Capítulo 4

Evolución tecnológica y ciberseguridad

*René Leiva Villagra**

Introducción

La ciberseguridad es un factor que ha tomado preponderancia en varios ámbitos de la vida actual. La conformación del ciberespacio, ya consolidado como el quinto dominio, ha traído consigo la necesidad de asegurarlo, ya que constituye una plataforma en que se desarrollan tareas fundamentales de transferencia de información en tiempo real, mando y control, automatización, visualización, entre muchas otras más. Claramente este nuevo ambiente virtual tiene repercusiones en lo real y concreto y pese a no ser un escenario tangible, sí tiene connotaciones que le dan presencia y existencia, todo ello generado por el enlace de múltiples puntos, bases de datos, redes y sistemas que sobre un empleo masivo de tecnología han permitido la aparición de este nuevo plató de conectividad como es el ciberespacio.

La discusión de la envergadura del impacto de lo cibertecnológico en la estrategia está presente en el pensamiento estratégico contemporáneo y es parte del aporte que en este texto se pretende entregar. Con esto se busca

* General de Brigada (R) del Ejército de Chile. Oficial de Estado Mayor, Licenciado en Ciencias Militares y Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica en la Academia de Guerra del Ejército de Chile. Diplomado de la Pontificia Universidad Católica de Chile en Gestión en Educación. Especialista en Inteligencia y Guerra Electrónica. Graduado del SOAC Fort Gordon del Ejército de Estados Unidos y del ADF POTC de las Fuerzas de Defensa de Australia. Es investigador del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. Es coautor del libro *La Ciberguerra: Sus impactos y desafíos*. En el ámbito privado se desempeña como consultor en ciberdefensa y cibertecnología para empresas nacionales y extranjeras. rene.leiva@acague.cl

enunciar las influencias en la evolución tecnológica generadas por el impacto de la ciberseguridad, teniendo con ello una visión desde la perspectiva multidimensional. Coherente con lo anterior, en primer lugar se describirá el ambiente multidimensional, considerando sus orígenes y alcances en las tendencias estratégicas globales. Luego se identificarán los íconos de evolución tecnológica, asociándolo a elementos de lo multidimensional. Seguidamente se examinará y describirá la ciberseguridad como elemento propio de la evolución tecnológica. Finalmente se enunciarán factores de comportamiento de lo tecnológico en relación con lo multidimensional, asociado a los impactos de la ciberseguridad, cerrando todo lo anterior con algunas reflexiones.

Con esto avanzaremos a levantar elementos presentes que ya están generando transformaciones globales, porque la estrategia es ciencia y arte, es dinámica, evolutiva y en desarrollo. Es tal la envergadura de este impacto y su rango de acción, que lleva a influenciar en otras áreas. Con ello se avanza en dar respuestas tecnológicas, y a la vez, como producto de avances en la ciencia, determinados elementos bélicos vienen a irradiar efectos en el actuar de la estrategia que la hacen replantear algunas de sus ideas, pero manteniendo siempre su esencia en alto, que no es más que un duelo majestuoso y a veces terrorífico de voluntades.

Hacia lo multidimensional

Coincidiremos en que la guerra y el empleo de estrategias han estado presentes en los grandes conflictos de la historia como Esparta y Atenas, Cartago y Roma, enfrentamiento de la dinastía Ming con la dinastía Qing (Manchú), invasión mongola, guerras napoleónicas, Primera Guerra Mundial o Gran Guerra, Segunda Guerra Mundial o de Aliados y el Eje, así como tantos otros. En cada uno de ellos, determinados artilugios militares han ido marcando la diferencia, donde normalmente un arma innovadora trajo efectos asociados que redundaron en la conformación de la maniobra.

Arquímides desarrolló tecnologías de defensa basadas en el diseño de nuevos modelos de fortificaciones que las hicieron muy eficientes para enfrentar estrategias de asedio. Da Vinci diseñó morteros y catapultas gigantes orientadas precisamente a derribar muros, difuminando la fortaleza de los castillos y llevando la batalla a estrategias de escenarios abiertos. También así fue el caso de la *mitrailleuse*, la ametralladora adoptada por el ejército francés en 1869, en vísperas de la guerra contra Prusia. Al comenzar la guerra, los artilleros franceses la emplearon como una pieza más, situada a retaguardia de las líneas de la infantería propia, fuera del alcance de sus blancos y vulnerable

al fuego de contrabatería enemigo, pero cuando de verdad pudo demostrar su valía como arma de primera línea, "fue en la batalla de Gravelotte (18 de agosto de 1870) contra una penetración de la infantería prusiana causándole más de 20 mil bajas, sentando así las bases del carácter decisivo que tendría en los años posteriores" (Luttwak, 2005: p. 151), sepultando las estrategias que contemplaban formaciones de orden cerrado para abrir paso a las de orden abierto, el empleo de trincheras y las concepciones de desgaste por fuego y tiempo.

Al seguir en la línea histórica en que tenemos presencia de la guerra de desgaste, verificamos que ella se emprende con métodos industriales. En esa visión, el adversario es considerado como un despliegue amplio de objetivos, donde la victoria es lograda por efecto acumulativo de acciones de fuego y disposición de amplias utilizaciones de personal y materia, en un afán de lograr superioridad y alcanzar una fortaleza que permita resistir los embates de desgaste que causa el enemigo. Al otro lado del espectro se encuentra la *relation-maneuver* (maniobra proporcionada o maniobra correlativa), una acción apuntada a las especificidades del objetivo, a desequilibrar su centro de gravedad, y que en lugar de pretender su destrucción trata de incapacitarlo por medio de la disrupción sistémica, en una analogía a lo que podría ser una llave de judo.

Otro caso atendible de destacar, fue la aparición del medio aéreo, el que abrió otro escenario a la estrategia dotándola de una nueva dimensión. El avance tecnológico extendió a un nuevo campo lo que ya se conocía como estrategia clásica en sus vertientes terrestre y naval, para con ello iluminar su proyección hacia un ámbito inexplorado que era el cielo, sin ataduras de obstáculos, alambradas, cotas o depresiones, con amplia velocidad, flexibilidad y capacidad de acción en profundidad. Más que un medio de fuego (que en sí no genera maniobra), su movilidad, oportunidad, inmediatez y efectos escalables la llevaron a conformar una raigambre nueva y distinta de estrategia, la aérea.

Del elemento aéreo, los ojos de la humanidad y la estrategia se orientaron a un componente hasta ahora ausente en el empleo, pero presente en la visión: lo aeroespacial. La imaginación de Verne y las teorías de Tsiolkovski se hacían presente y llevaban a concreción esfuerzos que lanzaban a la cohetería como artilugio diseñado para la extensión del poder artillero, a un empleo que excedía lo terrestre y se empinaba a tratar de alcanzar un minúsculo istmo de control espacial, armando con ello a la Guerra Fría de un instrumento de demostración de poder, que más que enfrentar fuerzas lo haría sobre la base de una carrera espacial, con preseas marcadas por íconos de logro tecnológico. La base tecnológica de los cohetes alemanes, conocidas como las bombas volantes V2, sustentaría posteriormente el diseño de cohetes lanzadores que

pondrían en el espacio objetos orbitales experimentales, que con el pasar del tiempo pasarían a ser complejos satélites de observación y comunicaciones.

En este avance de la tecnología fuimos conociendo de satélites orbitales y estacionarios, primeras personas en ser lanzados al espacio y regresar, el logro del primer hombre en la Luna, entre otras gestas, tejiendo con ello una enmarañada estructura de sensores y visores satelitales, para pasar de cohetes balísticos de largo alcance a misiles intercontinentales de alta precisión, con capacidad convencional, química o nuclear, todo lo que daba una nueva dimensión al escenario estratégico, en el ámbito de lo aeroespacial.

Habida consideración de lo anterior y recapitulando, partiendo por la Guerra clásica, esta se desarrollaba inicialmente en dos dimensiones: un escenario terrestre y uno marítimo. En el avance del tiempo, el uso del avión, como ingenio de combate, lo proyectó a un vector aéreo y más adelante pasó a incorporar lo espacial, quedando este cuarto escenario integrado a la confrontación de voluntades.

Así dados los pasos hacia la modernidad, apareció el ciberespacio como el *Quinto Dominio*, junto con lo terrestre, marítimo, aéreo y lo aeroespacial, dando cabida a varios conceptos, como ciberguerra, ciberdefensa, ciberseguridad y otros, que siguieron los lineamientos de ser una herramienta más en una estrategia de acción. La guerra no se extendió a un nuevo medio físico, sino que a uno virtual, pero con amplias repercusiones en los otros dominios tangibles. Luego entonces estábamos ante un ciberespacio que se materializaba en un elemento de poder dentro la gran estrategia, y es por medio de este dominio nuevo y artificial que se presentaba un factor de repercusión. Acá había presencia de un ícono estratégico, en un escenario virtual donde todos los actores, hasta los más desprovistos de envergadura de poder, estaban en condiciones de alcanzar la clasificación de amenaza, generando nuevos agentes de desbalance y asimetría. La potencialidad de ello iba de la mano con la tecnología.

Surgió entonces la pregunta: ¿Ha cambiado la estrategia o la estrategia ha forzado la tecnología al cambio? La interrogante tenía el desafío de implicar una suerte de *loop* como la del huevo o la gallina. ¿Qué había sido primero?

Lo propio era aplicable al ciberespacio, donde la conformación de grandes bases de datos desconectadas unas de otras, contenidas en computadores aislados de su entorno, acumulaban enormes cantidades de datos que no podían salir de ellos. Lo anterior pasó a constituir un problema tecnológico, creándose para ello una red global que permitiese la transferencia de inmensos volúmenes de datos: la conectividad evolucionó desde ARPANET y el protocolo TCP/IP (1983) hasta lo que conocemos hoy como INTERNET, con soluciones diseñadas como dispositivos de arquitecturas abiertas y con amplia conectividad a sistemas locales, regionales e incluso internacionales,

de transferencia de información de gran velocidad y compleja identificación de su punto de origen. Esta mutación desde ordenadores aislados a constelaciones interconectadas de bases de datos, computadores, servidores, redes y macrorredes los hizo escalar a configuraciones de las que los suprasistemas pasaron a ser absolutamente dependientes, con una suerte de relación adictiva con los anchos de banda y las capacidades de almacenamiento de memoria, lo que a su vez trajo consigo una disminución en los niveles de ciberseguridad.

Prueba de lo anterior es la forma cómo ha aumentado considerablemente la dependencia de las plataformas digitales, por lo que su disponibilidad y accesibilidad se vuelven recursos críticos. 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 respecto de plataformas de ciberespacio y espectro electromagnético en general, lo que ha hecho necesario adoptar medidas de protección para enfrentar estos riesgos. Por ello, las ciberredes 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 que por su importancia pasan a ser críticas. Si eso lo proyectamos al impacto que traerá 5G, la influencia de lo cibernético será aún mayor, particularmente en la automatización de procesos, unos más sensibles y vulnerables que otros.

Al detenernos en lo que son las ciberinfraestructuras críticas, por definición, son conjuntos físicos y sistemas basados en redes computacionales complejas que forman parte importante en una sociedad moderna y su funcionamiento fiable y seguro es de suma importancia para la vida económica y la seguridad nacional (Chen_Ching, 2010: pp. 853-865). El someter a intrusiones de seguridad a estos complejos "puede producir incidentes de conectividad, integridad, reserva, proceso, entre otros, con impactos que pueden escalar de lo local a lo nacional con altísima celeridad, para de ello remontar a interferencias en lo regional/internacional, con impacto en los sistemas físicos que dependen de tales sistemas" (Anabalón y Donders, 2014: p. 56) y efectos en la vida de los ciudadanos. Así, la seguridad en redes es tan importante como la seguridad física debido a la perturbación que se puede alcanzar al manipular maliciosamente, por ejemplo, los sistemas remotos (SCADA o PLC- Programmable Logic Controller) de una planta eléctrica, de agua, gas, petróleo, cobre u otro tipo, lo que los hace situarse en infraestructura crítica con relevancia estratégica. Por ello, en ciberseguridad, una vulnerabilidad implica que existen puntos débiles en la infraestructura tecnológica, políticas o de procedimientos, por lo que un atacante puede utilizar

un conjunto de aplicaciones o métodos para romper la seguridad y explotar los puntos débiles en las redes y comprometer los sistemas.

En esta presencia de infraestructura crítica con relevancia estratégica aparece la ciberguerra como un elemento nuevo, una potencialidad que modificó un segmento virtual del planeta que era interrelacionado sin mayores regulaciones, pero que con esta nueva amenaza comienza a adoptar medidas de índole defensivo y ofensivo, dimensión que prontamente fue identificada como un área de interés estratégico, con amplia repercusión de lo que en este ciberespacio se podía lograr, 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.

Establecida la fundamentación del impacto de la quinta dimensión, o ciberespacio, en la estrategia moderna, volvamos a la naturaleza de lo clásico como enfrentamiento, donde mientras el desgaste es un proceso de naturaleza casi física que garantiza resultados proporcionales a la calidad y volumen del esfuerzo asignado, "el efecto de la maniobra correlativa depende de la precisión con que se identifiquen las debilidades del enemigo, la sorpresa que se obtenga, y la velocidad y exactitud de la acción" (Romero, 2018: p. 151). Por ello, ya avanzados desde la guerra de desgaste a la de maniobra proporcionada/correlativa, la línea de pensamiento de Estados Unidos se enfrentó a múltiples capas del desafío estratégico, donde se producía una especie de enganche o estancamiento, sin avances en lograr niveles de superioridad. Se requería innovación para la solución del problema estratégico, rompiendo así el amarre, en que una potencia, que es fuerte en capacidades tradicionales, podía ser retada y amenazada por otra que, en lugar de buscar colisionar usando las clásicas acciones o vectores, lograba el desequilibrio mediante acciones en diversos dominios, con un desbalance estratégico.

EE.UU. reconocía con ello que en la actualidad no le era posible obtener una libertad de acción como lo hizo en la Operación Tormenta del Desierto, ya que "sus potenciales adversarios habían desarrollado capacidades A2/AD[1] que le impedían obtener superioridad en los dominios aéreo, marítimo, espacial y ciberespacio" (León, 2017: p. 47). Las opciones para lograr ese desmoronamiento de capacidad superior se proyectaban al uso desde el ciberespacio y satélites a lo terrenal de balas y bayonetas.

Para entender la evolución del concepto MDO[2], debemos remontarnos a la Doctrina de la Batalla Aeroterrestre en su versión 2.0. Es esta doctrina la que es cuestionada en cierta forma por el libro *Average Is Over: Powering*

1 Corresponde a capacidades antiacceso/denegación de zona (A2 / AD) diseñada para interrumpir la proyección de poder de un adversario determinado.

2 En inglés se denominan *Multi-Domain Operations* y se abrevian MDO.

America Beyond the Age of the Great Stagnation (Cowen, 2013), poniendo en la mesa para su análisis y solución ciertos interrogantes que abrió la discusión para ir dando así paso a sucesivos documentos, como "Capstone Concept for Joint Operations" (CCJO, 2012), "Army Operating Concept" (AOC, 2014), "US Marine Corps Operating Concept" (MOC, 2016) y posteriormente el "Concept Version 1.0 for Multi-Domain Battle", junto con muchas otras publicaciones relacionadas. La complementación que cada uno de estos documentos aportó es largo y amplio de recorrer, pero se pueden sintetizar en dos grandes conceptos: *Convergencia* e *Integración de Fuerzas*. Así entonces, desde la visión de Cowen a la fecha, y después de este amplio y profundo análisis a la epidermis estratégica del concepto *Multidominio de la Batalla*, se pudo identificar tanto la convergencia y la integración como variables críticas para el éxito militar en la guerra moderna. La categorización de esta nueva forma de hacer guerra del siglo XXI pasa por ser una "Guerra basada en la información", con un actuar en combinación de cibernética, guerra electrónica, operaciones de información, engaño y negación, buscando interrumpir la capacidad de mando y control (C2) y, por tanto, con ello lograr en el enemigo una ventaja en el ciclo de decisión.

Bueno es concurrir hacia el General Perkins del Ejército de Estados Unidos para considerar que "las operaciones multidominio engloban el concepto que el éxito militar depende de las capacidades en el aire, ciberespacio, tierra, mar y espacio y en el espectro electromagnético. Es un concepto que ayudará a las unidades a evitar una posición de desventaja relativa contra un adversario igual o casi igual en zonas geográficas críticas en cualquier parte del mundo" (Perkins, 2017: p. 32), lo que estimamos debe ser complementada para entender que ello es diseñado para grandes potencias que se desafían unas a otras, pero reconociendo que hay elementos en este juego de poderes que pueden ser extraídos y llevados a la praxis de la estrategia actual en países de estructura y tamaño menor.

El surgimiento de la ciberseguridad desde la evolución tecnológica

La naturaleza de lo que hoy es entendido como "ciberseguridad" es particularmente desafiante de analizar desde el punto de vista de los cambios y la evolución tecnológica con impactos en lo estratégico. Esta nueva disciplina ha traído consigo un cambio de visión, conformación de fuerzas y forma de ejecución. Ante la identificación de un nuevo campo, como es la quinta dimensión o ciberespacio, se ha instado a la incorporación a ella de nuevas formas de empleo para el logro de desbalances, quebrando con ello lo que en su momento era el establecimiento de una suficiencia estratégica.

El empleo del espectro electromagnético en fonía y telegrafía, como parte de las comunicaciones clásicas, dio puerta a la manipulación de sus emisiones, en atisbos de una naciente guerra electrónica, con connotaciones ofensivas, como lo fue en la batalla de Tsushima (27 y 28 de mayo de 1905), en la que un operador telegráfico ruso detectó la emisión de señales de radio por parte de la escuadra japonesa y procedió a generar contramedidas de comunicaciones, perturbando el intercambio de mensajes mediante la emisión de portadoras de radiofrecuencia (CW), impidiendo así la efectividad de los fuegos de artillería naval que amenazaban los buques rusos fondeados en la rada de Puerto Arturo. Con ello iniciaba la primera acción documentada como operación de guerra electrónica (EWO).

Después de ello existieron muchos sucesos en que el uso del espectro electromagnético con fines bélicos fue marcando hitos de una guerra electrónica que crecía con el desarrollo de la Guerra Fría. La capacidad de las operaciones de guerra electrónica de generar enfrentamientos no físicos entregaba una opción estratégica que era muy consecuente con los propósitos de este período histórico, caracterizado por un entorno bipolar con un enfrentamiento entre Occidente y la denominada órbita soviética, escalada en tecnología militar, uso de conflictos del llamado Tercer Mundo –o guerras subsidiarias– para prueba de armamento convencional y soporte logístico y de asesoría militar, escalada en la potencialidad nuclear, junto con una carrera espacial, todos ellos conformando ámbitos donde se competía por demostrar poder estratégico. En ello, la guerra electrónica era un valle propicio para desarrollar acciones de hostigamiento estratégico, buscando desde la perturbación a la decodificación, pasando incluso por la decepción imitativa y otras.

Así avanzado el enfrentamiento estratégico, este tuvo otro ámbito de actuación con la ya descrita aparición del ciberespacio, como dominio nuevo y artificial, con presencia virtual global y gravitante factor de repercusión. En este avance de aportes y desarrollo tecnológico vino a desplegarse esta nueva arista de acción, la quinta dimensión. En este nuevo ambiente se conformaron acciones de ciberguerra, destacándose que la velocidad de los cambios que permite esta nueva modalidad de enfrentamiento 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. Si lo comparamos con lo que sucede en el espacio físico supera en inmediatez a las operaciones convencionales durante conflictos armados tradicionales. Con ello se quebraba la tendencia de escalar en potencialidades de fuerza, buscando desequilibrios de poder basados en la focalización de los efectos, en la sincronización de la oportunidad de ellos, engrandeciendo el valor y mérito de la identificación del centro de gravedad,

condiciones que pueden ser muy bien logradas cuando se diseñan para ser aplicadas en el ciberespacio.

Consecuentemente, la ciberguerra, dada su celeridad, agudeza de acción sobre infraestructura crítica, oportunidad en su actuar e inmediatez en sus efectos, pasó a ser vista como una opción mayor para avanzar en derrotar múltiples capas donde no existe avance en la potencialidad de lograr desbalances y donde haya estancamiento del duelo de voluntades, tanto en la escalada como en el conflicto propiamente tal. Esta ciberconcepción fue asociada a la nueva realidad estratégica en que una potencia, que es fuerte en capacidades tradicionales, se ve desafiada y amenazada por otra que, en lugar de buscar colisionar usando las clásicas acciones o vectores, busca el desequilibrio mediante acciones en diversos dominios, donde el uso del ciberespacio es altamente rentable y eficiente. Si ello lo confrontamos con el concepto de *defensa*[3], se debe disponer de todo el conjunto de medios materiales, humanos y morales que permitan oponerse a las amenazas de un adversario. Luego, la orientación de empleo de medios para la conformación de una capacidad de ciberdefensa debe ir necesariamente asociado a lo que el concepto de defensa nacional impone, es decir la consecución de un grado de libertad de acción en el uso del ciberespacio, como también una capacidad de oposición a la ciberamenaza.

De lo netamente ciber, a tener en alta consideración por las plataformas de conformación CEMA[4], que son actividades ciberelectromagnéticas que implican el uso, explotación, aprovechamiento y retención de ventajas en el adversario, tanto en el ciberespacio como en el espectro electromagnético, mientras que simultáneamente buscan negar y degradar su uso, protegiendo el sistema de C2 dispuesto para la misión. CEMA engloba operaciones en el ciberespacio (CO[5]), guerra electrónica (EW[6]) y operaciones de gestión del espectro (SMO[7]). Entonces las plataformas de configuración CEMA basan su eficiencia en su capacidad defensiva como red, ofensiva para con el espectro y el ciberespacio, 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 (efecto del MDO), pero pese a ello podrán

3 Sintetizado el concepto de *defensa* es la acción y efecto de conservar la posesión de un bien o de mantener un grado suficiente de libertad de acción para alcanzarlo.

4 CEMA: Sigla en inglés proveniente de *Cyber Electromagnetic Activities*, actividades ciberelectromagnéticas.

5 CO: Sigla en inglés asociada a *cyberspace operations*, Operaciones de Ciberespacio.

6 EW: Sigla en inglés correspondiente a *electronic warfare*, Guerra Electrónica.

7 SMO: Sigla en inglés para *spectrum management operations*, Operaciones de Gestión del Espectro.

seguir operando, sino total al menos parcialmente, en una gama que permita seguir apoyando al mando y control.

En esta síntesis de avances de modernidad, no solamente se debe tener a la vista lo tecnológico, sino que también marca notoriamente el factor humano, como creador, articulador, usuario e innovador. La preparación de ese factor, como masa crítica de conocimiento, es parte de la cadena de mejoramiento continuo, permitiendo que el derrotero de desarrollo y avances pueda de verdad ser útil y aplicable. Aun cuando hay cada día más procesos automatizados, de inteligencia artificial o de *machine learning*, es el individuo quien inclina la diferencia, donde su conocimiento y capacidad integra el balance de factor de potencia, lo que no puede estar ausente en cualquier análisis militar.

Pero volviendo al entendimiento del diseño y alcances de una capacidad de ciberdefensa, se pueden generan confusiones que, más que ser conceptuales o semánticas, tienen impactos en la operacionalización de las acciones y recursos a emplear. Nace entonces la interrogante de la delimitación de la disyuntiva entre ciberdefensa y ciberseguridad.

La ciberdefensa (OTAN, 2008)[8] es una connotación sistémica y sistemática que deben desarrollar los gobiernos y sus entes subordinados o asociados, para comprender sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos, como nos orienta It-Insecurity, requiere la comprensión de variables como las vulnerabilidades en la infraestructura crítica de una nación, las garantías y derechos de los ciudadanos en el mundo *online*, la renovación de la administración de justicia en el entorno digital y la evolución de la inseguridad de la información en el contexto tecnológico y operacional (It-Insecurity, 2011). Contempla la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. Por ello, la ciberdefensa se relaciona con el desarrollo y aseguramiento de capacidades, preocupándose de sus recursos, actividades, tácticas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta acerca de los sistemas necesarios para garantizar el libre acceso al ciberespacio.

Como realidad complementaria de la ciberdefensa, se materializa el concepto de defensa nacional digital, en un conjunto de variables claves, en las que son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de

8 El Manual OTAN MC0571, NATO Cyber Defence, define ciberdefensa como "la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques".

una realidad digital y de información instantánea. Por ello, la ciberdefensa contendrá un conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al adversario en oposición.

Correlaciona entonces "un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes, que incluye Internet, los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores" (CARI, 2013). Es de notar que incluye a usuarios y operadores, en realidad redundante, pues los sistemas por definición ya incluyen a las personas y los procedimientos. Por ello, la ciberdefensa va notoriamente ligada al desarrollo y aseguramiento de capacidades.

Por su parte la ciberseguridad, al decir de Cano, puede ser entendida como el conjunto de actividades dirigidas a proteger el ciberspacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan (Cano, 2015). Entonces, asegura el uso de las redes propia y niega su empleo a terceros.

A mayor abundamiento, el concepto de ciberseguridad es descrito como "el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y a los usuarios en el ciberentorno" (Larrieu-Let, 2015). Por ello, implica un conjunto de acciones de carácter preventivo que tienen por objeto asegurar el uso de las redes propias y negarlo a terceros. Con ello la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, cuáles son amenazas de seguridad correspondientes en el ciberentorno (Unión Internacional de Telecomunicaciones).

La ciberseguridad consta de tres elementos fundamentales, que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, conocido como la tríada CIA[9] (INFOSEC, 2018).

Sintéticamente entonces, la ciberseguridad puede ser definida como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. Por ello, la ciberseguridad va notoriamente ligada al desarrollo y aseguramiento de prácticas.

9 Tríada CIA, viene de la expresión abreviada en inglés que contempla *Confidentiality-Integrity-Availability.*

En los pasos ya descritos se ha sintetizado la evolución tecnológica que fue requiriendo en el trazado de sus avances la protección de la dimensión ciberespacial, trayendo consigo el desarrollo e implementación de lo que hoy conocemos como ciberseguridad.

Factores de comportamiento de lo tecnológico en lo multidimensional, con relación a los impactos de la ciberseguridad

Al contrastar tendencias de comportamiento de lo tecnológico con las características de lo multidimensional, es aporte de este análisis ofrecer algunos factores que se relacionan con los impactos de la ciberseguridad en ello, los que se pueden enunciar como la oportunidad, la sincronización y la visión multicapas.

La OPORTUNIDAD es uno de esos factores, debido a que lo multidimensional, en el grado de ambición estratégica que se defina, necesariamente es dependiente de la oportunidad, lo que conlleva mantener panoramas operacionales comunes que estén actualizados en tiempo real, con clara visualización de las ventanas de oportunidad de objetivos que se presenten, para de ahí, sobre la plataforma de mando y control desarrollada, coordinar y sincronizar esfuerzos y efectos.

La SINCRONIZACIÓN es otro factor, porque el actuar de los recursos requiere ser coordinado e integrado, pero más que eso, el comportamiento de los efectos es fundamental que sea sincronizado. Por ello, la necesidad de priorizar y asignar medios orgánicos, subordinados, segregados o asignados temporalmente, define los flujos de información en que la evaluación del daño es reportada es un requerimiento de sincronización dependiente de la base tecnológica, que ayudará a la detección del momento de acción oportuno y a la confluencia de todos los esfuerzos necesarios para optimizar su resultado. La corriente de enlaces requeridos, en especial por su exigencia de monitoreo permanente del panorama estratégico, operacional y táctico, implicará contar con un mínimo de latencias, o idealmente que estas sean inexistentes, debido a que las brechas que puedan aparecer serán de reducida apertura en tiempo y desprotección, momento que de ser detectado activará la concurrencia de todas las medidas de acción preplanificadas y las que se generen como objetivos de oportunidad. Proteger ese enlace de monitoreo y operación será una gravitante tarea de responsabilidad de la ciberseguridad, asociando lo tecnológico, lo multidimensional y lo ciber.

El factor de VISIÓN MULTICAPAS surge de la proyección de lo multidimensional, enfrentada a un estrangulamiento estratégico, donde para salir de ello se busca un desequilibrio que permitiera romper el amarre. La solución

ideada para quebrar el estancamiento de ese problema pasó por avanzar hacia una visión multicapas, contenida en varios niveles que eran observados y vigilados para encontrar en alguno de ellos puntos de desbalance, para así recuperar la libertad de acción. Con ello se definieron y extrajeron determinadas prácticas primordiales que por un lado buscarían contener y fortalecer frentes críticos; asimismo ofender en segmentos en los que se habían detectado vulnerabilidades o se podría infringir daño, carencia o fatalidad a sistemas críticos adversarios. Cuando la gran estrategia se ocupó de este punto, hizo confluir respuestas clásicas, como lo bélico en puridad, hasta acciones que englobaban lo económico, lo social, lo político y lo diplomático, incluyendo lo tecnológico de forma transversal y como una herramienta complementaria. La tecnología, junto con su gestor fundamental que es el componente humano, toma presencia cruzada en todas las capas, actuando en un enfrentamiento que se da en todos los dominios donde se requiere actuar con previsión, y basado en métodos de gestión, acciones, prácticas idóneas y directrices; con el fin de conformar un ciberentorno estable y seguro.

Conclusiones

Los conflictos con repercusiones armadas se enfrentan hoy a un escenario aún más complejo que en el pasado. El campo de batalla se ha extendido a cinco dominios, lo que le da amplitud, volumen, dinamismo, cambio y con mayor carga de incertidumbre. En gran parte ello está dado por lo multidimensional de los contextos de enfrentamiento, donde lo tecnológico toma día a día mayor preponderancia, sin desmerecer el efecto que la fuerza convencional pueda generar. Esta característica aporta a la convergencia y permite que todos los esfuerzos, en todos los dominios y tipos de fuerza, sean orientados a penetrar las defensas enemigas, donde el común denominador es articularse para complementar efectos que vayan minando la fortaleza del adversario en el máximo de vectores posibles, potenciando así la voluntad estratégica propia.

Por ello, quien busque desafiar en lo estratégico se encontrará con mayores dificultades de logro de su nivel de ambición y de imposición de su voluntad, ya que lo multidimensional de su entorno requerirá contención en varios de sus flancos y acción coordinada y sincronizada en lo que defina como centro de gravedad, que es por donde buscará la ruptura y desbalance. Lo anterior, da contexto a un entorno estratégicamente complejo.

En este marco estratégico, la opción para los Estados de porte estratégico similar, más que ir a la solución armada, es la de maniobrar con las herramientas que son previas a ello, desafiándose y haciendo gestión de crisis y

conflicto, lo que hace que la contienda de voluntades sea más compleja, con dominios entrecruzados que requieren ser capaces de trabajar juntos en una convergencia que va en pos de la sincronización, donde la articulación requiere un elemento tecnológico fuerte para llevar a favorable concreción el entorno de la disputa de objetivos contrapuestos en un escenario actual.

Una de las plataformas principales de sincronización corresponde al espectro electromagnético y al ciberespacio, ambientes que han sido parte del avance de la tecnología, que en su momento fueron elementos complementarios a su aplicación bélica y hoy han cimentado bases en lo que es una de sus dimensiones, el ciberespacio, el que cada día aumenta sus demandas de seguridad. Asociado a ello, el paso siguiente de la tecnología será el de asegurar en forma robusta el ciberespacio, o al menos aportar en su resiliencia, en ello es fundamental la ciberseguridad.

Los riesgos relacionados a la Seguridad de la Información que comprometen la integridad, la confidencialidad y la disponibilidad de la misma, 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. Luego, junto en un aporte económico superior para llegar a una plataforma tecnológica pertinente, la preparación del personal a ser integrado en ciberprotección, en especial en la ciberseguridad, será un factor muy importante a desarrollar y a mantener actualizado. Consecuentemente, el pilar de soporte, como eslabón crítico de la cadena de unión entre tecnología y ciberseguridad, será el factor humano, como depositario y gestor de lo que los avances de la modernidad aporten en conocimientos y protocolos de acción y respuesta.

Bibliografía

Anabalón, J. y Donders, E. (2014). *Una Revisión de Ciberdefensa de Infraestructura Crítica.* Trabajo de titulación para obtener el grado de Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos de la Universidad de Santiago de Chile.

Cano, J. (2015). *Ciberdefensa y Ciberseguridad, desafíos emergentes para los profesionales de Gobierno* TI., CFE, ECOPETROL, Colombia.

CARI (2013). *Ciberdefensa-Ciberseguridad Riesgos y Amenazas.* Recuperado de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf.

Chee-Wooi, T.; Chen-Ching, L. (2010). "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling". IEEE *Transactions on Systems, Man and Cybernetics*, Part A: Systems and Humans. 40, pp. 30-36.

Cowen, T. (2013). *Average Is Over: Powering America Beyond the Age of the Great Stagnation.* Penguin Group. Estados Unidos.

Department of the Navy Headquarters United States Marine Corps (2016). *US Marine Corps Operating Concept*. Estados Unidos.

It-Insecurity (2011). *Ciber seguridad y ciber defensa: Dos conceptos emergentes en la gobernabilidad de una nación*. Recuperado de http://insecurityit.blogspot.cl/2011/01/ciber-seguridad-y-ciber-defensa-dos.html

Joint Chiefs of Staff (2012). *Capstone Concept for Joint Operations*. Estados Unidos.

Larrieu-Let, E. (2015). *Ciberataques ¿Estamos preparados?* Buenos Aires Chapter. Argentina. Editorial CISM, ISACA. Argentina.

León, P. (2017). *La batalla multi-dominio*. Revista Escenarios Actuales. CESIM. Chile.

Luttwak, Edward (2005). La Estrategia de la Paz y de la Guerra. Madrid: Siglo XXI de España. España.

OTAN (2008). MC0571, *NATO Cyber Defence*.

Perkins, D. (2017). "Multi-Domain Battle, Driving Change to Win in the Future". *Military Review*. Estados Unidos, Jul.-Ago. 2017, pp. 6-12.

Romero Serrano, J. (2018). *La huella de la historia*. Fundación Siglo Futuro: España.

TRADOC (2017). *Concept Version 1.0 for Multi-Domain Battle*. Estados Unidos.

US Army Combined Arms Center (2014). *Army Operating Concept*. Estados Unidos.