CAPÍTULO VIII

PROSPECTIVA DE LAS OPERACIONES NAVALES*

Capitán de Navío (RA) Jorge R. Espinel Bermúdez

* Capítulo de libro resultado de investigación del proyecto de investigación "El Poder Marítimo como fundamento estratégico del desarrollo de la Nación", adscrito al grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias, registrado con el código COL0123247, vinculado al Departamento Armada, adscrito y financiado por la Escuela Superior de Guerra General Rafael Reyes Prieto, de Colombia.

Introducción

Durante la Segunda Guerra Mundial el mundo se encontraba en plena era industrial, esta etapa marcó un cambio tecnológico e impactó la manera de desarrollar las operaciones. Pero estos desarrollos de la tecnología en la industria fueron evolucionando con el pasar del tiempo, lo que llevó a entrar en una nueva era llamada la de la información. Esta nueva era de lo digital ha traído un desarrollo de las tecnologías de la información y la computación, en el cual se viene avanzando cada día de una forma muy rápida. Además, estos nuevos desarrollos impactan al ser humano en casi todos los sectores como el social, económico, político y cultural. Pero no solo ha impactado a la población mundial, sino que la ha hecho cada vez más dependiente.

Por otra parte, esos nuevos cambios en las tecnologías de la era de la información no son ajenos al ambiente militar. En el que juega un papel muy importante, porque de ese crecimiento acelerado de las tecnologías ha generado que emerjan nuevas amenazas que atenten contra la seguridad y la estabilidad de las naciones. Algunas de estas nuevas amenazas son de carácter transnacional y de alcance global, y actúan de una forma asimétrica. Lo que hace que las Fuerzas Militares tengan que adaptarse y entenderlas para poder combatirlas y así garantizar la seguridad y defensa nacionales. Es por eso que las formas tradicionales de operar deben revisarse.

En el presente capítulo se pretende evidenciar cómo las nuevas tecnologías impactan en la forma de llevar a cabo las operaciones actuales y futuras. Además, cómo han modificado el campo en donde se desarrollan las acciones militares en un futuro cercano y cómo a través de estas se

puede alcanzar una ventaja operacional que permita obtener una victoria con el menor costo de material y personal.

De este modo, se caracterizarán primero las operaciones de información, con el propósito de comprender cuáles son estas, cuáles hacen parte de este conjunto y cuáles no son de información. Seguidamente, se revisará el concepto de guerra centrada en redes conocido en inglés como *Network Centric Warfare* (NCW) y se explicarán algunos términos que ayudarán a entender mejor el tema principal de cómo afecta la tecnología las operaciones a través del uso de la NCW.

Posteriormente, se abordará la implicación de esta revolución tecnológica en la manera en la que se están llevando a cabo las operaciones y cómo hay que desarrollarlas en el futuro. Se tomó como base de análisis la estrategia realizada por la OTAN, desde la guerra híbrida a una hiperguerra a través de una ciberguerra. Lo cual permite entender mucho mejor los tres conceptos enlazados para las operaciones futuras y cómo es la mejor manera de abordarlas. Se tratará cada uno de los conceptos por separado y sus implicaciones en las operaciones futuras.

Por último, se tratará un tema que no es menos importante que los anteriores y que está muy involucrado en el desarrollo de las futuras operaciones navales. Es el caso de los vehículos aéreos no tripulados, para lo cual se iniciará con una breve historia de estos equipos, la definición que existe sobre este tipo de elementos, su uso actual y el uso que se prevé en un futuro.

Todo lo anterior para concluir que los avances tecnológicos impactan la forma en la que se están llevando a cabo la guerra y las operaciones. Además, que es necesario adaptarse a estos recientes desarrollos que generan cada día nuevas amenazas, a las que las Fuerzas Militares tendrán sin duda que aprender a enfrentarse.

Operaciones de información

La información ha estado en el centro de las operaciones militares a través de los siglos. Durante toda la historia, los líderes militares han

reconocido el rol clave de la información como un colaborador de la victoria en el campo de batalla. Los comandantes siempre han codiciado la ventaja de una información decisiva sobre la de su adversario. Escritores como Sun Tzu y Clausewitz resaltan ese papel importante de la información en la guerra. Sun Tzu, quien escribió hace 2.500 años, enfatizó acerca de la importancia del conocimiento en la guerra.

Los escritos de Carl von Clausewitz son famosos por su articulación de la niebla y la fricción de la guerra. Como resultado de esta perdurable característica de la guerra, las organizaciones militares por siglos han sido diseñadas para adaptarse a la falta de información disponible, esto es, cómo tratar con la niebla de la guerra. La niebla es sobre todo la incertidumbre. La incertidumbre es acerca de d**ó**nde está, cuáles son sus capacidades y la naturaleza de sus intenciones.

Hasta hace poco un comandante no podía tener un oportuno y adecuado panorama de sus propias fuerzas dejándolo solo con el conocimiento de donde estuvo el enemigo y lo que hizo.

La fricción se refiere a las fallas que ocurren al llevar acabo los planes para sincronizar fuerzas o inclusive para completar la más simple tarea. Alguna de estas fricciones puede ser atribuida a la niebla, otras a las comunicaciones pobres y a la falta de conocimiento compartido.

Los recientes avances en la tecnología ofrecen una oportunidad de reducir la niebla y la fricción. Sin embargo, a pesar de los avances existentes y los que se harán, un significante residuo de niebla y fricción aún persisten. La naturaleza de ese excedente de incertidumbre no es clara y sus implicaciones no son totalmente entendidas. No obstante, hay una oportunidad histórica para reconsiderar cu**á**l es la mejor manera de tratar la niebla y la fricción que persistirá, y es probable que tenga profundas implicaciones para las operaciones y organizaciones militares.

La Guerra de Ideas: un concepto más amplio

Resultaría obvio decir que un Estado o Nación no puede derrotar a su adversario únicamente a través del uso de la fuerza y de las armas. Aplicado a las "guerras de larga duración", refiriéndose a la lucha contra

el terrorismo o en una guerra de guerrilla, esto sugiere una "guerra de ideas" o una "batalla por el corazón y las mentes", expresión utilizada durante la guerra de Vietnam. Algunos observadores expresan su preocupación acerca del lenguaje militar utilizado para estas tres expresiones. Por lo tanto, sugieren que sea menos orientado a un conflicto o al menos una metáfora menos militar que pueda liderar un pensamiento más productivo para resolver esas tensiones.

La guerra de ideas es una respuesta al ambiente global de información, en gran medida debido a los medios de comunicación, televisión satelital, internet, y otras formas de comunicación global que crean una gran cantidad de oportunidades para compartir ideas, aunque a su vez estas compiten entre sí, la guerra de ideas únicamente llega a ser 'real' cuando se pierde. Esto es, si se falla al derrotar al terrorismo, persisten las ideologías de odio o las ideas que promocionan la destrucción física.

La victoria en la guerra de ideas se da cuando se persuade a otros de que las políticas que se están usando no son amenazas para ellos, que el comportamiento del antagonista no obtendrá lo que desea o que arriesgando o gastando sus vidas no es el mejor camino para alcanzar sus objetivos (Paul, C., 2008).

Donald Rumsfeld dijo "*our enemies have skillfully adapted to fighting wars in today's media age, but for the most part, we, our country, our government, has not*", lo que nos indica que cada día se generan nuevas amenazas y formas de lucha que debemos estar preparados porque hoy gracias a los avances de las tecnologías de la información, los medios de comunicación juegan un papel fundamental en la seguridad y la defensa de las naciones (Paul, C., 2008).

Sin embargo, no se puede dejar de lado que el término "guerra de ideas" sea un imperativo a la guerra de larga duración y que solo esté orientado a la lucha contra el terrorismo, sería perder un espacio mayor en el que juega esta guerra de ideas. Por esto, es necesario que existan esfuerzos de comunicaciones estratégicas y de diplomacia pública que apunten a cubrir los vacíos que se crean cuando se orienta hacia un solo objetivo, planteado para este caso, las guerras de larga duración.

Las operaciones de información, por la naturaleza de su nombre, en virtud de algunos de los elementos que la constituyen, como es el caso de las operaciones sicológicas que están relacionadas a las relaciones públicas, suenan como si pudieran participar en la guerra de ideas. Las operaciones de información pueden contribuir apoyando los temas y los objetivos establecidos por el más alto nivel de autoridad de un gobierno.

Las comunicaciones estratégicas hacen referencia a la coordinación de todo lo que tiene que ver en el ámbito de las comunicaciones del gobierno con el propósito de alcanzar sus intereses nacionales. Es un concepto muy amplio, pero que se ajusta bien a la noción de "guerra de ideas" en la cual todo lo que se da al país contribuye a crear una impresión ideológica.

Si se quisiera dar una definición de comunicaciones estratégicas es muy difícil. El reto tiene al menos dos obstáculos. El primero, actualmente toda coordinación que un gobierno hace se centra en comunicar ciertos temas y mensajes. Y el segundo, es buscar exactamente qué temas y mensajes serán los que realmente avanzan hacia los intereses de la nación. Sin embargo, puede darse la situación de que las conexiones entre comunicaciones, las ideas que se generen, y las políticas que apoyan esas ideas no siempre se vean totalmente transparentes para la población de un país (Paul, C., 2008).

Uno de los esfuerzos que debe ser coordinado por las comunicaciones estratégicas es precisamente el de la "diplomacia pública", el cual puede ser uno de los más nebulosos. La diplomacia pública es comúnmente entendida como la patrocinadora del gobierno en aspectos relacionados con lo cultural, la educación, en programas de informaci**ón**, intercambio de ciudadanos y en la divulgación y promoción de los intereses nacionales de un país a través del entendimiento, información e influencia de la audiencia en el extranjero.

Otra definición ofrecida por el Departamento de Defensa de los Estados Unidos en su publicación JP1-02, esta se ajusta en esa definición tradicional:

> Public diplomacy – Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad.

La anterior definición del JP1-02 trata sobre las actividades de información abiertas, públicas e internacionales de un gobierno, que están diseñadas para promover los objetivos de la política exterior del gobierno, a través de entender, informar e influenciar la audiencia extranjera, los generadores de opinión, y para ampliar el diálogo entre la población del país y las instituciones, de igual manera, con sus contrapartes en el exterior.

Básicamente, si la diplomacia son las comunicaciones de un gobierno a otro, entonces la diplomacia pública son las comunicaciones de un gobierno con las personas de otros gobiernos.

El interrogante es en qué punto el sector de defensa y las operaciones de información se relacionan con la diplomacia y c**ó**mo los recursos de defensa y de las operaciones de información deberían ser parte del amplio y coordinado esfuerzo de la diplomacia pública. Sobre todo, cuando se tiene la intención de llevar a cabo operaciones de carácter militar fuera del país en donde participen varios Estados, como cuando se hace parte de una coalición y es necesario llevar a cabo una operación en el exterior. Para esto es necesario integrar los esfuerzos de comunicación entre los actores y el de las comunicaciones estratégicas de los países que intervienen.

Operaciones de Información Contemporáneas

En la actualidad las operaciones de información están basadas en ciertas doctrinas que les permiten tener principios fundamentales, además de guiar sus acciones en apoyo de los objetivos nacionales. En el contexto militar, son documentos que tienen el propósito de mostrar cómo es la manera de hacer las cosas en cada área del esfuerzo militar.

Para el caso de las operaciones de información (IO), el presente escrito se basará en lo expuesto por las doctrinas de la Organización del Tratado del Atlántico Norte (OTAN) y la publicación JP3 -13 de los Estados Unidos de América, debido a su experiencia y puesta en prácticas durante el desarrollo de operaciones como la Guerra de Irak. De acuerdo con el JP3-13 su propósito es proveer a los comandantes de fuerzas conjuntas y la dirección de sus estados mayores para ayudar a preparar, planear, ejecutar y evaluar las operaciones de información en apoyo a las operaciones conjuntas (JP3-13, 2014, p i).

Para el caso de la NATO, utilizan el documento AJP-3.10 y su propósito es explicar cómo las operaciones de información apoyan el planeamiento, la conducción y la evaluación de las operaciones.

Objetivos y Propósitos de las Operaciones de Información

Uno de los principales propósitos de las operaciones de información (IO) es conseguir y mantener la superioridad de información propia y la de los aliados, por medio de la integración de las acciones militares, fuerzas y capacidades a través de los dominios del aire, tierra, mar y del espacio; del ambiente operacional con el propósito de crear efectos de un daño deseado y medible sobre los líderes, las fuerzas, la información, los sistemas de información y otras audiencias; mientras se protegen y defienden la propias.

Las operaciones de información están orientadas sobre un adversario, al cual se le pretende, influenciar, engañar, trastornar, dañar o usurpar su proceso de toma de decisiones automáticas y humanas. Esto debido en gran medida al concepto original en el pensamiento acerca del impacto de las tecnologías de la información explícitamente sobre la guerra en lugar del amplio espectro de las operaciones. Esta orientación de las operaciones de información también procede debido a que las operaciones de información surgen de la guerra de comando y control, de la cual se heredó una estrecha visión. Tampoco es un único enfoque, a menudo la doctrina militar se orienta sobre la acción de combate en contra de un adversario dejando a un lado otro tipo de operaciones militares, como son las llamadas operaciones diferentes a la guerra o de no

guerra, entre las cuales se tienen las de estabilidad, seguridad, transición y la de reconstrucción.

Este tipo de orientación sobre el adversario suele ser problemático, sobre todo cuando el lugar en el cual se encuentra la información relevante va más allá de solo de la información suministrada por los amigos y por el adversario. Varios factores como lo neutral de la información, la procedencia de la información o la preocupación de los no combatientes, pueden ser críticos a la hora de alcanzar los objetivos de la política nacional (Paul, C., 2008).

El Futuro de las Operaciones de Información

Todo lo orientado y relacionado con las capacidades de las operaciones de información tiene un lugar prominente en el futuro de las operaciones militares.

Las capacidades de las operaciones de información están creciendo en respuesta a dos tendencias en el probable futuro de las operaciones. La primera, después de los sucesos del 9/11, la guerra en contra del terrorismo, las clases de operaciones que se caracterizan, principalmente, en una estrategia para luchar esa larga guerra que incluyen las operaciones de contrainsurgencia, asistencia humanitaria, mantenimiento de la paz, intervención en apoyo a los estados fallidos y otras operaciones que se encuentran en el espectro de los conflictos de mediana y baja intensidad.

La segunda, el abrumador poder que tienen las fuerzas convencionales de las grandes potencias que son empujadas por potenciales adversarios a buscar entrar en un conflicto, a sabiendas que no están listos o con una gran desventaja. Uno de esos ámbitos de ventaja asimétrica es el ambiente de la información y el ciberespacio (Paul, C., 2008).

En respuesta a esas dos tendencias, varias de las capacidades de las operaciones de información llegarán a ser más destacadas. Primero, las capacidades que generen y distribuyan contenido, como las operaciones sicológicas, relaciones públicas y las **cívico-militares tomarán un rol** mayor. La influencia, la información y la formación de percepción son importantes en contrainsurgencia y en cualquier contexto en el cual se

pretenda ganar el apoyo de poblaciones locales, ya que son la clave para el éxito de la misión. Estas capacidades llegarán a ser más importantes cuando el adversario intenta envenenar el ambiente con desinformación o a persuadir a una importante población para que realice acciones adversas a los intereses durante el desarrollo de la operación. Con esto, se convierte en algo crítico incrementar, de manera prominente, la integración exitosa de las capacidades de las operaciones de información y prevenir la anulación de la información propia.

Como segundo, los adversarios se mueven cada vez más a la lucha dentro del ciberespacio y el rol de las operaciones cibernéticas en la red se incrementará. A medida que los adversarios hagan un mayor uso del internet, las Fuerzas Armadas del Estado tienen un gran peso en la protección contra ataques y la gran oportunidad de trastornar o impedir las actividades del adversario.

El prominente crecimiento de esas capacidades en el futuro representa una oportunidad para las operaciones de información. Si estas pueden alcanzar una mejor integración de las operaciones sicológicas, de las relaciones públicas y de las operaciones cívico-militares, el organismo encargado de la defensa del Estado que, para el caso de Colombia debería ser el Ministerio de Defensa, estará mejor preparado para luchar en contra de las futuras amenazas de la nación (Paul, C., 2008).

Si las operaciones de información pueden facilitar el mejoramiento de la integración entre las operaciones cibernéticas de redes y otras actividades militares, se podrán enfrentar de una mejor forma esos conflictos que sucedan en el ciberespacio. Esa clase de actividades integrativas están en el corazón del concepto de las operaciones de información, porque para hacer eso es que fue diseñado el concepto.

Concepto de Guerras Centradas en Redes (*Network Centric Warfare* - NCW)

La guerra centrada en las redes y en la revolución en asuntos militares crece y saca su poder de los cambios fundamentales de la sociedad. Esos cambios han sido dominados por la evolución de las economías,

las tecnologías de la información, los procesos en los negocios y las organizaciones, los cuales se encuentran vinculados en tres temas fundamentales:

1. El cambio en la orientación de la plataforma a la red.
2. El cambio de la visión de actores como independientes a una visión de ellos como parte de un ecosistema en constante adaptación.
3. La importancia de hacer escogencias estratégicas para adaptarse o inclusive sobrevivir a un ecosistema cambiante.

La economía de los Estados Unidos ha crecido de manera continua, en especial, atribuida a los mercados globales emergentes, la globalización del trabajo y el capital; asimismo, a la amplia utilización de las tecnologías de la información en las empresas. Para tener una idea de la magnitud de la inversión de tecnologías de la información, hay que considerar el hecho de que el sector de la tecnología en 1996 ocupaba el 3% de la economía; en los últimos tres años su contribución al crecimiento de la economía ha sido del 27% en promedio (Cebrowsky, 1998).

Las tecnologías de la información están sufriendo un cambio fundamental, pasando de ser plataformas centradas en informática a ser redes centradas en informática. Estas plataformas emergieron en la amplia proliferación de computadores personales en los negocios y en los hogares. La gran inversión en investigación y desarrollo en el sector de tecnologías de la información ha sido la clave para que se crearan las condiciones para que emergieran las redes centradas en informática. Ese cambio es gracias al crecimiento del internet, intranets y extranets (Cebrowsky, 1998).

Los avances en las tecnologías de la información y las nuevas dinámicas en la economía mundial obligaron a que las empresas cambiaran su atención para ser mucho más adaptativas, aprendiendo de los ecosistemas en los cuales operan. Asimismo, compartir información permite que las empresas obtengan mejores resultados. Por otra parte, esos avances tecnológicos han hecho que el tiempo incremente su importancia. En consecuencia, las empresas más ágiles usan la superioridad del cono-

cimiento para obtener una ventaja competitiva y comprimir la línea de tiempo entre el vínculo de proveedores y clientes.

Todo esto se puede trasladar a las operaciones centradas en redes realizadas por una fuerza militar en la misma poderosa dinámica producida en los negocios.

Implicaciones para las operaciones militares

Superioridad de la Información

Peter Haynes (2015), en su libro "*Toward a New Maritime Strategy*", afirma que la visión conjunta de 2010 adoptada por los Estados Unidos después de la posguerra fría, que marcó los conceptos de operaciones para las fuerzas militares, se basó en cuatro principios: 1. La maniobra dominante, 2. Precisión en el combate, 3. Una dimensión total de protección y 4. Enfoque logístico.

En ese sentido, esa visión conjunta de 2010 declaró que la tarea primaria militar es evitar el conflicto, pero si esa disuasión fracasa, hay que pelear y ganar las guerras de la nación, ya que la proyección del poder, debido a la presencia en el extranjero, probablemente mantendrá el concepto estratégico fundamental para las futuras operaciones. Además, esta visión apunta que parte de su éxito es a través del desarrollo de las nuevas tecnologías lo que llevaría a buscar una superioridad de la información. El estado final deseado es la supremacía del dominio del espectro (Haynes, 2015).

La definición de la superioridad de la información suministrada por la publicación conjunta JP3-13, direcciona a una posición de la superioridad de la información, y esta dice así: "*The ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same*" (JP3-13, 2014, GL-3).

Entendiéndose como la habilidad para recolectar, procesar y diseminar de manera ininterrumpida el flujo de la información, mientras se explota o se le niega al adversario la habilidad para hacer lo mismo.

La superioridad de la información deriva de la habilidad para crear una relativa ventaja de cara a un adversario. Aunque el concepto de la ventaja de la información no es nuevo, los comandantes siempre han deseado ganar una ventaja decisiva de la información sobre su adversario. De hecho, la sorpresa, como uno de los principios de la guerra, es vista como un tipo de ventaja de la información que una fuerza es capaz de establecer sobre otra (Albert D., 2004).

Si se hace un paralelo con el sector comercial, la información tiene la dimensión de la pertinencia, la exactitud y la puntualidad. De esa manera, el límite superior en el campo de la información es alcanzado si la pertinencia, la exactitud y la puntualidad se alcanzan en un ciento por ciento. Claro está, que es muy difícil llegar a ese límite, para lo cual el efecto deseado durante el desarrollo de operaciones ofensivas de información es direccionar que el volumen de la información de uno o más de los componentes del enemigo no aumente y disminuya de su estado original, mientras que las operaciones defensivas de información pretenden mantener el volumen propio para que no sea disminuido.

La superioridad de la información en las operaciones militares puede verse como el estado adquirido cuando la ventaja competitiva se deriva de la habilidad para explotar una posición de superioridad, y esa posición en parte es ganada desde las operaciones de información que protegen la habilidad para recolectar, procesar y diseminar de manera ininterrumpida el flujo de la información mientras se explota o se niega la habilidad del enemigo para que haga lo mismo.

Claramente, la superioridad de la información es un concepto comparativo o relativo. Es más, su valor claramente proviene de los resultados militares que él puede permitir. En ese sentido, esta es análoga a la superioridad aérea y al control del mar. La adquisición de la superioridad de la información incrementa la velocidad de la obtención y el análisis de la información, de manera que se pueda adelantar o prevenir las opciones creadas por el enemigo.

En consecuencia, se aumenta la efectividad para crear nuevas opciones y seleccionar las más acertadas. De forma, que se puedan llevar las operaciones a un resultado exitoso de manera más rápida y a un menor

costo. El resultado es una habilidad para incrementar el tiempo de las operaciones y para adelantarse o debilitar las iniciativa y opciones del adversario. La superioridad de la información es generada y explotada por la adopción del concepto de lo centrado en redes (Network-centric), el cual nació en el sector comercial, y les permite a las organizaciones adquirir una conciencia compartida y una autosincronización (Albert D., 2003).

Lo fundamental para la creación de valor en las operaciones militares involucra la detección, identificación y la eliminación de los más blancos importantes en cualquier tiempo. El mayor reto se encuentra ligado con los blancos fugaces, estos son móviles para quienes el tiempo es un factor importante.

El Cambio a Operaciones Centradas en Redes

Si bien el concepto centrado en redes inició desde la década de 1990 aún se encuentra en desarrollo, hay una clara evidencia de que las operaciones centradas en redes ya se iniciaron. Como es el caso de la Marina de los Estados Unidos, que ha demostrado que, a través de sus capacidades de combate cooperativo, ha aumentado su poder de combate, el cual está asociado con una robusta conexión de redes de sensores, armas y las capacidades de comando y control (C2) en el contexto de una defensa aérea. Es así, como la alerta táctica y la valoración de ataque al área de la misión y la capacidad del comandante del espacio aéreo para atacar y lanzar un reporte temprano al teatro de operaciones está demostrando el beneficio operacional de tener una conexión robusta de redes de sensores en el incremento de la conciencia del espacio de la batalla.

De la misma manera, Alberts (1999), en el resumen ejecutivo de las lecciones aprendidas del experimento sobre la superioridad de la información, afirma que el Espacio basado en Sistemas Infrarrojos, que se encontraba en desarrollo en la década de 1990, aborda el mismo tema. De la misma manera, hay otras áreas operacionales que ayudan a la misión, se encuentran explorando el concepto de una fuerza con una conexión robusta incrementa el poder de combate, es el caso de la eliminación conjunta de una defensa aérea enemiga (JSEAD) (Alberts, D., 1999).

La doctrina incorporada por el servicio conjunto sobre la lucha centrada en redes tiene el propósito de acelerar el ritmo del movimiento de las fuerzas, mantener un constante tiempo operacional y entablar un combate decisivo con el enemigo en el tiempo y el lugar que se desee. En ese sentido, en el nivel operacional de la guerra se gira alrededor de los comandantes, su Estado Mayor y sus relaciones con otros elementos del ecosistema de la lucha. El cambio hacia las operaciones centradas en redes tiene un potencial, el cual no solo está en el cambio de las relaciones de comando, sino también en las nuevas clases de comandantes. Por ejemplo, el concepto de un comandante con sensores en red, con la responsabilidad de sincronizar el espacio de la batalla, que tiene la oportunidad de poder explorarlo en un ambiente de juego guerras.

En el nivel estratégico, los líderes de alto nivel y los estrategas del liderazgo militar están afirmando el potencial que tiene el efecto acumulado sobre los eventos en un espacio muy cercano, tal como una rápida secuencia de desastres táctico-locales ocurriendo sobre un período de horas, para trastornar y confundir a un enemigo al punto que sus estructuras de lucha sean rápidamente desintegradas, y sus posibles cursos de acción, reducidos, como resultado de una clara decisión militar con un costo mínimo para ambos lados. Al darse cuenta de ese potencial se requerirá un esfuerzo concentrado para trabajar cercanamente con aliados y una coalición de socios a medida que se avanza con la guerra centrada en redes.

Guerra Centrada en Redes (*Network Centric Warfare* - NCW)

De acuerdo con Alberts D. (2003) la guerra centrada en redes (NCW) tiene que ver con el comportamiento humano y organizacional. La NCW está basada en la adopción de una nueva manera de pensamiento –el pensamiento centrado en redes– y una aplicación son las operaciones militares. La guerra centrada en redes se enfoca sobre el

poder de combate que puede ser generado desde un enlace efectivo o conexión en la empresa de la lucha, se caracteriza por la habilidad de fuerzas geográficamente dispersas para crear un alto nivel de conciencia compartida del espacio de la batalla, el cual puede ser explotado por medio de la autosincronización y otras operaciones centradas en redes, que permitan alcanzar la intención del comandante.

También la guerra centrada en redes apoya la velocidad de las órdenes, y la conversión de la información superior a la acción. De igual manera, es transparente a la misión, tamaño de la fuerza y la geografía. Además, la NCW tiene un potencial para apoyar la integración de los niveles tácticos, operacional y estratégico de la guerra. En resumen, la guerra centrada en redes no está restringida solo la tecnología, sino que a grandes rasgos se aproxima a una respuesta militar emergente en la era de la información (Alberts, 2003).

En la figura 1 se muestra cómo sería la organización militar como una empresa centrada en redes según Alberts (2013), en la cual se pueden ver los elementos básicos necesarios para generar un poder de combate utilizando el modelo de las empresas centradas en redes. Como se observa, se inicia con una estructura informática. Esto a su vez permite la creación de una conciencia y el conocimiento de un espacio de batalla compartido. Esta conciencia y conocimiento es apalancado por un nuevo enfoque de un comando y control adaptativo y unas fuerzas autosincronizadas, que permitirán incrementar el tiempo de las operaciones, incrementar las respuestas, bajar los riesgos y los costos; de manera que se incremente la efectividad en el combate.

Figura 1. La organización militar como una empresa centrada en redes

Fuente: *Network Centric Warfare* (2000).

De acuerdo con lo mencionado por Cebrowski (1998) en las operaciones centradas en redes en el nivel estratégico el elemento crítico es el entendimiento detallado del espacio apropiado competitivo, con todos los elementos que conforman el espacio y el tiempo de la batalla. Operacionalmente, se da en el enlace y las interacciones que existen entre las unidades y el ambiente operacional. Tácticamente, el elemento crítico es la velocidad. En el nivel estructural, la guerra centrada en redes requiere una arquitectura operacional con tres elementos críticos: redes de sensores, servidores de redes de operaciones con una alta calidad de información y el almacenamiento en discos duros (*backplane*).

Estos ayudan a conseguir el valor agregado a los procesos de comando y control, muchos de los cuales pueden ser automatizados para alcanzar la velocidad requerida.

La guerra centrada en redes permite un cambio en el estilo de la guerra de desgaste a un estilo de combate mucho más rápido y efectivo, caracterizado por el nuevo concepto de velocidad de las órdenes y la autosincronización (Cebrowsky, 1998).

De la misma manera, la guerra centrada en redes, en la que el tiempo de la batalla juega un papel crítico, la velocidad de respuesta y el aumento de la eficiencia son necesarios para adquirir esa ventaja sobre el enemigo, será lo que permitirá obtener resultados exitosos. Por otra parte, los altos y acelerados índices de cambio tienen un impacto profundo en los resultados, por lo que es necesario mirar las posibles alternativas de estrategia que pueda generar el enemigo y así buscar el éxito. Cebrowski (1998) propone dos formas complementarias para alcanzar esa ventaja a través de la guerra centrada en redes: la NCW permite a las fuerzas propias desarrollar la velocidad sobre las órdenes, y posibilita a las fuerzas organizarse de abajo hacia arriba o auto sincronizarse para satisfacer la intención del comandante.

La velocidad de las órdenes tiene tres partes: 1) La fuerza naval consigue la superioridad de la información, teniendo una mejor conciencia o entendimiento del espacio de la batalla, que tener una simple cantidad de datos en bruto. Tecnológicamente, se requiere de sensores excelentes, redes rápidas y poderosas, despliegue de tecnología, y unas capacidades sofisticadas para modelar y simular. 2) Las fuerzas navales actúan con velocidad, precisión y de esa manera obtienen un efecto de masa versus la masa de las fuerzas enemigas. 3) Los resultados se dan por una rápida ejecución de los cursos de acción del enemigo y el choque de eventos cercanamente asociados. Esto altera la estrategia del enemigo y se espera que logre detener cualquier acción antes de que inicie. Una de las fortalezas de la guerra centrada en redes es su potencial, dentro de los límites, de compensar una desventaja en números, de tecnología o de posición.

Las operaciones militares son complejas, y la teoría de la directa complejidad dice que la mejor organización de las empresas es de abajo

hacia arriba (*bottom-up*). Tradicionalmente, los comandantes militares trabajan para obtener un comando de arriba hacia abajo (*up-bottom*) dirigido a la sincronización que le permita alcanzar el nivel requerido de masa y fuego para enfrentar al enemigo.

Porque cada elemento de la fuerza tiene un único ritmo, y además los errores de una fuerza en movimiento necesariamente consumen el poder de combate, el combate en el nivel operacional es reducido a una función dentro de una etapa de un proceso, el cual toma tiempo y proporciona oportunidades al enemigo. Después del enfrentamiento inicial hay una pausa operacional y el ciclo se repite (Cebrowsky, 1998).

En contraste, la organización de abajo hacia arriba produce una manera autosincronizada, en la cual las funciones de las etapas llegan a ser una curva suave y los combates se mueven continuamente a una gran velocidad. El ciclo de observar, orientar, decidir y actuar tiende a desaparecer y al enemigo se le niega la pausa operacional. Recobrar el tiempo y el poder de combate amplifica los efectos de velocidad de las órdenes, acelerando el ritmo de cambio y liderazgo de búsqueda.

Por consiguiente, la autosincronización se puede ilustrar durante la crisis, en 1995, cuando la población de la República de China intent**ó** influenciar las elecciones de Taiwán con un alto nivel de alarde de su poder militar, los Estados Unidos en respuesta desplegaron su portaviones con su grupo de batalla, lo cual permitió una disuasión y que se llegará a un acuerdo. Pero para efectos de lo que se está tratando, lo más importante fue el cambio en el modo en que se ejecutó el proceso de comando y control durante el desarrollo de la operación. Lo que permitió al Vicealmirante Clemins, comandante de la Séptima Flota y a sus subordinados reducir la línea de tiempo de la planeación de la operación de días a horas. Esta magnitud de cambio sugiere que algo fundamental está pasando (Cebrowsky, 1998).

El almirante Cebrowsky (1998) ve que existe un amplio impacto de la guerra centrada en redes; en 1997, un simple portaviones en el Pacífico oriental envió 54.000 correos electrónicos en un mes, alrededor de la mitad de la cantidad de todos los mensajes enviados por el tráfico tradicional en el Pacífico oriental durante el mismo período de tiempo.

Este es un ejemplo de una compleja organización empresarial de abajo hacia arriba. Ahora es la norma. Tales capacidades permiten un movimiento dentro del campo de la velocidad de las órdenes. Las preguntas y la ambigüedad disminuyen, aumenta la globalidad y las líneas de tiempo se acortan.

Guerra Híbrida, Hiperguerra y Ciberguerra

Para iniciar esta parte de la prospectiva de las operaciones, se va a tomar como base el concepto estratégico de la guerra del futuro, adoptado en la OTAN, teniendo en cuenta la velocidad de cambio de las relaciones entre la estrategia y la tecnología en la guerra. La guerra del siglo XXI será una que se librará con sistemas autónomos, en el cual la perturbación masiva de un enemigo puede ser presagio de destrucción masiva, por eso la OTAN se pregunta ¿Cómo es posible defenderse de este tipo de enemigo? y ¿Cómo la alianza puede luchar y ganar ese modo de guerra? Para dar respuesta a estos dos interrogantes Bernard Brodie afirma que el camino es la disuasión, es una estrategia destinada para disuadir a un adversario de una acción que aún no ha tomado (Chambers J. (1999) citado por Allen J. (2017: 13). por eso los primeros pasos hacia una guerra del futuro debería ser una postura de disuasión y defensa.

Por eso Chambers J. (1999) afirma que una verdadera y creíble estrategia de la OTAN para las futuras guerras debería ser más holística, hacia lo conjunto, ambiciosa y evidentemente combatir un adversario a través de una continua estrategia híbrida-ciber-hiper. Una futura disuasión también descansa sobre una fuerte capacidad de recuperación y una manifiesta redundancia sistémica disponible de sistemas e infraestructura.

De una manera sencilla, una nación o una alianza requieren la capacidad para bloquear un mensaje falso "estratégico" masivo y ser capaz de golpear al enemigo con un mensaje. Esto tendrá un giro que requerirá tener una estrategia efectiva contra de la guerra híbrida construida sobre

una ágil y resistente estrategia de comunicaciones. Asimismo, las sociedades también necesitan llegar a ser más fuertes en contra de atentados terroristas, ataques a infraestructura crítica, y la negación de los servicios críticos. De modo que la dirección y la recuperación de las consecuencias de estos ataques también lleguen a ser demostrados de manera más ágil (Allen J., 2017).

Describiendo la Guerra Híbrida

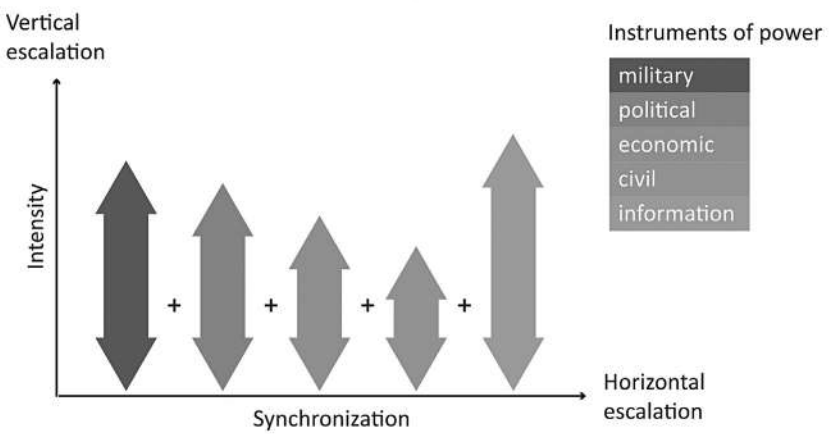
Si bien, tanto actores estatales como no estatales se enfrentan en una guerra híbrida, estos varían ampliamente sus medios y acciones. De acuerdo con lo expuesto, los actores exhiben la capacidad de sincronizar varios instrumentos de poder en contra de las vulnerabilidades específicas del enemigo para crear efectos lineales y no lineales. De manera que, centrándose en estas características de las capacidades de los actores de una guerra híbrida, junto con las vulnerabilidades de los objetivos en esas áreas y luego superponiéndolas con los medios y efectos, la evaluación de la línea base fue capaz de crear una descripción genérica de la guerra híbrida. De tal manera que, se puede describir la guerra híbrida como el uso sincronizado de múltiples instrumentos de poder adaptados a vulnerabilidades específicas por medio del espectro de las funciones sociales para alcanzar los efectos sinérgicos (Cullen P., 2017).

Cullen P. (2017) afirma que la evaluación de la línea base concluyó que la guerra híbrida es asimétrica y usa múltiples instrumentos de poder a lo largo de los ejes horizontal y vertical y los grados de variación comparten un incremento en el énfasis sobre la creatividad, la ambigüedad y los elementos cognitivos de la guerra. Esto establece una guerra híbrida diferente al enfoque basado en la guerra de desgaste, en la cual la fortaleza de uno coincide con la del otro, ya sea cualitativa o cuantitativamente para degradar las capacidades del oponente.

La figura 2 muestra cómo un actor de la guerra híbrida puede sincronizar sus instrumentos de poder militar, político, económico, civil y de información para escalar vertical y horizontalmente una serie de ac-

tividades específicas para crear efectos. También muestra cómo un actor de la guerra híbrida puede escalar verticalmente para aumentar la intensidad de uno o varios instrumentos de poder o escalar de manera horizontal a través de la sincronización de varios instrumentos de poder para crear efectos mayores que solo la escalada vertical.

Figura 2. Escalamiento de la guerra híbrida



Fuente: Cullen, P. & Reichborn-Kjennerud E. (2017).

La clave es entender que los diferentes instrumentos de poder son usados en múltiples dimensiones y niveles simultáneamente de una manera sincronizada. Este tipo de pensamiento permite a los actores de la guerra híbrida usar sus medios militares, políticos, económicos, civiles y de información de maneras diferentes, los cuales están a su disposición para crear paquetes de ataque sincronizados que se adapten para percibir las vulnerabilidades del sistema de blancos. Los instrumentos de poder usados dependerán de las capacidades del actor de la guerra híbrida y de la percepción de las vulnerabilidades de su oponente, también de los objetivos políticos del actor de la guerra híbrida y sus formas planeadas para obtener esos objetivos. Como con todos los conflictos y las guerras, el carácter de la guerra híbrida depende del contexto.

Entender la Guerra Híbrida

Como medida inicial hay que entender que un adversario de la guerra híbrida no se prestará solo a un análisis tradicional de la amenaza, basado en su capacidad e intención, por un número importante de razones.

En primer lugar, la guerra híbrida utiliza un amplio conjunto de herramientas y técnicas que usualmente no se verán en la evaluación de amenazas tradicionales. En segundo lugar, está dirigida a las vulnerabilidades a través de sociedades en formas que tradicionalmente no se piensan. En tercer lugar, esta sincroniza sus medios de una manera novedosa. Por ejemplo, solo mirando los diferentes instrumentos de poder que un adversario tiene, no es posible predecir cómo y cuál será el grado en el que él puede estar sincronizado para crear determinados efectos. De este modo, las capacidades funcionales de un adversario de la guerra híbrida, aunque importantes, no necesariamente proporcionarán la información correcta para entender el problema.

En cuarto lugar, la guerra híbrida intencionalmente aprovecha la ambigüedad, la creatividad y la comprensión de la guerra para llevar a cabo ataques menos visibles. Esto se debe al hecho de que los actores pueden adaptarse para mantenerse bajo ciertos umbrales de detección y respuesta, incluyendo los umbrales legales internacionales, de ese modo se dificulta el proceso de toma de decisiones y hace que sea más difícil reaccionar a un ataque de la guerra híbrida.

En quinto lugar, relacionado con el punto anterior y lo más probable a diferencia de los otros tipos de guerra convencional, una campaña de guerra de híbrida tal vez no podrá ser detectada hasta que esta ya est**é** en marcha, con efectos perjudiciales, porque ya se ha manifestado y degradado las capacidades de un objetivo para que este pueda defenderse.

Hiperguerra

Para Allen (2017) el impacto de las nuevas tecnologías y de las interacciones entre estas ha generado un cambio muy rápido del carácter y la conducta de la naturaleza de la guerra, la hiperguerra verá un aumento de la velocidad del conflicto relacionado con una reducción

amplia de los ciclos de acción y decisión. Del mismo modo, se podrá ver una enorme compresión del tiempo y sus consecuentes efectos, con las órdenes de la guerra convirtiéndose en más autónomas de manera constante necesariamente, y como parte de una nueva carrera de escalamiento que asciende desde el caos a la rendición. El incremento de la dependencia de las personas a internet, sobre todo con las redes sociales, ha hecho que las diversas sociedades sean vulnerables a la manipulación política a través de la diseminación de noticias falsas. También esto hace parte de una nueva guerra híbrida la cual transciende de la separación civil-militar.

Del mismo modo Allen (2017) afirma que el término de hiperguerra no es nuevo y fue utilizado durante la Segunda Guerra Mundial, su uso implicaba una naturaleza global y concurre en muchos teatros de la guerra. Ahora bien, en el contexto actual, la hiperguerra pudiera ser bien aplicada de forma global, pero el elemento de una guerra panorámica no es una característica singular definida. En cambio, qué hacer con esa nueva manera y única de hacer la guerra sin precedente de velocidad disponible debido a la automatización del proceso de toma de decisiones y a la simultaneidad de las acciones que pueden ser llevadas a cabo, será posible por el aprovechamiento de la inteligencia artificial.

Describiendo las guerras del futuro, la palabra 'hiper' es usada teniendo en cuenta la raíz griega de la palabra que significa 'por encima de'. Esta es una nueva clase de combate que será mucho más importante de lo observado hasta el momento. En términos militares, la hiperguerra se redefine como un tipo de conflicto en el cual la toma de decisiones humanas está casi ausente desde el ciclo observar-orientar-decidir y actuar (OODA). Como consecuencia, el tiempo asociado con un ciclo OODA será reducido a una respuesta instantánea. Las implicaciones de esos desarrollos son muchas y son un juego cambiante.

Hasta el momento, una decisión para actuar depende del conocimiento del ser humano. Aunque la toma de decisiones en las cuales interviene el ser humano es potente, también tiene limitaciones en términos de velocidad, atención y diligencia. Por ejemplo, hay un límite con respecto a qu**é** tan rápido los seres humanos pueden tomar una decisión,

evitando el peso cognitivo que contiene cada decisión. Hay un límite entre qué tan rápido y cuántas decisiones pueden ser hechas antes de que un ser humano necesite descansar y reconstituirse para restablecer sus facultades cognitivas (Allen, 2017).

Las dos variables de interés son el tiempo y el espacio. El tiempo es lo que toma formular y ejecutar una acción, mientras el espacio es donde la acción es ejecutada. Esas variables son calculadas como consecuencia de tomar una importante decisión estratégica, operacional y táctica. La identificación de un lugar para la aplicación de la fuerza es el primer ingrediente. Cuando se hace de manera apropiada, esta involucra el cálculo de un conjunto de contingencias, llamado ramas y continuaciones en el lenguaje de planeación, en relación con la capacidad del enemigo para reaprovisionarse, reposicionarse y recibir refuerzos.

Por otra parte, la manera en que se identifican los blancos se maniobra para alcanzar una ventaja o evitar un contraataque, y la de direccionar un ataque propio, son variables que hay que adicionar al tiempo de la toma de decisiones y a la complejidad cognitiva. Con una máquina dedicada para la toma de decisiones, un gran grupo de sensores y armas pueden coordinarse de manera instantánea, favoreciendo la rápida o masiva formación de fuerzas y la ejecución de una acción cinética y una subsecuente dispersión (Allen, 2017).

El grado de simultaneidad de una acción puede ser logrado mediante una máquina dedicada a la toma decisiones, que alimenta la hiperguerra y que además supere las decisiones que puedan ser realizadas bajo el control y la dirección de un humano (Allen, 2018). Sin embargo, es necesario tener muy claro cuál es la responsabilidad y las consecuencias que pueda llegar a tener que una máquina tome las decisiones de una acción militar, sobre todo cuando se refiere a los derechos humanos y la participación de civiles.

Otro de los puntos que cada día entra a jugar un papel muy importante dentro del futuro de la guerra es la inteligencia artificial, que no solo es usada para llevar a cabo un ataque mediante la capacidad de tomar decisiones de forma autónoma, sino que puede ser utilizada en los sistemas de defensa. Un claro ejemplo puede ser el sistema de guiado de

misiles de un destructor, en el cual dentro de su Centro de Información y Comando (CIC) es el primero en detectar lo que podría ser un intento mayor de intrusión cibernética, o tal vez un ataque.

Por ejemplo, se lleva a cabo una intrusión penetrante, que busca tener fuera los sensores del buque y muchos de sus sistemas defensivos, y además se concentra en las baterías contra múltiples amenazas y sistemas de apoyo del buque. El inicio de un ataque cibernético y el tener una defensa exitosa es cuestión de microsegundos. De tal manera que el sistema defensivo debería haber funcionado exactamente como había sido diseñado, evitando la intrusión contra los sistemas del buque.

En consecuencia, el buque sería capaz de percibir, y detectar un ataque entrante masivo y complejo en forma de enjambre, llevando a cabo un seguimiento de un ataque abiertamente invisible. En efecto, el sistema debe ir más allá, al enviar de manera instantánea una alerta de amenaza al resto de la flota, permitiendo que otras unidades se preparen para un inminente ataque.

Ciberguerra

Teniendo en cuenta lo expuesto, esas nuevas amenazas y futuros escenarios de guerra se llevarán a cabo en un nuevo campo de batalla que no es precisamente real sino virtual, para lo cual es necesario revisar los siguientes términos:

Ciberespacio: Según Bejarano (2011) la comunidad de las tecnologías de la información y comunicaciones define al ciberespacio como el conjunto de medios físicos y lógicos que conforman la infraestructura de los sistemas de comunicaciones e informáticos. También se puede definir, de acuerdo con Rain (como lo citó Bejarano, 2011), como el conjunto de sistemas que están interconectados, que dependen del tiempo y de los usuarios que interactúan con esos sistemas.

De acuerdo con el diccionario de términos militares y asociados, el ciberespacio es: "*A global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the internet, telecommunications networks, computer*

systems, and embedded processors and controllers" (JP 1-02, 2016, p. 58). Entendiéndose como un campo global dentro del ambiente de la información el cual está conformado por una red interdependiente de una infraestructura tecnológica de información, la cual incluye el internet, las redes de telecomunicaciones, los sistemas de computación, procesadores y controladores integrados (Pub J., 2016).

Otra posible definición de ciberespacio es cuando se refiere a un ambiente que se caracteriza por el uso de la electrónica y del espectro electromagnético para almacenar, modificar e intercambiar una serie de datos, por medio del uso de sistemas informáticos en red y las infraestructuras físicas asociadas. También tiene que ver con la forma como están conectados los seres humanos mediante el uso de los ordenadores y las telecomunicaciones, sin que se tenga en cuenta la parte física.

De lo anteriormente expuesto, el ciberespacio es el lugar en el cual se van a llevar a cabo todo tipo de interacciones entre seres humanos, organizaciones y estados, los cuales utilizan los medios virtuales para almacenar, manejar y compartir información útil o necesaria para su día a día.

Asimismo, el ciberespacio será el escenario donde se desarrollarán las operaciones cibernéticas de carácter civil y militar, lo cual conllevará enfrentamientos debido a conflictos de intereses entre Estados, lo que hace pensar que es necesario el desarrollo de herramientas que permitan realizar acciones defensivas u ofensivas en ese nuevo ambiente virtual.

Ciberdefensa: De acuerdo con Cano (2011) es una nueva connotación sistémica y sistemática que tienen que llevar a cabo los gobiernos, de manera que comprendan las responsabilidades que tienen como Estado para con los ciudadanos y las fronteras nacionales electrónicas y digitales. De la misma manera, la ciberdefensa es un concepto estratégico que los gobiernos deben comprender, en el que hay variables como vulnerabilidades en la infraestructura crítica de la nación, garantías y derechos de los ciudadanos en el entorno on line, adaptación de la administración de justicia al entorno digital y evolución de la inseguridad de la información dentro de un contexto tecnológico y operacional (Cano, 2011).

Ciberseguridad: Para Cárdenas (2015) es un complemento de la ciberdefensa a través de un conjunto de herramientas, políticas, conceptos

de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías; las cuales son usadas para proteger los activos de una organización y de las personas que se encuentren en el ciberespacio, de manera que la población y el Estado pueda tener los niveles apropiados para usar los medios cibernéticos sin tener una amenaza o riesgo de ser atacados (Cárdenas, 2015).

Entonces, se puede decir que la ciberguerra es un conflicto entre Estados tecnológicamente avanzados, la cual se puede llevar a cabo a través de ciberataques aislados, o que hacen parte de una guerra convencional. Sin embargo, no siempre los conflictos o interacciones que se desarrollan en el ciberespacio pueden suceder en un ambiente de guerra o enfrentamiento general (Ferrero, 2013: 86).

De la misma forma, la ciberguerra es el conjunto de acciones que se llevan a cabo con el propósito de producir una perturbación en la información y en los sistemas del enemigo, y a la vez proteger la información y sistemas propios y de los aliados. El ciberespacio es el escenario principal en cual se llevan a cabo los conflictos, y los ataques cibernéticos no se consideran ataques armados (Ferrero, 2013: 86).

Según Miranda (2014) el primer ciberataque conocido tuvo lugar en 1982, cuando la Central de Inteligencia de los Estado Unidos (CIA) detectó un intento de intromisión por parte de la Unión Soviética para robar un software con el cual pudiera controlar su oleoducto transiberiano, el cual tenía un complejo sistema de bombas, válvulas y sistemas de control. La CIA al darse cuenta del intento de robo, permitió que la Unión Soviética robara el software, el cual había sido modificado, y cuando fue instalado en los sistemas de control de oleoducto, provocó que se descontrolará todo el sistema, lo que ocasionó una gran explosión del oleoducto. Desde ese momento, han ocurrido diferentes hechos, algunos públicos, otros no, haciendo que se tomara conciencia de que la ciberguerra se estaba consolidando y que era una amenaza real, la cual podría llegar a afectar países completos como el caso de Estonia en el 2007 (Miranda, 2014: 12).

El General Krulak, del cuerpo de Infantería de Marina de los Estados Unidos, afirma que existen 'tres bloques de la guerra' y sostiene que las decisiones de oportunidad pueden ser realizadas en los bajos niveles durante situaciones estresantes y complejas. Él se centró en el elemento humano en combate y cómo "la estrategia del soldado" puede tener un enorme impacto en relación con el rango. El concepto del General Krulak involucra las 'calles' como esos lugares en donde la Infantería de Marina es requerida para ejecutar operaciones de mantenimiento de la paz y humanitarias, de contrainsurgencia, así como operaciones en conflictos alta intensidad de forma simultánea o muy cercana. Hoy se tiene un cuarto bloque en el cual hay que luchar que es el ciberespacio (Parker, 2019: 2).

En ese sentido, la aplicación de la doctrina del cuerpo de Infantería de Marina de los Estados Unidos para el emergente y el rápido desarrollo del campo de la ciberguerra se ve como un desafío y una oportunidad. La forma como el cuerpo de Infantería de Marina piensa acerca de la ciberguerra, el entrenamiento, el planear y el ejecutar operaciones de combate está suministrando un modelo para el desarrollo de una ciberdoctrina naval. Tres aspectos del manual "*warfighting*" son espacialmente relevantes a la ciberguerra: la inseparable naturaleza de la operaciones ofensivas y defensivas, la maniobra de la guerra como un medio para crear y explotar las deficiencias y vulnerabilidades del enemigo, y el planteamiento de la combinación de armas para dejar al adversario en una situación de desventaja que le impida ganar (Parker, 2019: 2).

De la misma manera, la Marina de los Estados Unidos ha diseñado una estrategia para el desarrollo de operaciones en el ciberespacio, la cual ha llamado Ciber Poder Naval 2020 (Navy Cyber Power, 2020), esta se ha fundamentado en tres aspectos principalmente:

1. El aseguramiento del acceso al ciberespacio y la confianza del comando y control (C2). La Armada opera, defiende, explota y participa en el ciberespacio de manera efectiva para garantizar que las fuerzas navales mantengan el acceso al ciberespacio en todas las funciones críticas de una misión y para proveer a los comandantes navales del conjunto de capacidades de comando y control resistentes a cualquier ataque cibernético.

2. La estrategia de prevención de las sorpresas en el ciberespacio. De manera efectiva la Armada evalúa las acciones del adversario en el ciberespacio a través de una dedicada recolección y análisis de la inteligencia cibernética, por medio de una integración oportuna y total, una apropiada información cibernética y unas alertas de las amenazas dentro del panorama operacional del comandante.
3. La entrega decisiva de los resultados cibernéticos. La Armada entrega los resultados cibernéticos en un tiempo y lugar que esta elige a través de todo el rango de las operaciones militares en apoyo de los objetivos del comandante (Panetta L., 2012).

De acuerdo con este enfoque de la Marina de los Estados Unidos sobre las operaciones en el ciberespacio, se plantea que el ciberespacio se extiende más allá de los tradicionales límites de las redes navales y conjuntas. Prácticamente todos los sistemas principales de los buques, aviones, submarinos y vehículos no tripulados se encuentran interconectados en algún grado. Esto también incluye los sistemas de combate, y comunicaciones. Asimismo, el de ingeniería y navegación. Adicionalmente, el ciberespacio se extiende por igual a los sistemas conjuntos, administrativos e industriales de la Marina. Mientras la conectividad facilita de una manera sin precedente la velocidad y agilidad de las plataformas y los sistemas de armas, los sistemas de los buques también están abiertos a muchos vectores de ataque para expertos adversarios cibernéticos (Panetta, L., 2012).

Esas amenazas surgen en este nuevo campo del ciberespacio, además traen consigo una serie de actores que juegan en este escenario de batalla, entre los cuales se encuentran los de carácter estatal y no estatal, organizaciones terroristas, grupos de hackers, crimen organizado y hackers actuando por cuenta propia, con diferentes motivaciones como ganancia personal, robo de información, desacreditar a un gobierno, sabotaje, ganancia política, negar la degradación del acceso de la Marina al ciberespacio y al buen uso de sus redes.

La mayor preocupación es el incremento persistente de las amenazas a los actores estatales y no estatales con la capacidad y la intención de atacar las redes de manera despiadada como parte de una gran estrategia de no acceso y negación de zona (A2/AD: *Anti-access/Area-Denial*). Por lo tanto, se debe disponer de capacidad operacional para mitigar el impacto de las amenazas a través unas medidas defensivas y cuando sea necesario, de otras ofensivas.

Además, de las amenazas sobre las fuerzas navales en el ciberespacio existen otras menores que pueden afectar las redes de la Marina y reducir el alistamiento para el combate. Una gran cantidad de esas amenazas menores con las que se lucha todos los días podría ser mitigada a través una política de seguridad de las tecnologías de la información. No aplicar las políticas de seguridad incrementa el espectro de las amenazas, ya que estas desgastan tiempo necesario para defender e identificar cada una, desvían la atención de otras que pueden causar daños en las fuerzas de las Marina o del Comando Conjunto.

Asimismo, la maniobra de la guerra en el ciberespacio no varía el concepto del ambiente físico. Cuando los comandantes operacionales incrementan su habilidad de maniobra a través de la sorpresa, engaño, velocidad y agilidad, logran poner al adversario en una situación insostenible e invencible. En ese sentido, el coronel John Boyd afirma que la aplicación del ciclo de observar, orientar, decidir y actuar es un marco útil y que se debe considerar para llevar a cabo la maniobra de la guerra en el campo del ciberespacio (Parker, 2019: 3).

Finalmente, se puede decir que los líderes que se enfocan en el ciberespacio deben considerar que más allá del ambiente de la tecnología a la ciberguerra, hay una gran cantidad y diversidad de actores que aumentan la complejidad de esta guerra. Asimismo, los actores estatales, no estales, robots, inteligencia artificial, sector privado e instituciones públicas, todas aseguran un ambiente no lineal. Los fundamentos de la guerra no cambian porque el ritmo de la batalla y la complejidad del terreno se han incrementado, y la situación de conciencia se mantiene crítica para que el operador cibernético esté listo para responder a una acción maliciosa y minimizar el daño colateral si se lleva a cabo una operación ofensiva.

Las aeronaves no tripuladas (UAV)

Desde 1917 las Fuerzas Armadas de los Estados Unidos han investigado y empleado vehículos aéreos no tripulados. Durante este tiempo estos vehículos han sido conocidos como drones, aviones robot, aeronaves sin pilotos, vehículos y aeronaves tripulados de manera remota, y otros términos que describen a una aeronave que vuela bajo del control de una persona que no está a bordo. Ellos son los llamados UAV, por sus siglas en inglés, cuando se combinan con estaciones de control en tierra con ayuda de un enlace de datos, forman lo que hoy se conoce como sistemas aéreos no tripulados (AUS) (Getler J., 2012).

Para el Departamento de Defensa de los Estados Unidos los UAV son vehículos aéreos impulsados sin un operador humano, que pueden volar de manera autónoma o ser piloteados remotamente; asimismo pueden llevar una carga letal o no letal y ser recuperados. Los vehículos balísticos o semibalísticos, misiles de crucero y los proyectiles de artillería no se consideran como UAV de acuerdo con la definición dada por el Departamento de Defensa. Los UAV también son descritos como un simple vehículo aéreo asociado con sensores de vigilancia o a un sistema de UAV, el cual normalmente consiste en tres o seis vehículos, una estación de control, y un equipo de soporte (Getler J., 2012).

Si bien Estados Unidos recientemente ha obtenido una gran cantidad de UAV, estos fueron probados durante la Primera Guerra Mundial, aunque no se usaron en combate. De hecho, fue hasta la guerra de Vietnam que los Estados Unidos emplearon los sistemas aéreos no tripulados (AUS), tales como el AQM-34 '*Firebee*' en un rol de combate. El '*Firebee*' ejemplifica la versatilidad de los UAS, inicialmente, volaba en los años 50 como parte de la artillería aérea y en los 60 para recolección de inteligencia, posteriormente, fue modificado para entregar cargas útiles y tuvo su primer vuelo de pruebas como un UAV armado en 2002.

El uso militar del UAS en conflictos como el de Kosovo (1999), Irak (2003), y Afganistán (2001) ha mostrado las ventajas y las desventajas de las aeronaves no tripuladas. Los AUS encabezan los titulares nacionales

en los Estados Unidos porque desempeñan tareas que, históricamente, han sido realizadas por aeronaves tripuladas. Los AUS están pensadas para ofrecer dos ventajas principales sobre las aeronaves tripuladas: eliminar el riesgo de perder la vida de un piloto y mantener sus capacidades aeronáuticas, tales como la resistencia o maniobras, son las limitaciones humanas. Por otra parte, su costo es mucho menor al de una aeronave tripulada. Sin embargo, ese bajo costo puede estar pesando en su contra debido a la gran propensión a choques. Por otro lado, mientras el riesgo de tripulaciones a bordo de las aeronaves tripuladas se minimiza, este puede pesar cuando se producen complicaciones y emergencias inherentes en un vuelo de vehículo no tripulado en el espacio aéreo compartido con otros activos tripulados.

El incremento del uso de UAS tiene muchas razones. Primero, los avances en las tecnologías de navegación y comunicación estuvieron disponibles solo hasta hace pocos años; además el incremento en el ancho de banda de las comunicaciones militares satelitales ha hecho que la operación remota de los UAS sea mucho más práctica. Por otra parte, la naturaleza de las guerras como las de Irak y Afganistán también ha incrementado la demanda por UAS, debido a la necesidad de identificar y atacar objetivos ocultos dentro de la población civil, lo cual requiere una constante vigilancia y una capacidad de ataque rápido, con el fin de minimizar los daños colaterales. Además, los UAS dan una ventaja asimétrica en este tipo de conflictos.

Por muchos años la Fuerza Aérea de Israel lideró en el mundo el desarrollo de UAS y sus tácticas. Los exitosos usos de estos sistemas durante las operaciones en el Líbano en 1982 alentaron al entonces secretario de Marina de los Estados Unidos, John Lehman, para adquirir la capacidad del uso UAS para la Marina de ese país. De la misma manera, otras partes del Pentágono se interesaron también por el uso de los UAS, lo que llevó a que durante la administración de Reagan se asignarán presupuestos para pasar de proyectos experimentales a programas de adquisición.

La habilidad para ver el campo de batalla en cualquier momento mediante el uso de los sensores que puede llevar un UAV es una de sus

mayores ventajas. Los comandantes tácticos con UAV a su disposición pueden obtener la inteligencia de combate necesaria para anticiparse a potenciales problemas que puedan surgir en el campo de batalla. Esta capacidad natural puede reducir la dependencia de las aeronaves tripuladas, incluyendo en algunos casos la entrega de armas sin poner el riesgo al piloto (Kurkcu, 2008).

Durante la Décima Conferencia Anual sobre Liderazgo y Ética Militar de la Academia Naval de los Estados Unidos en 2010, se determinó que los actuales sistemas no tripulados reducen el riesgo para los combatientes debido a que estos proveen una sofisticada capacidad de enfrentamiento, apoyada por la inteligencia, comando y control, selección de objetivos y la entrega de armas. Estos sistemas también aumentan la conciencia situacional y reducen el riesgo inherente a un combate en tierra, mar o aire. Por otra parte, su precisión en los ataques minimiza la probabilidad de causar víctimas dentro de los civiles o no combatientes. Versiones autónomas de esos sistemas no tripulados pueden percibir, decidir y actuar de una manera más rápida que los humanos, impulsando la disuasión convencional en ambientes de acceso limitado, y reduciendo más los costos de personal (US Naval Academy, 2010).

De esa manera, los UAV están siendo utilizados por muchas fuerzas armadas del mundo y su principal función está dada en el desarrollo de misiones como:

- Inteligencia, vigilancia, adquisición de objetivos y reconocimiento (ISTAR).
- Guerra electrónica.
- Relé de comunicaciones y de datos.
- Evaluación de daños.
- Localización de personas en misiones de rescate (García, 2011).

Sin embargo, los Estados Unidos de América han adquirido la capacidad para que los UAS lleven armas de precisión guiadas para atacar blancos en tierra. Aunque conservan la capacidad de reconocimiento para la que fueron diseñados originalmente.

Otra clase de UAS está siendo diseñada para que desde una posición de tierra lleve a cabo misiones de combate. Esta ha sido llamada vehículo de combate aéreo no tripulados (UCAV), estos sistemas tienen características que les permiten llevar una gran capacidad de armamento, una alta velocidad y ser más sigilosos, en comparación con un actual UAS (Gertler, 2012).

De la misma manera, se espera que los UAS desarrollen otro tipo de misiones en el futuro, entre las cuales están:

- Reabastecer: La intención de esta capacidad para que los UAS puedan entregar material a los buques en alta mar o unidades de infantería de marina.
- Búsqueda y rescate: Desarrollar la capacidad para búsqueda, localización y evacuación de personal, más allá de las líneas enemigas.
- Reabastecimiento de combustible: Busca que los UAS puedan hacer retanqueo **aéreo como el que realizan los tanqueros KC-10 o KC-135** actualmente.
- Combate aéreo: Se considera que la tarea futura más difícil será que lleven a cabo combates aire-aire. Aunque en la actualidad el enfoque es hacia los blancos en tierra, existe un desarrollo para que los UAV lleven armas para un combate aire-aire y otros sistemas que les permitan llevar a cabo misiones para obtener una superioridad aérea. De hecho, se tiene un reporte de un UAV-Predator, el cual tuvo un contacto aire-aire con una aeronave iraquí, el Predator lanzó un misil aire-aire antes que el MiG disparará el suyo. Todavía se considera que se está en una etapa de desarrollo, por tanto, se espera que en un futuro no lejano los UAV lleven a cabo cualquier tipo de misiones que desarrollan las aeronaves tripuladas.

En ese mismo sentido, O'Donoghue (2018) propone que el futuro para la aviación naval está en la combinación de las plataformas tripuladas y no tripuladas. Asimismo, estas son probadas en una variedad de

roles. Por ejemplo, cuando se está utilizando un MQ-4C Trit**ó**n el cual satisface las necesidades para una patrulla marítima conjunta, mediante la expansión del conocimiento del panorama operacional y del radio de combate de un P-8 Poseidón, con el mejoramiento del rango de detección de blancos y con un panorama operacional más completo. De tal manera que el MQ-4C contribuye de forma decidida en el ciclo de observación, orientación, decisión y actuación (OODA), haciendo énfasis en los dos primeros pasos, permitiendo que el P-8 Poseidón se enfoque en los dos últimos. Este concepto hace que se extienda la misión de la plataforma MQ-4C para apoyar a mejorar la obtención de la conciencia (conocimiento) de la situación del espacio de la batalla, lo que puede traducirse a la ayuda en una simple tarea, lo cual le permita concentrar la atención del tripulante de la aeronave sobre las tareas más importantes. Adicionalmente, esta combinación de un equipo tripulado y no tripulado no solamente es útil para la obtención de blancos y del ciclo OODA, sino que también ayuda a aliviar el estrés actual físico de las plataformas tripuladas que se da al tener que llevar a cabo roles secundarios (O'Donoghue, 2018: 2).

De acuerdo con el Jefe de Operaciones Navales de los Estados Unidos, la Marina se encuentra en la búsqueda de la próxima generación de UAV que apoyarán las operaciones navales, para lo cual se ha desarrollado una hoja ruta para los futuros desarrollos, en los cuales esos UAV serán una componente fundamental de la visión de la Marina de ser una fuerza en red o una Red C4ISR (comando, control, comunicaciones, computadores, inteligencia, vigilancia y reconocimiento) y para roles específicos de combate (Polmer, 2003).

De manera que han propuesto tres categorías de UAV:

- Que permita cubrir áreas oceánicas y de litoral a gran altura por largos períodos, pueden ser días o semanas. Para eso han propuesto los llamados BAMS (*Broad Area Maritime Surveillance*), por sus siglas en inglés, que permiten una vigilancia en un área amplia. Los cuales suministrarían observación, reconocimiento, ser repetidores para comunicaciones e inteligencia. Sus sensores deberían ser radar, sistemas infra-

rrojos y electroópticos. Por parte de las comunicaciones, deberían estar en capacidad de servir de repetidoras para las comunicaciones en línea de vista para los buques, aeronaves o el enlace de las fuerzas navales y terrestres con satélites.

Además, estos BAMS, con un vuelo a gran altura se pueden utilizar con comunicaciones de láser entre un satélite y estas aeronaves no tripuladas, lo que incrementaría, de manera significativa, el ancho de banda, ser repetidoras para las fuerzas de aire, superficie, y submarinas, utilizando la radiofrecuencia. Este tipo de vehículo requerirá de una base en tierra.

- Con capacidad para penetrar una vigilancia y suprimir las defensas aéreas enemigas, el cual ha sido llamado un vehículo aéreo no tripulado de combate naval (UCAV-Ns). Este vehículo lo han visionado como multimisión ya que puede desarrollar ataque ISR y a la vez misiones de supresión de las defensas aéreas del enemigo (SEAD) en un ambiente hostil.

- Tácticos para vigilancia y selección de objetivos conocidos como T-UAV, que serían el reemplazo del actual Pioneer utilizado por la Infantería de Marina al nivel de batallón y en la Marina en los niveles de grupo de ataque y grupo expedicionario. Estos pueden ser usados en mar y en tierra, y serían particularmente importantes para las operaciones conectadas en red, porque tendrían bases en tierra y en el mar (Polmar, 2003).

McVety (2000) manifiesta que las aeronaves no tripuladas serán construidas para ser ligeras y rápidas para transportar armas a un área blanco, estos vehículos estarán bajo el control humano y en otros casos serán totalmente autónomos, controlados por sofisticados algoritmos y conjuntos de reglas, gracias al desarrollo de la inteligencia artificial, con vigilancia humana a distancia mediante monitores. Las aeronaves tripuladas y no tripuladas trabajarán en conjunto como una fuerza para la maniobra, de manera que se capitalicen las fortalezas de cada una y se minimicen sus debilidades (McVety, 2000).

De la misma manera, McVety (2000) visiona a la fuerza aeronaval del mañana, la cual lucirá en algunos aspectos similares a la que hoy vemos.

Portaviones con aeronaves tripuladas que aún son desplegadas desde esa plataforma, así como unidades de superficie protegiendo el portaviones y haciendo las tareas que ellos llevan a cabo ahora. Sin embargo, con los vehículos no tripulados sobre sus cubiertas y hangares, lo combatientes de superficie podrían llevar una capacidad adicional para la batalla. Se cree que entre 10 a 13 vehículos no tripulados de combate pueden estar en cada uno de los cruceros a disposición de todos los integrantes del grupo de batalla, con capacidad de combate, comunicaciones y sensores.

Conclusiones

El desarrollo tecnológico es cada día más rápido y sobre todo el de las tecnologías de la información, lo que hace que las amenazas emergentes crezcan en la misma medida que los avances, a diferencia del sector defensa porque el ritmo de crecimiento no se iguala al de los nuevos desarrollos, permitiendo que existan vulnerabilidades que ofrecen una ventaja a actores estatales y no estatales que pretenden vulnerar la defensa y la seguridad de las naciones y de las fuerzas.

Cada día las operaciones de información toman un lugar más importante en el rol actual que desempeñan las fuerzas militares en un país debido a la inclusión de actores como los medios de comunicación y que en algunos casos son de carácter global.

De igual manera, está el internet y las redes sociales, quienes cada día toman mayor partido dentro de la mente y las decisiones de la sociedad. En ese sentido, se hace necesario un trabajo en conjunto entre las Fuerzas Militares y el Estado para poder cumplir con los objetivos de los intereses de la nación. De esta forma pueden tomar las mejores decisiones para que no afecten la legitimidad del Estado y de sus Fuerzas Militares durante el desarrollo de operaciones en donde sea necesario aplicar el uso de las fuerzas y se puedan presentar bajas de las propias fuerzas o daños colaterales que involucren a las personas no combatientes.

El panorama al que se enfrentan y se van a seguir enfrentando las Fuerzas Militares es cada vez más asimétrico, como el que plantea la

guerra híbrida en donde se tienen actores estatales y no estatales, en los cuales todos tienen acceso a las nuevas tecnologías, con la capacidad para poder hacer daño o impactar a las fuerzas propias o la sociedad.

Además, no solo implicará el uso de medios diferentes a los convencionales para poder infligir su poder en contra del adversario, lo que hace que sea necesario ser adaptativos para identificar más rápido las vulnerabilidades del enemigo y proteger las nuestras, con el fin de obtener una ventaja decisiva en el espacio de la batalla.

Si bien no ha cambiado el principio de la guerra de seguridad de no permitirle al enemigo obtener una ventaja, sí han cambiado los medios para obtenerlo. En esto están involucradas las nuevas tecnologías, las cuales han permitido que se tengan herramientas que disminuyan la incertidumbre y la fricción en el desarrollo de las operaciones.

La superioridad de la información se convierte en un concepto esencial para el desarrollo de las operaciones. Si se observa desde el punto de vista en que se tienen unas fuerzas altamente interconectadas por medio del uso de equipos centrados en redes, operando en el ciberespacio, en un ambiente operacional asimétrico, es necesario buscar una ventaja que le permita a las fuerzas propias y amigas tener el mejor panorama del espacio de la batalla para la toma de decisiones y la menor cantidad de incertidumbre y de fricciones en el desarrollo de operaciones. De tal manera, que mientras se tenga la superioridad de la información, se podrán llevar a cabo operaciones más seguras, para que a las fuerzas amigas obtengan la ventaja para poder usar todos los equipos y medios sin que sean objeto de un ataque informático que les impida alcanzar la intención del comandante.

Las operaciones del futuro se llevarán a cabo en un lugar más amplio que el conocido como campo de batalla, que se ha identificado como el lugar físico en el cual se realizan las interacciones de una guerra. De tal manera, que cuando entran a jugar otros factores como son el ciberespacio, los sensores y las entidades que hacen parte de las interacciones, tanto las amigas como las enemigas y las neutrales, se amplía ese escenario donde se llevan a cabo las operaciones y las interacciones en una confrontación, convirtiéndolo en el espacio de la batalla, porque va más allá

de los espacios físicos, y entran jugar otros espacios virtuales. Además, será un espacio donde la información debe ser compartida de manera que se tenga un panorama más completo de la situación de la batalla.

Las aeronaves no tripuladas entrarán cada día a ser una parte importante en el desarrollo de las futuras operaciones navales, porque estas permitirán expandir las capacidades de los buques y de su flota, al poder tener con ellas sensores que les permitan vigilar, reconocer e identificar a la flota enemiga. Las capacidades que tienen estas aeronaves de estar por un tiempo muy prolongado en el área de operaciones permiten tener un panorama más amplio de la situación operacional y al estar dentro de un sistema centrado en redes en el cual se pueda compartir con todas las entidades que hacen parte del sistema, contribuye a tener un mejor poder de combate y de alistamiento de la flota. De igual manera, estos vehículos podrán ser utilizados para realizar operaciones ofensivas contra blancos específicos en tierra y en el mar, así como para llegar a apoyar a la defensa de la flota contra ataques de misiles, otros UAV y otras posibles amenazas de una manera oportuna y eficiente.

Estas capacidades de las nuevas tecnologías son una oportunidad para poder realizar el diseño de la flota del futuro. De manera que los nuevos buques que se piensen adquirir o construir deberán contar con este tipo de capacidades. Por lo tanto, esa flota deberá contar con una infraestructura para guerra centrada en redes, con capacidad de llevar UAV de diferentes configuraciones. Asimismo, con una fuerte capacidad para defenderse y atacar en el ciberespacio. Además, ser multipropósito, que puedan cumplir misiones de todo tipo que incluyan las necesidades de la guerra híbrida y para operaciones de no guerra, sin perder su propósito principal: la soberanía y la defensa de la nación.