas cariocas se ve taxativamente impedido por el aquí denominado "Principio demarcatorio" que imposibilita la proximidad eficaz de los funcionarios de la Defensa con los de la Seguridad, dos ámbitos de actuación (Militar/Policial) que una intelectualidad academicista encabezada por vestigios de pasados luctuosos, inhibe la reconciliación. La impracticabilidad legal de "mirar" hacia adentro del país impuesta a las Fuerzas Armadas por las normas que reglamentan el ejercicio de la conjura de específicas agresiones estatales convencionales, minimiza a extremos inauditos el compromiso adquirido por una legión de, aproximadamente, 60.000 "pacificadores" que desde 1958 participan en más de 31 de las 66 misiones desplegadas en zonas de conflicto... ¿o estaremos desentendiéndonos de este flagelo cuando Argentina ha logrado enormes estándares de efectividad y prestigio? ¿Nos interesa el mundo? ¿Nos interesa la Paz como valor?

Concebida así, la estrategia como una aproximación indirecta (Liddell Hart) y como una interrupción de la lógica causal (propia del universo táctico), el imperio de una lógica paradojal (Luttwak) domina el escenario de las relaciones internacionales que bien puede reconvenirse en el empleo del instrumento militar en la construcción de puentes de aproximación y cooperación sin, de hecho, dejar de lado la dimensión disuasiva que indispensablemente requiere de la comunicatividad como requisito imprescindible para el logro de su fin: entre la disuasión ampliada[29] (necesariamente nuclear) y la prevención, la convicción siempre latente de una destrucción mutua asegurada a partir del concurso del "Actor irracional", mantiene vigencia.

¿Existe disuasión no nuclear? A pesar de la opinión de Beaufre, la respuesta a este interrogante está dada más por la aversión al riesgo que a las capacidades nucleares (siquiera convencionales) de las sociedades postmodernas, aquellas que en la paz democrática "Informan" a sus mandatarios gubernamentales sobre los pasos a dar en la arena internacional y los costos que estarían dispuestas a asumir en caso de un diferendo irreconciliable.

La re-instrumentación de las herramientas concebidas para dirimir las diputas o conjurar las amenazas por la vía de la violencia institucional legítima del Estado, bien puede reconvertirse en una suerte de ingeniería inversa y su vector agresivo o su escudo defensivo en instrumento de entendimiento antes que de confrontación, de acercamiento antes que de disputa de construcción de entendimiento. No hay vínculo más fuerte que el de la sangre. Uniones aduaneras, mercados comunes, tratados de libre comercio jamás ofrecerán el compromiso del riesgo compartido en el que está en juego la vida de los ciudadanos y el futuro de nuestras naciones.

28. NdA: que sucede a la de las piedras (1987), a la de Al Aqsa (2000) y a la de los cuchillos (2015). Desde 2000 bajo la modalidad de ataque suicida y/o "Lobo solitario".

29. Sodupe, Kepa (1991). "La teoría de la disuasión: un análisis de las debilidades del paradigma estatocéntrico". Revista *CIDOB d'afers internacionals*, (22), 53-79. Consultado 03/03/2018 06:15:28 Disponible en http://www.raco.cat/index.php/revistacidob/article/viewFile/27870/57242 Consultado el 3 de marzo de 2018. 03/03/2018 p.m.

PARA QUIEN NO SABE HACIA DÓNDE VA, ALGUNOS CAMINOS SON MEJORES QUE OTROS

Por CR **PHILIP D. SMITH**

Palabras Clave:
> Pasado
> Estrategia
> Antifragilidad
> Opcionalidad

Introducción

Un elemento esencial en la elaboración de la estrategia militar es guiar el diseño de la fuerza futura. La tendencia actual es basar tal diseño en una visión de la naturaleza del conflicto en el futuro. A su vez, la tarea más difícil se convierte en cómo determinar esa naturaleza. Es común depender de la historia como guía, aún si se admite que el pasado no determina el futuro, porque es la única guía que existe –así va el argumento–. El autor de este trabajo toma otro rumbo y plantea que el uso de la historia como guía del futuro es, en el mejor de los casos, inútil. En el peor de los casos, usar la historia para guiar la construcción de un entorno estratégico porvenir puede resultar en la construcción de una fuerza futura inapta cuando

Un estado final deseado que exige la doctrina de planeamiento estratégico no es un ente estático pues cambia en la medida que el futuro va convirtiéndose en el presente. Nadie sabe hacia dónde va, solo saben hacia donde quieren ir en un determinado momento.

CV

PHILIP D. SMITH

Coronel de la Fuerza Aérea Estadounidense. Aviador, piloto de KC-10, C-21 y C-12. Licenciado en Ingeniería Mecánica de la Academia de la Fuerza Aérea de los Estados Unidos. Magíster en Relaciones Internacionales por la Universidad Estatal de Troy. Magíster en Ciencias Sociales por la Pontificia Universidad Católica de Río de Janeiro. Magíster en Arte y Ciencia Operacional Militar por la Universidad Aérea. Ha publicado la disertación, "A Formação Institucional e Social da Argentina e do Brasil: Um estudo comparativo do corporativismo estatal nos anos 1930-1955." Actualmente es alumno de la Maestría de Estrategia Militar en la Escuela Superior de Guerra Conjunta.

ese futuro es reemplazado por otro. Es necesario adoptar una estrategia distinta, una en la cual se enfoque en el presente de hoy y el presente de mañana, es decir, una estrategia que permita a las fuerzas adaptar el futuro cuando vuelva a ser el presente. Puesto de forma más sencilla: no es posible, ni necesario tener una visión del futuro para elaborar una fuerza del futuro. Si bien este trabajo no impugna la historia como disciplina, objeta el uso de modelos basados en la historia para determinar una visión del futuro.

El problema con el futuro

El deseo de saber el futuro parece ser resultado del miedo a lo desconocido, comportamiento inherente en todos nosotros, los seres humanos. Es este deseo que nos impulsa a estudiar el pasado, a simplificarlo, a combinarlo con teorías y crear modelos para aplicar a los problemas complejos del hoy (Waltz, 1979). Hay varios problemas con este abordaje. Primero, no es posible regresar en el tiempo para analizar todos los aspectos de un evento histórico. Aunque el autor de la historia haya vivido los acontecimientos, es imposible que él pudiera capturar todos los aspectos y las variables con precisión. Segundo, no se puede vincular definitivamente una causa histórica con un evento posterior (causa y efecto) –las hipótesis o teorías de causa y efecto elaboradas con el análisis histórico no pueden ser comprobadas, uno tiene que aceptarlas con fe. Incluso si se pudiera, usar adecuadamente el análisis histórico para descubrir las variables determinantes, esto no garantizaría que las mismas variables sean válidas para el futuro. Colin Gray (2008) admite que el futuro es incierto y es necesario ejercer mucha precaución en el planeamiento de fuerzas, afirmando que la historia es la única guía para el futuro que existe. Sin embargo, el cambio de paradigma necesario es dejar de buscar el futuro. Es necesario cambiar el adagio, "para quien no sabe hacia dónde va... cualquier camino es bueno". La verdad es que nadie sabe hacia dónde va, solo saben hacia dónde quieren ir en un determinado momento. Un estado final deseado que exige la doctrina de planeamiento estratégico no es un ente estático –cambia en la medida que el futuro va convirtiéndose en presente–. Los que trabajan (militares y civiles) en el nivel estratégico y que no entienden este punto son los que frecuentemente se quejan de que el poder político no especifica un estado final o, lo cambia en la mitad del camino. La esperanza, el deseo de tener un estado final estratégico representa el ansia de saber el futuro; y la dificultad de mantener un estado final estable revela la imposibilidad de dicho deseo. Cualquier camino no es bueno, pero existen caminos mejores que otros que se pueden descubrir con la aplicación de otro paradigma.

Antifragilidad

El trabajo de Nassim Taleb (2012) y su concepto de "antifragilidad" ofrece así nuevo paradigma en el cual indica que decisiones de alta importancia sobre fenómenos complejos (como el diseño de la fuerza futura), no deben basarse en visiones del futuro. Taleb aporta varios conceptos que los estrategos pueden emplear para confrontar mejor la incertidumbre. Uno es el concepto de antifragilidad. Taleb afirma que lo opuesto de frágil no es fuerte o robusto. Algo es frágil cuando padece de estrés o incertidumbre, mientras que algo es robusto cuando resiste estrés o incertidumbre. Por ejemplo, una copa de vino es frágil y el cemento es robusto. Taleb acuñó la palabra "antifrágil" para describir algo que mejora o que se hace más fuerte con estrés o incertidumbre. Los organismos son antifrágiles (hasta un punto): por ejemplo la aplicación de estrés (como el ejercicio, hasta un punto) al cuerpo humano produce músculos más fuertes. La antifragilidad existe también en emprendimientos humanos. Un avión es frágil a una falla mecánica. No obstante, la aviación es antifrágil a una falla mecánica porque los mejoramientos técnicos son incorporados en todos los aviones para evitar la misma falla mecánica en el futuro. Asimismo, para aplicar este concepto a la estrategia militar, los estrategos deben analizar el poder militar de su fuerza para determinar las áreas frágiles y buscar oportunidades de aumentar la antifragilidad.

Aplicado al diseño de fuerzas futuras, algunos ejemplos del concepto de antifragilidad siguen. Frágil: depender de un sistema de transporte aéreo para llevar fuerzas militares al teatro operacional tiene muchos elementos frágiles como la susceptibilidad al mal clima, los ataques enemigos a los aeródromos, más fallas mecánicas que otros medios de transporte, etc. Antifrágil: una estrategia de analizar e incorporar lecciones aprendidas de forma muy eficiente es antifrágil, pues cada error evitará (o minimizará) los chances de cometer el mismo error. Robusto: una estrategia militar robusta que cuenta con un sistema de comando y control con redundancia: si el adversario logra eliminar un dominio, como el espectro electromagnético, habría otros modos de comunicar las órdenes militares. Una forma "soft" de antifragilidad es el patriotismo o lealtad a una causa: mientras más estrés se aplica (hasta un punto) a un grupo patriótico, más esfuerzo realiza este grupo para ganar. Taleb ofrece una herramienta para determinar fragilidad y antifragilidad: se trata de analizar (con experimentos o hipotéticamente) los efectos de estrés o eventos aleatorios a un sistema; más beneficio que perjuicio = antifrágil; más perjuicio que benéfico = frágil; sin perjuicio o beneficio = robusto.

Opcionalidad

Un segundo concepto que propone Taleb para no depender de pronósticos del futuro es la opcionalidad. Tener opcionalidad quiere decir tener la capacidad de demorar decisiones hasta tener mejor información. Es decir, cuando uno tiene opcionalidad, se puede esperar que el futuro llegue en vez de depender de un pronóstico. Un ejemplo de una estrategia militar que se beneficia de opcionalidad es tener un sistema de logística genética altamente eficiente, que se podría movilizar en poco tiempo para producir materiales de guerra adecuados para confrontar un riesgo o ataque inminente. Esto se puede contrastar con el producir materiales de guerra para un futuro supuesto y encontrarse con armas inadecuadas cuando llegue otro futuro. De forma general, los recursos (recursos humanos, económicos, naturales, etc.) aumentan opcionalidad mientras que los déficits (préstamos, pocos recursos

La esperanza, el deseo de tener un estado final estratégico, representa el ansia de saber el futuro. A su vez la dificultar de mantener un estado.

naturales, etc.) bajan la opcionalidad. Otra herramienta estratégica que proporciona opcionalidad es el sistema de inteligencia. Mientras más robusto sea este sistema, mejor se puede adecuar las opciones a la realidad del presente.

Tal vez un componente de mayor potencial para aumentar la opcionalidad es la investigación básica. Una base fuerte de investigación básica abre las posibilidades de tecnologías pioneras capaces de superar obstáculos operacionales que existen en un país por falta de acceso a la tecnología de punta o por falta de recursos para tal tecnología. Por ejemplo, una investigación enfocada en sistemas de propulsión de cohetes podría eventualmente proporcionar la capacidad de colocar satélites en órbita para los países que carecen de esta capacidad. Sin embargo, el tiempo y los recursos para lograr esa capacidad asegurarían que tales países quedaran detrás de los que ya la tienen y los expondría a las vulnerabilidades resultantes de innovaciones en armas anti-satelitales. En cambio, nuevos descubrimientos originarios de la investigación básica podrían anular la necesidad del uso del espacio para funciones como comunicaciones y exploración. Otro beneficio de la investigación básica es su costo relativamente bajo versus las recompensas potencialmente altísimas.

Es importante reconocer que opcionalidad no quiere decir prepararse para todos los posibles escenarios de defensa, como Henry Bartlett, Paul Holman y Timothy Somes (1995) describen con la palabra hedging. Por el contrario, se trata de incorporar flexibilidad en el diseño de la fuerza futura. En mi opinión, los países militarmente más exitosos no son aquellos que mejor se prepararon para amenazas que pronosticaron, sino aquellos que cuentan con niveles elevados de antifragilidad y opcionalidad.

Conclusión

El título de este trabajo, "para quien no sabe hacia dónde va, algunos caminos son mejores que otros", es su mejor resumen. Para quienes tienen la tarea de elaborar estrategia militar y diseñar las fuerzas futuras no deben basarlas en la ilusión de una visión del futuro. Tal visión no es la única manera de asegurar la defensa de una Nación: los conceptos de antifragilidad y opcionalidad ofrecen otros caminos más estables. Se termina este trabajo con una última consideración para ponderar: ¿será que de alguna manera nuestra conciencia colectiva ya sabe y aplica lo que sugiere este trabajo? Es decir, ¿puede ser que la elaboración de estrategias militares basadas en visiones del futuro sirva un propósito escondido? ¿Será que tales estrategias sirven como herramientas de persuasión para influenciar las decisiones del gasto de recursos? Durante disputas de recursos es muy común observar el uso selectivo de componentes de estrategias nacionales para justificar algún programa, mientras que tales estrategias nunca son dotadas integralmente. En realidad, es muy difícil encontrar una estrategia militar nacional (en cualquier país) integralmente dotada e implementada antes de su reescritura, sea por causa de un nuevo gobierno, por cambios en el entorno estratégico, y otros. En tal caso, este trabajo se convierte en una observación de una realidad escondida en lugar de una propuesta de cambio.

BIBLIOGRAFÍA

Bartlett, Henry C.; Holman, G. Paul; and Somes, Timothy E. (1995) *"The Art of Strategy and Force Planning"*, Naval War College Review: Vol. 48:2, Article 9. Obtenido de https://digital-commons.usnwc.edu/nwc-review/vol48/iss2/9

Gray, Colin S. (2008) Coping With Uncertainty: Dilemmas of Defense Planning, Comparative Strategy, 27:4, 324-331, DOI: 10.1080/01495930802358414

Taleb, N. N. (2012). *Antifragile: Things that Gain from Disorder.* New York: Random House.

Waltz, Kenneth N. (1979). *Theory of International Politics.* McGraw-Hill, University of Michigan.

LA BIOTECNOLOGÍA DE USO DUAL EN LA TENDENCIA HACIA LAS FRONTERAS MICROFÍSICAS

Por LIC. **ESTEFANÍA BELÉN DUCASSE**

RESUMEN

-

El presente artículo analiza el papel y avance de la biotecnología de uso dual en el contexto de la guerra de cuarta generación hasta el año 2019. Esto está relacionado con las implicancias que tiene este tipo de tecnología sobre el concepto de fronteras, y marca una tendencia al desvanecimiento de los límites físico-políticos hacia el campo de la microfísica. La utilización de la biotecnología refuerza el comportamiento de los Estados, quienes se encauzan en una lucha por la obtención de poder en un marco de competencia interestatal y de un sistema internacional anárquico. Como consecuencia, las potencias desarrollan o usan tecnología de uso dual, ya sea para plantarse como hegemón o para controlar a aquellos Estados que representan una amenaza sin ser potencias. La utilización de esta biotecnología en su formato de armamento se puede explicar desde la geopolítica kjelleniana y la biopolítica que, en relación con los dos objetivos ya planteados, los Estados atentan contra la seguridad humana de aquella población, que representa una amenaza. Estados Unidos, por ejemplo, desarrolla desde 2017 el programa llamado Insect Allies, en el que se ve reflejado el potencial de la biotecnología de uso dual.

Palabras Clave:
> Biotecnología de uso dual
> Geopolítica
> Biopolítica
> Seguridad humana

ARTÍCULO CON REFERATO

Introducción

Según la teoría realista de las Relaciones Internacionales, el sistema internacional está caracterizado por la competencia interestatal. En esta dinámica "el objetivo primordial de cada Estado es maximizar su poder mundial, lo que significa ganar poder a expensas de otros Estados"[1]. A través de los años, uno de los elementos acreedores de poder fue la posesión de espacio físico, razón de la consecución de distintas guerras en pos de obtener mayor territorio. Al final de la Guerra Fría, William Lind[2] junto con un grupo de oficiales del Ejército estadounidense publicaron un estudio en el que se tipificaba el combate moderno de acuerdo a cómo evoluciona la esencia del conflicto. A partir de dicha tipificación, se desarrolla la llamada guerra de cuarta generación con el progreso de las nuevas tecnologías, entre otras características. En este contexto de avance de las nuevas tecnologías, los límites físico-políticos adquieren la suerte de desvanecerse y el conflicto comienza a abarcar un nivel microfísico.

Como resultado, en la actualidad existen dos planos de guerra: el primero comprende a las guerras tradicionales en las que se lucha por territorio y recursos naturales; y el segundo, se centra principalmente en el plano microfísico de la ciberseguridad o ciberguerra, pero también en el nivel biológico. Es aquí donde la biotecnología de uso dual, es decir aquella que puede ser utilizada tanto con fines civiles como militares, juega como elemento fundamental.

Evolución del combate moderno

Según los autores realistas, el objetivo último de toda gran potencia es convertirse en hegemón, lo que se condice con el fin estatal para lograr la seguridad o supervivencia. Esto se debe a que la estructura del sistema internacional obliga a los Estados a actuar en forma agresiva entre sí para ganar y preservar su seguridad[3]. En base a la dinámica del sistema internacional, William Lind describió la evolución del combate en 4 generaciones de acuerdo a ciertas características comunes e hitos que marcan los cambios entre una y otra. Se habla de la existencia de una quinta generación de guerra que consiste, primordialmente, en la utilización de los medios de comunicación para lograr la manipulación psicológica del blanco, el foco de este tipo de guerra se halla en el factor psicológico. Aquí se explican las distintas generaciones de guerra según lo tipificado por Lind[4], uno de los autores referentes en lo que respecta al conflicto de cuarta generación.

El conflicto de primera generación comienza con la Paz de Westfalia, firmada en 1648, donde se estableció un nuevo sistema de orden político en Europa y en el que prima el concepto de coexistencia estatal. El punto de relevancia de este tipo de guerra se basa en la creación de una cultura militar del orden, esto es, la instalación del uniforme, los saludos y demás elementos que refuerzan la cultura del orden.

La segunda generación ocurre durante y luego de la Segunda Guerra Mundial y conecta la cultura del orden de la primera generación con el ambiente militar, otorgándole una importancia central a la artillería dentro del combate. En este estadio, el poder de fuego está centralizado y sincronizado para la infantería mientras que la artillería "conducía la guerra". A diferencia del tipo anterior en el que el punto central lo tenía la infantería, el arma de artillería es la que dirige el combate a partir de este periodo. "El foco estaba en el interior, en las reglas, procesos y procedimientos. La obediencia era más importante que la iniciativa"[5]. Aquí la iniciativa no era deseada dado que actuaba en detrimento de la sincronización y de la disciplina impuesta de arriba hacia abajo.

Con la guerra de tercera generación la doctrina militar dio un salto diferencial en comparación con las generaciones precedentes. Mientras que en la guerra de segunda generación prevalecía la sincronización, la importancia de los procedimientos y la disciplina, en este nuevo tipo de conflicto se alienta la iniciativa más que la obediencia. Esta genera-

Los elementos esenciales con los que se caracteriza la Revolución de los Asuntos Militares son el avance tecnológico, la incorporación de esta tecnología a los sistemas militares, la innovación en la operatividad militar y, también, la adaptación organizacional.

ción se centra en "[...] la velocidad, sorpresa y dislocación tanto mental como física"[6], con lo que se busca colapsar al enemigo desde la retaguardia hacia adelante, para dejar el poder de fuego en un segundo lugar. Ahora el foco de atención está puesto sobre el exterior y sobre la situación; ya no son las reglas y los métodos lo que conllevó a una generación de combate no lineal.

Ahora bien, el quiebre más importante dentro de la línea de generaciones de guerra lo ocasionó la guerra de cuarta generación. Aquí si bien se mantiene la no linealidad, la descentralización y la prevalencia de la iniciativa, cambian los actores que interaccionan en la guerra. Hasta la Segunda Guerra Mundial las guerras eran llevadas a cabo entre Estados, pero en la guerra de cuarta generación, William Lind cambia la dinámica Estado-Estado del conflicto y la transforma en un juego entre un Estado y un grupo no estatal. De esta manera, el Estado pierde el monopolio de la guerra y se alza una generación marcada por la lucha entre culturas, principalmente, atribuyéndole este conflicto a un actor no estatal de religión islámica y un Estado.

De este modo, Lind le otorga a la guerra una característica fundamental de asimetría entre los actores intervinientes. Esta noción reduccionista de los actores que intervienen en la guerra de cuarta generación es cuestionada por Juan José Borrell[7], quien indica que la condición asimétrica preponderante en esta generación puede ser adjudicada tanto en la relación Estado-actor no estatal, como en el juego interestatal. Además de esto, Borrell[8] afirma que no existe la crisis de legitimidad del Estado, ni perdió el monopolio de la guerra, sino que Lind no tomó en cuenta aspectos como la contribución de la Revolución de los Asuntos Militares (RAM) a la que nos referiremos más adelante.

La tipificación de las diferentes generaciones de guerra es el resultado de la evolución en la relación dinámica entre el contexto y los actores intervinientes. Con el avance de las nuevas tecnologías, el plano en el que se desarrollan las guerras ha mutado. De modo que esto, sumado a la globalización, conllevó a la redefinición de la relación entre el territorio, el espacio y la escala[9]. Como resultado, existe una tendencia a actuar en un nivel microfísico que trasciende las fronteras políticas.

Tendencia a la microfísica

La relación entre el territorio, el espacio y la escala que interviene en la guerra de cuarta generación marca una tendencia hacia la actuación en el plano microfísico. Algunos ejemplos de esta tendencia son los eventos biológicos, los activos biológicos en zonas globales comunes, los materiales a nanoescala y los sistemas cibernéticos, entre otros[10]. El plano microfísico también se hace ver dentro de la competencia que caracteriza parte de la dinámica que relaciona a los actores del sistema internacional. En este sentido, teniendo en cuenta los ejemplos, se pueden encontrar en la competencia los recursos naturales que sobrepasan los límites políticos establecidos.

A lo largo de los años, la competencia por el territorio y los recursos naturales han caracterizado las relaciones interestatales y también entre Estados y actores no estatales. Los Estados buscan ganar poder a expensas de los demás por lo que compiten en distintos campos para cumplir con este objetivo. Tal comportamiento se debe a que

1. Mearsheimer, John. *"The tragedy of great power politics"*; segunda edición; Norton; Nueva York; 2001; página 2.
2. Borrell, Juan José; *"Microphysicalborders and fourth-generationwarfare: drawingthelines betweengeopolitics and biopolitics in the competitionfor natural resources"*; Cfr. Zentrumfür Geoinformationswesen der Bundeswehr; Jahresheft Geopolitik; Euskirchen (Alemania); 2017; páginas 18-23.
3. Mearsheimer, John; op. cit.
4. Lind, William; *"Understanding Fourth Generation War"*. Military Review; September/ October 2004;páginas 12-16
5. Ibid.; página 12.
6. Ibid.; página 13.
7. Borrell, Juan José; op. cit.
8. Ibíd.
9. Ibíd.
10. Ibíd.

los Estados están insertos en una estructura internacional de índole anárquica, es decir, no existe una policía que haga cumplir "la ley" en la comunidad internacional. Según los realistas, la condición anárquica del sistema obliga a los Estados a estar en una lucha continua al tener recursos escasos por los que compiten.

Junto con la competencia, se halla lo que Randall Schweller denomina como conflicto de posición, es decir, "[...] un subconjunto especialmente virulento de competencia posicional, en la que al menos una de las partes, y generalmente ambas, busca la destrucción total o subyugación del otro [...]"[11], En este sentido, la esencia del conflicto de posición está marcada por el planteamiento de Richard Betts[12], que consiste en que la raíz de toda guerra es convertirse en el que pondrá las reglas de juego dentro del orden internacional posterior al conflicto. De esta forma, la competencia por los recursos se adiciona al conflicto de posición para lograr una ventaja relativa respecto a los demás Estados. Esta concepción se ve reforzada con el objetivo de toda potencia de convertirse en hegemón y asegurar su seguridad.

Otra condición que aplica a las relaciones entre actores internacionales tanto estatales como no estatales es la asimetría. La asimetría puede ser medida en base a distintos elementos: económico, social, militar, etc. Por lo que, los actores utilizan diferentes herramientas para intentar preservar o revertir tal asimetría. Es decir, las potencias se encuentran en un nivel preponderante dentro de la comunidad internacional y lo que pretenden es, además de convertirse en hegemón, mantener el poder del que son acreedores y su posición dentro del sistema[13]. Mientras que las potencias buscan mantener el *statu quo,* otros Estados se conforman como revisionistas y buscan romper con el *statu quo* prevaleciente. En otras palabras, las potencias actúan en pos de mantener o aumentar la asimetría que les otorga mayor seguridad. Mientras que, otros Estados, revisionistas o no, buscan aumentar su seguridad a través de la disminución de la asimetría.

Se debe agregar que en esta dinámica de competencia, asimetría y conflicto de posición, "[...] los bienes posicionales son sujetos de limitaciones absolutas en suministro, crecimiento económico y prosperidad, [que] lejos de disminuir el conflicto entre grupos, tiende a exacerbarlo [...]"[14]. Entonces, el crecimiento económico y la prosperidad conllevan al aumento del conflicto a raíz del incremento de la desigualdad. En un contexto anárquico de competencia en donde las asimetrías se exacerban, los Estados luchan en pos de conseguir ventajas relativas, siempre y cuando los costos no sean mayores que las ganancias. Este comportamien-

Los países que son potencias actúan en pos de mantener o aumentar la asimetría que les otorga mayor seguridad. Mientras que, otros Estados, revisionistas o no, buscan aumentar su seguridad a través de la disminución de la asimetría.

to de los Estados también se ve explicado por el dilema de seguridad, que consiste en que muchos de los medios que utiliza un Estado para aumentar su seguridad generan el decrecimiento de la seguridad de otros Estados[15]. Por consiguiente, se fomentan las asimetrías en torno al nivel de seguridad.

A raíz de esto, cabe definir a la seguridad como una situación ideal caracterizada por la ausencia de amenazas o, también, como un conjunto de medidas dirigidas hacia ese objetivo. En la misma línea, la seguridad surge con la aparición del Estado para adquirir así una naturaleza de índole política dado que su principal objetivo es la supervivencia estatal[16]. Teniendo esta definición presente, algunos Estados buscarán aliarse entre ellos para "compensar" las asimetrías frente a una gran potencia en un contexto de autoayuda[17] de manera que aumente su poder relativo y, con esto, ganar seguridad y conseguir su supervivencia.

Al comprender el comportamiento de los Estados dentro del sistema internacional se da lugar a la relevancia del avance de la tecnología como herramienta que proporcione la obtención de una ventaja respecto a otros actores. En relación con eso, la revolución de los asuntos militares es un fenómeno de gran importancia en esta dinámica y no solo lo asociado a la materia militar sino también la tecnología de uso dual y, en particular, la biotecnología.

Con el avance de la informática y de la computación, los Estados se han concentrado en desarrollar herramientas dirigidas a la protección de su infraestructura crítica. La infraestructura crítica refiere a aquellas "[...] instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros"[18]. Por lo tanto,

11. Schweller, Randall; *"Realism and the present great power system: growth and positional conflict over scarce resources"* Cfr.Kapstein, E. y Mastanduno, M. (eds.); Columbia University Press. Unipolar Politics. Realism and state strategies after the Cold War; New York; 1999; página 2.
12. Ibid.; página 2.
13. Mearsheimer, John; op. cit.
14. Schweller, Randall; op. cit.; página 3.
15. Jervis, R. (1978) *"CooperationUnderthe Security Dilemma"*. WorldPolitics, 30 (2), páginas167-214. (http://www.jstor.org/stable/2009958), consultado el 8 de octubre de 2018.
16. Bartolomé, M. (2006). La seguridad internacional en el siglo XXI, más allá de Westafalia y Clausewitz; ANEPE; Buenos Aires; 2006.
17. Waltz, Kenneth;*"Theory of International Politics"*; McGraw Hill; New York; 1979.
18. Miranzo, Mónica. y del Río, Carlos;"La protección de infraestructuras críticas"; UNISCI DiscussionPapers; N.º 35; Mayo / May 2014; página 341. (http://dx.doi.org/10.5209/rev_UNIS.2014.n35.4), consultado el 21 de febrero de 2020.

CV

ESTEFANÍA BELÉN DUCASSE

Licenciada en Gobierno y Relaciones Internacionales – Política y Administración Pública de la Universidad Argentina de la Empresa (UADE). Candidata a Magister en Estrategia y Geopolítica de la Escuela Superior de Guerra "Tte. Gral. Luis María Campos". Actualmente se desempeña como investigadora en el Centro de Estudio de Medio Oriente Contemporáneo y dentro del personal civil de la Policía de la Ciudad.

una falla o ataque hacia este tipo de infraestructura representa una amenaza con potenciales resultados devastadores en distintos planos ya sean económicos niveles de seguridad u otros campos que repercuten directamente sobre el Estado. Es por eso que en el Libro Blanco de la Defensa de Japón, Francia y Estados Unidos, centran sus estrategias defensivas alrededor de los riesgos y las amenazas conducidos hacia la infraestructura estatal crítica, especialmente respecto a los ataques cibernéticos[19]. En particular, estas estrategias contemplan también ataques terroristas y de ciberterrorismo. Sin embargo, a pesar de la atención que recibe la infraestructura estatal crítica, especialmente en el ámbito de la cibernética, la biotecnología de uso dual no recibe el mismo tratamiento y pasa a un segundo plano.

Así como la cibernética, la biotecnología ha traspasado el campo de los límites políticos que marcan la división del espacio propio de un Estado. Con el desarrollo tecnológico se pueden generar compuestos químicos o incluso modificar genéticamente tanto a plantas como animales. Este tipo de tecnología tiene la particularidad de dificultar su identificación al no poder ser diferenciada como creación o modificación de un Estado y actuar dentro o fuera del espacio nacional. Como consecuencia de esta tendencia a la microfísica, los límites políticos se vuelven borrosos y las fronteras nacionales porosas.

Biotecnología de uso dual, geopolítica y seguridad humana

La acepción de tecnología de uso dual ha mutado a lo largo de los años de acuerdo al contexto y desarrollo de los diferentes períodos históricos. Luego de la Guerra Fría, la tecnología de uso dual hace referencia a "[...] aquellas tecnologías susceptibles de producir aplicaciones tanto en el ámbito civil, como militar, que generan sinergias de explotación y reducen los ciclos de desarrollo y evolución"[20]. De esta forma, con el interés conjunto del sector privado además del militar, la investigación y el progreso tecnológico logran reducir los tiempos de los procesos y obtención de resultados. Es así, que cada vez más, los límites que diferencian el ámbito de aplicación de estas tecnologías en el campo civil y militar se hallan más difusos y, en algunos casos, la diferencia entre la aplicación civil o militar gira alrededor solamente de algunas particularidades.

En esta línea, la intervención de la biología en la tecnología de uso dual es un hecho que tiene lugar desde la Segunda Guerra Mundial, aunque existe alguna evidencia inconsistente de que ya en la Primera Guerra Mundial se habían encauzado las investigaciones por parte de Alemania en torno a las armas biológicas[21]. Entonces, la biotecnología es un fenómeno que tiene lugar desde hace más de 50 años y que podría conformar uno de los avances pertenecientes a la Revolución de los Asuntos Militares (RAM).

Según Michael J. Ainscough[22], la biotecnología de uso dual debería ser considerada un potencial integrante de la RAM. Los elementos esenciales con los que se caracteriza la RAM son el avance tecnológico, la incorporación de esta tecnología a los sistemas militares, la innovación en la operatividad militar y, también, la adaptación organizacional. El resultado de la conjunción de estas características deviene en la alteración fundamental del carácter y la conducción del conflicto. No obstante, el uso de las armas biológicas está prohibido por la comunidad

internacional por lo que incluirlo dentro de la Revolución de los Asuntos Militares es un hecho en discusión en relación a su legitimidad.

La biotecnología que se desarrolla para fines como salvar vidas, tratamientos médicos, biocombustibles, etc. puede también ser usada para el desarrollo de armas biológicas. Esto compone el mayor riego del desarrollo de este tipo de tecnología, su faceta denominada *black biology* o "biología negra". La *black biology* es definida como "[...] el uso de ingeniería biológica para mejorar la virulencia de un patógeno"[23]. Algunos actores enfatizan el riesgo que conllevan estas tecno-

19. Ibid; páginas 339-352.
20. RiolaRodriguez, José María;"La situación actual de las tecnologías de doble uso"; Cuadernos de estrategia; N.° 169; 2014;página 159.
21. Christian, Michael; "Biowarfare and Bioterrorism";CritCareCli; N.° 29;2013; páginas 717–756. http://dx.doi.org/10.1016/j.ccc.2013.03.015
22. Ainscough, Michael;"Next Generation Bioweapons: The Technology Of Genetic Engineering Applied To Biowarfare And Bioterrorism";Future Warfare Series; N.° 14; 2002; páginas 1 – 39 (https://fas.org/irp/threat/cbw/nextgen.pdf), consultado el 21 de febrero de 2020.
23. Lawrence, Roberge;"Black biology: A threat to biosecurity and biodefense";Biosafet;N.°2(3); 2013;página 1.

logías puesto que las herramientas de ingeniería genética son cada vez más accesibles para los civiles, por lo que representan una amenaza ya que pueden ser usadas por actores no estatales como los terroristas. No obstante, en este trabajo se tomará en cuenta principalmente el uso de la biotecnología de uso dual por parte de los Estados.

En 1972, se llevó a cabo la Convención sobre la Prohibición del Desarrollo, la Producción y el Almacenamiento de Armas Bacteriológicas (Biológicas) y Toxínicas y sobre su Destrucción, que entró en vigor en 1975. El tratado hace referencia a un acuerdo respecto al desarme y prohibición del "[...] desarrollo, la producción y el almacenamiento de toda una categoría de armas de destrucción en masa [...]"[24]. En esta convención, parte de los Estados acordaron poner en práctica una serie de medidas tendientes a fomentar la confianza entre ellos. De este modo, se comprometieron a prevenir o reducir las incidencias, las dudas sobre estas o las ambigüedades y a mejorar la cooperación internacional. Este tratado encuentra su punto gris en las tecnologías de uso dual ya que, como se dijo antes, es sumamente difícil diferenciar las actividades dirigidas al desarrollo de tecnologías para el uso civil o militar.

A pesar de que el foco de atención lo continúa teniendo el mundo cibernético, hay pruebas de que las principales potencias están interesadas en el desarrollo y la prevención de la biotecnología de uso dual. En este sentido, China promueve un programa sobre guerra biológica y en agosto de 2019 fue acusada por Canadá en torno al espionaje sobre su Laboratorio Nacional de Microbiología. Por otro lado, Estados Unidos en septiembre de 2018 dio lugar a la creación de un comité directivo para proteger a sus ciudadanos tanto de ataques con armas biológicas como otras potenciales amenazas biológicas. A este respecto, el presidente Donald Trump expreso que "es de interés vital para EE.UU. manejar los riesgos de incidentes biológicos, lo que les da una idea de la prioridad que esta administración le ha dado a este aspecto"[25]. A este grupo se une Corea del Norte que, según un análisis del Instituto de Estudios Internacionales de *Middlebury* emitido a finales de 2018, colabora con investigadores extranjeros para adquirir habilidades biotecnológicas y construir maquinarias[26].

Al tener esto en cuenta, la biotecnología de uso dual conforma un instrumento que aumenta el poder del Estado que la desarrolla y, con esto, incrementa la asimetría de capacidad y poder en un contexto de competencia. En este sentido, esta biotecnología puede ser utilizada como un arma biológica para dos fines: aumentar su poder y plantarse como hegemón frente a otras potencias, o controlar a aquellos Estados que sin ser potencias representan una potencial amenaza.

Según la teoría de Rudolf Kjellen, el Estado funciona como un organismo con carácter, intereses y conducta cuyas relaciones exteriores son similares a las de los seres vivos, que luchan y compiten por su supervivencia en un mundo de intereses contrapuestos. Al mismo tiempo, el autor enfatiza la importancia de la relación entre el Estado

24. Oficina de Asuntos de Desarme.Convención sobre la Prohibición del Desarrollo, la Producción y el Almacenamiento de Armas Bacteriológicas (Biológicas) y Toxínicas y sobre su Destrucción (https://www.un.org/disarmament/es/adm/armas-biologicas/), consultado el 22 de febrero de 2020.

25. Sputnik News (18 de septiembre de 2018). Trump crea comité de Biodefensa para proteger a EE.UU. del bioterrorismo (https://mundo.sputniknews.com/america_del_norte/201809181082082815-como-planea-eeuu-proteger-a-eeuu-del-bioterrorismo/), consultado el 22 de febrero de 2020.

26. Baumgaertner, E. y Broad, W. (16 de enero de 2019). Corea del Norte y la amenaza de las armas biológicas. (https://www.nytimes.com/es/2019/01/16/espanol/corea-del-norte-armas-biologicas.html), consultado el 22 de febrero de 2020.

y su territorio puesto que "el Estado es menos concebido sin el pueblo que sin el territorio"[27]. La geopolítica de Kjellen vincula el espacio, la biología y las relaciones de poder, cuyos últimos dos elementos tienen en común con la biopolítica aunque esta abarca específicamente a la biología humana.

Tanto desde la geopolítica de Kjellen como desde la biopolítica se hace hincapié en la importancia del pueblo. Kjellen, particularmente, centra su atención en las relaciones entre las grandes potencias y resalta entre los distintos elementos que hacen a una potencia, el valor de su alma fuerte. En esta línea, ambas ciencias siguen la noción de que un Estado fuerte necesita un pueblo fuerte.

Ahora, la geopolítica kjelleniana y la biopolítica funcionan como teoría argumentativa del uso de la biotecnología de uso dual por parte de los Estados para ambos fines. Respecto al fin de establecerse como hegemón frente a otras potencias, se puede observar que el uso de biotecnología como armas biológicas es un elemento que exacerba la asimetría en la capacidad de los Estados en la que el pueblo es una parte de vital importancia. Si se busca debilitar realmente a un Estado adversario se puede atacar con un agente patógeno a la población del Estado con el que se tiene el conflicto.

El segundo fin se fundamenta con la amenaza que componen para un Estado del primer mundo por el crecimiento demográfico excesivo y las migraciones masivas. De acuerdo a la teoría de Malthus[28], la población aumentaría geométricamente mientras que la producción de comida lo haría en forma aritmética por lo que el alimento no alcanzaría para alimentar al "excedente poblacional". Esto llevaría a los países subdesarrollados a emigrar de su lugar de origen en busca de alimento y mejores condiciones de vida, componiendo un factor desestabilizador para el Estado receptor. Entonces, utilizar un agente patógeno en contra de la población que representa una amenaza conformaría una herramienta para su control.

Cabe destacar la variedad del gran espectro de modificación que ofrece el desarrollo de la biotecnología y el alcance que estos avances pueden llegar a tener si se utilizan como un arma. La posibilidad de aumentar la virulencia de un agente patógeno, que logre la diseminación de un virus en un corto periodo de tiempo, sumada a la dificultad que implica la identificación del origen de este agente, le da al Estado creador del arma un anonimato frente a toda responsabilidad política de las consecuencias del virus. Como resultado, el desarrollo de esta tecnología parece ser una apuesta segura en los conflictos del siglo XXI, siempre y cuando su fabricación quede inmersa dentro del uso dual para no violar los estatutos de la Convención.

Por consiguiente, el uso de armas biológicas atenta contra la segu-

La biotecnología de uso dual conforma un instrumento que aumenta el poder del Estado que la desarrolla y, con esto, incrementa la asimetría de capacidad y poder en un contexto de competencia. En este sentido, la biotecnología puede ser utilizada como un arma biológica para dos fines: aumentar su poder y plantarse como hegemón frente a otras potencias, o controlar a aquellos Estados que sin ser potencias representan una potencial amenaza.

ridad humana, que es una de las condiciones que un Estado debe garantizar. Desde el 2000, se utiliza una acepción amplia de la seguridad humana, pero en términos generales hace referencia a la protección de los elementos que garanticen la supervivencia, el bienestar y la dignidad de la población[29]. La biotecnología de uso dual es un elemento que refuerza la tendencia de los límites microfísicos; con este tipo de tecnología se puede incurrir en el territorio de otro Estado sin importar la frontera política que traspase.

Estados Unidos es un ejemplo de la potencial amenaza que representa la utilización de la biotecnología de uso dual para otros Estados. Desde el 2016, la potencia americana desarrolla un programa llamado *Insect allies program* en el que se usan ciertos insectos para diseminar virus modificados genéticamente. El objetivo del programa es inmunizar al sistema de cultivos a gran escala cuya plantación se encuentra ya en crecimiento frente a diferentes amenazas como los problemas medioambientales, las sequias, o producidas por otro actor estatal o no estatal[30]. No obstante, un artículo en la revista *Science* determinó las principales críticas respecto a este programa: en primer lugar, el programa podría ser usado con más facilidad como un arma biológica que con fines agricultores; en segundo lugar, puede alentar a otros Estados a incrementar sus estudios en actividades de este tipo[31]. Además, a raíz de la dualidad de esta biotecnología es difícil detectar si su desarrollo tiene un uso militar o meramente civil.

Conclusiones

La globalización junto con la innovación tecnológica han modificado la relación entre el territorio y la escala desarrollándose una tendencia que se dirige a pensar los límites como microfísicos para superar las fronteras políticas.

A raíz de esto, la utilización de la biotecnología de uso dual conforma un instrumento que fomentan las asimetrías entre Estados, dado que la posibilidad de su uso como armas biológicas, con la característica de tener un origen dificultosamente identificable y funcionar como potencial amenaza. Con esta tecnología, un Estado puede debilitar a otro atacando directamente su población, como también, los cultivos, el ganado, el agua o cualquier otro elemento cuya carencia o contaminación repercuta sobre la sociedad. Es así que la seguridad humana que deben garantizar los Estados corre peligro.

El uso de este tipo de herramientas por parte de los Estados responde a la dinámica de las relaciones interestatales dentro del sistema internacional. Los actores estatales actúan dentro de un sistema fundado en las asimetrías, en la competencia para obtener ventajas relativas y en el conflicto por la posición que cada uno ocupa dentro de la comunidad internacional. Como resultado del desarrollo tecnológico, las fronteras políticas ya no son un obstáculo para la intervención estatal sobre territorio extranjero.

27. Marini, José Felipe; El conocimiento geopolítico; Circulo Militar; Buenos Aires; 1985.
28. Malthus, Thomas; El principio de la población; Establecimiento Literario y Tipográfico de D. Lucas González y Compañía; Madrid; 1846.
29. Bartolomé, Mariano; op. cit.
30. Defense Advanced Research Projects Agency -DARPA-. Insect Allies. (https://www.darpa.mil/program/insect-allies) consultado el 23 de febrero de 2020.
31. Max-Planck-Gesellschaft; "A step towards biological warfare with insects?"; Science Daily; 9 de octubre de 2018; (https://www.sciencedaily.com/releases/2018/10/181009102511.htm), consultado el 23 de febrero de 2020.

NUEVOS DESAFÍOS PARA LA SEGURIDAD Y LA DEFENSA

Por CL **RODOLFO TRISTÃO PINA**

Palabras Clave:
> Seguridad
> Defensa
> Estados
> Poder

ARTÍCULO CON REFERATO

Introducción

El momento actual experimenta los efectos de los fenómenos de la globalización y del desarrollo científico-tecnológico, lo que trae una nueva dinámica al orden mundial. Estos dos fenómenos aumentaron los flujos internacionales de comercio, de capital, de personas, de cultura, de educación y de información. De esta manera, se crearon desafíos, oportunidades a las naciones y una mayor interdependencia.

El uso de la *World Wide Web* (internet) refuerza esta narrativa ya que diferentes actores de la sociedad civil, de las empresas, de las organizaciones no gubernamentales, de los movimientos pacíficos o incluso de los terroristas logran difundir y coordinar sus actividades sin que los Estados puedan controlar eficazmente estas acciones.

Estos cambios han traído nuevos actores al sistema internacional, lo que pone en discusión el papel de los Estados, los cambios en la forma en que se alcanzan los objetivos nacionales y los métodos de resolución de conflictos. De hecho, muchas de las formas en disputa y confrontación han salido del campo militar, impulsadas principalmente por la fuerza de la opinión pública y por los altos costos materiales, que imponen un conflicto bélico.

En el campo de la seguridad y la defensa se debate mucho sobre los desafíos planteados por la posmodernidad: si las nuevas amenazas son nuevas o simplemente viejas amenazas bajo una nueva dinámica. Los más ortodoxos y conservadores refutan categóricamente una nueva lectura de los problemas de seguridad y defensa, que abogan por la atemporalidad de sus principios fundamentales. La gran pregunta es si tenemos o no las herramientas y los mecanismos adecuados para abordar los peligros reales y potenciales para la sociedad, y si el aparato militar convencional ha demostrado ser útil a este respecto.

Este trabajo tiene como objetivo analizar brevemente la evolución de los conceptos de seguridad y de defensa hasta la actualidad, concluyendo sobre los reflejos de estos cambios en la estrategia militar.

Desarollo

El viejo modelo westfaliano en el que el Estado aparecía como actor exclusivo en las relaciones de poder ha quedado perimido. El mundo hacia finales de los años 80 sufrió un período de rupturas: el fin de la Guerra Fría, la apertura de la Unión Soviética, la caída del muro de Berlín y el fortalecimiento de las organizaciones no gubernamentales (ONG) son hechos que provocaron cambios en la dinámica de las relaciones humanas e institucionales.

"No vivimos hoy una Era de cambio [...] al contrario, estamos experimentando un auténtico cambio de Era, que es algo completamente distinto [...]. El término cambio de Era presupone una ruptura paradigmática que incide en los fundamentos de la sociedad, haciendo obsoletos modelos y patrones consagrados en el tiempo"[1].

En este sentido, hablar de la evolución de los conceptos de seguridad y de defensa es hablar de estos cambios que han ocurrido en el mundo de las nuevas amenazas, del crecimiento de la violencia contra los ciudadanos comunes y que ignora las fronteras, todo lo cual impacta en el sistema internacional y en las relaciones de poder para diluir las certezas, las creencias y las prácticas. Estos cambios han alterado radicalmente el fenómeno de la guerra, cuestionando el monopolio de la violencia y el papel de las instituciones estatales, especialmente el de las Fuerzas Armadas.

Van Creveld aporta la tesis de que la guerra ha sufrido una transformación en el sentido que pasa a ser una actividad que deja de perseguir objetivos racionales para convertirse en un fenómeno irracional como consecuencia del menoscabo de la legitimidad de los Estados. La guerra, de esa manera, pierde su propósito político en el sentido clausewitziano y pasa a estar impulsada por otros de orden religioso, cultural, étnico o tecnológico[2].

La investigación realizada por la empresa estadounidense RAND (Research ANd Development), en 2017, muestra que entre 1946 y 2015 el número de países involucrados en conflictos interestatales ha venido disminuyendo. En contraste, el informe también muestra que el número de conflictos intraestatales creció hasta la década de 1990. Después de 1994, tales conflictos cayeron y desde 2012 en adelante los números fueron aumentando, como se muestra en la figura 1.

Los datos muestran que la naturaleza del conflicto ha cambiado, lo que indica que también se necesitan nuevas formas de resolución de conflictos. Los Estados necesitan ajustar sus leyes para brindar apoyo legal a las actividades de sus fuerzas de seguridad, militares o policiales, pero estos cambios encuentran su punto de partida en la comprensión de los conceptos de seguridad y de defensa.

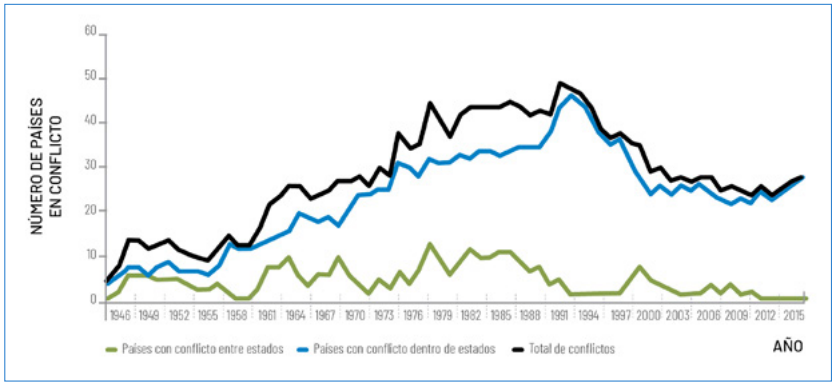
En el campo de las Relaciones Internacionales, el debate teórico sobre el concepto de seguridad está basado en los conceptos de poder y paz. El primero refleja el pensamiento de la escuela realista para la cual los Estados, como actores unitarios y racionales, están rodeados por una estructura en conflicto

1. Visacro, 2019, página 50.
2. Nieto y Cenit, 2015, p.12.

permanente y un sistema anárquico. La segunda perspectiva está asociada con el enfoque de la escuela idealista, que apuesta a conciliar el sistema internacional con la seguridad nacional.

> "Por lo tanto, los realistas tienden a ver la seguridad como derivado del poder: un actor con suficiente poder que alcanza una posición dominante adquiriría su seguridad. Los idealistas, por otro lado, tienden a ver la seguridad como consecuencia de la paz. Una paz duradera proporcionaría seguridad para todos"[3].

FIGURA 1. PAÍSES CON CONFLICTOS INTERESTATALES E INTRAESTATALES, 1946–2015



Fuente: Marshall, 2016.

En verdad, no hay acuerdo en cuanto al concepto de poder en el ámbito internacional. Los diccionarios definen poder como la capacidad de realizar u obtener resultados, pero hay muchas maneras de tener éxito en esa tarea en la que se emplea desde la violencia, la fuerza, la coerción, el control, la interferencia, la autoridad, el ejemplo, la atracción e incluso, la persuasión, es que hablo de una falta de consenso en cuanto a una única definición conceptual del poder.

En el escenario híbrido actual entre Estados nacionales, o con la participación de actores no gubernamentales, convive el llamado *hard power* (poder duro), instrumento de presión tradicionalmente protagonizado por la coerción militar, y el *soft power* (poder blando), concepto teórico creado en 1990 por Joseph Nye, o poder del convencimiento y de las relaciones de atracción y confianza. Este último coloca en escena la dimensión humana de los acontecimientos, para generar un grado mayor de inestabilidad en las mencionadas relaciones de poder. Su obra fue lanzada antes del final de la Unión Soviética y tenía el propósito de ser una alternativa a lo que el autor llamó teoría de la declinación.

En esa época, académicos como Paul Kennedy señalaban el declive de la hegemonía estadounidense en el escenario internacional. La propia población de Estados Unidos creía que su país perdía espacio en la esfera económica contra Japón y Europa (especialmente Alemania). Nye argumentó que ese pensamiento era un error porque Estados Unidos era la Nación más fuerte del mundo en el aspecto militar, económico y en una tercera dimensión que llamó poder blando.

En un análisis posterior de la política exterior de EE.UU., en su libro *La paradoja del poder norteamericano,* Nye plantea que la Casa Blanca, incluso con el respaldo de la fuerza, no podría ejercer la supremacía mundial siguiendo una postura aislacionista, ya que necesitaría cooptar países para abaratar el costo de las alianzas. Por su parte, Evaristo (2019) afirmó que "él defendía el uso de instrumentos de los ámbitos de la cultura, ideología y política para alcanzar objetivos por medio de influencia en lugar de la coerción".

Henriques y Paradelo (2006) afirman que "parte de la agenda política mundial funciona por medio de *hard power,* con amenazas y la aplicación de fuerza militar y la condicionalidad de las ventajas y sanciones económicas. Mientras que el *soft power* es ejercido mediante cooperación y no por coerción. Esta otra perspectiva de ejercer poder permite alcanzar objetivos a través de la autoridad, la persuasión, la atracción y el ejemplo. Un país puede obtener los resultados deseados en política internacional porque otros países admiran sus valores, emulan su ejemplo y aspiran alcanzar su nivel de prosperidad y apertura"[4].

Volviendo a la seguridad, cuando esta se entiende desde la perspectiva política, se puede deducir que la seguridad nacional está relacionada con la supervivencia del Estado, por lo tanto, sus objetivos son mantener la integridad del territorio y el funcionamiento de las instituciones. Desde este punto de vista, se considera que las vulnerabilidades que amenazan las estructuras territoriales e institucionales y el régimen político pueden ser internas y externas, por lo tanto, la dimensión militar, deja de tener protagonismo absoluto entre las expresiones de poder de los Estados, ya que la agresión externa deja de ser la única fuente de amenaza para su existencia.

Esta visión de seguridad se amplía cuando se suma al bienestar de la población, lo que genera una búsqueda de sistemas sectoriales más seguros para la alimentación, el medio ambiente, la salud, el comercio y las finanzas, que aumentan la importancia de los gobiernos, puesto que estos son los principales actores en la construcción de políticas públicas. El concepto de "seguridad humana" surgió en 1994 con el informe sobre desarrollo humano preparado por el Programa de las Naciones Unidas para el Desarrollo (PNUD). "La idea

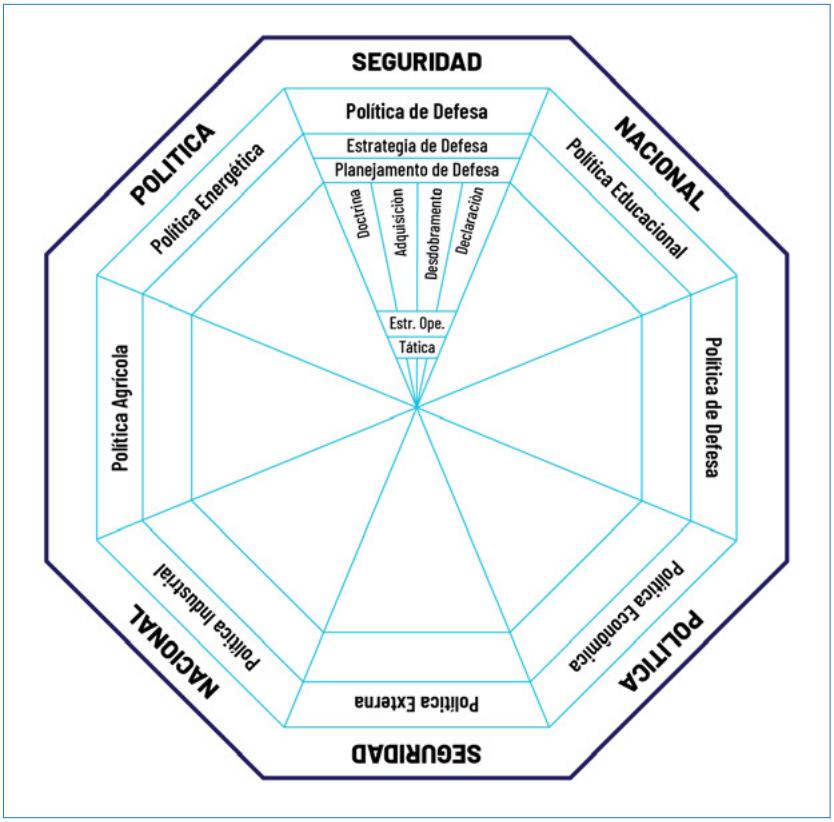
Cuando la seguridad se entiende desde la perspectiva política, se puede deducir que la seguridad nacional está relacionada con la supervivencia del estado, por lo tanto, sus objetivos son mantener la integridad del territorio y el funcionamiento de las instituciones.

de la seguridad humana resultó ser bastante innovadora, ya que contrastaba con la doctrina establecida de la seguridad nacional, cuyo enfoque sigue siendo la defensa y protección del propio Estado como institución y entidad legal"[5].

Este nuevo concepto apunta a amenazas que están más allá de los antagonismos estatales, como la violencia grupal interna, el crimen organizado, el terrorismo, los desastres naturales, las pandemias, las migraciones masivas, el hambre y la miseria. En este escenario, la prevalencia de recursos no militares tanto en la prevención como en la resolución de conflictos está ganando fuerza y el mayor desafío para los estados es encontrar la mejor manera de implementar, interna y externamente, una lista de políticas sectoriales, con el objetivo de garantizar seguridad según su propia percepción de las amenazas, obviamente, sin descartar el uso de la fuerza bajo los auspicios de una política militar de defensa.

> "Se puede ver que los conceptos de política de defensa nacional, planificación de defensa o estrategia de defensa se usan libremente y de la misma manera. En lugar de descifrar la complejidad semántica, Stephanie Neuman utilizó el modelo de telaraña, que se adaptó en la figura a continuación, para pensar mejor sobre todos estos conceptos juntos y que resultó una forma muy apropiada de demostrar la jerarquía de esferas políticas"[6].

FIGURA 2 . ADAPTACIÓN DEL CONCEPTO DE STEPHANIE NEUMAN (1984)



Fuente: Gunther Rudzit e Otto Nogami (2010).

La política de defensa se sitúa así dentro de la política más amplia de seguridad nacional, cuya función principal es alinear los medios militares con los objetivos políticos del Estado. El problema con este escenario es que los límites de acción de cada política ya no son tan claros como en

3. Rudzit, 2005, p.299.
4. Henriques y Paradelo, 2006, p.4.
5. Visacro, 2019, p. 60.
6. Rudzit y Nogomi, 2010, p.11.

La política de defensa se sitúa dentro de la política más amplia de seguridad nacional, donde su función principal es alinear los medios militares con los objetivos políticos del estado.

CV

RODOLFO TRISTÃO PINA

Coronel, Oficial de Estado Mayor del Arma de Comunicaciones y Licenciado en Ciencias Sociales por la Universidad Federal de Río de Janeiro. Posee la Maestría en Ciencias Militares y especialización en Guerra Electrónica. Fue jefe del Centro de Telemática en la ciudad de Fortaleza y asesor de Inteligencia del Comandante del Ejército en Brasil. Actualemente se desempeña en el Comando de la 2da Región Militar en la ciudad de San Pablo en Brasil.

el pasado, debido a los cambios que la posmodernidad trajo a las variables de tiempo, distancia y poder.

"Hoy, lo que está cambiando el mundo tiene menos que ver con la rivalidad de mega-actores que con el surgimiento de los micropoderes y su capacidad para desafiar con éxito a los mega-actores. [...] Ya no es el poder masivo, abrumador y a menudo coercitivo de las grandes organizaciones ricas en recursos con una larga historia, sino el poder de vetar, contrarrestar, combatir y limitar el alcance de grandes actores. Es negar a grandes el espacio eterno para la acción y la influencia que siempre se ha dado por cierto. Es un poder que nace de la innovación y la iniciativa, sin duda, pero también del hecho de que cada vez hay más espacio para que los micropoderes empleen técnicas como el veto, la interferencia, la distracción, el aplazamiento de las decisiones o la sorpresa. Las tácticas clásicas de los rebeldes en tiempos de guerra ahora están disponibles y muestran efectividad en muchos otros campos".

Desde esta perspectiva, el mayor riesgo está relacionado con la posibilidad de vincular actores estatales y no estatales, poco comprometidos con los valores universales que buscan a cualquier costo sus propios intereses (políticos, económicos, ideológicos, éticos, entre otros), en un intento de establecer dinámicas cooperativas basadas en actividades ilegales e informales, para derrocar cualquier ortodoxia que defienda los preceptos tradicionales de seguridad y de defensa.

Conclusión

Se puede concluir que todos los desafíos que plantea la posmodernidad no son más que viejas amenazas sometidas a una nueva dinámica. El problema es que los patrones tradicionales de respuesta estatal han sido anacrónicos y completamente ineficaces. Los marcos conceptuales disponibles y los escenarios actuales se han interpretado de acuerdo con preceptos rígidos y arcaicos, como si los nuevos problemas se subordinan a soluciones preexistentes y no al revés.

Los conceptos de seguridad y defensa están fuertemente influenciados por la fluidez de la coyuntura posmoderna y cada vez es más difícil establecer una clara diferencia entre ellos. Además, esta misma coyuntura hace posible que los Estados nacionales, cuando compiten entre sí, descuiden el uso deliberado de la fuerza para buscar alternativas estratégicas menos agresivas y menos costosas para mantener el apoyo de la opinión pública internacional y su libertad de acción.

Este escenario fortalece el concepto del *soft power,* a pesar de las críticas existentes hechas por pensadores realistas. Es así otra dimensión de poder que asigna distinto protagonismo a la defensa, principalmente en países pacíficos, porque las cuestiones tratadas de forma compartimentada en el ámbito político, económico y social pueden reflejarse

en problemas ligados a la seguridad interna y relativa a la soberanía.

El poder blando, como una forma indirecta de poder, debe ser una preocupación permanente de las Fuerzas Armadas en el contexto de la Estrategia Militar. Eso porque el interés de actores no estatales, o mismo de otros gobiernos, pueden convertirse en un riesgo para la soberanía de los países o amenazar sus objetivos nacionales. Tan importante como preocuparse por cómo será la guerra del futuro, la Estrategia Militar necesita comprender estas relaciones de poder.

Además, la motivación para que haya cooperación entre países también puede encubrir intereses velados. En este siglo, países con pretensiones de convertirse en superpotencias han adoptado políticas de intervención con el propósito de controlar mercados y beneficiarse con ellos de manera significativa. ¿En qué medida esas acciones pueden influir negativamente la cohesión nacional de los países que sufren esas acciones intervencionistas?

El punto importante es que el *soft power* amplía el planeamiento estratégico militar porque puede involucrar variables del campo político, económico, científico-tecnológico o social que el planificador militar muchas veces no tiene facultades para identificar sin el apoyo de expertos, lo que puede contribuir a la construcción de escenarios de defensa incompletos y poco consistentes. Si la incertidumbre ya es una constante de peso en la elaboración de escenarios futuros, la falta de capacidad técnica para elegir las variables correctas agrava la solidez del proceso de planificación estratégica militar, lo que puede ser una vulnerabilidad del proceso.

Se puede decir que las formas de pensamiento, la emoción y el comportamiento humano se destacan como variables de las más importantes en la guerra. Llevar la realidad del poder blando a la planificación de la estrategia militar es una forma de acercar estos conceptos al pensador militar.

Por último, seguridad y defensa son temas transversales, ya que son campos complejos relacionados con diversas actividades humanas. Los militares y la policía, como los principales operadores por sí solos, no podrán actuar de manera efectiva sin el apoyo experto adecuado, ya que este esfuerzo debe ser multidisciplinario.

Por lo tanto, la multidisciplinariedad en la construcción de políticas públicas en los sectores de seguridad y de defensa arrojará mejores resultados en comparación con los modelos actuales desarrollados de forma aislada, en los que la sinergia se produce de manera episódica y no planificada. Necesitamos administradores, ambientalistas, antropólogos, economistas, educadores, ingenieros, geógrafos, juristas, matemáticos, profesionales de la tecnología, profesionales de la salud, sociólogos, urbanistas y otros profesionales calificados como vectores que actúen en estos temas junto con agentes que tienen esta actividad como su oficio. Sin embargo, no hay una solución lista. Este nuevo camino debe construirse con cada paso adelante. ▮

BIBLIOGRAFÍA

Ávalos, A., y Durán, M. (2008). *Fuerzas armadas, seguridad y relaciones internacionales.* Revista Académica de Relaciones Internacionales, núm. 9, octubre de 2008, GERI – UAM, ISSN 1699 – 3950; Recuperado de *http://www.relacionesinternacionales.info*

-

Duarte, P. (2013). *Soft China: O Caráter Evolutivo da Estratégia de Charme Chinesa.* Vol. 34, nº 2, julho/dezembro 2012, p. 501-529. Rio de Janeiro, Brasil. Contexto Internacional.

-

Evaristo, M. (2019). *O paradoxo do poder americano.* O ufanismo americano. O paradoxo do poder americano de Joseph Samuel Nye Junior. p. 2-6. Recuperado de *https://www.academia.edu/35007568/O_paradoxo_do_poder_americano.*

-

Gueraldi, R. G. (s.f.). *A aplicação do conceito de poder brando (soft power) na política externa brasileira.* Trabalho final integrador. Rio de Janeiro, Brasil. Editora Fundação Getúlio Vargas.

-

Henriques, M. C., y Paradelo, A. (2006) *Uma fórmula de Softpower.* Instituto da Defesa Nacional (IDN). Primavera 2006, N.º 113 - 3.ª Série pp. 107-127

-

Masigan, A.J.(2018) *soft power: defense chinese century.* Business World. Recuperado de *https://www.bworldonline.com/soft-power-defense-chinese-century/.*

-

Mcclory, J. (2018). *Soft Power 30.* A Global Ranking of Soft Power 2018. The University of Southern California Center on Public Diplomacy (CPD) & Portland.

-

Oliveira, R.S. de (2010). *A mídia como ator emergente das relações internacionais: seu protagonismo no uso do soft power frente aos desafios das mudanças climáticas.* Tese de doutorado, Centro de Ciências Jurídicas, Universidade de Santa Catarina, Florianópolis, Brasil.

-

Prazeres, J. P. (s.d.). *As FA como Vector de Política Externa.* Recuperado de *https://www.academia.edu/11463624/As_FA_como_Vector_de_Pol%C3%ADtica_Externa.*

-

Reyes, V. (2000). *Filipinas: país latino en Asia.* Estudios Internacionales, 33(129), p. 76-89. doi:10.5354/0719-3769.2011.14979.

-

Visacro, A. (2019). Fazendo as coisas certas: Segurança e Defesa do Estado Moderno. *Cadernos de Estudos Estratégicos* (01/2019), Escola Superior de Guerra, 49-80.

LA REPÚBLICA ARGENTINA Y SUS ESFUERZOS EN CIBERDEFENSA

EL COMPROMISO CON LAS BUENAS PRÁCTICAS COMO PARTE DE SU IDEARIO

Por el GB **TOMÁS RAMÓN MOYANO**

ARTÍCULO CON REFERATO

Palabras Clave:
> Comando Conjunto
> Ciberdefensa
> Ciberseguridad
> Infraestructura

El presente artículo, elaborado por el Estado Mayor del Comando Conjunto de Ciberdefensa, es parte de una ponencia realizada por su anterior Comandante, el GB **Tomás Ramón Moyano,** ante el Inter-American Defense College, en el marco de la "1.a Conferencia sobre Ciberseguridad y Ciberdefensa, Mejores Prácticas y Lecciones Aprendidas", desarrollada en Washington DC el 6 y 7 de noviembre de 2019.

"El propio concepto de "Buena Práctica" otorga una validación que destaca e institucionaliza propiedades y cualidades que hacen a una práctica buena más allá de su contexto específico. El reconocimiento de una Buena Práctica lleva implícito el de su transferibilidad, dado que se la entiende susceptible de convertirse en referencia para la acción en otras situaciones similares. Es necesario considerar sin embargo que una práctica no sólo es buena porque es eficaz y eficiente sino porque lleva incorporados valores que se consideran positivos, en este sentido las prácticas nunca son neutras [...]".

Extraído de Reflexiones en torno al Intercambio de Buenas Prácticas El Ágora – Asociación Civil sin fines de lucro

INTRODUCCIÓN

1. Creación del Comando Conjunto de Ciberdefensa. Pilares organizacionales

En el marco de la transformación que ha experimentado el conflicto en el contexto internacional y los desafíos que este aspecto plantea en materia de Defensa, la República Argentina vio como necesario asumir el compromiso de preparar a sus Fuerzas Armadas para este nuevo escenario. Las acciones liminares a la creación del Comando Conjunto de Ciberdefensa las podemos representar en una sucesión cronológica, materializada en distintos documentos hasta mayo de 2014, momento de su creación. Posterior a ese año, otros documentos fueron complementando o adecuando la nueva organización.

La consideración del ciberespacio como una dimensión operacional utilizada por el hombre con distintos fines, que puede derivar en situaciones de tensión, crisis y conflicto, y la adecuación del Sistema de Defensa Nacional a las nuevas variables del conflicto, sumado a la característica de no ser propia de un ámbito específico, dio origen a la creación del Comando Conjunto de Ciberdefensa (en adelante CCCD) para garantizar la defensa de aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar y aquellos dirigidos a afectar los Objetivos de valor

El Comité de Ciberseguridad surge como una respuesta a la necesidad de reunir a los representantes de las principales áreas del gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada, desarrollar el plan de acción necesario para la implementación de dicha Estrategia.

CV

TOMÁS RAMÓN MOYANO

General de Brigada, Licenciado en Estrategia y Organización de la Escuela Superior de Guerra "Teniente General LUIS MARÍA CAMPOS" y Egresado del Centro de Estudios Hemisféricos de Defensa "WILLIAM J. PERRY". Se desempeñó en 2019 como Comandante Conjunto de Ciberdefensa, representando al Estado Mayor Conjunto como expositor en esta materia en Brasil, Colombia y Estados Unidos. Actualmente es el Comandante de la Fuerza de Despliegue Rápido del Ejército.

estratégico que se determinen para su protección.

Con los documentos rectores que establecen las bases fundacionales del CCCD, se dio inicio a la ardua tarea organizacional con un grupo destacado, pero a la vez reducido de personas. Sobre ellos recayó la responsabilidad de redactar los postulados que fijan la impronta de esta joven, dinámica y cada vez más experimentada estructura. Como es propio de aquellas organizaciones destinadas a evolucionar en el tiempo, se puso énfasis en aquellos aspectos trascendentes que NO van a cambiar y que van a acompañar al CCCD en su tránsito al futuro. En este marco se redactó la Visión, como leitmotiv de sus integrantes y los Valores que sustentan a la organización, los cuales una vez internalizados en cada uno de sus miembros, representan un intangible que trasciende a la organización de la que forma parte.

Comando Conjunto de Ciberdefensa

Visión
El Comando Conjunto de Ciberdefensa aspira a constituirse como la máxima instancia militar de coordinación del Estado Mayor Conjunto de las Fuerzas Armadas de la Nación, con el fin de alcanzar solidaria y armónicamente los objetivos que se determinasen, en un entorno caracterizado por la disciplina, la discreción y la vocación de servicio.

Valores
Ética – Lealtad – Discreción – Disciplina - Vocación de Servicio - Excelencia profesional – Alegría – Armonía -Trabajo en Equipo

Guiado por la visión y coherente con los valores expresados, el CCCD materializa sus acciones a partir de una Misión, clara y definida, otorgando de esta manera a sus integrantes fronteras dentro de las cuales poder desarrollarse.
–

Misión
Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

De acuerdo a la evolución que ha evidenciado la Ciberdefensa en la República Argentina desde el 2010 hasta la actualidad, se ha conformado una estructura que ha trascendido el ámbito del Sistema de Defensa Nacional, pero en el cual el CCCD participa activamente. Dentro de esa estructura y a través de distintas relaciones o vinculaciones, desarrolla las actividades que le son propias, manteniendo como premisa fundamental excluyente el ejercicio de las Buenas Prácticas.

2. El Sistema de Ciberseguridad de la República Argentina

El plexo legal de la República Argentina tiene diferenciados los ámbitos de Defensa y Seguridad a partir de la ley N° 23.554 - Defensa Nacional y la ley N° 24.059 – Seguridad Interior. Excepto en las circunstancias excepcionales que establecen las normas citadas, las Fuerzas Armadas no poseen atribución para involucrarse en aspectos que sucedan en el ámbito de la Seguridad Interior. Tal situación aplica a la protección cibernética. En este marco referencial, la Ciberdefensa en la República Argentina forma parte de un sistema mayor constituido por otros organismos del Estado, que adecuadamente integrados permiten a la Nación el ejercicio pleno de su soberanía.

El ápice del Sistema Nacional de Ciberseguridad está materializado por el Comité de Ciberseguridad, creado por Decreto del Presidente de la Nación Argentina N° 577/17. Posteriormente, esa norma jurídica fue actualizada y ampliada por el Decreto 480/2019.

El Comité de Ciberseguridad surge como una respuesta a la necesidad de reunir a los representantes de las principales áreas de gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada esta, desarrollar el plan de acción necesario para la implementación de dicha Estrategia. Es conveniente aclarar que a pesar de que los ámbitos de actuación en el ciberespacio están divididos en Ciberseguridad y Ciberdefensa, cuando hablamos de Ciberseguridad en términos de políticas o estrategias, nos referimos a un concepto sobre la situación en la cual una Infraestructura Crítica se considera protegida de amenazas o agresiones cibernéticas, proporcionando libertad de acción para el empleo de dicha infraestructura, de acuerdo a los lineamientos establecidos en la Estrategia Nacional de Ciberseguridad.

En el ámbito de la Ciberdefensa propiamente dicha, mediante Decreto del Presidente de la Nación N° 42/2016, se crea en la órbita del Ministerio de Defensa, la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares, con Control Funcional sobre el Comando Conjunto de Ciberdefensa.

Como se puede apreciar, la multiplicidad de actores involucrados en la problemática de la Ciberseguridad, la actualización de normas, la ampliación de atribuciones, entre otros aspectos, dan cuenta de la dinámica que presenta el ciberespacio como nuevo ámbito de operaciones. Para desenvolverse en él, el CCCD considera que adquieren particular relevancia en su accionar las "Buenas Prácticas", las cuales proporcionarán legitimidad a sus actos, convirtiéndose de esta manera, en una eficaz herramienta del Estado para hacer frente a este nuevo escenario del conflicto.

DESARROLLO

1. El Comando Conjunto de Ciberdefensa y la materialización de las Buenas Prácticas

A fin de poder enmarcar las acciones del CCCD en las Buenas Prácticas, hemos tomado como marco teórico las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad"[1], que ofrece la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad", para buscar trazar una relación de correspondencia entre lo descripto en ese documento y el accionar del CCCD, observando que algunas de las Esferas de Interés consideradas en las Buenas Prácticas han sido debidamente desarrolladas por este Comando. Si bien la Guía de referencia apela a un trabajo integral como es el desarrollo de una Estrategia Nacional de Ciberseguridad, también las Esferas de Interés pueden ser aplicadas a una escala menor (el CCCD), para alcanzar los propios objetivos y prioridades de acuerdo con la visión, valores y misión.

El siguiente esquema grafica las siete esferas de interés de las buenas prácticas.

Seguidamente, se describirán aquellas Esferas de Interés asociadas a las Buenas Prácticas en las que mayor injerencia tiene el CCCD.

a.Cooperación Internacional

Desde su creación, el CCCD ha buscado relacionarse internacionalmente con aquellos países de mayor trayectoria y experiencia en Ciberdefensa y con otros países con los cuales, por poseer experiencia similar a la nuestra y por formar parte del marco regional, interesa vincularse. En este sentido, este Comando sostiene tres tipos de relacionamien-

Fuente: elaboración propia del CCCD

1. La Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). 2018. *"Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad"*. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

tos, el primer tipo: Recibimiento de Autoridades, a través de visitas de militares o autoridades extranjeras al CCCD; el segundo tipo: Relaciones Bilaterales, a través de intercambios de personal, reuniones bilaterales, ejercicios y cursos. Tal es el caso de las experiencias realizadas con Brasil, Chile, Colombia, Italia, Japón, Perú, España, Alemania, Israel y Estados Unidos. El tercer tipo de relacionamiento es a través del Foro Iberoamericano de Ciberdefensa. La iniciativa del foro surge como una impronta del Reino de España en la que firma una Carta de Intenciones en mayo de 2016, inicialmente ocho países (Argentina, Brasil, Chile, Colombia, España, México, Perú, Portugal). Posteriormente solicitaron su incorporación al foro Uruguay y Paraguay, sumando a la fecha diez países. El objeto del foro fue promover la colaboración en Ciberdefensa entre las Fuerzas Armadas de los países miembros en las áreas de formación, ejercicios, intercambios de información, investigación, desarrollo e innovación, en el ámbito del ciberespacio como otro dominio inherente a la Defensa Nacional y por lo tanto motivo de análisis, estudio, formación y adiestramiento por parte de las Fuerzas Armadas. En atención al espíritu con que fue creado, en octubre de 2017 se desarrolló en Brasilia el I Ejercicio Iberoamericano de Ciberdefensa. En dicha oportunidad se propuso a la República Argentina como país sede del II Foro Iberoamericano de Ciberdefensa, a fin de continuar los esfuerzos de cooperación para alcanzar los objetivos comunes trazados, para fortalecer las relaciones existentes.

Entre el 20 y 22 de marzo de 2018 se desarrolló en Buenos Aires el II Foro Iberoamericano de Ciberdefensa (FIC) organizado íntegramente por el CCCD donde, además de los representantes de los Estados miembros, se invitó a representantes de los países de la región interesados en la problemática. Asimismo, participaron autoridades militares del Estado Mayor Conjunto de las Fuerzas Armadas, del Ejército, la Armada, y la Fuerza Aérea, autoridades del ámbito académico y de distintas áreas de Gobierno. Durante el desarrollo se dieron exposiciones por parte de las diferentes delegaciones asistentes al evento, donde se reflejaba la problemática de cada país y la manera como abordaban la solución. Como resultado de las intensas jornadas se firmó una Carta de Intenciones cuyos puntos salientes fueron:

1. Desarrollar durante el mes de marzo de cada año el FIC en aquellos países que sean designados sede y durante el mes de octubre de cada año se desarrollará el Ejercicio de Ciberdefensa.
2. Designar al país que se desempeñe como Sede del FIC como Secretaría Pro Tempore y responsable de la carga administrativa que devenga hasta el siguiente Foro.
3. Trabajar para el establecimiento de un protocolo de cooperación

El Comando Conjunto de Ciberdefensa asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de Ciberdefensa.

para la difusión de avisos, alertas y alarmas de ciberataques.
4. Trabajar en la creación y aplicación de una MISP *(Malware Information Sharing Platform),* para intercambio de información entre países iberoamericanos.
5. Brindar apoyo entre países amigos para grandes eventos.
6. Evolución de la Carta de Intenciones del FIC.
7. Evaluar posibilidades de colaboración en actividades de educación y entrenamiento (cursos).

A su vez se dejó plasmado en dicho documento el procedimiento para la incorporación de nuevos países que pretendan incorporarse al FIC. Portugal asumió la responsabilidad de redactar las normas que regirán tanto para la organización de los próximos foros como así también para las pautas que regulan el desarrollo de los ciberejercicios, las cuales fueron aprobadas durante el III FIC. También se propuso integrar al FIC a la República Oriental del Uruguay, para lo cual y conforme al procedimiento establecido y a las comunicaciones efectuadas por la Secretaria del Foro, se aprobó de manera unánime su inclusión.

El 30 de agosto de 2018, en el marco de las Ciberolimpíadas organizadas por Colombia, en su etapa *on line* el CCCD obtuvo el 3er puesto entre 13 países, lo que permitió que este Comando, en representación de las Fuerzas Armadas de la República Argentina, participara en la etapa presencial de ese importante evento. Para tal ocasión el personal seleccionado viajó a Bogotá – Colombia en noviembre de 2018, donde participó a lo largo de tres jornadas de las Ciberolimpíadas.

Entre el 22 y 25 de octubre de 2018 un equipo integrado por personal del CCCD, personal de la Dirección de Ciberdefensa del Ejército y personal de la Dirección de Ciberdefensa de la Fuerza Aérea, participaron del 2do Ejercicio del Foro Iberoamericano de Ciberdefensa, que tuvo lugar en España, en la Base de Retamares, sede del Mando Conjunto de Ciberdefensa español (MCCD). Los objetivos del ejercicio se elaboraron según las Normas para el Funcionamiento del Ejercicio a desarrollarse en el marco del Foro Iberoamericano de Ciberdefensa y fueron:
1. Fomentar la cooperación entre los países pertenecientes al Foro Iberoamericano de Ciberdefensa en este ámbito, sin espíritu de competición.
2. Mejorar la preparación para conducir un Ejercicio Internacional en el marco del Foro Iberoamericano de Ciberdefensa.
3. Entrenar las capacidades técnicas cibernéticas de los equipos involucrados en la actividad.
4. Identificar las posibilidades para realizar intercambio de información.
5. Fomentar el establecimiento del protocolo de cooperación para la difusión de avisos, alertas y alarmas de ataques cibernéticos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.
6. Fomentar la creación de una plataforma electrónica de intercambio de información de *malware* (MISP), para intercambio de información entre los países Iberoamericanos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.
7. Incrementar el conocimiento mutuo de las doctrinas de empleo en el espacio cibernético.

Conforme a las propuestas efectuadas, el FIC 2019 se desarrolló en Brasil y el Ciberejercicio en su tercera edición también tendrá a ese país como Sede.

De la Carta de Intenciones suscripta por los representantes de los países miembros, los puntos más salientes fueron:
1. Elaborar un "Marco de Referencia Doctrinario del Ciberespacio" que defina el rol de las Fuerzas Armadas y su marco de actuación general; y que incluya, además, un glosario de términos unificado en la materia.
2. Estudiar la posibilidad de compartir información, bilateralmente, acerca los siguientes asuntos:
   a. La forma en que están

El Comando Conjunto de Ciberdefensa se impuso como responsabilidad, "Especificar, coordinar la concientización, formación y el adiestramiento especializado en materia de Ciberdefensa para el Personal integrante de las FFAA".

desarrollando operaciones ofensivas, cuál es el proceso y si hay un marco jurídico que respalde estas acciones.

b. Difusión de doctrina conjunta, combinada y multilateral con aliados para el desarrollo de operaciones cibernéticas.

c. Plan de carrera para los cibercomandos y qué estrategias existen para retener el capital intelectual humano capacitado.

d. La forma en que están generando doctrina conjunta para Ciberdefensa.

3. El III Ejercicio Iberoamericano de Ciberdefensa definirá como objetivo integrar y fortalecer la cooperación entre países miembros para reaccionar ante un ataque cibernético con capacidad de respuesta. Se propuso incluir en el objetivo del III Ejercicio Iberoamericano de Ciberdefensa la integración del Planeamiento de Ciberoperaciones en apoyo a las Operaciones de mar, aire y tierra, a fin de continuar generando doctrina en este rubro.
4. Llevar a cabo los desarrollos y gestiones necesarios para implementar, en todos los países miembros integrantes del Foro Iberoamericano, bases integradas en la plataforma MISP (dicha intención ya se materializó).
5. Efectuar sesiones virtuales con los representantes de los países miembros cada 3 meses para dar a conocer buenas prácticas, lecciones aprendidas y casos emblemáticos en cada uno de los países, para compartir con los demás (dicha intención se viene cumplimentando de manera periódica a través de videoconferencias).

b. Legislación y Reglamentación

En esta esfera de Interés, la promulgación de la Legislación respectiva por parte de las distintas carteras ministeriales, como así también las necesidades que surgen para incorporar la Ciberdefensa al planeamiento y ejecución de las operaciones que realiza el Instrumento Militar, proporcionan el *input* para que el CCCD se aboque a la elaboración de la doctrina necesaria para el adecuado empleo de los medios de Ciberdefensa a disposición. La doctrina de Ciberdefensa elaborada en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas (denominada Doctrina Conjunta) sirve de base para la elaboración de la doctrina propia, por parte de cada una de las organizaciones de Ciberdefensa de las Fuerzas Armadas (denominada Doctrina Específica). De esta manera y desde el punto de vista de la Ciberdefensa, el circuito doctrinario queda debidamente articulado para todo el Instrumento Militar. A su vez, personal del CCCD con amplia formación y experiencia participa en equipos *Ad Hoc* para la actualización doctrinaria, asesorando sobre aquellos conceptos de Ciberdefensa que son necesarios incorporar en los diferentes reglamentos.

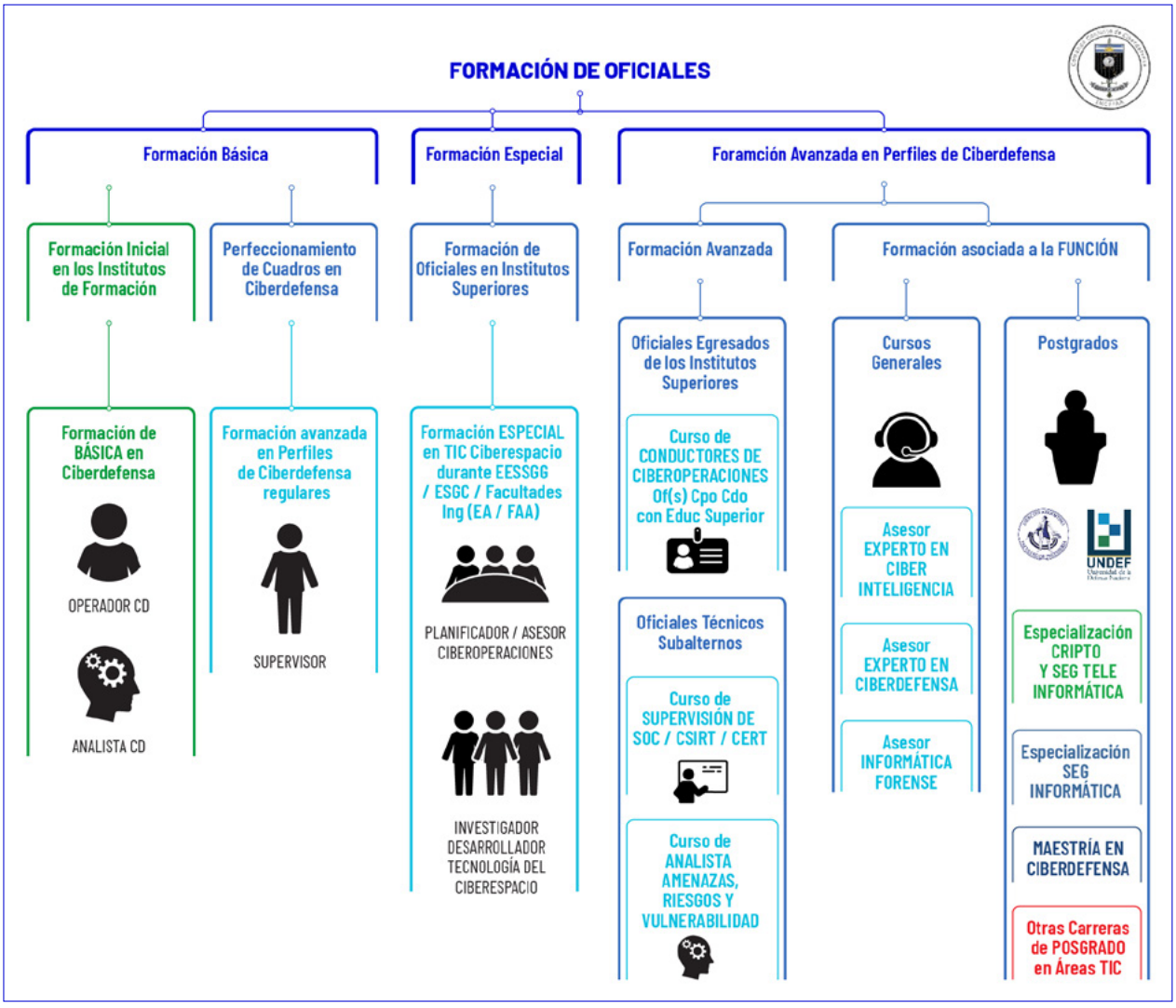
Vinculado con la Cooperación Internacional, a partir de acuerdos bilaterales que el Estado Mayor Conjunto de las Fuerzas Armadas suscribe con países amigos, se ha avanzado en la elaboración de Doctrina de Ciberdefensa Combinada en un paso más para lograr el adecuado entendimiento y avanzar en la aplicación de las Buenas Prácticas de la Ciberdefensa en la ejecución de Operaciones Combinadas.

c. Capacitación, Creación de Competencias y Sensibilización

1. Plan de Formación en Ciberdefensa

En esta esfera de Interés, el CCCD ha trabajado bajo la consideración de que la construcción de una Ciberdefensa eficaz y eficiente no sólo contribuye a mejorar en su conjunto la Seguridad de la Información del Instrumento Militar, sino que, como factor de disuasión, es un objetivo irrenunciable que depende en gran medida de la calidad de la formación de todos cuantos tienen alguna responsabilidad directa en la materia. La consecución de este objetivo debe basarse en la definición, implementación y continuo perfeccionamiento de una formación orientada hacia las funciones de cada uno de los puestos directamente relacionados con activi-

ESQUEMA DEL PLAN DE FORMACIÓN DE OFICIALES



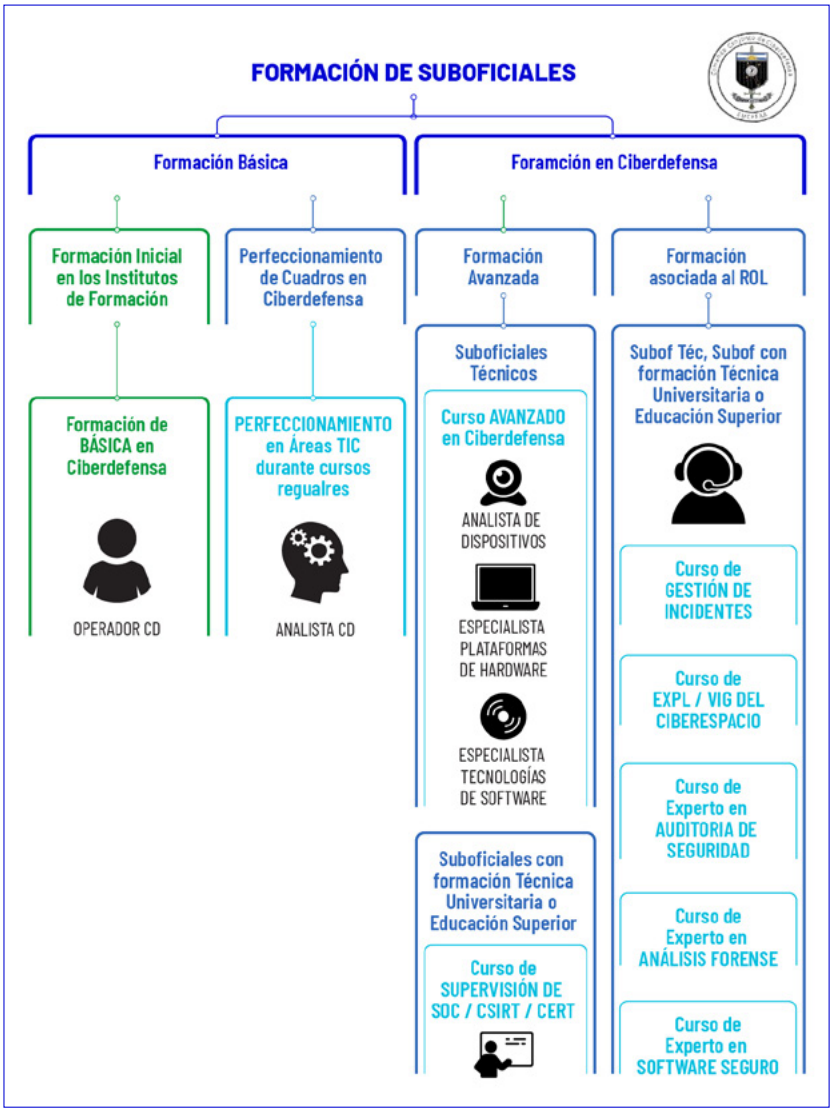
Fuente: elaboración propia del CCCD

dades de Ciberdefensa, tanto en la conducción de Operaciones del Ciberespacio como en los aspectos técnicos y eminentemente operativos. En ese sentido, es necesario alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita el Instrumento Militar para sustentar todos los objetivos de Ciberdefensa.

Conforme a lo expresado precedentemente, el Comando Conjunto de Ciberdefensa asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de Ciberdefensa. Del estudio de los cometidos relacionados con la Ciberdefensa y de las necesidades formativas que de todo ello se derivan, el Comando Conjunto de Ciberdefensa ha desarrollado un Plan de Formación en Ciberdefensa, que será el instrumento para la adquisición, mejora y actualización de competencias necesarias en aspectos relativos a la Ciberdefensa. Este plan facilita, además, la implementación de los trayectos formativos que permitirán alcanzar la capacitación necesaria a cada uno de los distintos grupos de formación identificados.

Un análisis de la situación ha permitido determinar que, en la actualidad, la formación en este ámbito es escasa, parcialmente satisfecha con perfiles técnicos del área TIC, sin conocimientos profundos de las Operaciones Militares ni de Operaciones del Ciberespacio, no está debidamente estructurada ni homologada, y no garantiza la capacitación del personal para el acceso a formación de mayor nivel tecnológico ni para satisfacer las necesidades reales de las FFAA en

ESQUEMA DEL PLAN DE FORMACIÓN DE SUBOFICIALES



Fuente: elaboración propia del CCCD

la Conducción de Ciberoperaciones. No obstante, se considera que la formación en Ciberdefensa se debe apoyar en gran medida en los activos de las FFAA y se acreditarán mediante títulos o certificados obtenidos de la forma que se determine para cada caso.

El Plan fue concebido con el objetivo fundamental de definir los requisitos de formación basados en perfiles, en materia de Ciberdefensa, que deberían alcanzar los integrantes de las FFAA que ocupen puestos de trabajo relacionados con la Ciberdefensa. Será también de aplicación tanto para el personal militar como para el personal civil que se incorpore a las organizaciones de Ciberdefensa. A su vez, este Plan persigue como finalidad la descripción de las responsabilidades generales en formación de Ciberdefensa en el ámbito de las FFAA. En este sentido, y a futuro, los programas de formación y los planes de estudio de los Institutos Militares en donde se desarrolle la formación en Ciberdefensa deberán tener en consideración el presente Plan. En su diseño se ha contemplado, en el mayor grado posible, el aprovechamiento de las estructuras de los Planes de Carreras vigentes en las FFAA. De igual manera, se definen también los mecanismos para la actualización continua en las competencias del personal.

El proceso de evaluación de este plan se llevará a cabo de acuerdo con las normas de evaluación del sistema de enseñanza militar, de manera progresiva, con el propósito de que se encuentre completamente implementado en el corto plazo. El análisis y estudio de los resultados de este plan servirán de base para los futuros reajustes.

Dentro del presente documento se establecen dos partes diferenciadas, una primera relacionada con la identificación de los grupos funcionales del personal relacionado de alguna forma con la Ciberdefensa y sus necesidades formativas, y una segunda relacionada con la mejora y adaptación de este Plan.

2. Plan de Concientización y Sensibilización

Por similitud a lo que sucede en otras áreas, se puede afirmar que en Ciberseguridad el eslabón más débil es el individuo como usuario del sistema. A su vez, si se considera que la innovación y avance tecnológico son continuos y aventajan, en algunos casos, la capacidad de adopción de medidas de seguridad resulta entonces necesario implicar activamente a todos los usuarios en la protección y defensa de las redes y de los sistemas de información vinculados a las FFAA. En este sentido se debe tener presente que la gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de Ciberseguridad. Ello requiere de los usuarios una comprensión particular respecto de los riesgos que existen al operar en este medio, así como del conocimiento de las herramientas para la protección de su información, sistemas y servicios.

La instalación en la conciencia del personal de las Fuerzas Armadas de una sólida cultura de Ciberseguridad proporcionará a todos los actores la responsabilidad y la confianza necesaria para su interacción en un medio tan complejo y sensible como es el del ciberespacio. El CCCD se impuso como responsabilidad la de "especificar, coordinar la concientización, formación y el adiestramiento especializado en materia de Ciberdefensa para el personal integrante de las FFAA", definiendo a la

EJEMPLO DE LÍNEAS DE CONCIENTIZACIÓN Y OBJETIVOS PERSEGUIDOS DEL PLAN DE CONCIENTIZACIÓN EN CIBERDEFENSA

Nro	Líneas de concientización	Objetivos generales de concientización	
1	General	1.1	Dar a conocer los riesgos del ciberespacio.
		1.2	Informar que las FFAA son objetivo de ciberataques, aumentando esta circunstancias el nivel de amenaza al que está sometido su personal.
2	Identificación y Credenciales de acceso	2.1	Concientizar de la importacia de una gestión adecuada de las contraseñas y de otras credenciales de acceso en la protección de la información.
3	Navegación de Internet	3.1	Promocionar el uso responsable de Internet.
		3.2	Difundir hábitos y buenas prácticas de navegación por Internet.
		3.3	Enseñar cómo identificar enlaces potencialmente peligrosos.
		3.4	Recomendaciones específicas para el uso de servicios electrónicos homebanking y pagos on-line
4	Correo electrónico	4.1	Advertir que el correo electrónico es uno de los medios más frecuentes de ciberataque, puesto que no es un método totalmente seguro para intercambiar información fuera del ámbito de las FFAA.
		4.2	Enseñar cómo identificar mensajes potencialmente peligrosos ("pishing" y fraudes on-line)
5	Servicios en la red	5.1	Difundir recomendaciones de uso seguro de servicios de internet, conciliando la productividad con la seguridad.
		5.2	Recomendaciones específicas para proteger la información personal en Internet.
6	Actividad en redes sociales	6.1	Explicar a los usuarios cómo pueden ser víctimas de ataques de "ingeniería social", especialmente en las redes sociales.
		6.2	Promover la prudencia en el uso de las redes sociales, especialemente a la hora de publicar información.
		6.3	Prevenir situaciones de riesgo para las FFAA o terceras personas que tienen relación con los usuarios.
7	USB y soportes de información	7.1	Avisar de los riesgos asociados al uso de soportes y dispositivos de almacenamiento USB (infección, pérdida de información y posible infracción de la normativa)
8	Protección del entorno personal	8.1	Explicar a los usuarios cómo pueden proteger su PC personal.
		8.2	Enseñar cómo es posible trasladar esta protección a los dispositivos y redes personales en el ámbito personal.
9	Fuera de la oficina: Movilidad	9.1	Informar a los usuarios de su especial vulnerabilidad en situación de movilidad fuera de su puesto de trabajo.
		9.2	Explicar a los usuarios cómo pueden proteger los dispositivos móviles y portátiles tanto en el ámbito profesional como el personal.
10	Prevención y reacción ante los incidentes	10.1	Poner de manifiesto la importancia de la participación de los usuarios en la detección temprana y respuesta a incidentes de ciberseguridad.
		10.2	Fomentar que el usuario acuda a informarse sobre los riesgos y alertas de seguridad a través de los portales falsos.
		10.3	Enseñar a identificar incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
		10.4	Difundir el procedimiento para comunicar incidencias de seguridad, sean reales o falsas alarmar a las unidades encargadas de gestionarlas.

Fuente: elaboración propia del CCCD

El Comando Conjunto de Ciberdefensa elaboró un Plan de Concientización de Ciberdefensa para el Personal de las Fuerzas Armadas, que tiene por finalidad definir un conjunto de acciones dirigidas a todos los usuarios de las Tecnologías de la información y la comunicación (TIC), integrantes de las FFAA para que sean conscientes de los riesgos y amenazas a los que diariamente se enfrentan en el ciberespacio.

concientización como las acciones necesarias para facilitar al personal la compresión de las amenazas generadas por los potenciales adversarios o elementos hostiles en el ciberespacio; así como la manera en la que, tanto a nivel individual como colectivo, se puede y debe contribuir a evitar o contrarrestar estas amenazas, reaccionando oportuna y adecuadamente. Al respecto se debe dejar establecido que la seguridad de la información es responsabilidad de todos los miembros de las Fuerzas Armadas, los cuales deberán estar adecuadamente formados y concientizados para el satisfactorio cumplimiento de sus responsabilidades.

A fin de contribuir a la toma de conciencia del personal, el CCCD elaboró un **Plan de Concientización de Ciberdefensa para el Personal de las Fuerzas Armadas,** el mismo tiene por finalidad definir un conjunto de acciones dirigidas a todos los usuarios de las Tecnologías de la información y la comunicación (TIC) e integrantes de las FFAA para que sean conscientes de los riesgos y amenazas a los que diariamente se enfrentan en el ciberespacio, así como la forma de prevenir, atenuar y mitigar sus efectos. Como aspecto secundario se persigue la extensión de estas acciones a su ambiente familiar, con independencia a que su puesto de trabajo implique o no el uso de las TIC, toda vez que este personal es susceptible de hacer uso de estas en otros ámbitos, con impacto posible en el entorno de las FFAA. A su vez, el plan describe las responsabilidades generales de la concientización en el marco de las FFAA y los recursos necesarios para su implementación.

d. Gestión de Riesgos para la Ciberdefensa / Preparación y Resiliencia

El CCCD ha confeccionado bajo un enfoque sistémico un manual de procedimientos estandarizados, los que pueden considerarse como actividades de procesos y subprocesos de Ciberdefensa Pasiva. Se enfocan principalmente en la descripción de los Procedimientos Operativos Normales destinados a ejecutar la Ciberdefensa de las Infraestructuras Críticas de la Información del Instrumento Militar (Sistemas de Comando y Control, Sistemas de Comunicaciones, Sistemas de Armas, Sistemas de Control, Sistemas Computarizados en apoyo a las Operaciones Militares) y otros Recursos Esenciales de Sistemas, Redes, Datos e Información de las FFAA, siendo de aplicación en tiempo de paz para adiestrar, entrenar y ejecutar las acciones del Sistema de Respuesta de Ciberdefensa por parte del Centro de Operaciones de Ciberdefensa del CCCD principalmente. El Manual de Procedimientos fue difundido a las FFAA para su implementación como así también para la incorporación de mejoras, conforme a las Lecciones Aprendidas de la Experiencia de cada organización, dado que las amenazas a la Ciberseguridad se presentan tan dinámicas como impredecibles, cualquier procedimiento que se instaure, requiere una actualización constante.

e. Servicios de Infraestructura Fundamental y Servicios Esenciales

Conforme a la misión impuesta, el CCCD debe estar en capacidad de repeler aquellos ciberataques contra las Infraestructuras Críticas de la Información y las Comunicaciones y los activos del Sistema de Defensa Nacional[2] y del Instrumento Militar. No obstante, a lo largo de los años y con especial énfasis desde la creación del CCCD, diversos documentos políticos han coincidido en señalar que:

1. Relacionado a Amenazas Cibernéticas: Resulta necesario encarar el abordaje de esta problemática desde la perspectiva de la Defensa Nacional a fin de adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional como así también aquellas que sean asignadas a dicho sistema para su protección.

2. El Sistema de Defensa Nacional se encuentra definido en el Art 9 de la Ley 23.554 - Defensa Nacional

CIBERDEFENSA

PROCESOS Y SUBPROCESOS

Análisis en Tiempo Real
> Centro de llamadas
> Monitoreo de eventos y priorización de incidentes en tiempo real

Inteligencia y Análisis de Tendencias
> Recopilacion y análisis de noticias del ciberespacio
> Distribución de noticias del ciberespacio
> Creación de noticias del ciberespacio
> Fusión de noticias del ciberespacio
> Observatorio de Tecnologías y Tendencias
> Advertencias, alertas y alarmas de amenazas, vulnerabilidades, incidentes y ciberagresiones
> Evaluación de amenazas

Análisi de Incidentes y Respuesta
> Análisis de incidentes
> Análisis de actividad sospechosa o maliciosa
> Servicios de detección de Intrusiones
> Coordinación de respuesta a incidentes
> Implementación de costramedidas
> Respuesta "en sitio" a incidentes
> Respuesta remota (on-line / off-line) a incidentes
> Respuesta a vulnerabilidades
> Coordinación de Respuesta a vulnerabilidades
> Respuesta a componentes o dispositivos afectados
> Coordinación de Respuesta a componentes o dispositivos afectados
> Continuidad de las operaciones y planeamiento de recuperación antes desastres

Auditoría y Amenza Interna
> Recopilación, retención y almacenamiento de datos para auditorias
> Creación de contenido y administración de datos para auditorias
> Apoyo en caso de amenaza interna
> Investigación en caso de amenaza interna

Exploración y Evaluación
> Mapeo y estadística de redes
> Búsqueda de vulnerabilidades
> Evaluación de vulnerabilidades
> Prueba de intrusión

Aptitudes de Máxima Capacidad
> Análisis de riesgos
> Protección de IICC / Recursos Esenciales
> Consultoría en seguridad (Tecnológica y Legal)
> Sensibilización y concientización
> Formación y Capacitación
> Evaluación de producto
> Certificación de producto

PROCESOS Y SUBPROCESOS

Análisis de Dispositivos y Componentes
> Manejo de componentes, dispositivos o imágenes forenses
> Análisis de implantes y malware
> Análisis de componentes, dispositivos o imágenes forenses

Apoyo al Ciclo de Vida de Herramientas del Sistema de Respuesta
> Obtención y mantenimiento de Dispositivos de Protección de Borde
> Obtención y mantenimiento de Infraestructura del Sistema de Respuesta
> Ajuste y mantenimiento de sensores
> Servicios de soporte en lúnea para descarga de software y firmware
> Distribución de actualizaciones de software, firmware y hardware
> Creación de "firmas" personalizadas
> Ingeniería y despliegue de herramientas de ciberseguridads
> I+D de herramientas de ciberseguridad y ciberdefensa
> Scripts y automatización

Aptitudes de Máxima Capacidad
> Planeamiento de Operaciones del Ciberespacio
> Conciencia de la situación
> Coordinación, comando y Control de Operaciones
> Gestión de la Interoperabilidad de sistemas y redes
> Integración de metadatos y Correlación de eventos
> Servicios de mesa de ayuda para PPOONN
> Construcción de Conocimiento y Entrenamiento
> Virtualización y simulación
> Servicios de Ciberequipo Colorado
> Actualización de normas legales, técnicas o doctrinas
> Difusión de Tácticas, Técnicas y Procedimientos (TTPs)
> Relación con los Medios de Comunicación
> Acciones de Respuesta Inmediata (Canalizar, Bloquear o Detener, Neutralizar o Mitigar, Degradar, Anular)

FUNCIONES
> Reactivas
> Proactivas
> Gestión de Calidad de Seg Información
> Preventivas
> Otras

2. Relacionado a Riesgos (ataques a objetivos estratégicos): El Sistema de Defensa Nacional debe planificar y proteger los objetivos estratégicos que puedan ser objeto de una agresión. La atención de este riesgo debe focalizarse particularmente en aquellas infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes.

Considerando los dos conceptos referidos, será responsabilidad del CCCD, planificar la protección cibernética de aquella Infraestructura Crítica y Objetivos Estratégicos, alguno de los cuales prestarán un servicio esencial a la Nación. En esa planificación adquirirá un valor especial las vinculaciones con todos aquellos estamentos del Estado, necesarios para lograr las coordinaciones a fin de evitar superposiciones en el esfuerzo que demande la protección. Asimismo, debe contemplarse un estrecho relacionamiento con el ámbito privado, ya que muchos de los servicios esenciales del país están en manos de ese sector. En tal sentido, el ejercicio de las Buenas Prácticas y fundamentalmente los antecedentes que se tengan de su correcta implementación en otras esferas de Interés, serán de particular importancia ya que operarán como un catalizador para generar los lazos de confianza necesarios para la eficiente y eficaz Ciberdefensa del objetivo que se trate.

La República Argentina, en la búsqueda de la Ciberseguridad y Ciberdefensa de sus Infraestructuras críticas, viene realizando esfuerzos que se materializan en el ámbito político, legislativo, judicial, académico y científico tecnológico.

CONCLUSIONES

Los distintos Estados han buscado enfrentar las amenazas y riegos que implica el ciberespacio y que afectan a los conceptos de seguridad y defensa de diferentes maneras, pero que básicamente responde, entre otros aspectos, a la conformación de estructuras organizativas que permitan proteger sus activos digitales; a la adecuación del marco legal que le permita desenvolverse en ese ambiente para marcar los límites que tiene su accionar y penalizar a quienes los infringen; a la incorporación de contenidos en sus programas educativos, buscando desde la temprana edad crear conciencia de los riesgos que acechan en el ciberespacio y facilitar la formación de especialistas; a la suscripción de acuerdos internacionales que favorezcan la cooperación de esfuerzos y a la creación de estrategias y políticas que permitan alcanzar los objetivos deseados.

Las organizaciones internacionales también se han esforzado en dotar con modelos o estrategias para afrontar las amenazas de Ciberdefensa y Ciberseguridad de los Estados. Han publicado varios documentos o estándares, como la *Guía de la ciberseguridad para los países en desarrollo* (ITU 2007) o el *National Cybersecurity Strategy Guide* (ITU 2018). Ambos son modelos de referencia basados en la valoración de activos, capacidades, necesidades, amenazas y riesgos en sectores públicos y privados del Estado para construir y ejecutar una estrategia de ciberseguridad nacional. No podemos dejar de hablar de entidades de estandarización como la Organización Internacional de Normalización (ISO), que con sus *Sistemas de Gestión de Seguridad de la Información (SGSI)* contenidas en la ISO/IEC 27000, *Tecnologías para la seguridad de la Información y Técnicas de Seguridad* pretende dar una propuesta más orientada a los aspectos específicos de seguridad en una entidad u organización.

La República Argentina, en la búsqueda de la Ciberseguridad y Ciberdefensa de sus Infraestructuras críticas, viene realizando esfuerzos que se materializan en el ámbito político, legislativo, judicial, académico y científico tecnológico. La creación del Comando Conjunto de Ciberdefensa es parte de la respuesta, desde el punto de vista de la Defensa, a la problemática que plantea el ciberespacio. A pesar de que, como se expresara en el párrafo precedente, existen modelos integrales para encarar la Ciberseguridad y la Ciberdefensa, el país no ha logrado adaptarse completamente a alguno de estos modelos.

No obstante, desde su origen, el CCCD ha buscado erigirse como un referente en materia de Ciberdefensa, donde el ejercicio de las Buenas Prácticas en todo su accionar responde a los conceptos rectores de su creación. Asimismo, y a partir de las relaciones orgánicas y funcionales otorgadas para su vinculación con las Direcciones de Ciberdefensa de las Fuerzas Armadas, permite trasladar su impronta a ellas. Su relacionamiento internacional, fundamentalmente a través del Foro Iberoamericano de Ciberdefensa como así también la participación en otros espacios de debate, es un intento de intercambiar experiencias y conocimientos que resulten beneficiosos para la organización. En el ámbito de la formación y concientización, se considera que la excelencia en la capacitación de los recursos humanos es fundamental. A partir de esa premisa y a través de la elaboración de sendos planes, el CCCD pretende dar un aporte a los decisores que tienen en sus manos la posibilidad de su implementación y articulación. La gestión de riesgos a partir de la elaboración de un Manual de Procedimientos, que se suma a la elaboración de Doctrina Conjunta y Combinada, ha tenido su correlato de éxito en la ciberseguridad y Ciberdefensa de grandes eventos, tal como fue la colaboración prestada con miembros del CCCD en el Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT por su sigla en inglés: *Computer Security Response Team*) del Gobierno de la Ciudad Autónoma de Buenos Aires, durante la realización de los Juegos Olímpicos de la Juventud en el 2018, como así también durante la Ciberdefensa de la Cumbre del G-20, realizada en Buenos Aires

en diciembre de 2018. El enfoque que adoptan distintos documentos políticos, en los aspectos referidos a riesgos y amenazas cibernéticas, le confieren al CCCD la posibilidad de la planificación de la Ciberdefensa de aquellas Infraestructuras Críticas y Objetivos Estratégicos que el nivel político le asigne para su protección, en un ambiente tan difuso y sin límites físicos como es el ciberespacio, a lo que se suma la dificultad de la atribución y donde el CCCD deberá articular su accionar con el ámbito público y privado, resulta casi condición *sine qua* non la transparencia y las buenas prácticas.

En el desarrollo del presente trabajo se ha intentado establecer, por analogía, pero a un nivel sensiblemente inferior, utilizando como marco conceptual las esferas de interés establecidas en las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad" que ofrece la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad", aquellos aspectos que ha podido desarrollar el CCCD, en su reducido radio de acción como es la Ciberdefensa. Muchos de los aspectos referidos fueron realizados por iniciativa propia. Es de prever que, a partir de la recientemente promulgada Estrategia de Ciberseguridad Nacional, la expansión del Comité Nacional de Ciberseguridad con la participación de otras carteras ministeriales, la definición de términos a partir de un glosario común, sumado a la manera de definir las infraestructuras críticas, impulsarán acciones sobre los distintos actores responsables de la Ciberseguridad/Ciberdefensa, que en el caso particular del CCCD potenciarán el crecimiento de los aspectos ya referidos en un intento de alcanzar las Capacidades de Ciberdefensa planificadas para el corto, mediano y largo plazo, a fin de proporcionar a la República Argentina de una organización valiosa para la Ciberdefensa de sus activos digitales y al Instrumento Militar de un elemento multiplicador de fuerzas. En ese escenario incierto que representa el futuro, el CCCD no abandona un instante el esfuerzo que la tarea le demanda.

BIBLIOGRAFÍA Y SITIOS WEB CONSULTADOS

Marco Legal

Ley N° 23.554 – Defensa Nacional. *Boletín Oficial de la República Argentina*, 13 de abril de 1988.

-

Ley N° 24.059 – Seguridad Interior. *Boletín Oficial de la República Argentina*, 6 de enero de 1992.

-

Decreto Presidencial N° 42/2016 – Administración Pública Nacional (Modificación). *Boletín Oficial de la República Argentina*, 08 de enero del 2016.

-

Decreto Presidencial N° 577/2017 – Comité de Ciberseguridad (Creación). *Boletín Oficial de la República Argentina*, 31 de julio del 2017.

-

Decreto Presidencial 480/2019 – Comité de Ciberseguridad (Modificación). *Boletín Oficial de la República Argentina*, 12 de julio del 2019.

-

Resolución Ministerial N° 343, Ministerio de Defensa, del 14 de mayo de 2014.

Doctrina Militar

Estado Mayor Conjunto de las Fuerzas Armadas. Reglamento Orgánico del Comando Conjunto de Ciberdefensa – Proyecto (OC 30-19), Buenos Aires, 2019.

-

Comando Conjunto de Ciberdefensa, Plan de Formación en Ciberdefensa, Buenos Aires, 2018.

-

Comando Conjunto de Ciberdefensa, Plan de Concientización en Ciberdefensa, Buenos Aires, 2018.

Acuerdos Internacionales

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Madrid, España, 27 de mayo de 2016.

-

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Buenos Aires, Argentina, 22 de marzo de 2018.

-

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Brasília, Brasil, 17 de abril de 2019.

Material Académico

Unión Internacional de Telecomunicaciones, Banco Mundial, Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. 2018. "Guía para la elaboración de una estrategia nacional de ciberseguridad

-

Participación estratégica en la ciberseguridad". Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). Consultado en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf, el 25de octubre de 19.

-

Unión Internacional de Telecomunicaciones. "Guía de ciberseguridad para los países en desarrollo", 2017. Consultado en http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf, el 25 Oct 19.

-

Unión Internacional de Telecomunicaciones. "Guide to developing a national cybersecurity strategy", 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf, el 26 Oct 19.

-

Organización Internacional de Normalización, norma ISO/IEC 27001. "Tecnologías para la seguridad de la Información y Técnicas de Seguridad", 2017. Consultado en https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/, el 26 de octubre de 19.

-

El Ágora Asociación Civil sin fines de lucro. "Reflexiones en torno al Intercambio de Buenas Prácticas". Consultado en https://www.elagora.org.ar/site/documentos/Intercambio-BP.pdf, el 20 de octubre de 19.

LAS BUENAS LECTURAS COMO FORMADORAS DEL LIDERAZGO

Palabras Clave:
> Doctrina
> Pensamiento crítico
> Lectura

Por GD (R) **GUSTAVO JORGE L. MOTTA**

No existe un buen comandante con intelecto limitado
Clausewitz en *De la Guerra*

Así como un médico actualiza sus conocimientos para curar y decidir mejor en el quirófano o en el consultorio; o un contador moderniza su biblioteca virtual para identificar problemas y determinar las mejores soluciones contables, la profesión de las armas requiere de una constante preparación intelectual.

Detrás de un porte marcial, la uniformidad, las rutinas y los procedimientos más cercanos a una ajustada máquina que a un homo sapiens, son las Fuerzas Armadas (FFAA) de todo el mundo que han prohijado pensadores brillantes, originales y conductores de fuste.

El ejercicio de la profesión de las armas no sofoca la libertad de pensamiento. Por el contrario, la estimula, porque los conflictos modernos requieren de una gran capacidad de adaptación. Las soluciones a los problemas militares complejos no son copias regimentadas de la doctrina vigente. Ella no es infalible y siempre requiere juicio en su aplicación. El oficial poco imaginativo se resguardará en sus definiciones y contenidos y la recitará de memoria. Pero no entenderá el sentido de su aplicación para cada caso particular.

La doctrina cumple un rol fundamental. Fue redactada sobre la base de la experiencia y la sangre de muchos soldados. En los niveles inferiores, la doctrina de procedimientos se aplicará, en general, tal como se enseña. En otros niveles, será un sistema más amplio que abarcará la esencia, las metas y la naturaleza de la guerra a enfrentar.

De alguna forma, la historia nos enseña que debemos conocer la doctrina en profundidad, porque nos ayudará en el caos de la guerra. Esta nos da una forma de pensar que no está limitada a reglas prescriptivas. Una doctrina bien aplicada lleva a un comportamiento consistente, a la confianza mutua y a una acción colectiva, pero siempre, sin restringir la iniciativa.

Para contribuir con el desarrollo del pensamiento crítico y las habilidades como conductor militar se requiere, además del estudio de la doctrina, la realización de una lectura permanente y continua a lo largo de toda la carrera militar (y de toda la vida).

La palabra es la expresión del pensamiento. Como cualquier otra cosa en la vida, el pensamiento se forma con la lectura abundante de buenos libros. Si la palabra es confusa, es porque el pensamiento lo es y porque ha sido formado focalizándose en la urgencia, antes que ser formado en la importancia y en el análisis de contenidos.

La formación del conductor militar debe ser siempre integral, para abarcar lo intelectual, lo técnico-profesional, la aptitud física y lo espiritual. Aspectos que nunca deben descuidarse y en ello la lectura juega un rol fundamental. El hábito de la lectura es sano, formativo y rinde frutos en forma constante.

Si pensamos en el liderazgo actual (y de todos los tiempos), este se verá sólidamente reforzado cuando los subordinados vean que quien está frente a ellos se expresa y conduce con la autoridad que da el conocimiento.

Las urgencias en la vida del oficial son tantas, que los libros buenos se van apilando “para leer cuando haya tiempo”, y al final uno se encuentra con esa pila de libros sin leer cuando se retira.

El oficial no puede conformarse con ser un especialista, aunque de por sí es bueno que lo sea en alguna

rama de la profesión. Cuanto más ascienda en sus responsabilidades, más generales y abarcativos deberán ser sus conocimientos. Como se dijo anteriormente, la historia es fundamental, pero además, la táctica, la estrategia, la geografía, la defensa, la psicología, las relaciones internacionales, la geopolítica y la sociología, entre otras disciplinas, ayudarán a completar la mochila del conductor. Probablemente, sin darse cuenta, en momentos de su vida militar deberá valerse de esos contenidos para tomar una decisión.

Cada integrante de las fuerzas militares debería tener una lista de lectura básica y otra expandida de libros necesarios para cultivar su mente, sea como conductor, integrante de un Estado Mayor o miembro de una rama determinada de su fuerza.

Estos libros deben ser infaltables en su biblioteca. La lectura meditada y profunda es una obligación individual y su comprobación debería ser sistémica, a lo largo de toda la carrera. Pero cuidado, que leer sin comprender, es una pérdida de tiempo. Repetir o leer resúmenes elaborados por algún lector o camarada "aplicado" no sirve. Leer para entender demanda interés, esfuerzo y habilidades cognitivas.

En la actualidad, los medios sociales han incrementado el uso de la tecnología y eso ha causado que el gusto por la lectura haya decrecido notablemente, en beneficio de la urgencia. Ahora se ejercita más la reacción que la acción meditada. Es positivo que se ejercite la reacción inmediata, siempre y cuando se haya formado bien el pensamiento para dar lugar al sentido común. Se ha priorizado el análisis –la separación de partes de un todo– antes que la síntesis y la composición de un pensamiento nuevo deducido o inducido de diferentes análisis. La toxicidad de algunas redes y plataformas y la falta de conocimiento aplicado producen efectos negativos y posiblemente irreversibles.

El reflejo de esta tendencia moderna ha llevado a que los oficiales jóvenes y de edad media tiendan únicamente a leer reglamentos militares del nivel táctico. Esta moderna tendencia se refleja en hablar o emitir juicios de razón prescriptivos –los que indican qué hacer y cómo hacer, sin reflexión previa– y la tendencia de hablar comenzando por infinitivos, i.e. "atender aquí" o bien "los de tal nombre, levantar la mano", etc.

Asimismo, la lectura apresurada y prescriptiva ocasiona que cuando se escribe, se haga en forma confusa, en párrafos largos que solamente dificultan la comprensión. Hasta se pueden leer documentos oficiales compuestos de oraciones sin verbo, u oraciones de una página de extensión.

Por esta razón, se propone una lectura formativa y continua, como contribución a la base común de pensamiento. Por supuesto, que esto no significa minar la libertad intelectual imprescindible en el avance del conocimiento. La propuesta permitirá comprender contextos, analizar fuentes, comparar con otra información disponible, detectar tergiversaciones, descartar lo que no sirve y, sobretodo, desarrollarse y decidir mejor, para evitar las manipulaciones con otros propósitos que, lejos están de contribuir a la comprensión y al estudio de un tema.

Seguramente, el lector estará pensando que está de acuerdo con lo dicho hasta aquí, pero que no sabe por dónde empezar o seguir y, es posible, que lo vea como un vano esfuerzo. La profusión de publicaciones sobre algunos temas puede marearnos. Por ello, se deberían fijar algunas prioridades. La lectura profunda es algo que lleva años. Se sugiere contar con la ayuda de jefes o de camaradas y, seguramente, con aquellos profesores y especialistas de las diferentes materias que podrán guiarnos en la búsqueda y adquisición, para tener en cuenta que algunos de ellos están disponibles en Internet.

Más abajo se agrega, a modo de ejemplo una lista de libros básicos y otra expandida a modo de menú. El criterio es que para el profesional de armas un buen comienzo puede girar alrededor de la lectura de tácticas, operaciones militares, historia militar, estrategia y ciencias sociales (relaciones internacionales y geopolítica), etc. También en las lecturas de los fracasos y éxitos de las campañas militares, en las memorias de aquellos que vivieron de cerca los conflictos y en las fallas en las operaciones militares, como además en la estrategia general, militar y operacional.

El orden empleado no significa prioridad alguna. Seguramente, que ella es materia muy opinable. Por esa razón, dejo librado a cada uno de los interesados a elaborar su propia lista de lectura, teniendo en cuenta que lo que encuentran más abajo constituye "una" lista y no "la lista".

Y recuerde... es un deber de todo superior estimular, motivar y fomentar la lectura de los integrantes de su unidad.

Continúa >

CV

GUSTAVO JORGE LUIS MOTTA

El General de División (R) Gustavo Motta es Oficial de Estado Mayor del Ejército Argentino, Licenciado en Estrategia y Organización del Instituto de Enseñanza Superior del Ejército (2002) y posee un Diploma en Gestión Gerencial del Instituto Tecnológico de Buenos Aires (ITBA). En ese Instituto ha realizado estudios de Dirección de Proyectos y de Tablero de Comando / Balance Scorecard. Actualmente se desempeña como Profesor de la Materia Bases de las Contingencias en la Maestría de Estrategia Militar y es titular de Cátedra de la Escuela Superior de Guerra Conjunta. En la FADENA es Profesor de Bases y Doctrina de la Defensa Nacional y de Instrumento Militar en la Maestría en Defensa Nacional.

LISTA BÁSICA DE LIBROS

TÍTULO	AUTOR	OBSERVACIONES
La estrategia La aproximación indirecta	Basil H. Liddell Hart	Biblioteca del Oficial - Círculo Militar Volumen 719
La Segunda Guerra Mundial (1939-1945). Historia Táctica y Estratégica	J F C Fuller.	Biblioteca del Oficial - Círculo Militar
Estrategia, el camino	de Vergara Evergisto.	Editorial Universitaria del Ejército (EUDE)
Estrategia, métodos y rutinas	de Vergara, Evergisto.	EUDE
El arte de la guerra	Sun Tzu	Varias ediciones
Understanding Modern Warfare	David Jordan (Autor), James D. Kiras (Autor), David J. Lonsdale (Autor), Ian Speller (Autor), & 2 más	Idioma Inglés
Modern Strategy	Gray, Colin S.	Idioma Inglés
Creadores de la Estrategia Moderna. 3 tomos	Edward Mead Earle	Biblioteca del Oficial - Círculo Militar
Estrategia Una Historia	Freedman, Lawrence	La esfera de los libros
The direction of War *Contemporary Strategy in Historical perspective*	Hew Strachan	Idioma Inglés
Historia del General San Martín	Bartolomé Mitre	
Manuel Belgrano Estadista y prócer de la Independencia Hispanoamericana	Aníbal Jorge Luzuriaga	Universidad de Morón
Guillermo Brown	Guillermo A. Oyarzábal	Instituto de Publicaciones Navales
General Norman H. Schwarzkopf AUTOBIOGRAFIA Tapa dura (1993)	Norman Schwarzkopf	Plaza & Janes S.A Editores
Manual de la guerra de maniobras	William S. Lind	Biblioteca del Oficial - Círculo Militar
Infortunios Militares, la anatomía del fracaso en la guerra	Cohen Elliot; Gooch John	Instituto de Publicaciones Navales
Memorias de un soldado	Heinz Guderian	Biblioteca del Oficial - Círculo Militar
The utility of force	Rupert Smith	Idioma inglés
Routledge Handbook of Air Power-1st Edition	John Andreas Olsen	Idioma inglés
Principles of Maritime Strategy	Julian Stafford Corbett	Idioma inglés
Los Comandantes	Bob Woodward	Ediciones B
Escipión, El Africano.	Liddell Hart, B.	Ed Rioplatense
El pensamiento y la guerra	Jean Guitton	Ediciones Encuentro
Historia de la Guerra	John Keegan	Turner Noema
Estrategia, la logica de paz y guerra	Edward Luttwak	Instituto de Publicaciones Navales
Auge y caída de las grandes potencias	Kennedy, Paul	DEBOLSILLO
Geopolítica del Mar Argentino	Koutoudjian - Martin - Ohanessian - Caruso - Flores Zapata – Anschutz - El Mankabadi	Instituto de Publicaciones Navales

Continúa >

TÍTULO	AUTOR	OBSERVACIONES
Tropas Blindadas en la Batalla. Contraofensiva de las Ardenas y Defensa de St. Vith	Carlos Peralta	Biblioteca del Oficial - Círculo Militar
Geopolítica tridimensional Argentina: Reflexiones para el siglo XXI	Koutoudjian – Fraga – Auel – Quellet	EUDEBA
La Seguridad Internacional Post 11S	Bartolomé, Mariano	Instituto de Publicaciones Navales
Ganso Verde	Piaggi, Italo	Sudamericana Planeta
Operaciones Terrestres en las Islas Malvinas	Aguiar - Cervo - Machinandiarena – Balza - Dalton	Biblioteca del Oficial - Círculo Militar
La Guerra Inaudita – La Historia del Conflicto del Atlántico Sur	Ruben O. Moro	Edivérn
No Picnic (No fue un paseo – Guerra de Malvinas)	Thompson Julian.	Editorial Atlántida
Influencia del Terreno y del Clima en las Operaciones Militares	Hermenegildo Tocagni	Biblioteca del Oficial – Círculo Militar
Mosconi, Petróleo para los argentinos.	Alonso, J.V y Speroni José Luis.	TAEDA Editora
El Petróleo Argentino (1922-1930)	Mosconi, Enrique	Biblioteca del Oficial – Círculo Militar
La guerra en los Balcanes	Sánchez Mariño, Horacio	EUDE
Guerras justas: de Cicerón a Irak	Bellamy, Alex J.	Buenos Aires: Fondo de cultura
Supreme Command. Soldiers, Statement and Leadership in Wartime	Cohen, E.	New York: The Free Press.
Relato de un soldado	Bradley, A	Biblioteca del Oficial – Círculo Militar
Historia de la Fuera Aérea Argentina Tomo Malvinas (III)	Vélez y Quellet	Fuerza Aérea Argentina

LISTA EXPANDIDA

TÍTULO	AUTOR	OBSERVACIONES
Meditaciones	Marco Aurelio	
Magallanes La aventura más audaz de la humanidad	Stefan Zweig	Ed Claridad Argentina
Before the first shots are fired	Zinni, Anthony	Idioma inglés
La Guerra del Yom Kippur	Herzog, Chaim	Inédita Ediciones
La Guerra Árabe- Israelí	Maffey, Alberto Jorge	Biblioteca del Oficial – Círculo Militar
San Martín. Una biografía política del Libertador	Beatriz Bragoni	Editorial Edhasa Argentina
Manuel Belgrano Los ideales de la Patria	Instituto Nacional Belgraniano	
Güemes, Padre de los gauchos, Mártir de la emancipación	De Marco, Miguel Angel	Emecé
Military perspectives on Cyberpower	Wentz, Larry y otros	Idioma inglés
Napoleón Bonaparte Una biografía íntima	Vincent Cronin	Vergara

Continúa >

TÍTULO	AUTOR	OBSERVACIONES
La Guerra de las Galias	Julio César	
La cartera de un soldado	Garmendia J. I.	Biblioteca del Oficial – Círculo Militar
Memorias Póstumas del General Paz	Beverina, Juan	Biblioteca del Oficial – Círculo Militar – Biblioteca de Suboficial
Pensar la guerra Clausewitz	Aron, R.	Instituto de Publicaciones Navales.
Twenty-First-Century Peace Operations	Durch, William (editor)	Idioma inglés
Del Río IV a Limé Leuvu	Alberto Scunio	Biblioteca del Oficial - Círculo Militar
Winning (ganar) Las claves para el éxito del Ejecutivo más admirado del mundo.	Jack Welch	Vergara
Manual de teoría de la gestión económica de las Fuerzas Armadas	Scheetz, Thomas Pfurr, Ariel Ansorena Gratacos, Miguel	Nuevo hacer
Principios que funcionan En la vida y el liderazgo	Colin Powell con Tony Koltz	Harper Collins Español
Acts of War (The behavior of men in battle)	Holmes, Richard	Idioma inglés
La vida de un soldado	Fotheringham	Biblioteca del Oficial - Círculo Militar
Crónica de las grandes batallas del Ejército Argentino	Alberto Maffey	Biblioteca del Oficial - Círculo Militar
Juan Gregorio de Las Heras Su vida su gloria	Fued G. Nellar	Biblioteca del Oficial - Círculo Militar
Antártida. Pasado, presente y ¿futuro?	Quevedo Paiva	Biblioteca del Oficial - Círculo Militar
Una excursión a los indios ranqueles	Mansilla, Lucio V.	Varias ediciones
Comandos en acción	Ruiz Moreno, Isidoro	Claridad
La medicina en la Guerra de las Malvinas.	Ceballos, Enrique y Buroni José	Biblioteca del Oficial - Círculo Militar
Malvinas La Trama Secreta.	Cardozo, Kirschbaum, Vander Kooy.	Ed Sudamericana – Planeta
Patton, *A genius for war*	D Este, Carlo.	Idioma inglés
La primera guerra del siglo XXI Irak 2003 (3 tomos)	Autores varios	Biblioteca del Oficial - Círculo Militar
Un mundo ofensivo. El balance ofensivo defensivo y los conflictos de Kosovo, Afganistan, Irak y Chechenia.	Battaleme, J.	Temas Grupo Editorial UADE.
Las nuevas guerras. Violencia organizada en la era global.	Kaldor, Mary.	Tusquets.
Guerra. Desde nuestro pasado prehistórico hasta el presente.	Dyer, Gwaynne.	Belacqua
Invasión 1944	Speidel Hans	Biblioteca del Oficial - Círculo Militar

REPOSITORIO INSTITUCIONAL

CEFADIGITAL

Para acceder a la producción académica y científica de docentes, investigadores, alumnos y egresados del Centro Educativo de las Fuerzas Armadas (en español e inglés), ingrese en:

http//www.cefadigital.edu.ar

NORMAS DE PRESENTACIÓN DE COLABORACIONES PARA LA REVISTA *VISIÓN CONJUNTA*

Visión Conjunta cuenta, para análisis de los trabajos presentados, con:

> Comité de Referato: Su función es asegurar un estándar académico y garantizar la calidad de los trabajos presentados.
> Comité Editorial: Su función es resguardar la línea editorial institucional.

La Dirección de la revista determina la publicación de los artículos propuestos por las instancias previas evaluadoras.

El material editado, en forma gráfica o en otro medio, queda amparado por la Ley de Propiedad Intelectual Nro. 11723. Siendo autorizada la reproducción parcial o total de los artículos con expresa mención de la fuente.

Estructura del artículo

> Título
> Nombre y apellido del autor, acompañado por un breve currículo de, aproximadamente, 700 caracteres.
> Palabras clave
> Resumen o abstract, 200 a 300 palabras en idioma español.
> Subtítulos, finalizando con conclusiones, reflexiones o cierre.

Requerimientos

> Los artículos podrán ser de opinión, resultados de investigación, traducciones y recensiones o comentarios de artículos u otras fuentes de consulta.
> Tendrán una extensión máxima de 35.000 caracteres con espacio, en página A4, interlineado sencillo.
> Numeración en cada página.
> Artículo realizado en Word; letra arial, tamaño de fuente 11 para todo el texto, en una sola columna.
> Cursivas (itálica o bastardilla) se utilizarán sólo para palabras de otro idioma o citas textuales.
> Evitar el empleo de abreviaturas y siglas, en su defecto aclararlas en oportunidad de su primer uso.
> Inclusión de gráficos, mapas o material histórico se permitirá 2 por artículo y se citará la fuente correspondiente.
> Las citas y notas se incluirán al pie de cada página.

Para más información ingresar en la página web:
www.esgcffaa.edu.ar

Toda la correspondencia relacionada con la publicación será dirigida a la Dirección de la Revista.
Secretario de redacción de la revista Visión Conjunta
Eliana de Arrascaeta

Secretaría de Extensión
Escuela Superior de Guerra Conjunta de las Fuerzas Armadas
Av. Luis María Campos 480, 2º piso
C1426BOP,
Ciudad Autónoma de Buenos Aires

Correo electrónico:
visionconjunta-esgc@fuerzas-armadas.mil.ar

DESCRIPCIÓN DEL ESCUDO DISTINTIVO Y SIGNIFICADO HERÁLDICO

En el centro se destaca la insignia del Estado Mayor Conjunto de las Fuerzas Armadas.

El fondo está formado por el ajedrezado, que simboliza el Arte Militar, con los colores celeste y blanco de la Bandera Nacional. El celeste representa la justicia, el celo, la lealtad, la verdad; y el blanco, la pureza, la integridad, la obediencia, la firmeza, la vigilancia, la elocuencia.

Como contorno, en la parte superior se destaca el nombre de la Escuela en letras doradas y en la parte inferior, tres palabras en latín, embanderadas: *Nexus, Sententia y Actio,* que significan Unión, Pensamiento y Acción.

MISIÓN

"Capacitar a los alumnos en el ejercicio de la conducción en el nivel Operacional y en el desarrollo de las funciones del estado mayor en los niveles Operacional y Estratégico Militar en el marco de la acción conjunta y conjunta-combinada, a fin de optimizar el empleo del Instrumento Militar de la Nación, y de perfeccionar profesionales interesados en la Defensa Nacional, mediante el desarrollo de ofertas educativas de posgrado, proyectos de investigación y actividades de extensión".

A ese efecto, la Escuela dictará carreras de posgrado en dos niveles:

NIVEL 1: para ser impartida a Oficiales Jefes de las Fuerzas Armadas Argentinas y de otros países, en la jerarquía de Mayor o equivalente.

NIVEL 2: para ser impartida a Oficiales Superiores y Jefes de las Fuerzas Armadas Argentinas y de otros países, en las jerarquías de Coronel y Teniente Coronel o equivalentes.

VISIÓN

La Escuela Superior de Guerra Conjunta será el instituto académico militar de mayor nivel en el perfeccionamiento del Personal Militar Superior argentino y de otros países y graduados universitarios, en conocimientos y habilidades afines a la Defensa Nacional.