Las operaciones de información como elemento disuasivo para el conflicto armado

Coronel (jubilado) Blane R. Clark, Ejército de EUA

Debemos mantener las mentes alertas y receptivas en cuanto al uso de métodos y armas desconocidas.

—General Douglas A. MacArthur

LAS OPERACIONES DE información (OI) proporcionan opciones flexibles y no letales a nuestros comandantes. El utilizar las OI de esta manera es viable tanto para los adversarios estatales como para los no estatales. El efecto más importante variará conforme a la capacidad principal específica que tenga el adversario. Las capacidades principales de las operaciones de información producen el efecto estratégico más significativo como un elemento disuasivo para el conflicto cuando se usa en la primera fase de las operaciones conjuntas. De hecho, la meta estratégica principal de las OI es impedir las amenazas presentadas por posibles adversarios.[1] La disuasión producida por las operaciones de información obliga a un adversario a aceptar una política o a tomar una acción que cumple o beneficia a los intereses de EUA y sus metas de seguridad nacional. En realidad, los usos de las OI a nivel estratégico, han constado de sólo una o dos capacidades principales como facilitadores tácticos en lugar de combinaciones sinergísticas para producir un efecto estratégico.

Las operaciones de información que se planean, integran y ejecutan como parte de un plan de campaña de un comando de combate en la primera fase ofrecen opciones no cinéticas y no letales a un comandante para lograr sus metas estratégicas. La probabilidad de la eficacia en la primera fase incrementa cuando los comandantes integran las OI en los ciclos de planeamiento deliberado y de medidas en caso de crisis. La integración de esa índole, debe ocurrir desde el inicio de las operaciones e incluirse en rigurosos procesos conjuntos de adquisición de blancos. Se debe elaborar medidas aprovechables para que sirvan de base en toda decisión de reiniciar o terminar las acciones de las Operaciones de Información.

El emplear Operaciones de Información concentradas, integradas y sincronizadas para disuadir a un adversario sobre un curso de acción e impedir el inicio del conflicto armado no constituye un acto bélico.[2] No obstante, si bien no es un acto de guerra, tiene que ver con la adquisición de blancos. Si el motivo del uso de las OI es el de lograr un efecto disuasivo deseado, hay tres componentes facilitadores que deben alinearse, a saber: la capacidad de enfrentar un blanco, tener acceso al blanco y la autoridad para enfrentar al mismo.

Fundamentos de las operaciones de información

Las capacidades militares básicas de las operaciones de información incluyen la guerra electrónica, las operaciones de redes informáticas, las operaciones de apoyo de información militar, las operaciones de desinformación militar y la seguridad de operaciones. Si son debidamente coordinadas y estrechamente concentradas, estas capacidades pueden disuadir el conflicto armado. La meta principal de las operaciones de información a nivel estratégico es la de hacer

---

El Coronel (Jubilado) Blane R. Clark, Ejército de EUA, fungió como el jefe de la División de Información, Operaciones (J3), del Comando Central de EUA, desde enero de 2005 hasta junio de 2008; como director de Operaciones de Mando, Control, Comunicaciones y Computadoras (C4) y Operaciones de Información; y como profesor en la Escuela Superior de Guerra del Ejército de EUA de julio de 2008 a diciembre de 2009. Recibió su Maestría de la Universidad de Southern California. Ha desempeñado puestos de mando y estado mayor en el territorio continental de EUA, Corea, Alemania e Irak. Actualmente, el Coronel Clark funge como vicejefe de la sección J3 de la Fuerza de Tarea Conjunta-Operaciones de Redes Globales (JTF-GNO) y subcomandante de la Operaciones Actuales (J33) del Comando del Componente Funcional Conjunto-Guerra de Redes/JTF-GNO, en el Fuerte Meade, Maryland.

que un líder o grupo de líderes claves desistan de una acción específica o, si no, que tomen una acción compatible con los intereses de EUA.[3]

Las operaciones de información no constituyen el uso de cualesquiera de las capacidades principales por sí solas. La integración sincronizada y coordinada de las combinaciones de las capacidades básicas caracteriza las operaciones de información, y esto genera el componente de ofensiva no cinético de fuerza que podría disuadir el conflicto armado.

Fuerza Aérea de EUA, Sgto. Jason T. Bailey

Soldados del Ejército de EUA de la 213ª Compañía de Operaciones de apoyo de información militar observan una reacción después de emitir un aviso por altoparlante desde la Estación de Seguridad Conjunta de Oubaidy, ubicada en las periferias de la Cuidad al-Sadr, Irak, tras una serie de ataques por misil y morteros, 29 de marzo de 2008.

La guerra electrónica. Esta capacidad básica consta de tres subdivisiones, a saber: el ataque electrónico, la protección electrónica y el apoyo electrónico. Todos estos representan acciones militares durante las cuales las armas electromagnéticas o de energía concentrada controlan el espectro electromagnético o atacan a un adversario.[4] Puesto que el enfoque radica en la disuasión, el ataque electrónico tiene la relevancia más directa.

El ataque electrónico establece como objetivo las instalaciones, equipamiento o personal del adversario para degradar, neutralizar y, de ser necesario, destruir los sistemas de apoyo electrónico del adversario.[5] Por ejemplo, los medios aéreos de ataque electrónico podrían realizar la interferencia de comunicaciones a gran distancia de la red de comunicaciones del sistema antiaéreo integrado del enemigo para degradar las capacidades de mando y control de su sistema.

Las operaciones de redes informáticas. La más reciente capacidad básica integrada en la Publicación Conjunta (*Joint Publication*) 3-13, *Computer Network Operations*, consta de tres subcomponentes: el ataque contra redes computarizadas, la defensa de redes informáticas y la explotación de redes informáticas.[6] Nuevamente, en vista de que el enfoque es producir un efecto disuasivo, el ataque de ofensiva de una red informática representa el subcomponente más viable "generador de efectos".

El ataque de redes informáticas implica el uso de redes informáticas para negar, interrumpir o degradar computadoras, redes informáticas o información establecida en cualesquiera de las mismas. En la actualidad, los posibles grupos adversarios dependen cada vez más de computadoras y redes informáticas para facilitar el mando y control, transacciones que hacen posible el apoyo y la coordinación de medidas.[7]

El ataque contra los redes informáticas ofrece la posibilidad de ser un arma de interrupción masiva contra blancos infraestructurales tanto militares como civiles.[8] Por ejemplo, un ataque de negación de servicio en la Internet compuesto por una carga de un flujo substancial de datos en una red informática del adversario puede consumir toda la anchura de banda disponible en esa red y degradarla de forma significativa o hasta sacarla fuera de uso.

Las operaciones de apoyo de información militar. Esta capacidad básica consiste en enviar información que influya o disuada a los líderes adversarios claves y sus estructuras de apoyo de manera que impida las subsecuentes medidas adversas por parte del adversario. Las operaciones de apoyo de información militar son más eficazmente empleadas como una capacidad integrada de las operaciones de información en apoyo de las operaciones en la primera fase.[9] Estas

operaciones ejercen influencia en poblaciones de otros países y neutralizan los mensajes del adversario. Los mensajes radiodifundidos por medio de onda corta, en donde se le advierte a toda la población que las medidas de sus líderes podrían llevar a tomar medidas militares, son un ejemplo de estas operaciones. En el Departamento de Defensa, sólo el personal encargado de llevar a cabo operaciones de apoyo de información militar cuenta con la autoridad de influir a públicos blancos de otros países mediante una gran serie de mecanismos como radio, medios impresos y otros medios afines para difundir mensajes.[11]

…la Política de Seguridad Nacional también destaca la "persuasión" como un elemento de alta prioridad para asegurar los intereses de EUA.

La desinformación militar. Esta capacidad básica enfoca, deliberadamente, blancos claves de adversarios encargados de la toma de decisiones para llevarlos a sacar conclusiones erradas favorables a nuestros objetivos. Como arma de disuasión, da pie a dudas, desconcierto y, tal vez, temor entre los líderes claves del adversario al desestabilizar o degradar su ciclo normal de toma de decisiones de mando y control mientras se afanan para evaluar la desinformación.[12] Un mensaje con miras a sacar provecho de una brecha entre un integrante clave del liderazgo adversario encargado de la toma de decisiones que ha tenido una relación contenciosa con otro integrante clave es un ejemplo de estas actividades. Este mensaje podría ocasionar un antagonismo interno dando como resultado que un adversario desista de un curso de acción planeado y adopte una postura más favorable a nuestros intereses.

La seguridad de operaciones. En la primera fase, la seguridad de operaciones niega al adversario información crucial que podría facilitarle una evaluación acertada de nuestras intenciones y capacidades. Además, las operaciones de seguridad eficaces ocasionan que el adversario, tome, ya sea, malas decisiones o posponga la toma de decisiones por falta de información creíble.[13] Negarle información crucial sobre nuestras intenciones y capacidades al encargado de la toma decisiones del adversario ayuda a aumentar su incertidumbre, desestabilizar su ciclo de toma de decisiones e incrementar, cada vez más, sus dudas, temor y confusión, lo que hace la disuasión una verdadera posibilidad .[14]

Otras cinco capacidades respaldan las operaciones de información, a saber: contrainteligencia, seguridad física, seguridad de información, servicio de fotografía de combate y ataque físico. Salvo por el ataque físico, estas medidas sirven para defender la infraestructura amiga o la documentación de información visual y no son tan relevantes para lograr la disuasión. El ataque físico implica el empleo de fuegos cinéticos contra un objetivo de las operaciones de información para influir a un público blanco específico.[15]

Si bien la doctrina establece que las siguientes tres capacidades relacionadas con las operaciones de información como son los asuntos públicos, las operaciones cívico-militares y apoyo de defensa a la diplomacia pública, ayudan al ambiente de información general y deben de ser coordinadas con las operaciones de información, discutiblemente, su uso, aunque relacionado con las operaciones de información de ofensiva para lograr la disuasión es indirecto, en el mejor de los casos. Las operaciones de información militares se centran en el enemigo y en las estructuras de apoyo del mismo. Las operaciones de asuntos públicos difunden mensajes tanto al público interno como externo. Las operaciones cívico-militares son más eficaces en la cuarta fase (estabilización) y quinta fase (facultar a las autoridades civiles). El apoyo de defensa en la diplomacia pública corresponde al apoyo de la difusión de mensajes y temas por soldados especializados en las operaciones de apoyo de información militar supeditados a la autoridad de un embajador. Estas capacidades afines no son tan eficaces como las capacidades de las operaciones de información en lo que respecta a lograr la disuasión en la primera fase.[16]

Las operaciones de información en la primera fase: una postura persuasiva

Basadas en una voluntad política comprometida, las operaciones de información brindan a los comandantes combatientes opciones no letales

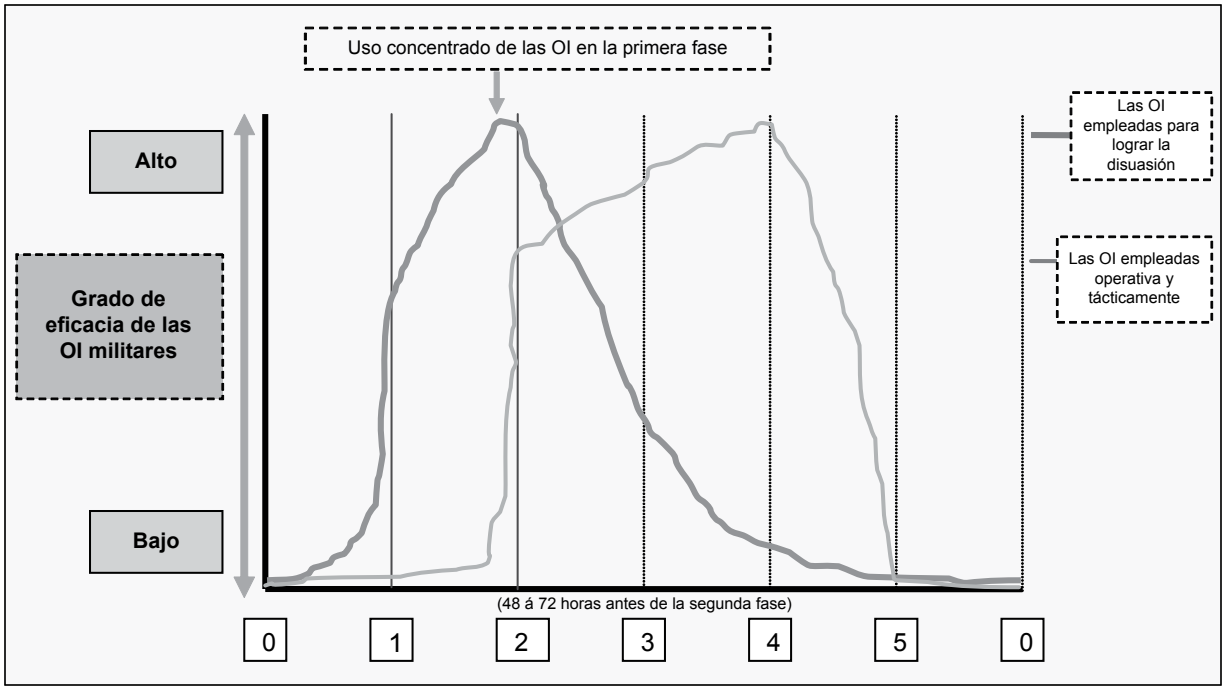

Figura 1. Las operaciones de información en la primera fase, disuasión

que, si se usan en el contexto de un conjunto general de metas estratégicas, pueden disuadir el conflicto. De hecho, el principal énfasis estratégico de las operaciones de información debe ser la disuasión y el uso de las capacidades básicas encaminadas a ese fin.[17] A fin de que las operaciones de información puedan disuadir a un posible adversario, debemos emplearlas con la misma fuerza y rigor que caracterizan nuestro uso de fuerza letal. Debemos dejar a nuestro adversario con una percepción abrumadora de que el seguir un curso de acción que EUA considera una amenaza a sus intereses nacionales será infructuoso, y que insistir en ese curso de acción llevará a terribles consecuencias. Las operaciones de información utilizadas eficazmente en apoyo de la disuasión llevan al adversario de duda, temor y desconcierto y lo induce a abandonar un curso de acción específico. Con las operaciones de información coordinadas para influir en el proceso de observar-orientar-decidir-actuar (OODA) del adversario, sus operaciones y percepciones sobre la posibilidad de lograr el éxito disminuyen. Esto crea una posibilidad verdadera de que el adversario pueda abandonar o cambiar la política opugnada por EUA.[18]

Todos reconocemos cuán atractivo resulta el valor de emplear las operaciones de información para disuadir el conflicto. En el informe de la *National Security Strategy of the United States*, se establece que la disuasión de un posible enemigo es una de las prioridades principales para asegurar los intereses nacionales de EUA.[19] El documento trata directamente la necesidad de enfrentar a un posible adversario con las capacidades de las operaciones de información antes de que comience un conflicto armado.

Curiosamente, la Política de Seguridad Nacional (*National Security Policy*) también destaca la "persuasión" como un elemento de alta prioridad para asegurar los intereses de EUA.[20] La "persuasión" incluye esas actividades relacionadas con la Fase Cero (operaciones de preparación). En la Fase Cero, las operaciones de información militares sólo deben jugar un rol de menor importancia. Por ejemplo, otros elementos de poder nacional como el —diplomático, informativo y económico, deben llevar el control de las iniciativas de EUA para hacer que un adversario desista de continuar una política que amenaza los intereses de seguridad de EUA.

La diferencia que existe entre la "persuasión" y la disuasión de un posible adversario yace en la concentración de fuerza. A menudo, con las iniciativas de "persuasión", el enfoque toma un planteamiento menos directo hacia el adversario.

En cambio, la disuasión requiere presión dirigida contra un posible adversario. Los blancos para el uso de las operaciones de información disuasivas deben corresponder, directamente, con los componentes críticos humanos, infraestructurales y de contenido que sostienen al posible adversario y la política o curso de acción que está buscando.

En la Directiva 3600.1 del Departamento de Defensa se tratan las operaciones de información y se apoya la necesidad de aprovechar las capacidades de las OI para lograr la disuasión. En la directiva se establece que las operaciones de información deben tener como meta disuadir conflictos y que el potencial de mitigar una crisis es su mejor promesa.[21] La Fase Cero constituye la fase de configuración de las operaciones conjuntas y la segunda fase, la de "tomar la iniciativa", representa el comienzo del conflicto armado. Las operaciones de información rápidamente se transfieren al uso táctico mientras que se usan ofensivamente en la segunda fase. En la primera fase, las operaciones de información cierran la brecha de disuasión estratégica que existe entre la persuasión en la Fase Cero y el inicio de la fuerza letal en la segunda fase. Mientras más agresivo sea el uso de las operaciones de información en la primera fase, más probable será que el adversario perciba nuestra disposición de usar la fuerza.[22] Las operaciones de información en apoyo de la disuasión estratégica puede consecuentemente llevar al mínimo el requisito de fuerzas desplegadas en posiciones avanzadas y apostadas.[23] Las operaciones de información influirán la toma de decisiones y las percepciones de un posible adversario mientras aumentan el efecto disuasivo de las opciones de proyección de fuerza.[24]

En la Figura 1, se describe la eficacia disuasiva de las operaciones de información a través de las fases de las operaciones conjuntas. El análisis de este diagrama dejará más claro el argumento persuasivo para las operaciones de información de ofensiva en la primera fase junto con el uso concentrado de las OI a medida que la primera fase se aproxima a su culminación y la segunda fase está a punto de comenzar.

La línea trazada a la izquierda representa las operaciones de información puestas en práctica para lograr la disuasión. En el diagrama también se muestra que la eficacia de las operaciones de información es mínima en la fase Cero, sin embargo, se acelera rápidamente con el inicio de la

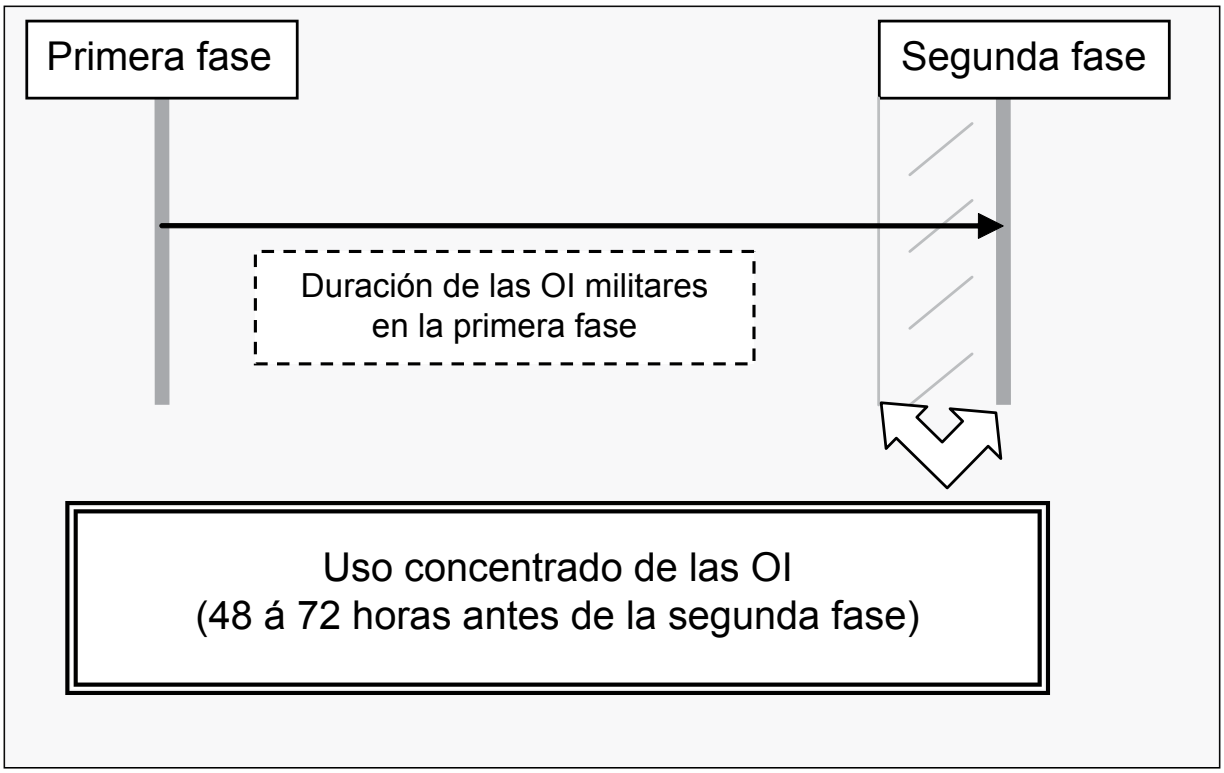

Figura 2. Las operaciones de información durante la primera fase

primera fase e incrementa de manera acumuladora durante la primera fase. Esta creciente eficacia refleja una reacción por parte del posible adversario con respecto al uso sincronizado de las capacidades básicas de las operaciones de información militares. En la primera fase, las operaciones de información deben tener como meta afectar a los líderes adversarios y sus estructuras de apoyo, incluyendo la población, hasta el grado que EUA logre su meta de disuadir el conflicto apremiando el cambio favorable de una política por parte del adversario.[25] A medida que se acerca el comienzo de la segunda fase, en el diagrama se explica que debe darse una iniciativa concentrada de las operaciones de información que garantice, en primer lugar, la disuasión con éxito y la disuasión fallida, la superioridad informacional de las fuerzas amigas en la fase de preparación para el inicio del conflicto armado en la segunda fase. La característica principal de la iniciativa concentrada de las operaciones de información es el redoble de iniciativas y la concentración de los "fuegos" de operaciones de información. De fracasar las iniciativas de disuasión, se deberá iniciar el uso concentrado de las operaciones de información en la primera fase en un período de 48 a 72 horas del inicio anticipado de la segunda fase. En la Figura 2 se describe los eventos de manera cronológica para el inicio y ejecución de las actividades concentradas de las operaciones de información en la primera fase.

A medida que comienza la segunda fase, el efecto estratégico de las operaciones de información como una opción para rápidamente lograr la disuasión queda sujeto subordinado al uso de las operaciones de información en apoyo de las demandas operativas y tácticas.

Los mismos recursos utilizados en la primera fase para llevar a cabo las operaciones de información también apoyan la lucha operacional y táctica e incrementa su implementación desde el inicio de la segunda fase hasta su culminación en la tercera fase, las operaciones de combate principales. Al inicio de la cuarta fase, la eficacia de las operaciones de estabilización y las OI operacionales y tácticas disminuye.

El uso dinámico, sincronizado y coordinado de las cinco capacidades principales para disuadir las acciones de posibles adversarios estatales debe darse de la siguiente manera:

- La guerra electrónica puede focalizarse en el mando y control y en los radares del comando de mísiles balísticos del adversario, a fin de degradar la capacidad de lanzamientos. Podría interferir las señales de las emisoras estatales de radio y televisión para aislar a la población de la propaganda política del Estado.
- Un ataque de redes informáticas contra una red de telecomunicaciones del estado puede impedir, deteriorar o interrumpir su uso para fines de mando y control de las fuerzas militares o su uso por parte de los líderes claves a fin de coordinar una respuesta nacional. Tal ataque, llevado a cabo conjuntamente con operaciones de apoyo de información militar, puede difundir mensajes discretos a los líderes claves de las distintas facciones para crear fricción e incrementar la presión interna sobre los líderes estatales enemigos para que desistan de sus políticas contenciosas.
- Las operaciones de apoyo de información militar pueden difundir mensajes a la población con el fin de crear una división entre ésta y los líderes estatales adversarios y añadir más presión interna.
- Las operaciones de desinformación militar pueden sembrar la duda, el temor y la confusión entre los líderes militares claves con respecto a las verdaderas intenciones militares de EUA. Dichas operaciones obligarán a los líderes militares adversarios a enfrentar a los líderes políticos con fútil resistencia.
- La seguridad operacional puede envolver las operaciones de fuerzas amigas con un manto de seguridad y frustrar la detección de las verdaderas intenciones de EUA.

…el uso de las operaciones de información de ofensiva puede disipar una crisis y evitar la necesidad de pasar a la fase de conflicto armado…

El comandante combatiente busca la manera de aislar a los líderes de posibles adversarios

del apoyo físico y psicológico que poseen, sobre todo, de sus fuerzas militares e infraestructura de apoyo.[26] Si el actor es una nación-estado, la dependencia de una burocracia y de una tecnología más formalizada, tales como las redes de telecomunicaciones y de radar, probablemente será mayor que la de un actor no estatal. Por lo tanto, los ataques electrónicos y los ataques a las redes informáticas podrían tener un efecto mayor contra un actor estatal que contra un actor no estatal. En cualquier de los dos casos, el uso de las operaciones de información de ofensiva puede disipar una crisis y evitar la necesidad de pasar a la fase de conflicto armado que comienza en la segunda fase.[27]

…las operaciones de información dan cabida a los esfuerzos de ceñirse a las restricciones tradicionales de carácter moral y jurídico encaminadas a fomentar la moderación y a reducir al mínimo el uso de la fuerza.

La falta de sofisticación tecnológica y de un mando y control menos formalizado por parte de los enemigos no estatales típicos, en comparación con los enemigos estatales, podría limitar la eficacia directa de los ataques electrónicos y del ataque a redes informáticas. No obstante, puesto que los enemigos no estatales podrían usar la infraestructura de telecomunicaciones del país anfitrión en el que se desenvuelven, el ataque a las redes informáticas tiene el potencial de funcionar como una capacidad habilitadora para la difusión de mensajes directos de las operaciones de apoyo de información militar. Asimismo, los ataques a redes informáticas pueden habilitar los mensajes de las operaciones de apoyo de información militar dirigidos a los líderes claves del país anfitrión, lo cual estimulará medidas más osadas contra el adversario.

Las operaciones de influencia que emplean operaciones de apoyo de información militar y la desinformación militar tendrán el mayor efecto en un adversario que carece de la sofisticación tecnológica en términos de mando y control. La desinformación militar puede hacer que los líderes de un grupo adversario no estatal comiencen a dudar de la tolerancia futura de sus actividades por parte del país anfitrión y temer las operaciones militares contra ellos por las fuerzas de la coalición encabezadas por EUA. Las operaciones de apoyo de información militar contra la población local pueden socavar el apoyo del cual goza el adversario. Por ejemplo, al ofrecer recompensas por información, la población local tendrá un mayor incentivo para denunciar las actividades del grupo adversario.

Ambos casos demuestran que el uso con éxito de las operaciones de información militares contra cualquier posible adversario exige los siguientes elementos:

- El análisis del entorno para asegurar la sincronización adecuada de las capacidades principales.
- La evaluación de los intereses vitales de un posible adversario para asegurar que la planificación de las operaciones de información se centre en el objetivo correcto.
- La evaluación de los puntos de presión decisivos de un posible adversario para asegurar que la fuerza que se use en las operaciones de información logre la máxima eficacia.
- El uso de la capacidad o de las capacidades de las operaciones de información en el grado y envergadura de fuerza necesarios para lograr el efecto disuasivo deseado.[28]

La planificación, adquisición de blancos y eficacia

Las operaciones de información deben incorporarse plenamente en la planificación y adquisición de blancos, y los sistemas de medición de la eficacia deben proporcionar la retroalimentación necesaria para asegurar su efectividad. La clave de la eficacia es el uso de todas las capacidades principales sincronizadas e incorporadas.[29] La eficacia de las operaciones en la primera fase es incierta a menos que las operaciones de información estén incorporadas en la planificación y en la adquisición de blancos.

Los planificadores de las OI deben participar como integrantes activos en los equipos de planificación de las operaciones establecidas y estar preparados para defender el valor de los aspectos de las OI tanto como un conjunto de capacidades sin igual, así como un multiplicador de fuerza en todas las fases de las operaciones conjuntas.[30]

El empleo de procedimientos tradicionales para la adquisición de blancos es necesario y adecuado porque las operaciones de información ofrecen opciones que producen efectos, de la misma manera que lo hacen las opciones letales. Una matriz de sincronización de adquisición de blancos que ilustre la incorporación de blancos es tan pertinente tanto para las operaciones de información como para las capacidades letales.[31] Debe haber una sola matriz de sincronización de adquisición de blancos que incorpore blancos letales y no letales. Los sistemas que miden la eficacia deben estar lógicamente relacionados con un estado final deseado. Sin embargo, hay que reconocer que la medición de la eficacia representa un gran desafío. El efecto acumulativo de las operaciones de información que se necesita para lograr la disuasión dificulta la evaluación del efecto de cada capacidad de manera individual.[32]

Según se arguye, un sistema de medición de la eficacia para cada una de las capacidades principales es irrelevante si se necesita la sincronización de dos o más capacidades para lograr el efecto deseado. Sin un sistema de medición de la eficacia que se base en el análisis deductivo para los efectos de primer orden, y el análisis inductivo razonable para los efectos de segundo y tercer orden, la aceptabilidad de las operaciones de información como un conjunto de opciones no letales fáciles de predecir para el comandante es aparente.

La justificación jurídica y moral

El conflicto armado se rige por el Derecho Internacional.[33] Las operaciones de información caen fuera de este marco jurídico. El Derecho Internacional no menciona el uso de operaciones de información como uno de los aspectos del conflicto armado y, por lo tanto, el uso de las OI como elemento disuasivo no constituye un acto bélico.[34]

El Artículo 41 de la Carta de la ONU es un ejemplo de órganos jurídicos rectores que no clasifican el uso de operaciones de información como un acto bélico. En este artículo, se establece que los actos que interrumpen las comunicaciones de un adversario no implican el uso de fuerza armada.[35] Por lo tanto, el uso de las operaciones de información como parte de las operaciones de disuasión, tales como la guerra electrónica y ataques de redes informáticas, no constituye un acto de guerra.

En el marco conceptual de la Ley del Conflicto Armado, las condiciones de *jus in bello* (Derecho de Guerra), es decir, la manera en que se emplea una fuerza durante la guerra, implica principios de necesidad, proporcionalidad, discriminación y humanidad. Los Convenios de Ginebra y de La Haya clasifican las condiciones para *jus in bello*. Dichos convenios no contienen acuerdos de control específicos que limiten el uso de las operaciones de información.[36] De hecho, las operaciones de información dan cabida a los esfuerzos de ceñirse a las restricciones tradicionales de carácter moral y jurídico encaminadas a fomentar la moderación y a reducir al mínimo el uso de la fuerza.[37] Por ejemplo, el principio de proporcionalidad exige que el valor de un objetivo militar se sopese contra la pérdida de vidas y los daños causados por una acción militar.[38] Las operaciones de información ayudan a satisfacer las demandas para cumplir con este principio. El principio de discriminación, por su parte, exige que los blancos que se ataquen posean un valor militar y que su carácter no sea exclusivamente civil.[39] En vista de que las capacidades de las operaciones de información no provocan directamente la pérdida de vidas o daños a la infraestructura y, según se arguye, tampoco lo hacen los efectos de segundo o tercer orden, el precepto de este principio queda satisfecho. Asimismo, la "humanidad", como uno de los principios de *jus in bello*, requiere la mitigación del sufrimiento humano durante la guerra.[40] Nuevamente, las operaciones de información pueden traducirse en resultados más morales.

Conclusión

Las capacidades principales de las operaciones de información militar pueden disuadir el conflicto armado tanto con posibles adversarios estatales como los no estatales. Los resultados

de las medidas que EUA adopte para disuadir a un posible adversario de tomar un curso de acción o una política desfavorable para los intereses de EUA, y no las armas empleadas, constituirán la manera en que tanto la comunidad internacional como la nacional juzguen a Estados Unidos. La habilidad de justificar el uso de las operaciones de información de ofensiva como algo prudente, desde el punto de vista moral, contribuirá, considerablemente, a que la comunidad internacional acepte el uso de las operaciones de información no constituye el uso de la fuerza en el sentido tradicional.[42]

Mientras mejor se comprenda el uso de las operaciones de información para fines de disuasión, habrá más líderes estadounidenses encargados de formular las políticas o militares que estén de acuerdo en que las operaciones de información militar…

Actualmente, los líderes estadounidenses encargados de formular políticas o líderes militares tienden a ceñirse a una restricción operacional que procura minimizar las bajas, especialmente entre las fuerzas estadounidenses y la población civil afectada.[43] Claro está que, las operaciones de información con características no letales y no cinéticas satisfacen esta restricción operacional y ofrecen una justificación para las operaciones de información de ofensiva. Mientras mejor se comprenda el uso de las operaciones de información para fines de disuasión, habrá más líderes estadounidenses encargados de formular las políticas o militares que estén de acuerdo en que las operaciones de información militar, realizadas de forma ofensiva en la primera fase, lograran los efectos disuasivos con el menor número de muertes y con un mínimo de pérdidas infraestructurales. Entonces y sólo entonces aceptará la nación el valor de las operaciones de información lo suficiente para permitir su aporte pleno a la seguridad nacional como elementos disuasivos.[44]

El uso de las operaciones de información como una medida de disuasión de conflictos armados es considerablemente prometedor tanto para los líderes políticos como militares. Sin embargo, actualmente el país carece de la voluntad política y de ciertos factores facilitadores para permitir operaciones de información de ofensiva como una opción de fuerza en la primera fase al momento de procurar lograr una meta estratégica.

Los cinco factores facilitadores que se presentan a continuación apoyarían las operaciones de información ofensivas en la primera fase. De ser aceptados e implementados de manera conjunta, ofrecen una verdadera esperanza para el progreso.

- Ampliar la doctrina de las Publicaciones Conjuntas 3-0 y 3-13 para especificar que el uso de las operaciones de información de ofensiva en la primera fase de las operaciones conjuntas constituye lo que vendría a ser una primera opción para un comandante combatiente. La doctrina podría especificar un enfrentamiento concentrado de las operaciones de información como el uso culminante en la primera fase, un último esfuerzo conjunto para obligar a un posible adversario a ceder ante la presión de disuasión de EUA, o como elemento precursor para las operaciones favorables en la segunda fase.
- Establecer las operaciones de información como una capacidad fundamental en todos los comandos combatientes.[45] A fin de hacerlo, se necesitarán nuevos armamentos, técnicamente superiores, de las operaciones de información, junto con una adecuada estructura de fuerza para incorporarlos. Hay muy pocos recursos disponibles, tanto de armas como de personal, para apoyar a todos los comandos combatientes en relación con todo enfrentamiento simultáneo o focalizar adecuadamente los "fuegos" de las operaciones de información en las cantidades necesarias para obtener la eficacia. Se debe establecer una sección conjunta de desarrollo y adquisición, destinados a la exploración, desarrollo y entrega de sistemas de armamentos técnicamente superiores de las operaciones de información en cantidades suficientes para el uso en ambientes aéreos, terrestres y navales. Además, es necesaria una estructura de

fuerza conjunta que proporcione a cada Comando Combatiente Geográfico, Comando de Operaciones Especiales y Comando Estratégico de EUA una organización de apoyo directo. Cada una de estas organizaciones podría ejecutar operaciones de información con capacidades orgánicas o adjuntas.

- Abordar temas básicos relacionados con la preparación de la zona de combate para apoyar las operaciones de información de ofensiva en directivas, políticas y doctrina.[46] Es indispensable emitir una directiva presidencial a la comunidad de inteligencia que ordene una preparación de inteligencia activa y dinámica de la zona de combate contra todos los adversarios posibles a fin de obtener acceso a los nodos esenciales de información de dicho adversario para apoyar las operaciones de información de ofensiva. El proceso de obtener acceso a un blanco sigiloso de las operaciones de información es demasiado lento y molesto, sumamente politizado y sólo favorece al proceso de inteligencia en lugar de a la necesidad operacional.

- Facultar a los comandantes combatientes para que puedan ejecutar las operaciones de información ofensivas imprescindibles para asegurar que sean una opción de disuasión para la fuerza. Debe establecerse una política integral que ordene que todas las capacidades actuales de las operaciones de información y las estructuras de fuerza de apoyo puedan ser utilizadas por comandante combatiente en apoyo de las operaciones de disuasión. Unas pruebas específicas deben establecer los criterios que dicten las condiciones permisibles para el uso de las operaciones de información en la primera fase.

- Hacer un llamado al gobierno de EUA para que utilice las operaciones de información a fin de lograr las metas de nacionales estratégicas y proteger los intereses nacionales. A menos que exista la voluntad política para usar las operaciones de información en la primera fase para disuadir a un posible adversario, es probable que ocurra el conflicto armado, con sus muertes concomitantes y gastos de recursos.***MR***

REFERENCIAS BIBLIOGRÁFICAS

1. El Estado Mayor Conjunto (JCS), Joint Publication (JP) 3-13, *Information Operations*, (Washington, DC: U.S. Government Printing Office [GPO], 13 de febrero de 2006), págs. 1-12.
2. Miller, Earl E., *Army Transformation and Information Operations: The International Legal Implications* (Strategy Research Project, Carlisle Barracks, Pensilvania: U.S. Army War College, 9 de abril de 2002), págs. 8-9.
3. Armistead, Leigh, (ed.) *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc., 2004), p. 16.
4. JCS, Joint Publication 3-51, *Joint Doctrine for Electronic Warfare* (Washington, DC: GPO, 7 de abril de 2000), p. vii.
5. *Ibíd.*, p. 1-2.
6. JCS, *Information Operations*, p. II-6.
7. *Ibíd*.
8. Williamson, Jennie M. *Information Operations: Computer Network Attack in the 21st Century* (Strategy Research Project, Carlisle Barracks, Pensilvania: U.S. Army War College, 9 de abril de 2002), p. 9.
9. JCS, JP 3-53, *Joint Doctrine for Psychological Warfare* (Washington, DC: GPO, 5 de septiembre de 2003), p. ix.
10. *Ibíd*., p. x.
11. *Ibíd*., p. xii.
12. JCS, JP 3-58, *Joint Doctrine for Military Deception* (Washington, DC: GPO, 31 de mayo de 1996), págs. v-vi.
13. JCS, JP 3-54, *Joint Doctrine for Operations Security* (Washington, DC: GPO, 24 de enero de 1997), págs. v-vi.
14. *Ibíd*., p. I-4.
15. JCS, *Information Operations*, págs. II-7–II-10.
16. JCS, *Information Operations*, págs. II-10–II-13.
17. Barnett, Roger W., "Information Operations, Deterrence, and the Use of Force", *Naval War College Review* (primavera de 1998): p. 1.
18. Guevin, Paul R., "Information Operations", *Air and Space Power Journal* 18, nro. 2 (verano de 2004): p. 122.
19. El Departamento de Defensa (DOD), *The National Defense Strategy of the United States of America* (Washington, DC: GPO, marzo de 2005), p. iv.
20. *Ibíd*.
21. Fredericks, Brian E., "Information Warfare at the Crossroads", *Joint Force Quarterly* (verano de 1997): p. 100.
22. *Ibíd*., p. 98.
23. DOD, *Joint Operations Concepts* (Washington, DC: GPO, noviembre de 2003), p. 19.
24. Tulak, Arthur N., "Information Operations in Support of Demonstrations and Shows of Force", *Military Intelligence Professional Bulletin* 29, nro. 3 (julio-septiembre de 2003): p. 10.
25. Grange, David L.; Kelley, James A., "Information Operations for the Ground Commander", *Military Review* (marzo-abril de 1997): p. 9.
26. JCS, JP 3-0, *Doctrine for Joint Operations* (Washington, DC: GPO, 10 de septiembre de 2001), p. IV-2.
27. Rhodes, J.E., "A Concept for Information Operations", *Marine Corps Gazette* 82, nro. 8 (agosto de 1998): p. 48.
28. Armistead, Leigh, (ed.), p. 21.
29. Murphy, Dennis M., "Information Operations on the Non-traditional Battlefield", *Military Review* (noviembre-diciembre de 1996): p. 18.
30. Lawlor, Maryann, "Information Operations Specialists Move to the Mission Planners' Table", *Signal* (diciembre de 2005): p. 47.
31. Gonzales, Richard L.; Romanych, Marc J., "Nonlethal Targeting Revisited", *Field Artillery Journal* (mayo-junio de 2001): págs. 6-8.
32. Grohoski, David C.; Seybert, Steven M.; Romanych, Marc J., "Measures of Effectiveness in the Information Environment", *Military Intelligence Professional Bulletin* 29, nro. 3 (julio-septiembre de 2003): págs. 12-14.
33. Dicenso, David J. "Information Operations: An Act of War?" *Law Technology* 33, nro. 2 (2º Trimestre de 2002): p. 28.
34. Miller, p. 14.
35. *Ibíd*., p. 29.
36. Barnett, p. 6.
37. Dicenso, p. 31.
38. *Ibíd*.
39. *Ibíd*.
40. *Ibíd*.
41. Miller, p. 11.
42. Barnett, p. 7.
43. *Ibíd*., p. 5.
44. *Ibíd*., p. 1.
45. Myers, Richard B., "Shift to a Global Perspective", *Naval War College Review* 56, nro. 4 (otoño de 2003): p. 11.
46. Jajko, Walter. "A Critical Commentary on the Department of Defense Authorities for Information Operations", *Comparative Strategy* 21 (2002): p. 111.