Capítulo 4

El desafío del combate por el mando y control

*Mario Arteaga Velásquez**

Introducción

El concepto de "ciberguerra" sigue siendo tema de discusión, a tal punto que se ha convertido en un inevitable tópico de debate en el ámbito de la seguridad internacional debido a que se le atribuye ambigüedad y se le califica de controversial. Por otra parte, también persiste la tendencia a confundir ciberguerra con ciberataques, siendo pertinente revisar el aporte de Javier Jordán y Josep Baqués al respecto, porque ambos se encargan de transmitir la conceptualización de ciberguerra que propone Adam P. Liff al manifestar que ella constituye "una situación de conflicto entre dos o más actores políticos, caracterizada por la ejecución de ataques deliberados, hostiles y dañinos contra redes de ordenadores en la infraestructura crítica civil o militar de un adversario con intención coercitiva y orientada a la obtención de concesiones políticas; o como una medida de fuerza bruta contra redes militares o civiles con el fin de reducir la capacidad del adversario para defenderse o para llevar a cabo represalias semejantes o mediante fuerzas convencionales, así como contra objetivos militares o civiles con objeto de afectar a un actor

* Mario Arteaga Velásquez es General de División (R) del Ejército de Chile. Doctor en Relaciones Internacionales, Universidad Complutense de Madrid. Magíster en Ciencias Militares con mención en Política de Defensa, Academia de Guerra del Ejército de Chile. Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile. Diplomado en Gestión Educacional, Pontificia Universidad Católica de Chile. Director ejecutivo del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. marteagav@acague.cl

por motivos estratégicos"[1]. De lo expresado por Liff se infiere que los ciberataques constituyen acciones que son parte de la ciberguerra, que esta última compromete a actores políticos como son los Estados; y que el propósito es obtener ventajas políticas y estratégicas que impidan la respuesta del adversario.

Según Manuel R. Torres, existen analistas quienes sostienen que la tierra, el mar, el aire, el espacio y el ciberespacio son los cinco "dominios" donde se puede "librar la guerra"[2]. Luego, es lógico considerar que tanto las acciones ofensivas como las defensivas, en las que se lleva a efecto la ciberguerra, tienen como escenario lo que los Estados reconocen como el "quinto dominio", es decir, el ciberespacio, que además es considerado "como una zona de combate" donde es posible realizar actividades que cada día tienen un mayor impacto en las capacidades civiles y militares de los mismos Estados, atendiendo a que los objetivos corresponden, entre otros, a las funciones económicas, las funciones gubernamentales, la infraestructura vital del Estado, la estructura militar y, particularmente, la estructura de mando y control política y estratégica.

El ciberespacio es un ámbito o dominio extremadamente complejo, porque allí se facilita la ejecución de las acciones defensivas y se dificulta la ejecución de las acciones ofensivas; también, porque los límites son indefinidos y ello dificulta la detección y la identificación del adversario y, menos aún, se pueden determinar con algún grado de certeza la magnitud y capacidad de este mismo. Se suma a lo anterior, que el ciberespacio no constituye el escenario absoluto de la ciberguerra porque, así como lo sostiene Liff, las acciones que ella considera pueden ser llevadas a efecto por fuerzas convencionales, lo que significa accionar en los otros dominios (tierra, mar, aire y el espacio) para reducir la capacidad de respuesta del adversario.

En el debate respecto de los dominios existen autores que sostienen la existencia de dominios físicos y abstractos, situando al ciberespacio entre los últimos. Además, identifican al espectro electromagnético como un dominio independiente, junto con el ambiente de la información y el dominio cognitivo, considerando que todos ellos se localizan entre los abstractos. Al respecto, se estima que el espectro electromagnético sería parte del dominio del ciberespacio, en tanto se considera y acepta que la guerra electrónica se desarrolla en dicho espectro y que ella corresponde a uno de los elementos del combate por el mando y el control que tiene ocurrencia en el ciberespacio. Respecto del ambiente de la información y al dominio cognitivo, se estima

1 Javier Jordán y Josep Baqués. *Guerra de Drones: Política, tecnología y cambio social en los nuevos conflictos,* Madrid: Editorial Biblioteca Nueva, S.L., 2014, p. 130.

2 Manuel R. Torres. *Ciberguerra,* en: Javier Jordan: Manual de Estudios Estratégicos y Seguridad Internacional, Madrid: Plaza y Valdés S. L., 2013, pp. 331-333.

que ambos son parte de la guerra por la información y del combate por el mando y control, razón por la que no constituirían dominios sino que bastaría con identificarlos como condiciones que influyen en la toma de decisiones que se producen en los cinco dominios identificados con anterioridad. Como sea, lo anterior es algo que se tendrá que continuar analizando en el futuro.

Se ha establecido que existe una relación entre ciberguerra, guerra de información, mando y control y ciberespacio, pero junto con mantener el esfuerzo para conocer aún más de ellos, se advierte que es necesario investigar y reflexionar respecto del combate por el mando y control, de tal manera que sea posible identificar los factores que intervienen, las amenazas que puedan afectarle y las condiciones y desafíos para alcanzar la victoria en el citado combate. Esta tarea, de por sí compleja, se dificulta más considerando que la ciberguerra y su objeto de estudio, el combate por el mando y control, ocurren preferentemente en el ciberespacio que, como ya se dijo, es un dominio de extrema complejidad. Para dar respuesta a las inquietudes expresadas anteriormente, en este artículo se intenta establecer cómo alcanzar la victoria en el combate por el mando y control. Para ello, en la primera parte se aborda la relación entre la guerra de información y el mando y control en el ciberespacio. A continuación, en la segunda parte, se examinan los elementos que intervienen en el combate por el mando y control. Luego, en la tercera parte, se analizan las condiciones y desafíos para combatir por el mando y control con éxito. Finalmente se presentan algunas conclusiones que responden a la interrogante referida a cómo alcanzar la victoria en el combate por el mando y control.

El ciberespacio y el combate por el mando y control

El ciberespacio, según las Fuerzas Armadas de Estados Unidos, corresponde al "dominio global del ambiente de información que consta de infraestructuras de tecnología de información en redes interdependientes y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas computarizados, además de procesadores y controladores integrados"[3].

Otros analistas, con los cuales se concuerda, complementan lo anterior señalando que en el ciberespacio se lleva a efecto una verdadera competencia, con características propias de la guerra, para ello se requieren capacidades

[3] Michael Kolton. *La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras*, en: Military Review, Centro de Armas Combinadas, Fort Leavenworth, Kansas, Mayo-Junio 2016, p. 52.

que permitan afrontar los esfuerzos que permitan conducir política y estratégicamente el empleo del poder del Estado.

Por otra parte, anteriormente se indicó que la ciberguerra se relacionaba con la lucha por la información y que constituía una situación de conflicto entre actores políticos, los Estados, que realizan acciones coercitivas entre ellos recurriendo a la utilización del Poder Nacional, donde destaca el empleo de la capacidad militar. Refuerza lo anterior el hecho de que el combate por el mando y control implica una situación de conflicto y la ejecución de acciones para imponerse al adversario con el propósito de conseguir el dominio; de esto se infiere que la lucha por la información y el combate por el mando y control se encuentran relacionados.

Ahondando en el concepto de mando y control, es importante tener presente que este se distingue por ser el encargado de proveer la información necesaria para que la toma de decisiones se produzca con el menor grado de incertidumbre y con la mayor rapidez y oportunidad posible, de tal manera que la acción propia se anticipe a la del adversario, considerando, además, que también contribuye a la convergencia de los esfuerzos nacionales tanto políticos, económicos, diplomáticos como militares en beneficio del logro de los propósitos establecidos mediante la aplicación de la unidad de mando. Un asunto importante en lo referido al mando y control es que en pleno siglo XXI aún se debate acerca de la forma de llevarlo a efecto; y es así como algunos adhieren a la práctica del mando y control detallado, que se caracteriza por la emisión de órdenes que restringen la libertad de acción de los escalones subordinados y por la aplicación de sistemas de control que tienden a invadir los espacios de acción inferiores, con lo que la libertad de acción se restringe aún más. Por el contrario, existen otros que privilegian la práctica del mando y control directivo, que se distingue por el otorgamiento de libertad de acción para que los escalones subordinados puedan actuar aplicando su iniciativa orientados por la intención del escalón superior.

Es indudable que el ambiente político, estratégico u operacional influirá cuando se tenga que decidir el tipo de mando y control a utilizar; sin embargo, antes de hacerlo es conveniente recordar que las restricciones de libertad de acción inhiben la iniciativa y con ello se retarda el accionar. Lo más grave es que lo anterior puede transformarse en una pérdida de la libertad de acción general y que ello podría afectar la toma de decisiones en los niveles superiores, generándose un ambiente donde impere la voluntad del adversario. El asunto adquiere mayor complejidad al considerar que la acción de mando y control se ejecuta preferentemente en el ciberespacio, porque es en ese ambiente donde acciona la infraestructura de información y se produce la interdependencia de las redes, como fue mencionado anteriormente.

Jim Dunivan[4], refiriéndose al mando y control, sostiene que Sun Tzu, Von Clausewitz, Jomini y Von Molke, entre otros, coinciden en que la rápida toma de decisiones es fundamental para mantener la iniciativa y que de no hacerlo se corre el riesgo de ceder esa iniciativa al adversario y por consiguiente la libertad de acción que pasa a manos de ese adversario. Poseer libertad de acción significa disponer de una capacidad esencial para actuar sin que se oponga la voluntad de un adversario, ella facilita el cumplimiento de la propia intención y para obtenerla es indispensable aplicar la iniciativa, la sorpresa y la seguridad. Es improbable alcanzar un grado de libertad de acción absoluto, porque así como ella es indispensable para el cumplimiento de la propia intención, también lo es para que un eventual adversario pueda cumplir la suya, por tanto será necesario realizar acciones para impedir que ese adversario llegue a poseerla; y si cuenta con ella, realizar las acciones necesarias para que la pierda[5]. Lo anterior corresponde a la histórica lucha por la libertad de acción, donde la forma de ganarla, mantenerla y asegurarla constituye un desafío para los conductores políticos y militares, porque, finalmente, estar en posesión de ella significa disponer de oportunidades políticas y militares que favorezcan la propia intención.

En los niveles más altos de la organización del Estado, la libertad de acción para la toma de decisiones adquiere una importancia equivalente a la de los intereses nacionales, porque constituye un elemento fundamental para resolver con autonomía durante los procesos interestatales; y es por ello que debe ser protegida al igual que ocurre con los intereses nacionales citados anteriormente[6]. En el ámbito militar, especialmente en lo estratégico y en lo operacional, la libertad de acción es una condición fundamental para la toma de decisiones alejada de la atrición que provenga del adversario, lo que implica que este último debe estar afectado por la pérdida de la iniciativa y, por consecuencia, sometido a una condición reactiva, es decir, respondiendo a la presión de su oponente. Cuando un actor se encuentra en las condiciones descritas, es decir, sin iniciativa y reaccionando permanentemente, es altamente

4 Jim Dunivan. *C2 en el campo de batalla digitalizado: ¿Cediendo la iniciativa?* Military Rewiew, Fort Leavenworth, Kansas, March-April 2004, pp. 2-4.

5 André Beaufre. *Introducción a la Estrategia,* Madrid: Instituto de Estudios Políticos, 1965, p. 157. Beaufre sostiene que "la lucha por la libertad de acción es, en efecto, la esencia de la estrategia" y que su protección se obtiene mediante la seguridad, en tanto que la privación de ella para el adversario es el producto de la propia iniciativa combinada con la sorpresa. Señala, además, que ambos dan origen a un "juego estratégico".

6 Alexander Wendt. *Social Theory of International Politics,* United Kingdom, Cambridge: Cambridge University Press, 2006, p. 235. Según Wendt, Alexander George y Robert Keohane identifican tres intereses nacionales: supervivencia física, autonomía y desarrollo económico. Es por ello que la libertad de acción, si bien no constituye un interés nacional propiamente tal, contribuye a la obtención de uno de ellos: la autonomía.

probable de que se produzca la parálisis política, estratégica u operacional, que no es otra cosa que estar imposibilitado para continuar conduciendo el empleo de sus capacidades de manera coordinada y orientada al punto donde deben concentrase los esfuerzos para conseguir el éxito[7]. Cuando se consigue la parálisis del adversario, la acción de sus conductores políticos o militares se desordena, se transforma en reacción y la sensación de escasez de tiempo comienza a influir en sus decisiones acelerándolas a tal nivel que no es posible coordinar los esfuerzos ni conducirlos apropiadamente.

La función mando y control, al encargarse de proveer la información que se requiere para la toma de decisiones con la menor incertidumbre posible, se transforma en un objetivo que debe ser atacado o defendido en la guerra de la información. Siendo así, es indudable que la infraestructura que sirve a la función será objeto de acciones ofensivas para restarle capacidades o para neutralizarla con el propósito de impedir que cumpla su propósito. Con lo anterior, el atacante alcanzaría un grado de libertad de acción que le permitirá adelantar su ciclo de decisiones y, a la vez, interferir y quebrar el ciclo de decisiones del adversario, de tal manera que una autoridad política o militar y su respectiva cadena de mando se confunda, paralice y finalmente colapse. Considerando que todo esto ocurre preferentemente en el ciberespacio la acción del atacante se vería facilitada, en tanto que la defensa enfrentaría dificultades para detectar e identificar al atacante, para localizarlo y para intentar su neutralización.

Un ataque a la infraestructura de mando y control dificultaría la conducción de las acciones políticas o militares, más aún si se ha optado por la práctica del mando y control detallado. Si por el contrario, se ha resuelto practicar el mando y control directivo, es probable que los efectos del ataque no permitan que el adversario consiga imponer su voluntad y someter a su oponente con facilidad.

Definitivamente, en el complejo escenario que representa el ciberespacio no solo se llevan a efecto la guerra por la información y el combate por el mando y control, sino que también se genera una lucha por la libertad de acción; y si a ello se le agrega la incertidumbre propia de la guerra y particularmente de la ciberguerra, la complejidad se incrementa dificultando las acciones que deben realizar los conductores políticos y militares para coordinar las capacidades del Estado haciéndolas converger para conseguir la decisión, aplicando el principio de unidad de mando y de esfuerzo.

7 Se está haciendo referencia al centro de gravedad, que al ser atacado de manera exitosa genera la derrota del adversario.

Elementos y amenazas del combate por el mando y control

En el combate (algunos lo denominan guerra) por el mando y control intervienen numerosos elementos, destacando entre ellos: la guerra electrónica, las operaciones de seguridad, las operaciones psicológicas, la decepción y la destrucción física de la infraestructura de información. Este último elemento destaca entre los anteriores porque su aplicación no ocurre solo en el ciberespacio, sino que también puede llevarse a efecto en cualquiera de los otros dominios o escenarios, especialmente en el dominio terrestre.

La guerra electrónica cumple tres tareas que son fundamentales en el combate por el mando y control; la primera de ellas, denominada protección electrónica, consiste en asegurar el empleo del espectro electrónico en beneficio de la acción de mando y control con los medios propios; la segunda tarea, el ataque electrónico, tiene como propósito negar al adversario la capacidad de realizar una acción de mando y control efectivo de sus medios; y, la tercera tarea, apoyo electrónico, es la encargada de proporcionar información en tiempo real, monitoreando al adversario para detectar e impedir el ataque electrónico adversario.

Por su parte, las operaciones de seguridad se orientan a negar la información crítica de las propias capacidades al adversario, de tal manera que este se mantenga en una situación de incertidumbre que dificulte su toma de decisiones o que lo conduzca a resolver erradamente. Para su cometido, las operaciones de seguridad se realizan coordinándolas con las actividades de protección electrónica.

Las operaciones psicológicas, en el caso del combate por el mando y control, se accionan desde el nivel político y estratégico considerando actividades diplomáticas, económicas, militares y de información. Su función se resume en influenciar positivamente el ámbito externo, generar percepciones e inducir el comportamiento en beneficio de las propias metas. Estas operaciones se realizan de manera coordinada con las actividades de protección electrónica y de apoyo electrónico, las que permiten conocer el efecto logrado.

La decepción, por su parte, se orienta a producir una apreciación errónea de la situación propia en el conductor político o militar adversario y sus asesores, de tal manera que su toma de decisiones se dificulte especialmente en situaciones críticas donde el factor tiempo es fundamental. La decepción también se debe coordinar con las actividades de protección y de apoyo electrónico.

La destrucción física de la infraestructura de información adversaria se realiza empleando el armamento aéreo, naval, terrestre o la acción directa de fuerzas de operaciones especiales. Se lleva a efecto después de un riguroso

proceso de selección de objetivos y debe contar con el apoyo de la guerra electrónica, de las operaciones de seguridad y de la decepción.

Otro elemento que aporta sustancialmente en el combate por el mando y control es la Inteligencia, siendo ella la encargada de obtener, analizar, evaluar e interpretar la información relacionada con las capacidades de la infraestructura de mando y control del adversario y con las capacidades del armamento que pudieran afectar la propia capacidad durante el combate por el mando y control. La Inteligencia como función primaria apoya con información referida a los procedimientos, estructura organizacional y estimación de las áreas de despliegue de los sistemas de mando y control adversarios. Simultáneamente, apoya con operaciones de contrainteligencia para proteger la infraestructura de mando y control propia.

En el combate por el mando y control, que se lleva a efecto de preferencia en el ciberespacio, existen amenazas y riesgos que pueden afectar la infraestructura de información pudiendo reducir sus capacidades e inclusive neutralizarlas. La amenaza más presente y de la que existen ejemplos más que suficientes para demostrar su efectividad[8], tanto en el ámbito civil como en el militar, es el ataque cibernético, cuyos efectos van desde interrumpir las comunicaciones de teléfonos móviles hasta impedir el funcionamiento de infraestructura estratégica crítica y que, por supuesto, podrían afectar la infraestructura de mando y control militar. Respecto de esta amenaza, se tiende a pensar que ella es dependiente de la capacidad tecnológica disponible, sin embargo los hechos han demostrado que tecnología suficiente en manos de expertos[9] pueden producir efectos que se traducen en disminución y neutralización de capacidades fundamentales.

Otras amenazas provienen de los elementos del combate por el mando y control del adversario, es decir, de la guerra electrónica, las operaciones de seguridad, las operaciones psicológicas, la decepción y de la capacidad adversaria para destruir físicamente la infraestructura de información propia. Esto implica que para evitar los efectos de dichas amenazas o al menos minimizarlos, es indispensable accionar con anticipación y previsión empleando toda la capacidad propia para proteger las redes e infraestructura de información.

8 Kolton: *La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras,* p. 55, sostiene que el año 2014, cuando Rusia tomó el control de Crimea se produjo una "interrupción significativa de teléfonos móviles" y que el 23 de diciembre de 2015 un "supuesto ataque cibernético" habría afectado a más de setecientos mil ucranianos al dejarlos sin electricidad. A estos ejemplos se suman otros, como los ciberataques sufridos por Estonia el año 2007, como lo señala Torres en *Ciberguerra,* p. 337.

9 Se está haciendo referencia a los *hackers*, quienes son capaces de penetrar sistemas de alta sofisticación para introducir códigos "malignos", borrar archivos de relevancia o interrumpir el funcionamiento de infraestructura crítica, entre otros.

Es importante considerar que las amenazas provienen de actores estatales y no estatales, a los que se suman organizaciones criminales, amenazas de actores internos e inclusive los errores inconscientes de operadores propios. A estas amenazas se suman los riesgos provenientes de la ausencia de regulaciones y procedimientos para la operación de sistemas, incumplimiento de normas de seguridad, ausencia de programas de seguridad cibernética; desconocimiento o falta de experiencia en la aplicación de regulaciones, procedimientos y programas de seguridad cibernética; y, especialmente, ausencia de políticas, estrategias y directivas operacionales de seguridad cibernética que sean realmente efectivas.

Una de las formas de combatir las amenazas en el combate por el mando y control consiste en alcanzar la "supremacía en el ciberespacio"[10], que es sinónimo del "dominio cibernético" establecido por otros autores. Esto se relaciona con la capacidad de accionar en el ciberespacio conforme con la propia voluntad, de tal manera que se pueda emplear la infraestructura tecnológica de información con el máximo de libertad de acción y seguridad, tanto de manera defensiva como ofensiva. Así la supremacía y el dominio cibernético se relacionan con el poder, adquiriendo la denominación de ciberpoder y siendo conceptualizado como la capacidad de emplear el ciberespacio para generar ventajas, oportunidades y situaciones que influyan decisivamente en otros actores[11].

Para la obtención de la supremacía o dominio cibernético en el ciberespacio es necesario recurrir a las capacidades de la organización, a las estrategias y procedimientos, a la infraestructura tecnológica que interviene en la guerra de información, y a los elementos del combate por el mando y control. Para la obtención del dominio cibernético o supremacía en el ciberespacio se recurre a las capacidades que provienen tanto de la organización, estrategias y procedimientos como de la infraestructura tecnológica que interviene en la guerra de información, es decir, se emplearán las capacidades de operaciones sicológicas, de decepción, de guerra electrónica y de destrucción física de la infraestructura de información del adversario, entre otros.

De lo presentado respecto del propósito de la supremacía cibernética se confirma su estrecha relación con la libertad de acción; primero, porque la libertad de acción favorece el empleo de la propia capacidad cibernética con la menor oposición de un adversario en el ciberespacio; segundo, porque la

[10] Nigel Inkster. *China's Cyber Power,* London: The International Institute for Strategic Studies, 2016, pp. 97-100.

[11] Stuart H Starr. *Developing a theory of Cyberpower en:* Tarek Saadawi y Louis Jordan Jr. *Cyber Infraestructure protection,* Carliste: Strategic Studies Institute, U.S. Army War College, 2011, p. 17.

libertad de acción contribuye a que el empleo de la propia capacidad cibernética sirva a la obtención de la supremacía en el ciberespacio con economía de medios y fortaleciendo la seguridad; y tercero, porque como consecuencia de la obtención de la supremacía en el ciberespacio se consigue la parálisis política, estratégica u operacional del adversario, la que aporta condiciones óptimas para hacer realidad la propia intención. Para la obtención del dominio cibernético o supremacía en el ciberespacio se recurre a las capacidades que provienen tanto de la organización, estrategias y procedimientos como de la infraestructura tecnológica que interviene en la guerra de información, es decir, se emplearán las capacidades de operaciones sicológicas, de decepción, de guerra electrónica y de destrucción física de la infraestructura de información del adversario, entre otros.

Por otra parte, del análisis de la relación entre la supremacía cibernética y el combate por el mando y control se infiere que disponer de la citada supremacía contribuye a que la entrega de la información para la toma de decisiones se produzca con rapidez, oportunidad, mayor grado de certidumbre y, especialmente, con seguridad. Lo anterior se debe a que el adversario no estará en condiciones de oponerse e interferir de manera importante, porque sus capacidades para hacerlo se encontrarán disminuidas o neutralizadas y su actuar no dispondrá de la libertad de acción suficiente para oponerse de manera efectiva. Esta situación contribuirá a que el sistema de mando y control propio adquiera condiciones para fortalecer la unidad de mando y dirección que se requiere para que los esfuerzos confluyan en el punto de la decisión, así como fue planificado y de manera coordinada y segura.

Existe consenso respecto de que el empleo de la asimetría constituye una opción política y estratégica que de ser aplicada podría influir tanto en la libertad de acción como en el esfuerzo para conseguir la supremacía cibernética. Para entender el porqué de lo anterior, es necesario recordar que en situaciones de conflicto internacional la aplicación de la asimetría se evidencia cuando uno de los actores basa su actuar en el empleo de modos diferentes a los de su adversario y el empleo de sus medios se orienta a imponerse a las capacidades superiores de su oponente por medio de lo irregular con fuerte sustento psicológico. Lo anterior, produce un escenario de enfrentamiento extremadamente complejo, con presencia de amenazas difíciles de eliminar, situación que fortalece la sensación de vulnerabilidad y sitúa a los responsables de las decisiones políticas y militares en un ambiente de gran incertidumbre que produce atrición psicológica que puede conducir a la parálisis política y estratégica y, por consiguiente, a la pérdida de la libertad de acción.

El empleo de la asimetría para reducir la libertad de acción de un adversario superior debería orientarse especialmente a neutralizar las capacidades

de mando y control de este, empleando medios reducidos que son capaces de infringir grandes daños de manera imprevista, indirecta y desde posiciones desconocidas y múltiples que dificultan su neutralización o destrucción. Como consecuencia de la degradación de la capacidad de mando y control, es probable que quien toma las decisiones sufra los efectos de la atrición y se vea impedido para continuar conduciendo su accionar con una adecuada coordinación y sincronización de los esfuerzos, porque estará enfrentando niveles altos de incertidumbre debido a que no se puede identificar, localizar, ni atribuir el ataque asimétrico. En el caso de que la acción asimétrica se mantenga es probable que el afectado entre en la condición de parálisis que se mencionó con anterioridad.

El empleo de la asimetría para degradar el sistema de mando y control de un adversario superior puede combinar acciones en el ciberespacio con acciones directas en contra de la infraestructura física que contiene la tecnología de información, es por ello que cuando aparece en el combate por el mando y control la situación se torna más compleja y la incertidumbre se incrementa, pudiendo inhibir la decisión de emplear capacidades superiores, entre ellas las relacionadas con el ciberpoder.

En la búsqueda de la supremacía cibernética también son importantes las aproximaciones que realiza el Ejército de Tierra de Francia respecto del dominio del tiempo y el dominio de la tecnología[12]. Porque el dominio del tiempo se refiere a actuar con urgencia para aplicar la iniciativa que permite obtener libertad de acción para accionar oportunamente y anticipándose al adversario. En el dominio del tiempo son fundamentales las decisiones políticas y militares y, según la doctrina francesa, es probable que ante la presencia de la asimetría, las decisiones militares tengan que adoptarse independientes de las decisiones políticas. Respecto del dominio de la tecnología, lo que sostiene el Ejército de Tierra de Francia es que si se quiere actuar con urgencia, especialmente en un escenario asimétrico, ese dominio se convierte en un multiplicador de eficacia que incrementa el poder, porque permite integrar todo tipo de capacidades, incluidas las cibernéticas relacionadas con la información, optimizando la maniobra política, estratégica u operacional. Además, se sostiene que el dominio del tiempo en conjunto con el dominio de la tecnología contribuyen a disminuir las propias vulnerabilidades, a incrementar la seguridad y a enfrentar amenazas que sufren permanentes transformaciones.

12 Armée de Terre. *Ganar la batalla. Conducir a la Paz,* París: Centre de Doctrine d'Emploi des Forces, 2007, pp. 52-56.

De los planteamientos anteriores se desprende que en el ciberespacio se desarrolla una intensa interacción entre los elementos del combate por el mando y control con las amenazas y riesgos que se manifiestan en ese "quinto dominio". Lo sorprendente es que los mismos elementos del mando y control se transforman en amenazas para el mando contrario, sumándose a otras que se han identificado en esta parte del presente artículo. En igual sentido, llama la atención que muchos de los riesgos ya citados guardan relación con acciones u omisiones propias; y que la acción asimétrica debe ser considerada una amenaza. Frente a lo anterior, la solución parece ser alcanzar la supremacía cibernética, lo que implicaría la ejecución de acciones ofensivas y defensivas acompañadas por un permanente desarrollo tecnológico para asegurar la superioridad.

La disputa por el mando y control

La revisión y análisis realizados en los acápites anteriores contribuyen a demostrar la existencia de una disputa por el mando y control en el ciberespacio y también en los otros dominios, es decir, en lo terrestre, en lo naval, en lo aéreo y en lo espacial. También ha quedado en evidencia que dicha disputa incrementa progresivamente su complejidad e importancia, presentando la característica de un verdadero combate para conseguir la supremacía de mando y control y de esa manera poder imponerse al adversario.

Se entiende que la superioridad en mando y control impacta decisivamente en la lucha para obtener la libertad de acción y que esta, a la vez, repercute en la práctica de la unidad de mando que facilita la convergencia de los esfuerzos políticos y estratégicos, incluyendo entre los últimos a los esfuerzos militares. Se suma a lo anterior, que la victoria en la lucha por el mando y control contribuye al logro de la supremacía cibernética que, aunque sea temporal, incrementará los niveles de libertad de acción y la seguridad de quien esté en posesión de ella, facilitándole la toma de decisiones y su accionar posterior sin mayores interferencias por parte del adversario.

El combate para obtener la superioridad de mando y control requiere contar con un sistema que para estos fines sea robusto y resiliente, es decir, que por una parte tenga mayores capacidades que las del adversario para no transformarse en objetivo de su acción cibernética y menos aún de sus ataques por la vía convencional; y que por otra parte, sea capaz de resistir y de recuperarse con rapidez de los efectos provocados por eventuales ataques exitosos que provengan del mencionado adversario. Lo anterior, también se relaciona directamente con las amenazas que están presentes en el ciberespacio

y, además, con aquellas que provienen de la capacidad de destrucción física de la infraestructura de mando y control por parte del adversario.

Una de las mayores dificultades para desarrollar el combate por el mando y control cuando este ocurre en el ciberespacio, radica en la dificultad que existe para localizar geográficamente el origen del ataque debido a que regularmente este no "siempre deja tras de sí una estela que pueda ser rastreada"[13], lo que prácticamente impide identificar al responsable y, por consiguiente, dificulta y puede impedir la planificación y ejecución de algún tipo de respuesta. Al respecto, cuando el ataque responde a la propia intención lo anterior constituye una ventaja, pero cuando proviene del adversario se transforma en dificultad e inclusive en incapacidad para responder a la agresión.

Otro asunto importante en el combate por el mando y control se refiere a la permanencia de los efectos, asunto que deriva de la fortaleza y capacidad de resiliencia de las estructuras. Esto ha generado un planteamiento en donde se asume que una acción ofensiva exitosa contra la estructura de mando y control del adversario solo produciría una superioridad temporal y no absoluta, generando una ganancia en cuanto a libertad de acción que debe ser explotada con rapidez para no perder la oportunidad y la ventaja que se consiguió. Es aquí donde cobra importancia la aplicación del modelo de mando y control directivo, porque en las condiciones descritas no se dispondrá del tiempo necesario para emitir documentos ejecutivos detallados, tampoco para controlar los que elaboren los escalones subordinados y, menos aún, para controlar su ejecución. Lo anterior, constituye un desafío porque implica haber desarrollado niveles de confianza que favorezcan la entrega de facultades para que los mandos subordinados puedan aplicar su iniciativa y accionar con mayor independencia, practicando el ya conocido mando tipo misión.

Otro desafío radica en la generación de capacidades para que el combate por el mando y control conduzca a la victoria, debido a que por una parte existe la necesidad de contar con un sistema robusto y resiliente que resulte de la integración de todas las capacidades disponibles, es decir, tanto las civiles como las militares y, entre estas últimas, las que provengan de las diferentes instituciones de la defensa nacional; y por otra parte, se manifiesta la necesidad de emplear sinérgicamente las capacidades de mando y control, lo que implica procedimientos comunes, entrenamiento certificado, coordinaciones y sincronización de esfuerzos con el objeto de evitar interferencias,

[13] Torres: *Ciberguerra*, pp. 333-334. Torres denomina a esto "los problemas de atribución" señalando, además, que se debe a que los ataques pueden proceder "de diferentes puntos del planeta".

economizar medios y conseguir la unidad de mando y con ella la convergencia de los esfuerzos.

En la práctica, el combate por el mando y control significa inutilizar los sistemas del adversario, lo que requiere conocer con anticipación las vulnerabilidades de dichos sistemas demandando un tremendo esfuerzo de búsqueda para obtener la información necesaria. Al respecto, es indispensable que esa información se obtenga en tiempos de normalidad, explotando las oportunidades que se presentan cuando no existe conflicto o la intensidad de este es baja y los niveles de seguridad tienden a reducirse. En esta tarea, son los propios sistemas de mando y control, sumados a la capacidad de guerra electrónica, como uno de los elementos del combate por el mando y control[14], sumados al apoyo de la Inteligencia[15], los que pueden contribuir al descubrimiento de las citadas vulnerabilidades.

El secreto constituye un asunto fundamental en el combate por el mando y control porque consiste en impedir que el adversario conozca la propia infraestructura, menos aún que obtenga conocimiento de las vulnerabilidades que esta pueda presentar. Para esto es indispensable que las operaciones de seguridad propia sean efectivas y puedan negar la información crítica. Lo anterior puede ser más efectivo aún si es que se combinan con operaciones de decepción que conduzcan al adversario a una apreciación errada de las propias capacidades; y, también, si es que se combinan con acciones de protección electrónica que dificulten el empleo del espectro electrónico por parte del adversario. Si la mantención del secreto es exitosa, simultáneamente se generará la sorpresa que potenciará el accionar propio asegurando la supervivencia de los medios empleados.

Un asunto que no puede dejar de mencionarse se refiere a que aún cuando el combate por el mando y control se desarrolla preferentemente en el ciberespacio, siempre existirá el riesgo de que parte importante de la infraestructura (de mando y control) pueda ser neutralizada o destruida en su despliegue terrestre, mediante el ataque con armamento de precisión operado desde largas distancias o mediante la acción directa de fuerzas de operaciones especiales, inclusive por el empleo de actores asimétricos que puedan ser reclutados para esos fines.

14 Se refiere a la guerra electrónica que cumple la tarea de proporcionar información monitoreando al adversario para detectar e impedir un ataque electrónico de su parte.

15 Recordar que la Inteligencia es la encargada de obtener, analizar, evaluar e interpretar la información relacionada con las capacidades de la infraestructura de mando y control del adversario, incluyendo las capacidades del armamento que pudiera ser empleado en contra de la propia capacidad.

Cuando se esté combatiendo por el mando y control el dominio de la tecnología será un elemento fundamental para dominar el tiempo y de esa manera poder actuar con la rapidez necesaria para anticiparse al accionar del adversario. Esto constituye un desafío que impacta en el elemento humano, porque lo obliga a estar familiarizado con dicha tecnología, a entrenarse y a ser capaz de explotar al máximo sus capacidades, lo que implica altos niveles de capacitación y entrenamiento permanente. Se asocia a este desafío la necesidad de contar con el sostenimiento suficiente para que la infraestructura de mando y control se mantenga permanentemente operacional. Esto último requiere integrar las capacidades civiles y militares por medio de alianzas públicas y privadas para desarrollar tecnología, apoyar su operacionalidad e inclusive para contribuir a su protección, entre otros asuntos.

Un asunto que podría influir negativamente en el combate por el mando y control es el exceso de burocracia practicado especialmente en los procedimientos de transmisión de tareas, en la transmisión de información y en los procedimientos de control, porque ello impacta negativamente en los esfuerzos para conseguir el dominio del tiempo, actuar con rapidez y para anticiparse al adversario. Al respecto, se debe considerar que la superioridad cibernética es temporal y difícilmente absoluta, por tanto la rapidez se convierte en un requisito fundamental y la burocracia excesiva actúa en su contra.

La trascendencia, importancia y el carácter evolutivo del combate por el mando y control conducen a formular una estrategia que facilite la preparación, ejecución y la dirección de los esfuerzos para alcanzar los efectos deseados y conseguir la victoria en el ciberespacio, considerando que esa victoria beneficiará a la toma de decisiones por parte de líderes políticos y militares y será fundamental para la conducción de los esfuerzos en procura de los objetivos propuestos, permitiendo accionar con el máximo de libertad de acción, asegurando la unidad de mando y la convergencia de los esfuerzos políticos y estratégicos. El propósito de la citada estrategia debería orientarse a la disuasión del adversario, a conseguir la supremacía en el ciberespacio y a paralizar el accionar del adversario. Los mayores desafíos de la citada estrategia se relacionan con ganar la lucha por la libertad de acción, asumir la modalidad directiva del mando y control y a vencer las amenazas y riesgos que se manifiesten en el ciberespacio y en los otros dominios en que se encuentre desplegada la estructura de mando y control propia. Al mismo tiempo, la estrategia debería considerar lo necesario para impedir que el adversario pueda actuar empleando sus propias capacidades de mando y control, siendo este el fundamento que respalda la necesidad permanente de anticiparse a las decisiones adversarias y de actuar con rapidez y con el máximo dominio del tiempo.

Lo expuesto en los párrafos precedentes permite identificar algunos objetivos que debe contener una estrategia para el combate por el mando y control, entre ellos los siguientes:

- Potenciar las capacidades de mando y control mediante herramientas de detección, prevención y de defensa.
- Desarrollar capacidades de respuesta efectiva a los ataques adversarios.
- Consolidar el empleo seguro de la propia capacidad de mando y control para vencer en la guerra por la información.
- Potenciar la estructura de mando y control desarrollando un alto nivel de resiliencia.
- Capacitar y entrenar al elemento humano de la estructura de mando y control para dominar la tecnología, dominar el tiempo y ganar la iniciativa.
- Asegurar la utilización del mando y control directivo y el mando tipo misión.
- Generar la cooperación civil, militar, pública y privada para contribuir al sostenimiento de la infraestructura de mando y control.
- Contribuir a la obtención de la victoria en la guerra por la información.

Es importante considerar que la victoria en el combate por el mando y control sirve a la configuración del campo de batalla y que también puede contribuir a que la disuasión sea creíble en los términos que lo señala Beaufre[16]. Respecto del aporte para la configuración del campo de batalla, ello se consigue alcanzando la supremacía en el ciberespacio y venciendo al adversario en la lucha por la libertad de acción, porque lo obliga a tener que reaccionar permanentemente, disponiendo de escasa capacidad para accionar conforme a sus intenciones. En relación con la disuasión, la supremacía en el ciberespacio facilita el desarrollo de acciones que demuestren el ciberpoder alcanzado y la voluntad para emplearlo de manera ofensiva si es que ello fuera necesario. Como se puede apreciar, el aporte a la configuración del campo de batalla, que también puede aplicarse al escenario de conflicto y crisis, radica en la demostración de capacidad y en la advertencia, que en conjunto incrementan la incertidumbre dificultando y retardando la toma de decisiones.

16 Beaufre sostiene que para evitar "una prueba de fuerza" con el adversario es necesario disponer de una fuerza ofensiva que lo desanime a emplear la suya. En el caso de combate por el mando y control correspondería a una estructura con gran capacidad de penetración, de precisión y de destrucción.

Reflexiones finales

Así hemos podido establecer el cómo alcanzar la victoria en el combate por el mando y control, asumiendo como constante que dicho combate se lleva a efecto principalmente en el ciberespacio, pero sin que ello signifique que en el resto de los dominios, particularmente en el terrestre, nada ocurre. También se consideró que el citado combate se relaciona estrechamente con la guerra por la información y que sus acciones son tanto de carácter defensivo como ofensivo.

En la primera parte de esta reseña se profundizó el conocimiento respecto de la relación que existe entre la guerra de información y el mando y control en el ciberespacio, pudiendo establecerse que dicha relación gira en torno a la existencia de un tercer elemento, que influye notoriamente en el análisis y que se refiere a la necesidad de generar libertad de acción para fortalecer la unidad de mando y contribuir a la convergencia de los esfuerzos políticos y estratégicos y, finalmente, conseguir el o los objetivos propuestos. Además, se consideró que todo ello, por el hecho de ocurrir en el ciberespacio, adquiere una connotación especial, debido al factor tiempo que obliga a conseguir los estados deseados con rapidez para así mantener la iniciativa.

En la segunda parte se revisaron los elementos del combate por el mando y control y se identificaron las amenazas que se manifiestan durante la ejecución de dicho combate en el ciberpacio y en el dominio terrestre. En este segmento se analizó la interacción que se producen entre ambos, pudiendo determinarse que los elementos y amenazas son comunes para los actores en conflicto y que el dominio del tiempo es determinante para anticiparse a las intenciones de cada uno, para ganar la iniciativa y obtener la libertad de acción que se requiere para accionar con el mínimo de interferencia u oposición.

En la tercera parte se identificaron y analizaron los desafíos y las condiciones que demanda alcanzar la victoria en el combate por el mando y control, junto con ello se pudo establecer que para conseguir la supremacía cibernética es indispensable contar con una infraestructura de mando y control robusta y altamente resiliente, de tal manera que sus capacidades sean superiores a la del adversario. También se estableció que en el combate que se lleva a efecto en el ciberespacio es muy difícil identificar al atacante y localizar geográficamente el origen de un ataque, lo que, en conjunto, dificulta ejecutar una represalia. Además, surgió un asunto que es relevante al momento de evaluar los efectos de una acción ofensiva exitosa en el ciberespacio, porque dichos efectos son temporales y no absolutos debido a la robustez y resiliencia de las estructuras de mando y control, situación que obliga a actuar con rapidez para explotar el éxito. En esta parte también se identificaron y analizaron otras condiciones y desafíos de vital importancia en el combate por el mando