OPERACIONES TERRESTRES Y CIBERESPACIO: VULNERABILIDADES Y OPORTUNIDADES

Land operations and cyberspace: vulnerabilities and opportunities

GDB. René Leiva Villagra[1]

Los ataques son constantes y están creciendo en frecuencia e intensidad. Pueden destruir estructuras físicas y sistemas operacionales, paralizar ciudades y generar millonarias pérdidas, inclusive costar vidas. Pero los instrumentos de todo este caos no son balas, bombas o tanques; son "bits y bytes".

William J. Lynn III, Subsecretario de Defensa de Estados Unidos, 2011.

Resumen: En este artículo se presenta un análisis relacional de las operaciones terrestres, en un contexto operacional, sus vinculaciones con vulnerabilidades y oportunidades respecto a la quinta dimensión que lo compone (que es el ciberespacio), basado en un campo de batalla moderno, estableciendo vinculaciones con factores de consideración que resultan gravitantes en ello.

Palabras claves: Ciberdefensa –Ciberguerra – Ciberespacio – Operaciones terrestres – Campo de Batalla.

Abstract: This article presents a relational analysis of ground operations in an operational context, its links with vulnerabilities and opportunities regarding the fifth dimension that composes it (cyberspace), based on a modern battlefield, establishing links with factors of consideration that are important in it.

Key Words: Cyberdefense – Cyberwar – Cyberspace – Ground operations – Battlefield.

[1] René Leiva Villagra es General de Brigada (R) Ejército de Chile. Magister en Planificación y Gestión Estratégica. Diplomado de la Pontificia Universidad Católica de Chile en Gestión en Educación. Diplomado en Operaciones de Paz en la Fuerza de Defensa Australiana. Graduado del Curso Avanzado de Comunicaciones (Signal Officer Advanced Course) del Ejército de EE.UU. de América. Diplomado en Doctrina Operacional en la Academia de Guerra del Ejército. Egresado del programa Defence in the Wider Security Context Course, Academia de Defensa de Reino Unido. Especialista en Inteligencia y Guerra Electrónica. Profesor del Programa de Magister en Ciberdefensa de la Academia Politécnica del Ejército, Ciberdefensa en la Escuela Militar y en varias Universidades locales. Es autor de más de 16 publicaciones en temas de ciberdefensa y pensamiento estratégico y coautor del Libro "La Ciberguerra, sus Impactos y Desafíos", entre otros libros. Es Miembro titular del Instituto Geopolítico de Chile y fue Investigador Asociado del Centro de Estudios Estratégicos de la Academia de Guerra para temas de Ciberguerra. Email: rleivav@escuelamilitar.cl leivarene@yahoo.com

Introducción

En las operaciones terrestres existen fronteras y límites, mientras que en el ciberespacio no. Eso ha cambiado la dimensión de lo que son las operaciones terrestres, que ya no solo se circunscriben al alcance de sus elementos generadores de fuerza letal, sino que se extienden a brazos técnicos muchas veces inubicables.

La ciberguerra no está en un nivel equivalente a la guerra convencional, pero pese a que puede aparentar ser una amenaza menor, cuenta con una capacidad que en el tiempo ha ido incrementando exponencialmente su potencialidad de agresión asimétrica y desequilibrante. Para el desarrollo de sus acciones puede optarse por cursos de acción que requieren reducidos recursos, de alta latencia, facilidad de encubrimiento, dinamismo en sus recursos y con instancias de generar devastadores efectos.

Con ello, el impacto, connotación, influencia y trascendencia de las acciones que se desarrollan en el ciberespacio como parte de las operaciones terrestres ha ido incrementándose notoriamente.

Al desarrollar los puntos que se visualizaron en el enlace existente entre las operaciones terrestres y el ciberespacio, se buscó generar un análisis relacional con las vinculaciones de vulnerabilidades y oportunidades respecto a la quinta dimensión compone un campo de batalla moderno (que es el ciberespacio), estableciendo vinculaciones con factores de consideración que resultan gravitantes en ello. Para ello se avanzó desde algunas consideraciones propias del ciberespacio, para de ahí determinar vulnerabilidades iluminadas notoriamente por las operaciones CEMA (descritas en el texto), remarcar oportunidades que surgieron muy asociadas a la Inteligencia Artificial, cerrando con algunas reflexiones finales que destacan algunas ideas fuerza.

Ciberespacio

En el combate moderno, para realizar un ciberataque no es necesario desplazarse, moverse o tener que ingresar al área de responsabilidad de una determinada unidad desplegada en un territorio específico. Esta es una de las principales propiedades de las ciberoperaciones. El ciberespacio es un dominio que tiene sus propias características, que permite un actuar asimétrico y de desequilibrio, puede ocultar y proteger su actuar con encubrimiento físico o virtual y puede ser activado en tiempos que le son propios, incluso adelantándose a las escaladas de crisis o de empleo del potencial bélico.

Las acciones que se desarrollan en el ciberespacio buscando afectar operaciones terrestres, no obedecen a una forma de agresión no territorial, pues aun cuando las ciberagresiones se darán en una dimensión virtual (el ciberespacio), sus efectos buscados serán circunscritos a un espacio real específico y concreto del adversario, con efectos definidos que afecten su potencialidad. Es más, el conductor de la operación terrestre buscará coordinar el máximo de medios y sincronizar un alto nivel de impactos que coadyuven a

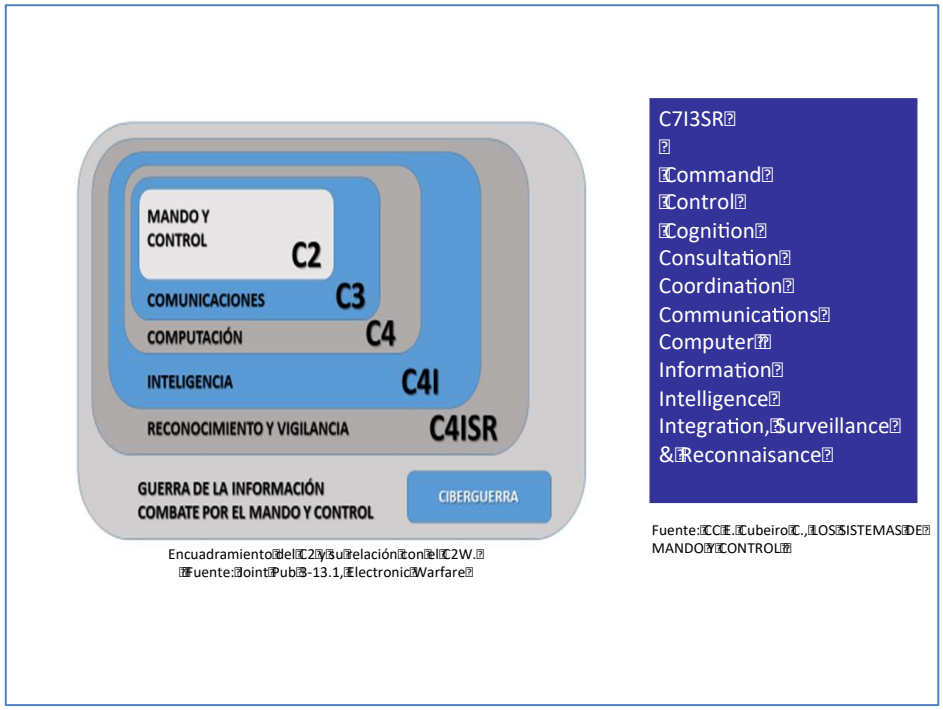
lograr lo diseñado como efecto deseado por el ciberataque. Entonces el ciberespacio existe en lo virtual, con efectos en lo real, conformando un escenario creado y sustentado, con una intangibilidad en su concreción, pero con un claro impacto cuando es afectado. Este es el escenario de la ciberguerra y a esto es lo que apunta particularmente en las operaciones terrestres.

Hoy se enfrentan nuevos riesgos y amenazas, cada vez más sofisticados y dinámicos, que pueden afectar la confiabilidad, transmisión, confidencialidad e integridad de la información a emitir y recibir sobre plataformas de mando y control, basadas en plataformas que usan el ciberespacio y el espectro electromagnético, lo que ha hecho necesario adoptar medidas de protección para enfrentar estos riesgos. Se agrega a lo anterior la preponderancia que el Mando y Control, tanto como función primaria o función de combate, ha ido alcanzando. Por ello, las ciber redes han ido tomando mayor connotación en el tiempo, ya no solo siendo una plataforma de transporte de información, sino que pasando a constituir brazos remotos que comandan, gestionan, monitorean, activan y conectan gran parte de los recursos tecnológicos de que disponemos, constituyendo en sí infraestructuras de combate que por su importancia pasan a ser críticas.

Sin el ánimo de extender este punto y desviar de lo que el título del análisis nos orienta, necesario es al menos solo enunciar que inicialmente conocimos como función Mando y Control o C2, orientada a proporcionar información al comandante y a su estado mayor, permitiendo la conducción de las operaciones militares, con el fin de asegurar el flujo de la información y la integración de todos los sistemas de asociados a la maniobra de cualquiera de las áreas de misión, manteniendo actualizado en tiempo y espacio la situación del ambiente operacional.

Esto ha ido ampliando la extensión de su base de actuar, debiendo considerar lo que se presenta como C7I3SR, contemplando su base de mando o conducción, control, conocimiento, confrontación con fuentes de confirmación (Cognition y Consultation), coordinación, plataforma de telecomunicaciones, computación (desde el punto de vista de automatización de sistemas), información, inteligencia, integración, vigilancia (surveillance) y el reconocimiento (reconnaisance), pudiendo encontrar autores que agregan otros elementos, como las actividades Ciber.

Figura 1
Del C2 al C73ISR



Encuadramiento del C2 y su relación con el C2W.
Fuente: Joint Pub 3-13.1, Electronic Warfare

Fuente: C.C.E. Cubeiro C., LOS SISTEMAS DE MANDO Y CONTROL

Nota. Elaborada por el Autor sobre la base de las fuentes indicadas.

Así, debido a que las ciber redes han ido tomando mayor connotación en las operaciones terrestres, la seguridad de esas redes es tan importante como la seguridad física, debido a la perturbación que se puede alcanzar en la capacidad de conducir las unidades.

En una aproximación a lo que nos señalan Anabalón y Donders respecto a infraestructuras críticas (Anabalón, J. y Donders, E, 2014: p.56), el someter a intrusiones de seguridad a estos sistemas de Mando y Control pueden producir incidentes de conectividad, integridad, reserva, proceso y otros efectos más, con impactos de altísima celeridad, con notorio detrimento en los sistemas físicos que dependen de tales sistemas.

En este efecto en la infraestructura crítica de combate, con relevancia e impacto en el campo de batalla moderno, aparece la ciberguerra, como un elemento nuevo, una potencialidad que modificó un segmento virtual del mando y control, que era interrelacionado antiguamente vía medios más bien análogos, para de ello pasar a ser digitales, enfrentando esta nueva amenaza, con modalidades defensivas y ofensivas, con amplia repercusión de lo que en este ciberespacio se podía lograr, progresando por lo tanto hacia la aparición de una nueva arma a disposición del conductor de la guerra, con aplicación en todos sus niveles y ámbitos de la conducción.

La velocidad de los cambios que permite esta nueva modalidad de enfrentamiento (la ciberguerra) implica que se requiere de poco tiempo para realizar un ataque o para implementar nuevas defensas, caracterizando estas operaciones por su dinamismo, asimetría, velocidad, sorpresa, variabilidad y agilidad, superando en inmediatez si lo comparamos con lo que sucede en el espacio físico, respecto de operaciones convencionales durante conflictos armados tradicionales. Retomaremos este punto cuando más adelante traigamos a notar el impacto de la inteligencia artificial (AI) en el combate moderno.

Vulnerabilidades en las Operaciones Terrestres y Ciberespacio.

En los inicios de la informática, los eventos de vulnerabilidad eran menores o casi inexistentes, precisamente porque los computadores eran cajas autárquicas, con circuitos de información cerrados, sin conexión externa, por lo tanto, aislados de amenazas y distantes de los riesgos. Pero hoy, la cantidad de ciberelementos disponibles en lo militar, desde el nivel táctico al estratégico, es exponencialmente mayor, con nuevos aparatos de presencia masiva en las tropas, cuarteles generales y en particular en los comandantes, elementos de costo alcanzable para fuerzas armadas de estados/naciones, e incluso para organizaciones no estatales con capacidad y voluntad bélica. Esto, en que se agregan no solamente computadores, sino que dispositivos con características informáticas de empleo táctico, como radios móviles con modulación regulada por software, aparatos "inteligentes" como parte de sistemas de mando y control, uso de tablets para representar panoramas operacionales comunes y otros, hacen mucho mayor el número de elementos conectados a algún tipo de red, que no necesariamente es Internet.

Sumemos a ello el impacto que ya está teniendo la aplicación de Actividades Ciber y de Espectro Electromagnético o CEMA [2], lo que agrega un universo enorme de dispositivos enlazados dentro del campo de batalla que pueden ser afectados por intrusiones en lo propio del ciberespacio y/o usando el espectro electromagnético que emplean para su enlace. La masificación de instrumentos desplegados en el combate moderno con capacidad computacional o de automatización ha aumentado el universo existente, por ende, se ha incrementado el número de dispositivos que pueden ser víctimas o victimarios.

Su aplicación en el campo de batalla moderno tiende a dos ejes bases, que son el asociado al proceso de manipulación del enemigo y sus capacidades para tomar decisiones, y por otra parte a la generación de una propia capacidad para obtención de inteligencia.

Para influir en las capacidades para tomar decisiones, la ciberguerra no puede actuar como compartimiento estanco y debe ser coordinada en sus medios y sincronizada en sus efectos, momento de aplicación y objetivos buscado, en lo que es denominado combate por el C2 (combate por el Mando y Control o C2W[3]), por lo tanto, se deberá tender al empleo de

[2] CEMA: Sigla en inglés proveniente de *Cyber Electromagnetic Activities,* actividades ciber electromagnéticas.
[3] C2W: Sigla en inglés proveniente de *Command and Control Warfare.*

estos elementos para así lograr un efecto de sinergia que catalizará, potenciará, magnificará y asegurará el resultado.

Así entonces, la ciberguerra es un término que en lo militar obedece a una parte de la guerra de la información, cuya operacionalización responde al combate por el mando y control (C2W), bajo el englobamiento de la guerra de la información o Infoguerra. Luego, su ejecución deberá ser enmarcada en una planificación que coordine adecuadamente la ejecución de operaciones psicológicas, operaciones de diversión (o demostración), operaciones de contrainteligencia, destrucción física y guerra electrónica (DOD, 2000).

Las plataformas de conformación CEMA, son actividades ciber electromagnéticas que implican el uso, explotación, aprovechamiento y retención de ventajas sobre el adversario, tanto en el ciberespacio como en el espectro electromagnético. Simultáneamente a lo anterior, buscan negar y degradar su ciberuso, protegiendo el sistema de C2 dispuesto para la misión. CEMA engloba operaciones en el ciberespacio (CO[4]), guerra electrónica (EW[5]) y operaciones de gestión del espectro (SMO[6]). Entonces las plataformas de configuración CEMA basan su eficiencia en su capacidad defensiva como red, ofensiva para con el espectro y el ciberespacio del adversario, como también tendrán a la vista la resiliencia como concepto de diseño, ya que saben que serán atacadas, que su defensa no podrá ser universal y perfecta, pero pese a ello podrán seguir operando, sino total al menos parcialmente, en una gama que permita seguir apoyando la capacidad de mando y control.

La potencialidad de ciberguerra, en sus componentes defensivos, ofensivos y exploratorios debe ser desarrollada, mantenida y sostenida con antelación, porque de no hacerlo se estará en riesgo real y concreto de ser víctima del desequilibrio esta capacidad busque, especialmente con su característica asimétrica. Esta factibilidad de accionar no puede ser improvisada, sino por el contrario contenida en previsiones de planificación, equipamiento, capacitación e integración, para así concurrir a los efectos deseados en apoyo a las operaciones terrestres.

Dada la aparición de nuevas, dinámicas y más corrosivas ciberamenazas, que se caracterizan por su sofisticación, precisión y grado de impacto, el nivel de riesgo ha aumentado y evolucionado. Esto trae como efecto una fragilidad de la infraestructura digital de combate, donde el escenario de campo de batalla hoy es muy dependiente de la plataforma tecnológica como parte del diseño de mando y control. Entonces se hace necesario potenciar la amalgama en que operan sincronizadamente la ciberguerra y la guerra electrónica.

Esta forma de combatir implica diversas tecnologías, medios de mando y control, de obtención, proceso y difusión de inteligencia, de comunicaciones, de armas inteligentes, etc., donde hay que considerar en la posibilidad (Enemy Course of Action - ECOA) el

[4] CO: Sigla en inglés asociada a *Cyberspace Operations,* Operaciones de Ciberespacio.
[5] EW: Sigla en inglés correspondiente a *Electronic Warfare,* Guerra Electrónica.
[6] SMO: Sigla en inglés para *Spectrum Management Operations*, Operaciones de Gestión del Espectro.

cegamiento electrónico, la perturbación (jamming), la decepción, la intrusión en los sistemas de información y comunicaciones, entre otros, llegando hoy a afectar hasta el "Internet de las cosas" de niveles tácticos y hasta domésticos.

La ciberguerra adquiere su importancia al concretar una extensión de la forma tradicional de obtener información en tiempo de guerra, es decir mediante un nivel superior de mando, control, comunicaciones e inteligencia, junto a buscar identificar, localizar, sorprender y engañar al enemigo antes de que él haga lo mismo contra nosotros (Arquilla, 1997). Esto es la base de lo buscado por el combate por el Mando y Control en las operaciones terrestres y otras.

La aplicación de la ciberguerra en las operaciones terrestres, más que estar orientada al envío de mensajes electrónicos o "e-mails" vía internet o afectar bases de datos de información o transferencia, lo que es más propio de los denominados "hackers", busca una connotación superior al identificar sus objetivos en la neutralización o bloqueo de infraestructura crítica de combate. Es una combinación de los conceptos de guerra y ciberespacio, que designa al conflicto militar en función de los medios de la tecnología de la información que utiliza en pro de la consecución de sus fines, destacándose que la velocidad de los cambios que permite el ciberespacio, implica que se requiere de poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con lo que sucede en el espacio físico, respecto de operaciones convencionales durante conflictos armados tradicionales.

En el dinamismo propio de las ciberagresiones, la forma de ejecución típica de un ciberataque ha ido mutando para desplazarse de acciones en esta quinta dimensión (el ciberespacio) al empleo del medio del espectro electromagnético. Con ello, el actuar centrado en intrusiones que aprovechan las vulnerabilidades de los sistemas informáticos, particularmente de las redes críticas ha evolucionado hacia buscar el uso malicioso de uno de los componentes del mando y control que es la plataforma tecnológica, en particular la de emisión y transmisión inalámbrica o radial, lo que resulta crítico para operaciones terrestres.

Oportunidades en las Operaciones Terrestres y Ciberespacio

Para visualizar las oportunidades que se nos presentan en lo que entendemos como amalgama de Operaciones Terrestres y Ciberespacio, se hace necesario aproximar desde la línea de lo que implica CEMA, como nueva forma de combatir, tendencia que emplea herramientas con diversas tecnologías, medios de mando y control, de obtención, proceso y difusión de inteligencia, de comunicaciones, de armas inteligentes, etc. Pero para el logro de efectos requiere una cercana coordinación con la maniobra, en todas sus otras dimensiones, más aún en escenarios de gran incertidumbre, para así asegurar los efectos deseados. Puede aportar en el cegamiento electrónico, la perturbación (jamming), decepción, la intrusión en los sistemas de información y comunicaciones adversarios, entre otros, abriendo nuevos segmentos de blancos a considerar en la planificación, como objetivos propios de las operaciones de configuración.

Aquellos subsistemas o componentes con baja capacidad de respuesta, detección o alarma a las intrusiones de CEMA, representarán objetivos de alto valor (HVT) para su empleo en operaciones terrestres. Así entonces, los objetivos caracterizados por un alto nivel de falsas alarmas requerirán previamente acciones que hagan perder la confianza de los operadores adversarios, para así retardar o anular sus reacciones. Normalmente este tipo de objetivos se emplearán como elementos secundarios que permitan amarrar la atención de quienes monitorean los sistemas, restando atención a la verdadera intrusión. Así dado el entorno, la importancia del objetivo será directamente proporcional al acceso que permita receptáculos de data de gran valor de uso y calidad, tanto para obtenerlos como para impedir que ela fuerza opositora tenga disponibilidad, integridad o logre proteger su confidencialidad. A su vez, la calidad de esa información se relacionará a la oportunidad y pertinencia para su empleo.

Detectado un objetivo, se presentan variadas oportunidades de batirlo, afectarlo, neutralizarlo, bloquearlo o degradarlo (DOD, 2012). Una de ellas es afectando la protección a la información y los sistemas informáticos, sus previsiones para el respaldo, restauración, detección y capacidad de reacción (Seguridad informática). Otra opción es dirigiendo recursos para degradar el Entorno Informático del Adversario, buscando saturar, perturbar, degradar o interrumpir la interacción de individuos, organizaciones, aparatos o sistemas de búsqueda, proceso o difusión de información.

También se podrían considerar Cursos de Acción (COA) que busquen Superioridad Informática, ya sea por medio de la negación de la capacidad del adversario de obtener, procesar y difundir información mediante un flujo ininterrumpido o de afectar su Sistema Informático, buscando incidir en la eficacia de su infraestructura, organización, personal y componentes para degradar o neutralizar su capacidad de obtención, proceso, archivo, transmisión, proyección, difusión y acción.

Teniendo claridad en todas las formas anteriores de actuar, se presenta la oportunidad de poder actuar con antelación y proactividad en pos de la seguridad, que otorgará libertad de acción. Para lo anterior, se debe tender a tomar previsiones para evitar brechas de oportunidad que den espacios a ciberataques. El targeting inverso obedece a un buen método para identificar los espacios en que el propio sistema pueda presentar vulnerabilidades y limitaciones, tomando medidas para poder bloquear oportunidades de ataque. Para ello se monitorea la estructura propia con una mirada de ubicación de falencias de todo orden (físicas, virtuales, de protocolo, de personal, de estructura y otras). Al encontrar una se logrará localizar las condicionantes que dan paso a ello, para así definir o traquear la línea de daño, de origen a fin, que esto puede provocar. Finalmente se diseñan y articulan medidas remediales, de bloqueo y de acción en caso de que se genere dinamismo en la falencia detectada. El hacking ético es una herramienta para ello, pero no constituye el método en sí, sino solo uno de los medios para ello.

De ello surgirán acciones que no son tan complejas de ejecutar como, entre otras, la separación de la información por grado de sensibilidad, aplicando distintas formas de protección, acceso y respaldo para con ellas, dependiendo del grado de daño que pueda generar su pérdida de confidencialidad, integridad o disponibilidad.

El concepto de resiliencia de las ciber estructuras de apoyo a la operación terrestre debe estar presente permanente. Resiliencia es definida por Holling (Calvente, 2007) como "la magnitud de perturbaciones que pueden ser absorbidas por el sistema antes que sea reorganizado con diferentes variables y procesos". Entonces, el concepto de la resiliencia está directamente asociado con la sustentabilidad de todo sistema complejo de batalla.

La resiliencia no es una propiedad absoluta y fija, sino que, por el contrario, es variable en el tiempo y el espacio, dependiendo en gran medida, de las acciones y relaciones del sistema y la volatilidad ambiental del contexto en el que se encuentre. Al hablar de un sistema robusto, ello debe ser entendido como la magnitud de volatilidad que puede ser compensada por el sistema complejo de batalla antes de llegar al colapso de sus características, procesos y funciones principales. Para ello, el diseño debería contemplar dentro del sistema un arquetipo de detección, otro de protección, uno compensatorio, y por último uno de desafío o contra-agresión (eventual). Cada uno juega un rol en el proceso y no necesariamente son secuenciales en su actuar, sino que pueden operar en forma simultánea, cooperativa y coordinada. Así el modelo de detección estará monitoreando constantemente la red de combate, para una vez detectada una amenaza real o potencial, activar las alertas y/o alarmas. En este punto inicia su labor el modelo de protección de la disponibilidad de recursos de Mando y Control, con las contramedidas que estén asociados al tipo de evento malicioso captado, las que pueden contener acciones automatizadas como también otras que el controlador aplique a criterio, dando así dinamismo a la respuesta. En este punto, el diseño de respuestas basadas en Inteligencia Artificial aportará a ese dinamismo.

El modelo compensatorio operará sobre la base de los recursos de redundancia y robustez del sistema, logrando con ello un grado abordable de resiliencia. Por ello, la aplicación de Inteligencia Artificial levanta una nueva oportunidad, sustentada en una capacidad de detección y respuesta, con una celeridad tal, dinamismo en las contramedidas y acción temporal y cambiante, que privará al oponente de lograr permanencia en el efecto que pueda pretender lograr, el que pasará a ser muy acotado o idealmente casi imperceptible. A lo anterior podría sumarse una capacidad exploratoria (control de daños) y otra ciberforense, que van en busca de la fuente de la agresión y aplican medidas de bloqueo, neutralización o mitigación de la acción hostil.

Se sostiene con esto que, avanzar hacia la protección total del sistema de Mando y Control en una operación terrestre es utópico, pero sí se pueden focalizar los esfuerzos de la plataforma tecnológica, de los protocolos, de los programas de respuesta y de los grados de resolución autorizado y jerarquizado, para así proteger los segmentos de ciberinfraetructura crítica.

En esas respuestas, se presenta para la aplicación de la Inteligencia Artificial en combate de una articulación nueva, distinta, innovadora porque deberán evaluarse las reglas de conducta, reglas de enfrentamiento, particularmente en su proporcionalidad, necesidad e inminencia, que será iluminada por el efecto que determinadas acciones cibernéticas puedan alcanzar y lo dinámico que la ciberguerra comporta, todo ello en el actuar del combate por el mando y control en las operaciones terrestres.

Reflexiones finales

En esta ciberguerra, se busca irrumpir o destruir, a lo menos, los sistemas de mando, comunicación e información del adversario, junto a tratar de obtener el máximo de información del enemigo, mientras se le niega el acceso a la propia. Implica tornar la ecuación de información y capacidad de su gestión a favor propio, para así emplear el conocimiento útil obtenido en beneficio de la economía de la fuerza y la reunión de los medios.

Los riesgos relacionados a la Seguridad de la Información que comprometen la integridad, la confidencialidad y la disponibilidad de esta, mantendrán una fuerte relación no solo al fortalecimiento de soluciones en tecnología y en procesos, sino también y, cada vez en mayor medida, al factor humano en cuanto al nivel de educación en la materia. Entonces, aún cuando hay cada día más procesos automatizados, de inteligencia artificial o de Machine *learning*, es el individuo quien inclina la diferencia, por lo que su conocimiento y capacidad integra el balance de factor de potencia.

Las operaciones terrestres enfrentan hoy un desarrollo de un amplio espectro de métodos y uso de ciberataques, con lo que hay dinamismo de la amenaza, debe ser considerada en la planificación, en la definición de capacidades militares, en el desarrollo de plataformas tecnológicas, en las formas de respuesta y comprendida por los comandantes de todos los niveles como una realidad a enfrentar.

Referencias

Arquilla, John, *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict, Cyber War is Coming, Comparative Strategy,* Vol12, RAND´s home page, p. 141-165, 1997.

Ciberdefensa-Ciberseguridad, Riesgos y Amenazas, CARI, Noviembre 2013 FM 3-38 "*Cyber Electromagnetic Activities*", Edición 2014.

Departamento de Defensa de Estados Unidos, DOD Directive S-3600.1, *"Information Operations (IO)",* Ed. Mayo 2012, pag. 12.

JP 3-12 (R) "*Cyberspace Operations*", Edición 2013.

TRADOC 525-7-8 "*The United States Army´s Cyberspace Operations Concept Capability Plan 2016 – 2028*", Edición 2010.