Un equipo cibernético expedicionario incorporado desempeña una misión de vigilancia y reconocimiento de varias redes locales, 10 de agosto de 2016 en el Centro de Adiestramiento Nacional, Fuerte Irwin, estado de California. El equipo forma parte de un programa piloto conocido como Apoyo Cibernético de nivel Cuerpo e inferior, o CSCB, desarrollado para proporcionar a los comandantes de maniobra una concientización de la situación mejorada del ambiente de información y herramientas para moldear el ambiente. (Foto de David Vergun, Servicio de Noticias del Ejército.)

«Maneras más curiosas y sutiles de matar»

El proceso de operaciones en la guerra futura

Mayor Wesley Moerbe, Ejército de EUA

Lo tiene a voluntad/Maneras más curiosas y sutiles de matar.

— James Shirley, «El último conquistador»

El 13 de septiembre de 1862, en un vivac recientemente desocupado por soldados de la Confederación, un soldado de la Unión notó un sobre olvidado por el campamento anterior. El soldado lo abrió y encontró que, además de unos cigarros húmedos, había descubierto la Orden Especial 191, firmada por el ayudante auxiliar de Robert E. Lee. Como resultado, el conjunto de los planes operacionales de Lee para la siguiente campaña habían caído en manos del general de división George McClellan[1]. Aunque famosamente tímido en el campo, McClellan se las ingenió para encerrar a Lee y luchó contra él hasta llegar a un estancamiento sangriento en Antietam el 17 de septiembre, poniendo fin a la primera táctica del Ejército del Norte de Virginia en Maryland[2].

Pocos de nosotros hemos tenido que enfrentar a un enemigo que, sin nosotros saber, obtuvo acceso parcial o total a nuestros planes o proceso de planificación, pero nuestra dependencia en la tecnología de información renueva viejos desafíos del campo de batalla para planificar y ejecutar operaciones de manera secreta y confiable. La búsqueda diligente de la ventaja asimétrica de nuestros adversarios nos lleva —casi inevitablemente— a nuestra dependencia de redes de comunicación y sistemas interconectados[3]. El problema ahora va más allá de lanzar golpes cibernéticos para interrumpir la comunicación. El uso intensivo de las redes para la planificación colaborativa y los procesos de toma de decisiones también significa que nuestro proceso de operación en sí puede ser atacado a través del sistema del mando tipo misión. Por consiguiente, es verosímil que podamos sufrir nuestra propia crisis de la Orden Especial 191.

Precisamente, esa contingencia se desarrolló durante el Ejercicio de guerra de la 3ª División de infantería en octubre de 2016. La ciberguerra dejó de ser un problema futuro. La competencia por la supremacía en el dominio cibernético se convirtió en un desafío táctico y personal urgente para el Estado Mayor.

Las lecciones aprendidas de esos eventos requieren una integración en nuestro adiestramiento y preparación para futuros conflictos. Propongo que las soluciones tienen poco que ver con la tecnología y bastante que ver con la forma en que visualizamos y pensamos en el proceso de operaciones y el mando tipo misión como un sistema en la guerra futura.

El proceso de operaciones y los sistemas desconectados del mando tipo misión

Antes de continuar, la base doctrinal y teórica de la toma de decisión del Ejército de EUA merece ser explorada. En términos más sencillos, el dominio de las fuerzas terrestres de nuestro país requiere una iteración entre el pensamiento y la acción— un ciclo de acción, reacción, aprendizaje y adaptación[4]. Es fácil darlo por sentado, pero cómo nuestro Cuartel General introduce pensamientos abstractos en algo tangible es de gran importancia. A fin de comprender mejor esto, primero debemos desenredar las ideas y los procesos desde los objetos físicos que apoyan la colaboración o mejoran el pensamiento.

El uso del lenguaje

El uso del lenguaje impreciso puede infectar la manera en que pensamos sobre la toma de decisión y mando de nuestras fuerzas. En su estilo conciso, S. L. A. Marshall explica que en nuestra profesión, «si una palabra llega a significar demasiadas cosas, pierde el sentido en el punto crítico»[5]. En este caso, habló de las comunicaciones y opinó que esto se había convertido en algo común para el militar, es decir, tantas cosas que «con bastante frecuencia no significan nada»[6].

Los conceptos incluidos tanto en el sistema de mando tipo misión como en el proceso de operaciones sufren una pérdida de claridad similar en la actualidad. El Ejército depende del proceso de operaciones y sus actividades —planificación, preparación, ejecución y evaluación— como andamiaje cognitivo a través de todas las operaciones. Esto significa que como el marco conceptual para los ejercicios del mando tipo misión, los comandantes y sus Estados Mayores usan el proceso operacional para considerar qué deben hacer a fin de resolver los problemas tácticos y operacionales[7]. El «cómo» de este marco conceptual se exterioriza como el sistema de mando tipo misión, esos componentes de un cuartel general de una unidad que la mayoría reconocería. El sistema de mando tipo misión consiste en personas, redes, sistemas de información, procesos y procedimientos e instalaciones[8]. Por lo tanto, algunos componentes son tangibles y otros teóricos.

Según la filosofía del mando tipo misión, este sistema se adapta al comandante, a su Estado Mayor y al ambiente[9]. Para ello, las relaciones entre estos componentes se ajustan a las personalidades, la naturaleza del conflicto y al ambiente. Parecido a muchos sistemas, si depende excesivamente de cualquier componente, se vuelve vulnerable porque es incapaz de «asimilar perturbaciones» y permanecer funcional[10].

Los componentes de los sistemas de mando tipo misión incluyen el aspecto abstracto y táctil con poca distinción entre los dos. Esto ayuda a explicar cómo algunos podrían equivocadamente mezclar los dos aspectos de los sistemas de mando tipo misión. Sin embargo, el error es más que semántico. El uso de un objeto físico para facilitar el esfuerzo intelectual no debe hacer creer que el objeto físico es un requisito para los procesos cognitivos. Si los integrantes del Estado Mayor combinan el producto, el proceso y las herramientas, dificultan su capacidad de reaccionar ante un ataque contra el sistema de mando tipo misión. Una consecuencia lógica e inevitable de tal confluencia es la parálisis de la toma de decisión ante la pérdida de redes o la capacidad de automatización. Nuestro Estado Mayor debe darse cuenta de que los cables, las computadoras portátiles y los servidores solo están diseñados para ayudar al pensamiento humano en las operaciones y que la planificación inteligente no comienza ni termina con tales facilitadores.

Durante mi propio servicio en un Estado Mayor de nivel división encontré que los líderes organizacionales (me incluyo) sienten un impulso de optimizar nuestro sistema de mando tipo misión para los ambientes de estabilización con un dominio cibernético no disputado. Ha requerido de disciplina y experiencia por parte de oficiales generales para eliminar tales hábitos. Carl von Clausewitz advirtió que un cierto método o rutina «fácilmente puede sobrevivir a la situación que lo originó; ya que las condiciones cambian imperceptiblemente»[11]. Sospecho que los hábitos desarrollados durante casi 15 años de

Un integrante del Equipo cibernético expedicionario proporciona protección a los operadores cibernéticos que se colocan en posiciones camufladas y ocultas para llevar a cabo vigilancia y reconocimiento, 10 de agosto de 2016 en el Centro de Adiestramiento Nacional, Fuerte Irwin, estado de California. Los equipos cibernéticos proveen a los comandantes de maniobra una concientización de la situación mejorada del ambiente de información y herramientas para moldear el ambiente. (Foto de David Vergun, Servicio de Noticias del Ejército)

operaciones de estabilización han creado expectativas poco realistas basadas en suposiciones no analizadas o anticuadas. La más peligrosa de estas suposiciones podría ser que las redes y los sistemas de información permanecerán relativamente libres de interferencia enemiga. Sin embargo, la evidencia indica que las intenciones y capacidades de los adversarios requerirán nuestro apresto para reconfigurar nuestro sistema de mando tipo misión debido, frecuentemente, a la acción enemiga. Los adversarios creen, al igual que algunos analistas occidentales, que las redes y los sistemas de información presentan tal vulnerabilidad[12].

La disminución de la seguridad de información

Conrad Crane comienza su artículo titulado «The Lure of Strike» diciendo, «hay dos enfoques para la guerra, asimétricas y estúpidas»[13]. Con este aforismo en mente, vale la pena detenerse un momento en los conceptos operativos de nuestros adversarios más capaces.

Los documentos de dominio público y la historia reciente muestran un patrón en que los militares, tanto rusos como chinos, intentan combinar métodos de guerra tradicionales y no tradicionales para socavar el consenso de que hay verdaderamente un estado de guerra, lo que crea ambigüedad en la naturaleza del mismo conflicto. Además, hace hincapié en una serie complementaria de operaciones entre los dominios destinadas a atacar las vulnerabilidades de EUA a un costo para ellos. De ello se desprende que el conflicto cibernético depende, en gran medida, de los conceptos operacionales de estos dos estados[14].

La ya ampliamente referida obra, *Unrestricted Warfare*, busca la combinación de una serie de maneras no tradicionales de guerra para ganar ventaja sobre Estados Unidos, lo que destaca la adicción a la tecnología sobre todo, las que tienen un efecto desproporcionado en las fuerzas occidentales[15]. En *Unrestricted Warfare* se destaca la simetría y los efectos sinérgicos, y critica severamente que la doctrina de EUA sea demasiado cinética y pierda un potencial más amplio en la guerra de información. Escrito en 1999 sin el respaldo del Ejército Popular de Liberación (PLA, por sus siglas en inglés), en este volumen se representan las teorías de dos coroneles chinos. Dicho esto, los patrones inequívocamente parecidos a la lógica conectan la obra *Unrestricted Warfare* a la obra de más autoridad *The Science of Military Strategy*[16]. El análisis occidental de este documento oficial del PLA señala que los chinos han priorizado la preparación para operar en redes degradadas o colapsadas, y sugiere que podrían infligir lo mismo a Estados Unidos[17]. Un estudio de 2015 de la corporación RAND concluyó que las publicaciones y los ejercicios del PLA ahora ordenan un primer ataque contra los sistemas y redes informáticas enemigas con la intención de «controlar el flujo de información» hacia y entre el enemigo[18].

En la doctrina rusa, el enfoque holístico enfatiza la guerra de información y el uso de medios no cinéticos a fin de dar forma al campo de batalla para el combate físico. Los rusos lo llaman *bespredel* y hace eco de los conceptos que sustentan la *Unrestricted Warfare*[19].

La reciente beligerancia de Rusia da prueba de su perspectiva sobre la ciberguerra. Durante su conflicto con Georgia en 2008, los hackers rusos deliberadamente atacaron las comunicaciones digitales militares, lo que retrasó la distribución de órdenes sembrando confusión entre los encargados de tomar decisiones[20]. En este enfoque, la combinación de formas tradicionales y no tradicionales de conflicto integra todo el espectro de capacidades ofensivas para crear ambigüedad.

Más recientemente, las operaciones en Ucrania demostraron una ejecución aún más refinada de la guerra gris, como los conflictos anteriores, paralizaron la respuesta militar de Ucrania, lo que rompió su ciclo de toma de decisión a través del control de la información[21]. Las fuentes rusas, tanto oficiales como no oficiales valoran mucho el aislamiento de información[22].

Es comprensible que los encargados de la política y especialistas en materia de seguridad de Estados Unidos fijen su atención en las posibles amenazas que estas doctrinas tienen para la patria. Ciertamente, preferiríamos evitar trastornos graves a la vida en la patria, pero en un conflicto de gran envergadura estos son inevitables hasta cierto punto. De hecho, John Arquilla, un conocido teórico de la corporación RAND, dice que los temores ante ataques cibernéticos contra la patria son exagerados citando la resistencia de las poblaciones civiles contra las campañas de bombardeo estratégicas en la Segunda Guerra Mundial[23]. Después de todo, los errores pueden ser enmendados, las instituciones financieras pueden rebotar y el orden se puede restaurar en una ciudad importante que sufre de ciberataques contra la infraestructura.

Sin embargo, las formaciones operacionales y tácticas de una Nación en medio de un conflicto activo cuentan con poco tiempo para recuperarse de un colapso de las redes de información. La toma de decisión oportuna no esperará a que se procese una orden para arreglar el problema. En la actualidad, los pensadores estratégicos deben preocuparse por los conflictos cibernéticos, pero también debemos tomar en consideración la resiliencia de las formaciones operacionales y tácticas contra lo que Arquilla llamó «bitskrieg» o ataque cibernético intenso[24].

En un capítulo revelador en el *Dark Territory*, Fred Kaplan describe cómo las fuerzas estadounidenses en concierto con los socios interinstitucionales ejecutaron una campaña sorprendentemente eficaz tras bastidores de la oleada iraquí llevada a cabo por el general Davis A. Petraeus. Con menos publicidad que las iniciativas de contrainsurgencia, pero igualmente importantes, fueron las iniciativas de las operaciones de localización y adquisición de blanco del general Stanley A. McChrystal, que perforó eficazmente el sistema de mando tipo misión de la red insurgente y ocasionó estragos desde adentro en su proceso de operaciones. El Comando de Operaciones Especiales Conjunto llevó a las fuerzas enemigas a emboscadas con información falsa y aisló a las células cortando los vínculos entre ellas[25]. A pesar de la fuerza y la resistencia de las organizaciones en red, en este caso, las fuerzas enemigas perdieron la iniciativa por completo. Más adelante, Petraeus señaló las operaciones de McChrystal como un componente crítico de la estrategia general, señalando que él había barrido a los «líderes de alta y mediana jerarquía» del campo de batalla, cuyos resultados otorgaron tiempo y espacio para que funcionara la estrategia centrada en la población[26].

Cabe destacar que los enemigos que McChrystal derrotó usaron herramientas y capacidades de Internet disponibles en el mercado, y aunque se podría suponer que las redes privadas establecidas por los militares del estado son más seguras, puede que esto no sea así por mucho tiempo. Estados Unidos informa que ahora tiene la capacidad de acceder a redes tácticas inalámbricas como las nuestras[27]. Ahora imagine si el enemigo, en lugar de McChrystal tuviera esas capacidades. Imagine que un adversario hubiera violado nuestro propio sistema de mando tipo misión. De hecho, parece imprudente suponer que los enemigos futuros no poseerán esa capacidad basada en estos acontecimientos y conclusiones de un panel de revisión de ciberseguridad de 2013[28].

Las redes de automatización de las organizaciones de los cuarteles generales del Ejército de EUA ahora constituyen nuestro cerebro colectivo. En *The Scientific Way of Warfare*, Antoine Bousquet aterriza en el problema que esto representa. En nuestro entusiasmo por el potencial de las redes y la información, él advierte que nos convertimos «totalmente dependientes» de esas capacidades[29]. En esencia, las herramientas con las que colaboramos y tomamos decisiones en nuestros cuarteles generales tácticos han creado una vulnerabilidad mortal al fusionar los productos con los procesos.

Considere cómo el Ejército ahora ejecuta el proceso de operaciones en un cuartel general en el nivel división. El Estado Mayor se forma en grupos de trabajo o equipos de planificación, a menudo, dispersos a través de la red. Incluso, si se reúnen en persona, el personal captura cada paso del proceso de planificación en un medio digital de algún tipo. Las sesiones de información para el comandante pueden tener lugar alrededor de un mapa análogo, pero casi todas las órdenes de difusión ocurren a través de medios digitales. A medida que progresan las operaciones, las órdenes fragmentadas salen por correo electrónico, los anexos se publican en portales y docenas de otros productos de apoyo se publican en varios medios digitales comunes.

Dado el riesgo de centrar a todo el Estado Mayor y comandantes de una división en un solo lugar de localización y adquisición de blanco, incluso los ensayos pueden darse no alrededor de un modelo de terreno sino con líderes alrededor de monitores en sus cuarteles generales. En cada caso, un adversario capaz puede penetrar realmente en el proceso de operaciones.

Una vez dentro de nuestro ciberperímetro, las posibilidades son tan diversas como perturbadoras. Un enemigo podría optar por interrumpir la planificación y ejecución mediante el cierre de la red, o podrían capturar en secreto los planes de la red y adaptar sus propias operaciones para aumentar sus probabilidades de éxito. Peor aún, podrían desarrollar la capacidad de corromper nuestro sistema de mando tipo misión alterando o incorporando información o datos falsos en nuestra red. Al tomar en consideración que los conceptos operativos de China y Rusia giran en torno a crear ambigüedad, desafiar la claridad de las operaciones de planificación es una búsqueda probable de sus operaciones.

Los sargentos de primera clase Richard Miller (izquierda) y Brian Rowcotsky de la Brigada de protección cibernética del Ejército de EUA discuten la respuesta a un ciberataque simulado el 6 de noviembre de 2015 en el 1er Equipo de combate de brigada, 82ª División aerotransportada con el sargento Frederick Roquemore (de pie), un defensor de la red cibernética de la 1-82 durante la rotación de la unidad en el Centro de Adiestramiento de Apresto Conjunto en el Fuerte Polk, estado de Luisiana. (Foto cortesía de Bill Roche)

Como ya hemos visto, estas no son capacidades hipotéticas— ya existe la tecnología para llevar a cabo esos fines. El punto no es que debamos vivir con temor de que el enemigo descubra todos nuestros planes, sino más bien que no podemos presumir la impenetrabilidad de nuestras redes o el secreto absoluto de nuestra toma de decisión. Esto genera la pregunta, ¿cuáles son las perspectivas de la victoria sin nuestras ventajas de información acostumbradas?

La preparación para una información atrofiada

Tan solemnemente graves como estas posibilidades podrían ser, no tenemos que entrar en pánico. Divinizar el concepto operativo detrás de la amenaza aclara nuestro problema. A fin de prepararnos para las posibles guerras por venir requerimos desarrollar y fortalecer dos competencias diferentes, a saber: la resiliencia en nuestras redes de información y, simultáneamente, la capacidad de planear, preparar, ejecutar y evaluar «en la oscuridad» en caso que las redes sean deshabilitadas o gravemente comprometidas.

Durante el Ejercicio de Guerrero en octubre de 2016 de la 3ª División de infantería, incluso después de que el enemigo entrara a nuestras redes y disfrutara de la capacidad de adaptar su esquema de maniobra para derrotar a los nuestros, la división tuvo éxito. Nos encontramos con el éxito no a través de ningún acto de presciencia, sino más bien a través de un plan que permitió a los equipos de combate de brigada la flexibilidad para responder a las circunstancias del campo de batalla. Vamos a desempacar la posibilidad de mitigar estos acontecimientos con respecto a la integridad de la red.

El llegar a dominar el proceso de operaciones penetrables requiere, sobre todo, que la mente se prepare

para una norma nueva. La idea de lo que podría suceder no debería ser una posibilidad lejana. Desde el sillín de Robert E. Lee, el peligro de una orden interceptada, aunque no necesariamente común, era una posibilidad conocida. Los cables del telégrafo podrían ser cortados o interceptados por cualquiera de los lados, y los mensajeros podían morir o ser capturados[30]. Ni los ejércitos federales ni los confederados poseían una ventaja decisiva en la seguridad de la información. El simple reconocimiento de esta condición significaba que todos los comandantes debían tener presente los indicadores de que sus planes eran conocidos por el enemigo, o que sus propias órdenes no habían alcanzado a los subalternos.

Eso no quiere decir que debemos evitar el poder multiplicativo de nuestros sistemas en red, sino más bien adiestrarnos para evitar la dependencia de los mismos. La mente puede acostumbrarse, tal vez volverse adicta, a la claridad o certeza que puede ser artificial o temporal. En *Certain Victory: The US Army in the Gulf War*, el general Robert H. Scales describe el hambre insatisfecha de inteligencia de precisión y comunicaciones infalibles de lo que muchos comandantes habían dependido durante su servicio en Europa[31]. Cuán fascinante es que cuando las condiciones meteorológicas y la distancia provocaron fallas en las comunicaciones, las órdenes basadas en la intención del general de división Frederick M. Franks hijo, permitieron que el Séptimo cuerpo continuara la planificación y ejecución con «lápices grasos y acetato»[32].

Con tales precedentes históricos en mente, un ciberataque grave o colapso de la red debe convertirse en un acontecimiento previsto—tan probable como el fuego indirecto en el área de seguridad. Además, el ajuste cognitivo y procesal de la planificación habilitada para la red al análogo puro no ocurrirá por sí solo, sino que requiere que los líderes actúen y el personal se reorganice.

La transición de un proceso centrado en la red de computadoras a un proceso manual tradicional requiere diferentes responsabilidades, salidas y medios de comunicación. El acto físico de planificación y ejecución depende de diferentes agentes. La agilidad, en parte, será la velocidad con la que un Estado Mayor puede reorientarse en un proceso análogo y, luego, regresar a una capacidad habilitada de red completa sin pérdida de potencia.

Los que diseñan los ejercicios y el adiestramiento tienen la responsabilidad de poner hincapié en estos procesos. El adiestramiento del proceso de operaciones «desconectado», por así decirlo, ayuda a los integrantes del Estado Mayor a sobrevivir esta turbulencia y mantener la cohesión y funcionalidad. Pueden comprender mejor la diferencia que existe entre el producto y el proceso mientras apoyan las decisiones del comandante. En resumen, cuando son golpeados por redes poco fiables, podemos recurrir a un adiestramiento sólido, pero el adiestramiento y el combate deben proceder de una filosofía operativa sólida y probada— en nuestro caso, el mando tipo misión.

Nos debe consolar el hecho de que nuestros antepasados hayan tenido éxito con el ambiente de información incierta mucho antes de nosotros. Durante la Campaña del Danubio de Napoleón en 1808, el ejército de Napoleón del Danubio y el ejército de Italia, bajo el mando de su hijastro, Eugene, avanzaron sobre Viena en dos ejes distintos separados por los Alpes italianos. Durante una semana de desplazamiento ambos comandantes se mantuvieron en la oscuridad. Eugene se equivocó en sus primeros combates, pero redescubrió su confianza y le dio al archiduque John una derrota decisiva[33]. Entonces se abrió paso en Austria para unirse a las fuerzas de Napoleón contra el archiduque Charles basándose en un enfoque un poco más operacional que le fue descrito por mensajes de su comandante antes de partir[34]. Propongo que más que una mayor seguridad o dominio de la información, nuestros esfuerzos deben engendrar un ejercicio más auténtico del mando tipo misión.

Durante nuestro ejercicio de división, escuché el comentario irónico de un oficial de mayor antigüedad, «Sé que el enemigo no sabe lo que vamos a hacer, porque yo no sé lo que vamos a hacer». Este comentario enmarca un punto final que vale la pena considerar. Si el enemigo penetra en nuestro sistema de mando tipo misión, los planes operacionales detallados y los planes de engaño se convierten en cargas. Mientras más amplia sea la gama de opciones del comandante, más difícil es contrarrestarlas. El engaño tiene valor, pero para los cuarteles generales tácticos y operacionales, las ganancias no ameritan grandes inversiones. El general de brigada (retirado) Huba Wass de Czege hace eco de este sentimiento al describir una epifanía personal como comandante de

brigada en el Centro Nacional de Adiestramiento: «Crear ambigüedad es mucho más importante que intentar crear el engaño»[35]. El crear ambigüedad no implica no planificar, sino más bien evitar patrones y mantener todas las opciones disponibles durante el mayor tiempo posible. En términos prácticos, esto se manifiesta como el uso de tácticas de punto de decisión. Las tácticas de punto de decisión respetan el dictamen de Helmuth von Moltke de que «se hace bien ordenar no más de lo que es absolutamente necesario» mientras se aprovecha la capacidad de planificación del Estado Mayor[36].

Pensamientos finales: Paz con incertidumbre

El estudio de Martin van Creveld Peace with Uncertainty, Command in War, profundiza en la naturaleza del proceso de operaciones y considera que la «patología de la información» estadounidense durante la guerra de Vietnam es suficiente para «desesperar la razón humana»[37]. Su crítica nos toca profundo pero da con el punto. Entonces y ahora, las capacidades tecnológicas nos seducen a la dependencia de una amante inconstante. La «búsqueda de la certeza», él nos asegura, es una búsqueda errante y el peso de la evidencia sustenta su afirmación[38].

Nuestros procesos de toma de decisiones deben postrarse ante la incertidumbre en lugar de intentar abolirla. La búsqueda de la ambigüedad y confusión forma la lógica de la respuesta militar de nuestros adversarios a la superioridad de Estados Unidos en la guerra tradicional. Los conceptos operacionales chinos y rusos ponen las operaciones a través de los dominios en su base y van de lo estratégico a lo táctico. El cibercombate figura en gran medida en su visión global de la guerra, y la capacidad para penetrar redes militares ya existentes. El aspecto cognitivo del proceso de operaciones no necesita cambiar, pero debemos prepararnos para la posibilidad de que nuestros mensajeros digitales sean interceptados, o algo peor. El columnista Sebastian Bae capta la esencia de nuestros tiempos afirmando que la victoria la obtendrán los que «efectivamente aprovechen la información para confundir, engañar y controlar al adversario»[39]. El descubrimiento de la Orden Especial 191 puede o no haber cambiado el curso de la Guerra Civil Americana, pero el potencial parece claro incluso para los historiadores aficionados. Haríamos bien en poner atención al espíritu de nuestro propio tiempo y preparar a nuestros Estados Mayores para un ambiente de información disputado donde incluso nuestro proceso de toma de decisiones no puede mantenerse fuera del alcance del enemigo. ■

El mayor Wesley Moerbe, Ejército de EUA, se desempeña como planificador en el Cuartel General de la 3ª División de Infantería en el Fuerte Stewart, estado de Georgia. Cuenta a su haber con una maestría de la Escuela de Estudios Militares Avanzados y una licenciatura en historia militar de la Academia Militar de Estados Unidos. Ha servido en la 101ª División aerotransportada (Asalto aéreo) y en calidad de comandante de compañía y asesor de combate en el 3er Equipo de combate de brigada de la 4ª División de infantería.

Referencias Bibliográficas

Epígrafe. Shirley, James, «The Last Conqueror», en *Palgrave's Golden Treasury of the Best Songs and Lyrical Poems in the English Language*, ed. Francis Turner (London: J. M. Dent, 1906), p. 70. El poema de Shirley señala la amplitud de los dispositivos de muerte y sugiere, como yo, que los mayores peligros son, a menudo, los menos obvios.

1. Francis Winthrop Palfrey, *The Antietam and Fredericksburg* (New York: Charles Scribner's Sons, 1910), págs, 21–23.

2. Allan, William; *Stonewall Jackson, Robert E. Lee, and the Army of Northern Virginia, 1862* (New York: Da Capo Press, 1995), p. 243.

3. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington, DC: Oficina del subsecretario de Defensa para la Adquisición, Tecnología y Logística, enero de 2014) accedido el 28 de diciembre de 2016 http://purl.fdlp.gov/GPO/gpo60252.

4. Publicación de Referencia de Doctrina del Ejército (ADP) 5-0, *The Operations Process* (Washington, DC: Oficina de imprenta federal [GPO], junio de 2012), p. 1-1.

5. Marshall, A., S. L., *Men Against Fire: The Problem of Battle*

Command (Norman, OK: University of Oklahoma Press, 1947), p. 85.

6. Ibíd.

7. (ADRP) 5-0, *The Operations Process*, págs, 1-2

8. ADRP 6-0, *Mission Command* (Washington, D.C.: GPO, 2012), págs, 3-8.

9. Ibíd., págs, 1-5.

10. Dorner, Dietrich, *The Logic of Failure* (Cambridge, MA: Perseus Books, 1997), p. 75.

11. Carl von Clausewitz, *On War*, ed. y traducción. Michael Eliot Howard y Peter Paret (Princeton, N.J.: Princeton University Press, 1976), pág. 154.

12. Bousqet, J., Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), p. 232; Ceballos, Stuth, Astrid; Garafola, L., Cristina; y Gombert, C., David, *War with China: Thinking Through the Unthinkable* (Santa Monica, CA: RAND Corporation, 2016), p. 14, accedido el 6 de enero de 2017, http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1140/RAND_RR1140.pdf.

13. Crane, C., Conrad, «The Lure of Strike», *Parameters* 43, nº. 2 (verano de 2013), accedido el 23 de diciembre de 2016, http://strategicstudiesinstitute.army.mil/pubs/parameters/issues/Summer_2013/1_Crane_SpecialCommentary.pdf.

14. Doldberg, Angus, «Bespredel and the Conduct of Russian Hybrid Operations», *Small Wars Journal* website, 26 de octubre de 2016, accedido el 28 de diciembre de 2016; Timothy Thomas, *The Three Faces of the Cyber Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), accessed 5 January 2017, http://fmso.leavenworth.army.mil/EPubs/Epubs/3Faces%20of%20the%20 Dragon.pdf.

15. Qiao, Liang, Al Santoli, and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America*, traducción. Central Intelligence Agency (Panama, ciudad de Panama: Pan American Publishing, 2002), p. 77.

16. *The Science of Military Strategy* permanece accesible solamente para los lingüistas chinos, pero los expertos chinos de la fundación de Jamestown han puesto a disposición el trabajo de su yeoman de la traducción y del análisis. McReynolds, Joe, «China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy», *China Brief* 15, no. 8 (Washington, DC: Fundación Jamestown, 16 de abril de 2015), accedido el 5 de enero de 2017, https://jamestown.org/ program/chinas-evolving-perspectives-on-network-warfare-lessons- from-the-science-of-military-strategy/.

17. Qiu, Mingda, «China's Science of Military Strategy Cross Domain Concepts in the 2013 Edition», Cross Domain Deterrence Project Working Paper (La Jolla, CA: University of California San Diego, September 2015), págs. 17–20, accedido el 28 de diciembre de 2016, http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20 Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf.

18. Heginbotham, Eric, et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2015), 276, accedido el 1 enero de 2017, http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR392/RAND_RR392.pdf.

19. Angus, Doldberg, «Bespredel and the Conduct of Russian Hybrid Operations», *Small Wars Journal* website, 26 de octubre de 2016, accedido el 28 de diciembre de 2016, http://smallwarsjournal.com/jrnl/art/bespredel-and-the-conduct-of-russian-%E2%80%9Chybrid- operations%E2%80%9D.

20. Bae, Sebastian, «Cyber Warfare: Chinese and Russian Lessons For US Cyber Doctrine», Georgetown Security Studies Review website (blog), 7 de mayo de 2015, accedido el 28 de diciembre de 2016, http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessonsfor-us-cyber-doctrine/.

21. Ghori, Shaheen y Unwala, Azhar «Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict», Military Cyber Affairs 1, nº. 1 (2015): págs., 6–7, accedido el 23 diciembre de 2016. http://scholarcommons.usf.edu/cgi/viewcontentcgi?article=1001&context=mca.

22. Ibíd., p. 2.

23. Arquilla, John, «Cyberwar is Already Upon Us», *Foreign Policy*, 27 de febrero de 2012, accedido el 28 de diciembre de 2016, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/?wp_login_redirect=0.

24. Ibíd.

25. Kaplan, M., Fred *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016, p. 160

26. Petraeus, David, «How We Won in Iraq» *Foreign Policy*, 29 de octubre de 2013, accedido el

28 de diciembre de 2016 http://foreignpolicy.com/2013/10/29/how-we-won-in-iraq/.

27. Freedburg, Sydney, «Wireless Hacking in Flight: Air Forces Demops Cyber EC-130», *Breaking Defense*, 15 de septiembre de 2015, accedido el 28 de diciembre de 2016, http://breakingdefense.com/2015/09/wireless-hacking-inflight-air-force-demos-cyber-ec-130/.

28. Defense Science Board, Task Force Report, p 5.

29. Bousquet, *The Scientific Way of Warfare*, p. 222.

30. Lanier, S., Robert; Miller, Trevelyan, Francis; Lanier, Wysham, Henry, *The Photographic History of the Civil War*, vol. 8 (New York: The Review of Reviews, 1911), págs. 288 y 362.

31. Scales, H., Robert, *Certain Victory: The US Army in the Gulf War* (Fort Leavenworth, KS: The US Army in the Gulf War, U.S. Army Command and General Staff College Press, 1994), p. 375.

32. Ibíd.

33. Epstein, M. Robert, *Napoleon's Last Victory and the Emergence of Modern War* (Lawrence, KS: University Press of Kansas, 1994), págs. 49, 85, 95 y 128.

34. Ibíd.

35. de Czega, Huba Wass, «Carousel of Deception», en *66 Stores of Mission Command*, eds. Frame, Adela y Lussier, W. James, (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2000), p. 27.

36. Moltke von, Helmuth, *Moltke on the Art of War: Selected Writings*, ed. Daniel J. Hughes (Novato, CA: Presidio Press, 1993), 184. Belknap Press, 1993), p. 184.

37. Creveld Van, Martin, *Command in War* (Cambridge, MA: Harvard University Press, 1985), p. 260.

38. Ibíd., p. 264.

39. Bae, «Cyber Warfare».