ESTRATEGIA MILITAR Y SU TRANSFIGURACIÓN EN LA ERA DE LA INFORMACIÓN

PALABRAS CLAVE:
INFORMACIÓN / CIBERDEFENSA / ESTRATEGIA COMUNICACIONAL / GUERRA CIBERNÉTICA / OPERACIONES DE INFORMACIÓN

Por **Leonardo Arcadio Zarza**

La era de la información del siglo XXI demanda tener en todos los países una estrategia nacional comunicacional adecuada, una estrategia militar que contemple las dimensiones del ambiente operacional aeroespacial, el ciberespacio y el espacio electromagnético. Impone desafíos en la organización territorial y la necesidad de tener en cuenta los efectos de las operaciones de información.

NTRODUCCIÓN

La Estrategia Militar es la aplicación de los recursos militares para contribuir al logro de los objetivos de la Estrategia Nacional. Es el componente militar de la estrategia nacional y se formula a partir de una dirección política: el presidente de la Nación y Comandante en Jefe de las Fuerzas Armadas ejerce la conducción estratégica nacional y militar; el Ministro de Defensa asiste al presidente en la conducción de la Defensa Nacional (Estrategia Nacional) y el Estado Mayor Conjunto de las Fuerzas Armadas asesora y asiste al presidente de la Nación en la conducción estratégica militar [1].

Para la conducción eficaz y efectiva, todo conductor militar debe conocer cómo apreciar el ambiente operacional moderno y los efectos que produce sobre las operaciones militares el tener que decidir bajo presión en un contexto saturado de información. Esta información que se presenta en el área de operaciones o catástrofe, actúa como un "catalizador de las percepciones": puede ser una ventaja o desventaja para el logro del estado final deseado e influye en forma intangible pero decisiva en la voluntad de vencer de las fuerzas y, en definitiva, en el éxito de la operación. Ya Napoleón Bonaparte expresaba en 1805 "En la Guerra, la moral es a lo físico, como tres a uno".

A pesar de los avances tecnológicos, la naturaleza violenta de la guerra no ha cambiado y los actores que en los últimos tiempos han constituido amenazas o potenciales escenarios de conflicto no se rigen normalmente por las mismas reglas legales que el estado de derecho. Por ejemplo, en la guerra del Golfo de 1991 quedó claro que las guerras futuras no serían del modo convencional que lo eran antes para los que no dispongan de poder militar suficiente y deban enfrentar a potencias de primer orden; por ello el inmortal arte de la guerra se ha tenido que ir adaptando y nació, así, el concepto de Guerra Asimétrica.[2]

En las operaciones militares de la era de la información, es importante hacer varias distinciones en los niveles de conducción: existen desarrollos de tipos de estrategias (Estrategia Comunicacional), de guerra (Guerra Cibernética) y de operaciones militares (Operaciones de Información).

Es importante distinguir "Inteligencia" de "Información", ya que en el primer caso, la información de interés es el "fin", y luego se la deberá procesar para obtener inteligencia; en cambio, en el segundo caso, la información es utilizada como "medio", incluso como lo que se conoce en la doctrina militar comparada extranjera como "Efecto No Letal" para manipular el sistema de decisión del oponente.[3]

Tampoco debe confundirse "Guerra Electrónica con Guerra Cibernética" ya que los ámbitos de aplicación son diferentes: el primero se da en el ámbito aeroespacial sobre aire, mar o tierra, y sus espectros electromagnéticos, y el segundo tipo, en el "ciberespacio".

Se infiere que es parte de la Defensa Nacional entender que, desde el inicio del nuevo milenio, se ha percibido en los países que se encuentran en guerra, un constante incremento de estrategias y operaciones militares en donde la primera fase de toda campaña militar es la búsqueda de la superioridad de información y mantenerla es un desafío aún mayor al de la superioridad aeroespacial.

Según Clausewitz, una de las premisas de todo exitoso conductor militar es conocer cuál es la naturaleza del próximo conflicto que deberá enfrentar. Para lograr este conocimiento, es necesario analizar el ambiente operacional moderno y, especialmente, los factores tecnológico, psicológico y comunicacional; y, dentro de éstos, el del fenómeno de las comunicaciones digitales, el dominio del ciberespacio y la información, que en la actualidad cobran un rol esencial por cuanto afectan la moral y pasión de los pueblos en forma positiva o negativa.

Hasta la revolución industrial, la base de la mayoría de las contribuciones tecnológicas era de naturaleza mecánica, una

1. Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la Acción Militar Conjunta –Nivel Operacional;* PC 20-01; 2015; p. 3.
2. Qiao Liang y Wang Xiangsui; *Guerra Irrestricta;* Ejército Popular Chino; Casa de Publicaciones de Arte y Literatura; Beijing; 1998.
3. Fuerzas Armadas de Estados Unidos de América; *Publicación Conjunta 3-13 Operaciones de Información;* Ed. 2012.

ciencia perceptiva a los ojos humanos. Con la revolución tecnológica moderna se ha dado un cambio sustancial estratégico de base y la electrónica junto con la informática, ciencia imperceptible a los ojos humanos, basadas en el movimiento de electrones y bits, han ocasionado otra revolución de naturaleza cultural.[4]

Por ejemplo, ya en 2004, se conocía que las fuerzas estratégicas nucleares de China, conocidas también como el Segundo Cuerpo de Artillería, habían sido el núcleo duro en donde se conformó la "Fuerza de Guerra de Información de China". A la Academia de Ingeniería de este Cuerpo de Ejército que se especializaba en misiles, se le han agregado sistemas electrónicos, servidores de redes y se ha incorporado un curso de psicología y capacidad de transmisión de información encriptada en tiempo real.[5]

Thomas Friedman afirma en su libro *"El mundo es plano en el siglo XXI": Cristóbal Colón en 1492 expresó a los reyes de España que la tierra era redonda porque pensó que luego de su expedición a América había arribado a las Indias. Hoy, la tecnología de las comunicaciones, internet, celulares inteligentes e información en red condicionan un mundo en donde se produce la percepción de la globalización de lo local achatando nuevamente la tierra y en donde todos disponen de la aptitud de enterarse en forma instantánea de todo lo que pasa en el mundo.*[6]

Esto demuestra que para actualizar el arte operacional propio es conveniente ampliar el espectro de conocimientos de los estrategas militares argentinos; adecuar los conceptos de organización territorial con la inclusión del ciberespacio; diseñar doctrina y opciones estratégicas de comunicación que contengan la Revolución de Asuntos Militares, tecnologías de impacto, operaciones de información, Ciberdefensa, probables contenciones de dilemas entre libertad de expresión, privacidad y seguridad, con el objetivo de preservar la libertad y, a la vez, enfrentar los desafíos de las amenazas a la seguridad nacional de la era de la información.

ESTRATEGIA SIN FRONTERAS

Cuando se examinan los materiales de Guerra de la Información de los últimos veinte años del Ejército Popular Chino, se pone en evidencia la importancia que ha cobrado este aspecto en la transformación de una fuerza mecanizada en una fuerza informatizada.[7]

A pesar de la mayor virtualidad y apariencia de intangibilidad de las relaciones humanas con los celulares inteligentes, las acciones en las redes sociales y la falta de contacto físico, la naturaleza física del ciberespacio, que se hace visible al ojo humano a través de la realidad virtual, hace que la estrategia siga cumpliendo fielmente su rol de estudiar el fenómeno del conflicto y las disputas de poder a través de las "percepciones" producto del lenguaje estratégico.

Siguiendo un método de razonamiento lógico, si la información en el siglo XXI se ha expandido del ámbito físico del papel, la carta, la radio, la oralidad, la televisión y la telefonía a la transferencia de datos digitales de hipertextos, mail, voz, imagen y videos a través del ciberespacio, se visualiza a priori que la estrategia que incluye estas acciones y efectos "no reconoce fronteras físicas soberanas, pero se debe comprender

"Existe una guerra allí afuera, querido amigo... una guerra mundial. Y no es acerca del que tenga más balas, es relacionada con el que tiene el control de la información". Film "Sneakers" -Cosmo, 1992.

que su naturaleza sigue siendo 'física' a través de la 'realidad virtual', y por lo tanto puede ser controlada.

En la actualidad y cada vez en mayor medida, existen métodos digitales para relacionarse y realizar actos financieros, comerciales, legales, políticos, económicos, de redes sociales, militares y tecnológicos. La pregunta que surge es: ¿cómo se deberá ejercer, desde el punto de vista de la Defensa Nacional, la soberanía efectiva, autodeterminación, y a la vez respetar los principios básicos de paz, derechos humanos y libertad consagrados en la Carta de Naciones Unidas?

Las potencias de primer orden ya han sufrido acciones que mostraron sus vulnerabilidades, lo comprendieron y han alineado sus estrategias de recursos-modos y fines para planificar e implementar organizaciones a fin de mantener la competitividad en las relaciones internacionales. Por ejemplo, en Estados Unidos se formulan estrategias particulares normalmente diseñadas al mayor nivel de conducción posible que se ocupan de este tipo de conflictos a través de la Estrategia Comunicacional. Existen también organizaciones de nivel estratégico nacional, como el Comando Estratégico de Ciberdefensa. En el nivel estratégico militar, todas las organizaciones militares de las fuerzas armadas disponen de personal militar o contratado capacitado en Operaciones de Información en condiciones de cumplir roles a nivel unidad, brigada y superiores y a nivel conjunto en una Plana Mayor/ Estado Mayor. Brasil ha actualizado su doctrina militar en el mismo sentido.

En Argentina, cualquiera sea la estrategia que se diseñe para operar en el espacio cibernético, debe generar un profundo cambio en todos los factores de poder de la defensa nacional. El incremento de políticas de vigilancia y control del ciberespacio, las especializaciones del derecho, la incorporación en el código de delitos informáticos, la reciente creación en el ámbito militar del Comando de Ciberdefensa y la actualización de la doctrina de las fuerzas armadas constituyen un paso importante.

Frente a las amenazas que no son exclusivamente del factor de poder militar, los países deben adaptar y proteger su sistema de poder político legítimo-democrático, todos sus recursos económicos, sus sistemas de energía y fuentes de poder de base para garantizar su normal funcionamiento y protegerlos de potenciales acciones terroristas. Todo Sistema de Defensa debe disponer de Comandos Estratégicos de Ciberdefensa dependientes del máximo nivel de conducción, enlazados con Sistemas de Telecomunicaciones Satelitales y con capacidad para ejercer un estricto monitoreo aeroespacial y del ciberespacio.

LA DINÁMICA TECNOLÓGICA DE REVOLUCIONES MILITARES Y REVOLUCIONES EN ASUNTOS MILITARES (RAM)[8]

Se debe distinguir que no es lo mismo Revoluciones Militares que Revolución en Asuntos Militares. En el libro "Dynamics of Military Revolution: 1300-2050", Williamson Murray y Mac Gregor Knox, cuando tratan el tema "Pensamiento acerca de la Revolución en Warfare", expresan que toda Revolución en Asuntos Militares está precedida de una Revolución Militar y que ésta no es precisamente sólo Militar sino que abarca aspectos políticos, económicos y sociales, y exponen la siguiente línea del tiempo:

- **Etapa Previa a la Revolución en Asuntos Militares Edad Media y Moderna:**
  Resultante: Lanzas, Estrategias Ofensivas-Defensivas-Pólvora, Arquitectura de Nuevas Fortalezas.

- **Primera Revolución Militar:** Creación del Estado Moderno del Siglo XVII y de Instituciones Militares Modernas.
  Resultante de la Revolución en Asuntos Militares 1: Reformas Tácticas suecas y holandesas, Reformas Tácticas y Organizacionales francesas, Revolución Naval y Revolución Financiera inglesa.

  Reforma Militar francesa luego de la Guerra de los Siete Años.

- **Segunda y Tercera Revolución Militar: Revolución Industrial y Revolución Francesa.**
  Resultante de la Revolución en Asuntos Militares 2 y 3: Movilización Política y Nacional, Guerras Napoleónicas (Aniquilamiento de las fuerzas enemigas en el campo de batalla).

  Poder económico y financiero basado en la Industrialización (Gran Bretaña).

  Revolución Tecnológica en la guerra terrestre y del transporte (telégrafo, vías ferroviarias, buques a vapor, armas de fuego automáticas, artillería).

4. Albano Do Amarante, Jose Carlos; *El Vuelo de la Humanidad y 101 Tecnologías que cambiaron la faz de la tierra;* Editorial Mas Letras-Comunicaciones; Buenos Aires; 2014; p. 426.
5. Timothy L Thomas; *Dragon Bytes-Chinese Information War Theory and Practice;* FMSO- Fort Leavenworth;Kansas, Estados Unidos; 2004; p. 144.
6. Friedman Thomas; *The World is Flat-A Brief History of the Twenty First Century;* Editorial Picador, Farrar, Straus, and Giroux; Nueva York, Estados Unidos; 2005; p. 5.
7. Timothy L. Thomas; op. cit.; p. 136.
8. Knox and Murray; *The Dynamics of Military Revolution-1330-2050;* Editorial Cambridge University Press; 2007; p. 13.

Revolución de Fisher en la guerra naval, acorazados y destructores.

› **Cuarta Revolución Militar: La Primera Guerra Mundial combina las Revoluciones en Asuntos Militares precedentes.**
Resultante de la Revolución en Asuntos Militares 4: Operaciones y Tácticas de Armas Combinadas, la guerra relámpago, bombardeo estratégico, guerra de portaaviones, anfibia y submarina, radar e inteligencia de señales.

› **Quinta Revolución Militar: Armas Nucleares y Sistema de Distribución de Misiles Balísticos.**
Resultante de la Revolución en Asuntos Militares 5: Bombardeo y Reconocimiento Preciso, Furtividad, Computarización, Comando y Control basado en Redes, incremento masivo de letalidad de municiones convencionales.

Williamson y Mac Gregor Knox hicieron referencia a cinco Revoluciones en Asuntos Militares. Se aprecia que en la actualidad existe una sexta revolución propia de esta era:

› **Sexta Revolución Militar: Guerra de Iraq 1991- Atentado a las Torres Gemelas en Estados Unidos 2001.**
Resultante de la Revolución en Asuntos Militares: Operaciones de Información.

OPERACIONES DE INFORMACIÓN

Ni en la Primera ni en la Segunda Guerra Mundial, la primera potencia del mundo había sufrido un ataque en su propio territorio. Luego de los sucesos de las Torres Gemelas del 11 de setiembre de 2001, y con el objetivo de proteger sus intereses vitales dentro y fuera de su propio país, Estados Unidos ha detectado graves vulnerabilidades, por lo que ha impulsado un incremento en el sistema de alerta situacional y ha intentado expandir su área de influencia a nivel global para mantener las amenazas potenciales lejos de su población local. Parte de ese esfuerzo ha sido canalizado con las Operaciones de Información.

Los Líderes de China están convencidos de que el corazón de la última Revolución en Asuntos Militares son las "Operaciones de Información".

En el caso de Estados Unidos, las Operaciones de Información son las acciones que tienen por objeto manipular el sistema de decisión del oponente y se estila asociar a los medios que se utilizan en este tipo de operaciones como "Efectos No

9. Fuerzas Armadas de Estados Unidos de América; Publicación Conjunta 3-13 Operaciones de Información; 2012.
10. Fuerzas Armadas de Estados Unidos de América; op. cit.

ELEMENTOS DE OPERACIÓN DE INFORMACIÓN	APOYO
Guerra Electrónica	Destrucción Física
Operaciones con Computadoras en Red Ataque a Red de Computadoras	Seguridad de la Información
Defensa de Red de Computadoras	Seguridad Física
Explotación de Red de Computadoras	Contrainteligencia
Operaciones Psicológicas	Contra Velo y Engaño
Operaciones de Seguridad	Contra propaganda
Operaciones de Velo y Engaño	

Letales". En la publicación conjunta JP- 3-13, el Secretario de Defensa de ese país define a las Operaciones de Información como "el empleo integral durante las operaciones militares de capacidades relacionadas con la información sincronizadas con las líneas de operaciones, para influir, dislocar, usurpar o corromper el sistema de decisión del adversario real o potencial y a la vez proteger el sistema de decisión propio."[9] En este caso, el Ambiente Operacional de Información dispone de tres dimensiones a tener en cuenta:

- Dimensión Cognitiva (Centrada en el Ser Humano).
- Dimensión Física (Tangible-Mundo Real)
- Dimensión Informacional (Centrada en Redes y Datos)

En cuanto a la dimensión física e informacional, en este tipo de fuerzas de potencias militares de primer orden de alta dependencia tecnológica, se conoce que se han utilizado como doctrina los siguientes elementos de las Operaciones de Información[10]:

En los estados mayores conjuntos modernos que ejecutan operaciones militares aparecen miembros que asesoran y asisten a los comandantes en operaciones y que ocupan roles tradicionales de Jefes de Inteligencia y otros innovadores como Jefes de Operaciones de Información y jefes de Estrategia Comunicacional como miembros del estado mayor especial de los comandantes. La existencia de estos miembros denota la importancia actual que se le asignan a estos campos de la conducción. Investigando en la doctrina comparada, las Operaciones de Información en las Fuerzas Armadas de Brasil, al igual que las de Estados Unidos, las conduce todo Comandante Militar asesorado por un miembro del Estado Mayor denominado Jefe de Operaciones de Información, y no se concentra en capacidades particulares individuales sino que concentra otras para lograr un determinado efecto.

Las responsabilidades más importantes del Jefe de Operaciones de Información son:

- Ser el oficial del estado mayor responsable de la integración de los efectos no-letales para destruir o dislocar el flujo de información de las fuerzas enemigas.
- Supervisar la protección de la información propia y de fuerzas enemigas.
- Coordinar con Asuntos Territoriales para proteger la red digital de Comando, Control, Comunicaciones, Ciberdefensa- Inteligencia, Informática de las Grandes Unidades de Batalla (Operaciones de Información Defensivas).
- Coordinar con el Jefe de Inteligencia las Medidas de Seguridad de Contrainteligencia (Operaciones de Información Defensivas).
- Integrar las Operaciones de Información dentro del "Proceso de Determinación de Objetivos" (Operaciones de Información Ofensivas).
- Coordinar con Operaciones y el Coordinador de Apoyo de Fuego operaciones de engaño, operaciones de comunicación social, y guerra electrónica (operaciones de Información Ofensivas, por ejemplo, Guerra Electrónica y Frecuencias propias).
- Autorizar "Efectos No-letales" sobre blancos planeados.
- Coordinar con el Oficial de Comunicaciones Institucional" para publicar información (relacionada con Operaciones de Información Ofensivas).

En conclusión, para las Fuerza Armadas argentinas, existen muchas capacidades militares relacionadas a desarrollar, y que contribuirían a lograr los efectos en las Operaciones de Información:

- Operaciones de Inteligencia.
- Estrategia Comunicacional.
- Comunicación Institucional.
- Operaciones de Asuntos Civiles.
- Operaciones de Ciberdefensa.
- Operaciones de Seguridad.

Leonardo Arcadio Zarza
Teniente Coronel del Ejército Argentino, Licenciado en Estrategia y Organización, Oficial de Estado Mayor del Ejército Argentino y del Ejército de los Estados Unidos. Fue Segundo Jefe de la Compañía de Ingenieros Conjunta Kosovo 4 en el marco de la OTAN en el 2002. Egresó de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Abogado, magíster en Defensa Nacional; Master en Business de la Universidad de Kansas, Estados Unidos; y Master en Artes y Ciencias Militares por el Colegio de Comando y Estado Mayor del Ejército de los Estados Unidos. Fue Jefe del Escuadrón de Aviación de Apoyo de Inteligencia 601 y del Batallón de Aviación de Apoyo de Combate 601. Actualmente es profesor de la Escuela Superior de Guerra y se desempeña como Jefe del Departamento Operaciones G-3 de la Dirección de Aviación de Ejército.

- Operaciones de Velo y Engaño.
- Operaciones de Guerra Electrónica.
- Operaciones de Comunicación Social Aplicativa al Combate[11].
- Construcción de Sistemas de Supervisión y Medición de Efectos de Operaciones de Información por Desempeño (para conocer si las acciones que se están ejecutando sobre el objetivo producen efectos correctos) o por Efectividad (para conocer si el objetivo seleccionado es el correcto o no y si es necesario reformular nuevamente el objetivo y su efecto).

ESTRATEGIA COMUNICACIONAL

En los países extranjeros que utilizan este concepto, no es lo que comúnmente se conoce en las Fuerzas Armadas argentinas como "Comunicación Institucional", sino que el objeto de este "Tipo de Estrategia" es lograr imponer efectos de interés sobre audiencias clave, y no mostrar solamente la imagen positiva de lo que hace o no.

La Estrategia Comunicacional surge justamente cuando existen otros discursos o relatos que se oponen a los intereses u objetivos fijados por la estrategia nacional. Son las acciones cuyo objetivo es el espacio cognitivo de la población.

Por ejemplo, en el caso de la doctrina conjunta de Estados Unidos J P 3-13 definen Comunicaciones Estratégicas como: *El proceso de focalización de esfuerzos del gobierno en la creación, fortalecimiento, y preservación de condiciones favorables para el avance de los intereses nacionales, políticas y objetivos, mediante la comprensión y captación de audiencias clave, a través de la coordinación de planes, programas, temas, mensajes, y productos sincronizados con las acciones de todos los instrumentos del poder nacional.*[12]

En la era de internet y la hiper-conectividad, la realidad es que cuando surgen nuevas tecnologías de comunicación capaces de dar mayor conectividad, paradójicamente al mismo tiempo producen mayor división social y mayor distracción. Esto es así por cuanto cada vez es más difícil mantener la reserva, privacidad y el diálogo franco directo entre organizaciones y personas por la aparición de la telefonía celular y las redes sociales: muchas conversaciones e imágenes privadas se transforman en públicas y cada vez se hace más complejo focalizar la atención incluso en el diálogo diario con personas que se ven atraídas por lo que pasa en el "celular".[13]

CIBERDEFENSA

Cuando se trata este tema es importante aclarar los actores, niveles de agresión y amenaza para tipificar lo que configuraría un Crimen Cibernético, Terrorismo Cibernético y Guerra Cibernética[14]. Esta distinción permite definir las jurisdicciones de actuación del estado ya que estos conflictos serán competencia de las fuerzas de seguridad en los dos primeros y de las fuerzas armadas en el tercero.

La construcción de "Sistemas de Soft-Destruction" va a ser tan importante como los Fuegos en las Operaciones Militares. ***Timothy L. Thomas***

Es importante también distinguir entre Operaciones de Información y Operaciones Cibernéticas: se pueden planificar algunos tipos de Operaciones de Información utilizando como "medio" las Operaciones Cibernéticas en el ciberespacio.

Según la doctrina nacional argentina la Ciberdefensa es el conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, o repeler una amenaza o agresión cibernética, sea esta inmediata, latente o potencial para permitir el empleo del instrumento militar de la Nación.[15]

Las Operaciones de Ciberdefensa según la doctrina militar de las Fuerzas Terrestres argentinas vigente pueden ser:

- **Ciberdefensa Directa:** su finalidad es vigilar y controlar las redes y sistemas en los ámbitos específicos y conjuntos.

- **Ciberdefensa Indirecta:** su finalidad es disputar el control del ciberespacio necesario para el accionar de las fuerzas militares.

En general, se puede definir la "Cibernética" como una ciencia de la comunicación, del procesamiento y del control, sea en el hombre o en la máquina. La cibernética está invadiendo el campo de la actuación del hombre en variados sectores de la sociedad. Es la sustitución del hombre por la máquina en actividades previsibles o repetidas, dejando para el hombre aquellas que son nuevas o inusitadas.[16]

El ambiente operacional cibernético es de naturaleza física, a pesar que el ciberespacio parezca intangible, y solo es percibido por el ojo humano a través de la realidad virtual. Por ejemplo, la doctrina de las fuerzas armadas de Estados Unidos JP 3-12 expresa respecto del Ciberespacio:

11. Ejército Argentino; ROB 00-01 Conducción de las Fuerzas Terrestres; 2015. 12. Fuerzas Armadas de Estados Unidos de América; Publicación Conjunta 3-13 Operaciones de Información; 2012.
13. Friedman Thomas, op. cit.; p. 515.
14. Uzal, Roberto; "Guerra Cibernética ¿Un desafío para la Defensa Nacional?"; revista Visión Conjunta; Escuela Superior de Guerra Conjunta de las Fuerzas Armadas; Nro 7; Buenos Aires; 2012, p. 42.
15. Ejército Argentino; ROB 00-01 Conducción de las Fuerzas Terrestres; 2015.
16. Albano Do Amarante, Jose Carlos; *El Vuelo de la Humanidad y 101 Tecnologías que cambiaron la faz de la tierra;* Editorial Mas Letras-Comunicaciones; Buenos Aires; 2014; p. 484.

¨Las Operaciones en el Ciberespacio descansan en una red interdependiente de una infraestructura Tecnológica de Información, incluido internet, redes de telecomunicaciones, sistemas de computación, controladores, procesadores y el flujo de contenidos que los atraviesan. Las Operaciones Espaciales en el Espacio Ultraterrestre dependen del Ciberespacio y porciones críticas del Ciberespacio pueden ser solo proporcionadas a través de Operaciones Espaciales en el Espacio Ultraterrestre (Satélites). Las Operaciones Cibernéticas pueden ser Operaciones Ofensivas, Defensivas y Operaciones de Defensa del Ministerio de Defensa.[17]

Para sincronizar este tipo de operaciones, las fuerzas armadas de Estados Unidos estructuran tres niveles de redes:

- **Red Física** (Sistemas, *hardware, software,* e infraestructura: alámbrica, inalámbrica, links, satelital, u óptica que apoyan a la red y a los conectores físicos (computadoras, *routers, servers,* cables, *switches,* etc.)

- **Red Lógica** (todos aquellos elementos de la red que están relacionados unos con otros fuera de la red física: como por ejemplo la Web que está anclada en servidores localizados en múltiples lugares y cuyo contenido puede ser accedido a través de un *Uniform Resource Locator* -URL-).
- **Red Ciber-Persona** (representa un mayor nivel de abstracción que el de la red lógica en el ciberespacio que utiliza reglas que se aplican en la red lógica para desarrollar una representación digital de un individuo o una entidad en el ciberespacio es decir "las personas usuarias en el ciberespacio").[18]

Existen "Armas de Nuevos Conceptos" y "Nuevo Concepto de Armas".[19] Las primeras evolucionan en función de su capacidad de movilidad y letalidad tecnológicas y van de la mano de la capacidad financiera de poder producirlas. Los "Nuevos Conceptos de Armas" han arribado, luego de las primeras y han sido desarrolladas por los que no pueden acceder a la tecnología para hacer frente a las potencias militares y bajo cuyo concepto, todo lo creado por el hombre puede convertirse en un arma. Esto tiene el potencial de producir una Devastación Cibernética, como por ejemplo:

A través de fuerzas cibernéticas organizadas o *hackers* y con el uso de virus informáticos, crackeadores, bombas lógicas a tiempo o a comando, caballos de Troya, atacantes sus-

17. Publicación Conjunta de las Fuerzas Armadas de Estados Unidos JP 3-12; United States Cyberspace Operations; 2013.
18. Publicación Conjunta de las Fuerzas Armadas de Estados Unidos JP 3-12; op. cit.
19. Qiao Liang y Wang Xiangsui; op. cit.; p. 25.

titutos, filtros de red, *firewalls, phishing,* programas espías, etc., se podrían producir los siguientes efectos[20]:

- Anular Sistemas de Defensa Nacional.
- Bloquear o saturar espacios de correos electrónicos.
- Desarticular sistemas de guiado espacial de satélites y guiado de aeronaves en vuelo.
- Deformar bases de datos de registros de personal.
- Ataque a través de un avión comercial utilizado como arma,
- Ataque cibernético a una red de internet determinada,
- Ataque a una red financiera nacional con virus a través de computadoras,
- Ataques para generar caos en las comunicaciones nacionales.[21]

Los desafíos para contrarrestar estas amenazas serán:

- Comprender que el tipo de amenazas en el ciberespacio no reconoce actualmente fronteras estatales.
- Entender que los actores que planifican y ejecutan las operaciones de guerra cibernéticas no necesariamente se muestran como un "Agresor Militar Estatal Externo".
- Mejorar una red intranet encriptada y robusta del área de Defensa con diseños propios nacionales para detección de intrusos a nivel nacional.
- Capacitar personal y diseñar la implementación de organizaciones que dispongan de capacidad de constituir una Fuerza de Defensa Cibernética con capacidad de interoperabilidad a nivel nacional y regional.

20. Stel Enrique; *Guerra Cibernética-Ciberespacio;* Círculo Militar; Buenos Aires; 2005.
21. Qiao Liang y Wang Xiangsui; op. cit.; p. 25.

SISTEMAS DE INFORMACIÓN GEOGRÁFICA

Estos sistemas han tenido un gran auge en los últimos tiempos como plataforma digital geográfica para orientación y navegación por el mundo. Es importante tener en cuenta que la alta dependencia de estos recursos puede traer consecuencias catastróficas para un conductor militar en el caso de no comprender que la información producida puede ser susceptible de afectación por operaciones de información o ataques cibernéticos. En la conducción militar, la cartografía en papel es un recurso que nunca desaparecerá.

Cada Fuerza Armada en la República Argentina ha desarrollado y dispone de un Sistema de Información Geográfica. Lo que reviste un constante desafío no resuelto es el accionar militar conjunto y la disponibilidad local y segura de una grilla global consistente en una plataforma cartográfica digital única para la ejecución de operaciones militares.

Un ejemplo de conjuntez en las Fuerzas Armadas argentinas es el Sistema de Protección Civil, que actualmente dispone del "Sistema de Manejo de Crisis" y es una herramienta

informática de gestión (a través del software "Sistema CRISIS") para la conducción y desarrollo de las operaciones de Protección Civil, en particular, una vez conformado el Centro de Operaciones de Emergencias. Este Sistema complementa y facilita la ejecución de las órdenes vigentes y, entre otras prestaciones, permite:

- Contar con una herramienta que facilite la coordinación de las tareas de apoyo a ejecutar por las fuerzas puestas a disposición a nivel nacional y regional.
- Disponer de información geoespacial que posea elComité Nacional de Actividades Espaciales, el Instituto Geográfico Nacional y todas las agencias estatales a nivel nacional y regional.

UNA PROPUESTA HACIA EL DOMINIO DE LAS WEBS: SISTEMA "W.A.R.F.A.R.E": SISTEMA DE WEB ARGENTINO-REGIONAL FUTURO ADAPTABLE A RESPUESTA DE EMERGENCIAS

"Warfare" es una palabra de origen inglés que en castellano significaría *"Guerrear",* ya que el equivalente de la palabra *"Guerra"* en inglés en realidad es *"War"*. Sin embargo, en este artículo se utiliza la palabra W.A.R.F.A.R.E como sigla de una propuesta de proyecto teórico innovador de defensa *"Pacificador"* para optimizar la estrategia comunicacional propia y regional, el comando, control y la gestión de la información, que sería de gran utilidad a las operaciones militares tanto

Las ideas de unificar el Ejército Popular Chino con las Operaciones de Información encontraron tierras fértiles en sus fuerzas de reserva de un millón y medio de hombres y mujeres.
Timothy L. Thomas

tácticas en conflictos armados, como Operaciones Militares de Paz, Protección Civil, operaciones en la Antártida y ante emergencias de seguridad y catastróficas de todo tipo que deban planificar y ejecutar las Fuerzas Armadas argentinas y de la región sudamericana.

Es preciso aclarar que "Internet" no es lo mismo que la "Web". Internet es la infraestructura digital sobre la que se montan una serie de servicios (Web, Mail, Chat, Streaming Video, etc.) y fue creada en 1969 por alumnos universitarios de Estados Unidos y perfeccionada por su Ejército para uso militar en 1971. En cambio, la Web, conocida hoy como World Wide Web (WWW), fue creada en el CERN (Laboratorio Europeo de Física de Partículas) por el inglés Tim Berners Lee veinte años más tarde, en 1989, quien se apoyó en Internet para resolver problemas de gestión de información y contenidos.

El poder de la Web y las redes sociales no tiene precedentes y los efectos que producen han ocasionado una aceleración vertiginosa en la evolución de la humanidad. Las ventajas saltan a la vista por cuanto se visualiza un sistema de alerta y asistencia global en donde toda crisis, guerra, protesta social o desastre producto de catástrofes es factible de ser informado en tiempo real y producir lo que se conoce como *"Ciber-Movilización"*. La desventaja es el uso que pueda darse para manipular las comunicaciones e información con intereses especiales que atentan contra la seguridad, soberanía, independencia y libertad de los pueblos.

Los aspectos más importantes a tener en cuenta para diseñar Sistemas Seguros de intranet, Webs nacionales y regionales como las de "WARFARE" de cara a las amenazas existentes serán:

- Diseñar, planificar, ejecutar y supervisar una Estrategia Comunicacional Transparente pero Segura.
- Agendar las Operaciones de Información de amenazas potenciales.
- Definir Políticas de Acceso y Control a Sistemas de Información Críticos de Defensa Nacional y Regional.
- Formación de recursos humanos especialistas.
- Firmar convenios de sistemas e informáticos de cooperación en el MERCOSUR, UNASUR y establecer alianzas regionales.

- Realizar análisis de riesgos de ataques cibernéticos.
- Diseñar el pasaje de fuerzas armadas mecanizadas a una informatizada.
- Potenciar los sistemas de comando y control digital militares existentes y sincronizarlos para que puedan operar en forma conjunta.
- Evitar que se utilice la región sudamericana como lugar de lanzamiento de potenciales ataques cibernéticos de terceros actores.

CONCLUSIONES

Uno de los primeros dilemas a dilucidar en el Arte de la Guerra es si se debe "Hacer la guerra con las Armas Disponibles o Hacer las Armas para un Cierto Tipo de Guerra". En el primer caso, se refiere a la forma tradicional de hacer la guerra y en el segundo, a la guerra futura.[22]

Estratégicamente, las guerras absolutas se están volviendo más controlables mientras que las guerras locales, más incontrolables. La guerra en la era de la información requiere que las acciones estratégicas y tácticas posean gran flexibilidad. Las fuerzas mecanizadas creaban ventaja por medio del movimiento; en cambio, una fuerza informatizada lo hace a través de la ocupación de posiciones ventajosas para la operación de la red de batalla. [23]

Las revoluciones tecnológicas modernas de la humanidad han determinado que el Arte de la Guerra haya tenido que adaptarse a las necesidades sociales.

Las Revoluciones de Asuntos Militares no son un sustituto de la estrategia, sino que están limitadas por ella y por la naturaleza de las guerras. Pero es importante detectar a tiempo la estrategia militar adecuada para los futuros conflictos armados.

Es imperativo aceptar la transfiguración de la Estrategia Militar en la era de la Información y aceptar los difusos y peligrosos límites de la estrategia comunicacional, de las operaciones de información y del ciberespacio. Sin embargo, siempre se debe bregar por la esperanza de que los estados que se involucren en el desarrollo de fuerzas para operaciones de información estructuren organizaciones territoriales adecuadas y habiliten una línea de comunicación fluida para negociar y entenderse mutuamente sobre todo a nivel regional.

Las potencias de primer orden compiten por el ejercicio de la supremacía de poder bajo el concepto de "el futuro detrás nuestro" y renuevan sus esfuerzos por innovar a pesar de sucesivos éxitos. Se conoce perfectamente que la clave está en la estrategia del "Cambio" oportuno y la superación está en la rápida recuperación de fracasos y en aprender haciendo.

En los conceptos rectores de Estrategia Comunicacional se pondera la facultad de lograr imponer la voluntad a través de "Comunicaciones Efectivas". Si existe una fortaleza en la región latinoamericana es justamente la "Comunicación Efectiva" en los últimos años que la han mantenido como una "Zona de Paz".

Respecto de Argentina, se debe encarar el pasaje definitivo de sus fuerzas armadas mecanizadas a una informatizada. Las fuerzas armadas no son ajenas a estos conceptos, simplemente los deben poner en práctica.

22. Qiao Liang y Wang Xiangsui; op. cit.; p. 19.
23. Timothy L Thomas; op. cit.; p. 136.