Las operaciones de información multidominio y el equipo de combate de brigada

Lecciones aprendidas del ejercicio Cyber Blitz 2018

Mayor John P. Rodriguez, Ejército de EUA

Las operaciones multidominio son el nuevo concepto del Ejército para el combate en el futuro, pero, ¿qué significa esto para los equipos de combate de brigada (BCT)? En el ejercicio Cyber Blitz 2018, se intentó contestar esta pregunta con un enfoque en la identificación de cómo un BCT integra las operaciones en el ciberespacio, la guerra electrónica (EW), inteligencia y operaciones de información (IO) para llevar a cabo las operaciones en múltiples dominios, el espectro electromagnético (EMS) y el entorno de información contra un adversario regional[1]. El Cyber Blitz demostró el potencial de las operaciones multidominio en el nivel de BCT. Sin embargo, también demostró que el Ejército debe garantizar la doctrina y organización de personal para aprovechar todos los beneficios de las operaciones multidominio. La brecha percibida entre las IO y las actividades cibernéticas y electromagnéticas (CEMA) es un gran problema que no ha sido resuelto. Muchos participantes no aceptaron el punto de vista doctrinal de que las IO funcionan como el integrador y sincronizador de las capacidades relacionadas con la información (IRC), incluyendo las CEMA, para afectar la toma de decisiones de un adversario. Un enfoque estrecho en las CEMA y una opinión limitada de las IO podrían incrementar el flujo de información canalizado e impedir la sincronización de las operaciones multidominio. Una solución para hacer más eficaces las operaciones multidominio es restaurar la posición del oficial de IO en la plana mayor de la brigada y prestar más atención al papel de las IO como integrador en el nivel de brigada.

Las operaciones multidominio

En *The U.S. Army in Multi-Domain Operations 2028*, publicado 6 de diciembre de 2018, se describe el concepto del Ejército para ganar las guerras futuras contra adversarios casi iguales[2]. Según la «Summary of the 2018 National Defense Strategy», la fuerza conjunta enfrenta un ambiente de seguridad más complejo «definido por cambios tecnológicos rápidos [y] desafíos presentados por adversarios en todos los dominios operacionales»[3]. El general Joseph Dunford, presidente de la Junta de Jefes de Estado Mayor Conjunto, escribió que «la ventaja competitiva que las Fuerzas Armadas de EUA han disfrutado desde hace mucho se ha erosionado» porque los adversarios se han adaptado y pueden contrarrestar las capacidades de EUA[4]. El concepto central de las operaciones multidominio es que las formaciones del Ejército, como parte de la fuerza conjunta, deben ser capaces de luchar en todos los dominios (terrestre, marítimo, aéreo, espacio y ciberespacio), el espectro electromagnético y el entorno de información. Debido a limitaciones de recursos y adversarios más peligrosos, las formaciones del Ejército deben maximizar todas las capacidades, sincronizar las operaciones en todos los dominios y concentrar sus fuerzas en el punto decisivo para ganar las batallas futuras.

El Ejército debe desplegar formaciones en varios escalones que son capaces de operar en múltiples dominios. El Ejército no puede permitir que la convergencia multidominio ocurra solo en el nivel de cuerpo de ejército o por encima. Las unidades de maniobra de propósito general del Ejército también deben ser capaces de luchar en múltiples dominios para triunfar contra amenazas casi iguales. Incluso si los escalones superiores retienen el control de algunos medios de nivel nacional, capacidades multidominio específicas deben estar disponibles en los niveles inferiores. De aún más importancia, las unidades en el nivel táctico deben pensar en términos multidominio para planificar el apoyo externo tal como los BCT incorporan los medios aéreos en su planificación.

El Cyber Blitz 2018

A través del Cyber Blitz, que es una serie de experimentos dirigidos por el Centro de Investigación, Desarrollo e Ingeniería de Comunicaciones-Electrónica (CERDEC) y el Centro de Excelencia Cibernético, el Ejército está ejecutando operaciones multidominio en el nivel táctico. Esos experimentos ayudan al Ejército a determinar cómo emplear las CEMA e IO en todo el espectro de la doctrina, organización, adiestramiento, materiales, liderazgo y educación, personal,

Página anterior: Un soldado participa en el Cyber Blitz 2018, 21 de septiembre de 2018, en la base conjunta McGuire-Dix-Lakehurst, New Jersey. El ejercicio Cyber Blitz proporcionó datos al Ejército sobre cómo emplear las cambiantes actividades cibernéticas y electromagnéticas y operaciones de información en las operaciones multidominio. En un ambiente de entrenamiento para tomar la acción decisiva, la serie de experimentos analizó cómo la integración de las operaciones ciberespaciales, de guerra electrónica, inteligencia, espacio e información podría ayudar a un equipo de combate de brigada a lograr y mantener la ventaja contra un adversario casi igual. (Foto: Steven Stover)

instalaciones y políticas del Ejército[5]. El CERDEC llevó a cabo el Cyber Blitz 2018 en Fort Dix, New Jersey, durante tres semanas en septiembre de 2018.

En el ejercicio, se adaptó el ambiente de entrenamiento de acción decisiva que se usa en otros ambientes de adiestramiento del Ejército. Los integrantes del CERDEC modificaron el escenario para aumentar las capacidades de ciberespacio y guerra electrónica del adversario y también lo adaptaron a las características del terreno de Fort Dix. Se diseñó el escenario como si fuera el año 2025 para probar tecnologías emergentes, con algunas todavía en fase de investigación y desarrollo, y experimentar con algunas actualizaciones al diseño de la fuerza y delegación de autoridad. El experimento tuvo lugar en la nación amiga de Atropia, que estaba sufriendo una insurgencia separatista. Ariana, un país vecino, apoyaba a los separatistas y amenazaba con una intervención de fuerzas convencionales. La mayoría de los participantes estaban familiarizados con el escenario de acción decisiva en el ambiente de entrenamiento, lo que les permitió centrarse en los aspectos de CEMA e IO del escenario durante el Cyber Blitz.

El 3er Equipo de Combate de Brigada (Patriot) de la 10ª División de Montaña proporcionó el núcleo de fuerzas para el ejercicio Cyber Blitz. La brigada formó un pelotón orgánico de guerra electrónica consolidando el personal de esta especialidad en toda la brigada para probar una modificación en el diseño de fuerzas. Otros integrantes de la brigada se incorporaron a la plana mayor de transmisiones y al pelotón de guerra electrónica. Un oficial de IO y un planificador de ciberespacio también se incorporaron a la plana mayor de la brigada.

Un equipo cibernético expedicionario (ECT), que contaba con personal de operaciones de ciberespacio ofensivas (OCO) y defensivas, así como un planificador de IO, fue quién más apoyo brindó a la brigada de forma externa. Este equipo podía realizar operaciones remotas y reconocimiento de blancos próximos. La división retuvo el control operacional del ECT durante el experimento. Sin embargo, la brigada podía solicitar efectos de ciberespacio del ECT a través de la división. El ECT realizó múltiples misiones para la división y la brigada durante el ejercicio.

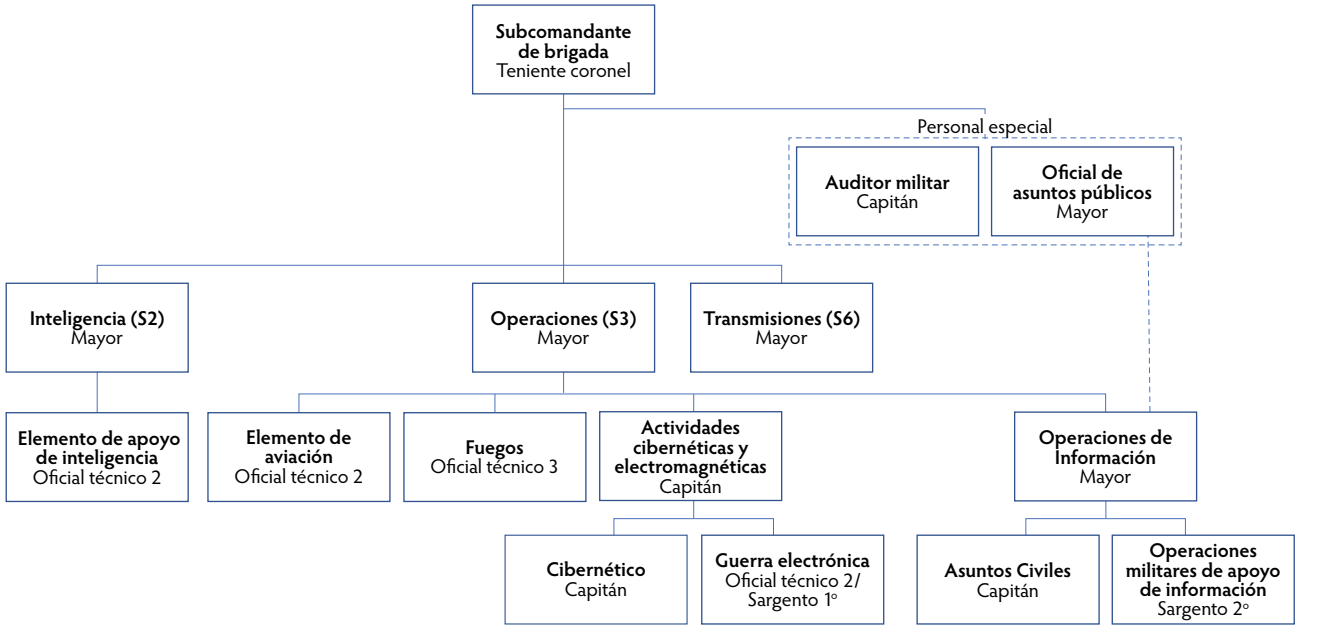
El experimento prácticamente simuló las fuerzas de maniobra mientras llevaba a cabo las actividades de CEMA en vivo con simulaciones suplementarias. El ECT realizó las operaciones de ciberespacio en vivo contra redes que simulaban internet global y la Red Secreta de Enrutador de Protocolo de Internet (Secret Internet Protocol Router Network). El CERDEC estableció emisores que simulaban emisiones enemigas, amigas y neutrales en varios polígonos de Fort Dix. Esto permitió a los equipos de guerra electrónica detectar, clasificar, localizar y causar interferencia en una variedad de señales.

La misión de la brigada era asegurar el área de operaciones (AO) y derrotar a las fuerzas convencionales del enemigo para proteger el AO de una unidad adyacente[6]. El esquema de maniobra de la brigada comenzó con un asalto aéreo para tomar control de un aeródromo y fue seguido por la concentración de potencia de combate por medio de entrega aérea. Luego, la brigada planeó asegurar la infraestructura clave en el sector y establecer medidas defensivas.

Los planificadores del experimento dictaron el esquema de maniobra y la plana mayor no tuvo que llevar a cabo la planificación detallada de los movimientos de los batallones de maniobra. Estos factores simplificaron la labor de la plana mayor, lo cual le permitió concentrarse en la integración de las actividades cibernéticas y electromagnéticas en el plan de maniobra. La brigada también planificó defenderse de las operaciones multidominio del enemigo. La plana mayor de la brigada llevó a cabo un proceso breve de toma de decisiones militares durante la primera semana del ejercicio Cyber Blitz. El subcomandante de la brigada ordenó a la plana mayor incluir las CEMA e IO tanto como fuera posible.

La brigada contó con múltiples IRC, pero la organización de la plana mayor dividió las IRC entre varias secciones (véase la figura). La oficial de guerra electrónica de la brigada, una capitana, sirvió en calidad de jefe de las CEMA de la brigada, y un oficial técnico y un sargento primero con la

El mayor John P. Rodriguez, Ejército de EUA, es un oficial de operaciones de información asignado a la División de Planes y Política, Dirección de Inteligencia del Estado Mayor Conjunto de la Guardia Nacional del Estado de Maryland. Recibió su licenciatura de Mount Saint Mary's University y una maestría de Georgetown University. Sirvió como el director de las operaciones de información de la Fuerza de Tarea Conjunta Combinada–Cuerno de África de 2017 a 2018 y participó en el ejercicio Cyber Blitz 2018.



(Figura por el autor)

Figura. Organización del cuartel general de brigada en el Cyber Blitz

misma especialidad la apoyaron. El planificador de ciberespacio agregado a la brigada nominalmente trabajó por el jefe de las CEMA. El mayor de IO agregado encabezó una sección de IO distinta que incluía un capitán de asuntos civiles (CA) y un sargento primero de operaciones psicológicas (PSYOP), que respectivamente planificaron las operaciones para los elementos de CA y PSYOP agregados, en teoría, a la brigada. El oficial de asuntos públicos de la brigada también era parte de la sección de IO para fines prácticos. Además, la sección de IO asumió la responsabilidad por la planificación de decepción y seguridad operacional (OPSEC).

Dividir las IRC en dos secciones hizo la integración más difícil. La brigada consideraba la sección de IO y la de CEMA como dos entidades distintas, pero iguales. Esto significó que las acciones de CEMA e IO solo convergieron en el nivel del oficial de operaciones de la brigada (S-3), creando una situación para que floreciera la planificación fragmentada e inconexa. Por lo tanto, el oficial de IO trabajó mediante el S-3 para desarrollar conceptos IO de apoyo generales para integrarlos con los esfuerzos de CEMA en las IRC. Afortunadamente para el S-3, el carácter del Cyber Blitz, con su esquema de maniobra dictado, le permitió tiempo suficiente para centrarse en la integración de las CEMA y otras IRC en el plan. El oficial de IO también pudo influenciar la sección de CEMA debido a su grado y experiencia a pesar de la falta de autoridad formal sobre la sección.

Las operaciones de información en el Cyber Blitz

La brigada integró y sincronizó las IRC con éxito para apoyar su esquema de maniobra durante el Cyber Blitz. Más allá de apoyar individualmente el esquema de maniobra, las IRC de la brigada frecuentemente trabajaron conjuntamente para lograr la sinergia. En una fase temprana de la operación, las IRC se centraron en el apoyo de un asalto aéreo. Más tarde, cuando el enemigo lanzó un potente ataque con fuerzas convencionales e insurgentes, una respuesta preconcebida con múltiples capacidades relacionadas con la información demoró el ataque y perturbó las redes de comunicación del enemigo.

Al principio, las IO se centraron en el apoyo dado a la operación decisiva de la brigada, un asalto aéreo para tomar control de un aeródromo en el Objetivo Desoto, ubicado al este del área de operaciones. El subcomandante de la brigada quiso impedir que el enemigo concentrara la potencia de combate contra el asalto aéreo porque serían necesarios múltiples entregas aéreas para amasar la fuerza de asalto completa sobre el objetivo. El oficial de IO usó la OPSEC como la estructura para

sincronizar las IRC. El concepto general era proteger la sincronización de tiempo y lugar del asalto aéreo. Idealmente, estas acciones obligarían al enemigo a asignar desacertadamente sus fuerzas, pero como mínimo, la meta era interrumpir el proceso de la toma de decisiones del enemigo para impedir que concentrara su potencia de combate contra el asalto aéreo.

El concepto de IO tuvo dos fases superpuestas. La primera fase constó de una finta para hacerle creer al enemigo que el ataque principal amigo ocurriría al oeste del área de operaciones. Esto requirió múltiples elementos que se reforzaban mutuamente. Había un aeródromo justo fuera del límite occidental de la brigada que proporcionó un objetivo realista para la finta. También había zonas de aterrizaje adecuadas en las proximidades del objetivo falso. Las fuerzas de EW, PSYOP y OCO apoyaron la finta. Además de interrumpir las comunicaciones enemigas, las OCO transmitieron mensajes de operaciones de apoyo de información militar (MISO). Esto permitió que las fuerzas de PSYOP influenciaran audiencias objetivos más amplias y reforzaran los mensajes tipo MISO transmitidos con otros medios. La finta no relevaba el lugar exacto donde ocurriría el ataque, sino que presentaba varios elementos que sugerían la zona de aterrizaje falsa como el objetivo real. El planificador de las PSYOP también intentó usar las plataformas de guerra electrónica para enviar los mensajes MISO que, al principio, no tuvieron éxito. En una fase subsecuente del experimento, las fuerzas de EW y PSYOP superaron estos obstáculos y diseminaron mensajes MISO con las capacidades de EW. Las fuerzas de EW también proporcionaron efectos en el EMS para producir características electromagnéticas consistentes con un asalto aéreo y degradar los medios de recolección de información y enlaces de comunicación del enemigo que podrían revelar o proporcionar información sobre la finta.

La segunda fase constó de apoyo directo para el verdadero asalto aéreo. Los medios de EW y OCO intentaron interrumpir el mando y control del enemigo en el objetivo y a lo largo del corredor aéreo. Se superpusieron los efectos para proporcionar capacidades redundantes. Esto resultó afortunado porque algunas capacidades no pudieron lograr los efectos deseados. No obstante, la plana mayor rápidamente comunicó este contratiempo y otros medios lograron los efectos deseados. La fuerza de asalto concluyó el ataque sin contratiempos.

El enemigo comenzó un ataque multidominio durante una fase subsecuente de la operación que puso estrés en las defensas de la brigada. El enemigo empezó ataques insurgentes y levantamientos populares cuando una de sus brigadas motorizadas de fusileros comenzó a avanzar. Los sistemas aéreos no tripulados y plataformas de ataque electrónico del enemigo apoyaron el avance y degradaron el mando tipo misión amigo. El enemigo también intentó interrumpir la infraestructura crítica con las OCO. Esto presentó múltiples dilemas para la brigada. La situación se hizo grave cuando las OCO del enemigo penetraron la red de la brigada mientras las fuerzas enemigas ponían presión sobre la línea avanzada de reconocimiento y observación de la brigada.

La brigada ejecutó un contraataque preconcebido con capacidades de IO para demorar el avance enemigo. Estas acciones permitieron que el personal de transmisiones reestableciera la red y los batallones de infantería finalizaran la preparación de sus posiciones defensivas. El contraataque comenzó con las OCO contra las redes de mando tipo misión enemigas. Las OCO corrompieron la integridad de los sistemas enemigos y transmitieron mensajes tipo MISO. La fricción producida en la toma de decisiones del enemigo y la confusión provocó que el enemigo cometiera errores. Los elementos de PSYOP aprovecharon los errores del enemigo con más mensajes MISO para degradar su cohesión e incrementar las divisiones entre las fuerzas convencionales e insurgentes enemigas. Los elementos de OCO continuaron atacando la red de mando tipo misión y transmitiendo mensajes MISO durante el resto del combate.

Lecciones aprendidas de las operaciones de información en el Cyber Blitz 2018: Lo bueno

Las dos lecciones más importantes del Cyber Blitz 2018 son la importancia de las operaciones de información para llevar a cabo las operaciones multidominio a nivel de BCT y cómo un punto de vista anticuado de las IO impide las operaciones multidominio unificadas. Las operaciones de la brigada fueron muchos más eficaces porque la plana mayor integró y sincronizó todas las IRC disponibles para perturbar la toma de decisiones enemiga. La BCT enfrentó una amenaza multidominio durante todo el Cyber Blitz y respondió

de manera multidominio. La brigada fue rápida porque pudo planificar y ejecutar las operaciones sin siempre depender de apoyo externo. Sin embargo, este éxito ocurrió a pesar de la organización de la plana mayor y la elaboración del papel de las IO en el experimento.

Durante el asalto aéreo, el concepto de apoyo de IO sirvió para proporcionar la unidad de esfuerzos en todas las IRC que permitió que la brigada concentrara los efectos. La metodología de IO garantizó que se llevaran a cabo las IRC en apoyo mutuo y se identificaran las oportunidades para que las IRC colaboraran entre sí, tales como los elementos de OCO y la transmisión de mensajes tipo MISO. Esto presentó al enemigo un desafío más complejo e impidió un empleo fragmentado de las IRC. La finta presentó múltiples elementos observables, incluso el EMS y redes sociales, en los que se seleccionaron distintos canales disponibles a los decisores del enemigo. Era más probable que la finta convenciera a los decisores porque se usaron diversos elementos observables.

El contraataque de la brigada creó más fricción para el enemigo porque combinó las OCO y PSYOP. Un ataque solo con las OCO contra las redes de mando y control del enemigo hubiera tenido efectos limitados porque hubiera sido una sola ejecución. En cambio, las acciones de la brigada continuaron durante el resto del combate mientras las OCO continuaron la entrega de mensajes tipo MISO. Más ejecuciones de MISO, no exclusivamente transmitidas por la OCO, prolongaron la duración de los efectos y aprovecharon cada oportunidad presentada por los errores enemigos. Además, este contraataque fue crítico porque ocurrió en un punto decisivo del combate. La brigada identificó la red de mando tipo misión del enemigo como un blanco de alto valor durante el análisis de la misión y el ECT obtuvo acceso muy pronto después de que comenzara el combate. El subcomandante de la brigada mantuvo esta capacidad en reserva para poder usarla para obtener los mejores resultados. Su paciencia conllevó riesgos porque el ECT pudo perder el acceso en el intermedio, pero en este caso, dio resultados.

Lo malo

El obstáculo más grande para llevar a cabo las IO eficaces en el ejercicio Cyber Blitz fue que muchos participantes y observadores no adoptaron la definición doctrinal de las IO. En la Publicación Conjunta 3-13, se definen las operaciones de información como «el uso integrado, en las operaciones militares, de capacidades relacionadas con la información en consonancia con otras líneas de operaciones para influenciar, desestabilizar, corromper o usurpar la toma de decisiones de adversarios o posibles adversarios mientras se protege nuestra toma de decisiones»[7]. Muchas unidades no consideraron las IO como una función generalizada que integró todas las IRC incluso las CEMA. En cambio, se trataron las IO como un elemento distinto de las CEMA. Si bien el nuevo concepto de operaciones multidominio aboga por cambiar las IO a las operaciones en el ambiente de información, todavía sigue haciendo hincapié en el papel de las IO/operaciones en el ambiente de información para sincronizar las IRC a fin de lograr efectos[8].

La elaboración del experimento reforzó la separación entre las CEMA y las IO. El planteamiento del problema para el experimento fue «¿cómo un IBCT con apoyo externo en 2025 integra las operaciones de ciberespacio, guerra electrónica, inteligencia, espacio e información para lograr y mantener la ventaja en las operaciones multidominio contra un adversario regional casi igual?»[9]. La jefatura de la brigada tenía poca experiencia en las IO o CEMA, por lo que esta pregunta determinó cómo el grupo abordaría la tarea. Su primera inclinación fue preguntar cómo las operaciones de ciberespacio, guerra electrónica y IO podían apoyar las distintas fases de la operación. Este planteamiento aumenta el riesgo de metodologías inconexas que no concentran los efectos en el enemigo.

Parecía que muchos participantes pensaban que las IO solo se centraban en temas y mensajes. Esto lleva a empujar al personal a concentrarse en las redes sociales e información públicamente disponible que, aunque importantes, no son los únicos espacios donde las IO deben ser usadas. El antiguo concepto de actividades de información e influencia, en el cual específicamente se mencionaron temas y mensajes en su definición, podría explicar esta creencia[10]. Este es un planteamiento muy centrado en humanos que saca conclusiones de los últimos diecisiete años de operaciones de contrainsurgencia. Pero las IO también deben centrarse en las redes de mando tipo misión enemigas mientras la fuerza conjunta se enfoca más en la competición de grandes poderes.

El mayor Alex J. Duffy (der.), oficial de operaciones del 3er Equipo de Combate de Brigada de la 10ª División de Montaña y el capitán Jacob M. Allen, el segundo jefe de operaciones, usan un mapa superpuesto con gráficas operacionales para apoyar los sistemas digitales de mando tipo misión y proporcionar la redundancia, 17 de septiembre de 2018, durante el ejercicio Cyber Blitz 2018 en la base conjunta McGuire-Dix-Lakehurst, New Jersey. Este método alternativo se convirtió en el medio principal para seguir el combate temporalmente cuando un ciberataque desactivó los sistemas. (Foto: U.S. Army Communications-Electronics Research, Development and Engineering Center)

Subestimar el rol que juegan las IO significa que la responsabilidad de integrar las IRC recae sobre el S-3 si el oficial de IO no está autorizado a hacerlo. En el Cyber Blitz, la organización de la plana mayor significó que el S-3 estaba oficialmente cumpliendo las tareas principales del oficial de IO para integrar y sincronizar las IRC. Si el experimento no hubiera dictado el esquema de maniobra, el requerimiento de coordinar los fuegos tradicionales y la maniobra junto con las IRC probablemente habría abrumado al S-3. Esto degradaría la sinergia y resultaría en efectos reducidos sobre el enemigo. Sin embargo, incluso si los líderes del Ejército adoptan un papel más extenso de la función de IO, el S-3 todavía será el integrador, puesto que el Ejército ya no autoriza un oficial de IO en la plana mayor de brigada.

El camino hacia el futuro

Las operaciones multidominio llevadas a cabo por la brigada hubieran sido mucho menos exitosas sin el oficial de IO agregado. Aunque en el Cyber Blitz el S-3 tuvo más ancho de banda de lo usual para centrarse en la integración de las IRC, el S-3 no puede reemplazar a un oficial de IO adiestrado. La perspectiva de un oficial de IO sobre los temas relacionados lo llevó a superar la compartamentalización entre las IRC. Los

planificadores de las operaciones en el ciberespacio y de guerra electrónica estaban muy ocupados y centrados en la planificación detallada de sus esfuerzos individuales. La EW y OCO exitosas requieren este enfoque pero también es impráctico anticipar que los planificadores vayan a desarrollar un plan holístico de IO para apoyar el esquema de maniobra. Sin embargo, la brigada habría perdido muchas oportunidades para multiplicar los efectos de sus operaciones sin un concepto unificado. El oficial de IO también garantizó la incorporación de la OPSEC y decepción en la planificación. Estas son IRC críticas y pueden ser buenas metodologías para elaborar un plan de IO integrado.

El Ejército debería considerar reestablecer la posición de un oficial de IO en los BCT. Mientras las brigadas adquieran más IRC e incrementen las operaciones ciberespaciales en apoyo de escalones inferiores a cuerpo de ejército, mayor será la necesidad de un planificador de IO en un BCT. Asignar un oficial de IO, entrenado en la OPSEC y decepción, también garantizará la integración de estas capacidades en las operaciones. Un BCT que no elabora planes para la OPSEC multidominio será cada vez más vulnerable contra adversarios casi iguales con capacidades de información avanzadas.

Un oficial de IO de división, o uno en un ECT, no puede sustituir a un oficial de IO a nivel de brigada. Lo ideal es incorporar las IO en los procesos de la toma de decisiones militares desde el principio y la mejor manera sería tener un oficial de IO en la plana mayor. Es probable que un oficial de IO a nivel de división solo tenga la oportunidad de aportar nuevas ideas tarde en el proceso de la toma de decisiones cuando el curso de acciones ya fue establecido. De manera similar, el planificador de IO en el ECT no pudo influenciar los planes del BCT durante el Cyber Blitz. El mando tipo misión depende de la confianza para aumentar el ritmo de la toma de decisiones y garantizar que aprovechamos y retenemos la iniciativa. Lamentablemente, es muy difícil para una jefatura de brigada confiar en un planificador fuera de la organización, especialmente si usan capacidades nunca antes vistas por la jefatura.

Un oficial de IO debe liderar una sección de guerra de información consolidada dentro de la sección S-3 de la plana mayor. La sección de guerra de información podría planificar las operaciones ciberespaciales, de EW, MISO, OPSEC y decepción. En lugar de una sección de CEMA distinta, una sección de IO consolida los planificadores de IRC bajo el mando de un solo oficial de grado superior que da informes directamente a la sección S-3. El oficial de asuntos públicos de la brigada es una excepción y debe seguir siendo integrante de la plana mayor especial para mantener su credibilidad con los medios de prensa y el público. La Fuerza de Tarea Conjunta Combinada–Cuerno de África usó exitosamente una organización de plana mayor similar con todas las IRC principales, incluso las CEMA, en la dirección de IO, salvo los asuntos civiles y asuntos públicos. Esto aumentó considerable la unidad de esfuerzos.

Si las limitaciones de mano de obra impiden la asignación de un oficial de IO en el servicio activo, otra solución podría ser la asignación de oficiales de IO del Componente de Reserva del Ejército o la Guardia Nacional a los BCT. Los reservistas podrían suplementar los BCT en sus despliegues. Esto mitigaría la tendencia de emplear ineficazmente a los planificadores con cargos adicionales no relacionados con las IO en la guarnición. En el mejor de los casos, los reservistas también apoyarían los BCT en las rotaciones en el centro de apresto de combate además de los despliegues para que las unidades entrenen como combaten. Sin embargo, esta propuesta podría poner presión en los reservistas si tienen que apoyar regularmente rotaciones de un mes en duración en los centros de entrenamiento y al mismo tiempo asistir a muchas escuelas y apoyar numerosos ejercicios además de los despliegues normales. Depender de los reservistas para llenar el vacío podría poner más presión en la fuerza y ser impráctico.

Conclusión

El Ejército debe adoptar la función de integración de las operaciones de Información para institucionalizar el éxito de la Brigada Patriot en el ejercicio Cyber Blitz 2018. El Cyber Blitz demostró que, si bien se necesitan nuevo equipamiento y organizaciones para apoyar las operaciones multidominio de los BCT, sin la doctrina adecuada y organización de plana mayor, no se aprovecharán estas capacidades al máximo. También demostró cómo un oficial de IO en la plana mayor de brigada puede mejorar radicalmente la eficacia de la brigada. El Ejército no debe

aceptar el empleo fragmentado de las IRC ni una división entre las CEMA y la IO. Las Fuerzas Armadas de EUA «no tienen un derecho predestinado a la victoria», y debemos implacablemente perfeccionar nuestras capacidades para ganar los combates multidominio del futuro[11]. ■

Notas

1. Cyber Blitz Team, «Cyber Blitz 2018 (CB18) Distinguished Visitor Day» (presentación PowerPoint, Fort Dix, New Jersey, 26–27 de septiembre de 2018).

2. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Washington, DC: U.S. Government Publishing Office [GPO], 2018), accedido 21 de marzo de 2019, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

3. Office of the Secretary of Defense, «Summary of the 2018 National Defense Strategy of the United States of America» (Washington, DC: Department of Defense, 2018), accedido 21 de marzo de 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

4. Joseph Dunford, «Gen. Dunford: The Character of War & Strategic Landscape Have Changed», DoDLive, 30 de abril de 2018, accedido 21 de marzo de 2019, https://www.dodlive.mil/2018/04/30/dunford-the-character-of-war-strategic-landscape-have-changed/.

5. Steven Stover, «Cyber Blitz 2018 Gives ARCYBER Opportunity to Test New Concepts, Capabilities and Techniques», Defense Visual Information Distribution Service, 3 de octubre de 2018, accedido 21 de marzo de 2019, https://www.dvidshub.net/news/295282/cyber-blitz-2018-gives-arcyber-opportunity-test-new-concepts-capabilities-and-techniques.

6. Cyber Blitz Team, «Cyber Blitz 2018 (CB18) Distinguished Visitor Day».

7. Joint Publication 3-13, Information Operations (Washington, DC: U.S. Government Printing Office, 27 de noviembre de 2012).

8. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* GL-5. Las operaciones en el ambiente de información son definidas como «el uso integrado de capacidades relacionadas con la información (IRC) en colaboración con otras líneas de operaciones para influenciar, decepcionar, interrumpir, corromper o usurpar la toma de decisiones del enemigo y adversarios mientras se protege nuestra toma de decisiones; influenciar las formaciones y poblaciones enemigas para socavar su voluntad de luchar e influenciar poblaciones amigas y neutrales para permitir las operaciones amigas».

9. Cyber Blitz Team, «Cyber Blitz 2018 (CB18) Distinguished Visitor Day».

10. Field Manual 3-13, *Inform and Influence Activities* (Washington, DC: U.S. Government Printing Office, 2013 [obsoleto]). Actualizado como el Field Manual 3-13, *Information Operations* (Washington, DC: U.S. GPO, 2016).

11. OSD, «Summary of the 2018 National Defense Strategy».