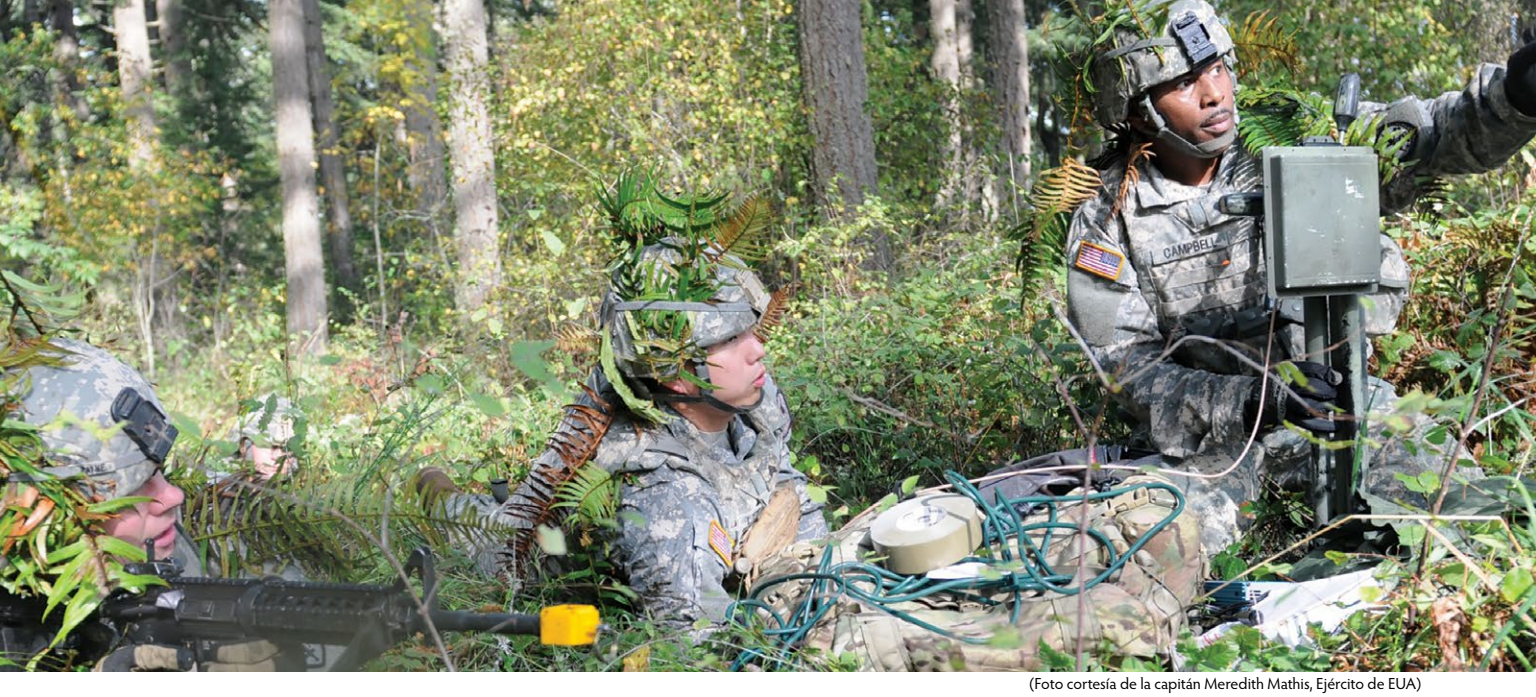


(Foto cortesía de la capitán Meredith Mathis, Ejército de EUA)

La especialista Casey Payne, (izq), 201ª Brigada expedicionaria de inteligencia militar y el sargento Andrew Lee, Compañía D, 14º Batallón de ingenieros en el nivel brigada, 2-2 ID (SBCT), brindan seguridad a un soldado de la 780ª Brigada de inteligencia militar mientras coloca un parche de antena de panel de red y tomas durante un ejercicio de adiestramiento ciberespacial el 20 de octubre de 2015 en la Base Conjunta Lewis-McChord, estado de Washington.

La comprensión situacional ciberespacial para los comandantes tácticos del Ejército

El Ejército quiere batear un jonrón, pero solo necesita pegarle a la bola

Teniente coronel (retirado) William Jay Martin, Fuerza Aérea de EUA
Emily Kaemmer

Jamás me culpo si no le pego a la bola. Simplemente, culpo al bate, y si eso continua, cambio de bate[1].

—Yogi Berra

Cuando el Ejército desarrolla capacidades, podría usar un poquito de la sabiduría paradójica de Yogi Berra que rápidamente llega al corazón de casi cualquier asunto. Como preguntar, «Si los comandantes tácticos del Ejército son completamente dependientes del ciberespacio, entonces ¿por qué no tienen una manera de verlo?». Todas las capacidades ciberespaciales del Ejército de EUA funcionan en algún tipo de red, sin embargo, casi no hay medios que proporcionen comprensión situacional en tiempo real del dominio ciberespacial para las unidades de combate tácticas[2]. Esto hace que los comandantes tácticos no puedan ver el potencial de las amenazas y oportunidades ciberespaciales, lo que merma sus capacidades para defender a sus propias redes, y pone en peligro las formas tradicionales del poder de combate.

El Ejército está muy consciente de esta grave situación y considera la comprensión situacional ciberespacial (SU ciberespacial) una prioridad principal, sin embargo, una solución tecnológica de implementar un sistema de SU ciberespacial en las unidades de combate convencional parece estar muy lejos[3]. En la actualidad, el Ejército sencillamente está luchando para definir, precisamente, *qué* es lo que el comandante táctico necesita saber acerca del ciberespacio. Lo que es más, incluso después de que el Ejército decida cómo quiere que sea la SU ciberespacial, tiene que sobrevivir la política realista del proceso de adquisición. Aun la mejor propuesta de capacidad puede verse algo diluida, distorsionada, o combinada con otros programas con resultados que dejan mucho que desear. Además, no es poco común para los desarrolladores de capacidades que, en un intento de crear una solución curalotodo, hagan los requerimientos tan rigurosos y complejos que toda la iniciativa queda paralizada. Todos estos escenarios pueden llevar a plazos prolongados, o soluciones marginales, o hasta obsoletas antes de lograr la capacidad operacional inicial. En este artículo se detalla por qué la búsqueda de la SU ciberespacial del Ejército está estancada y sugiere un planteamiento simplificado para arreglarla.

Una necesidad justificada para una SU ciberespacial

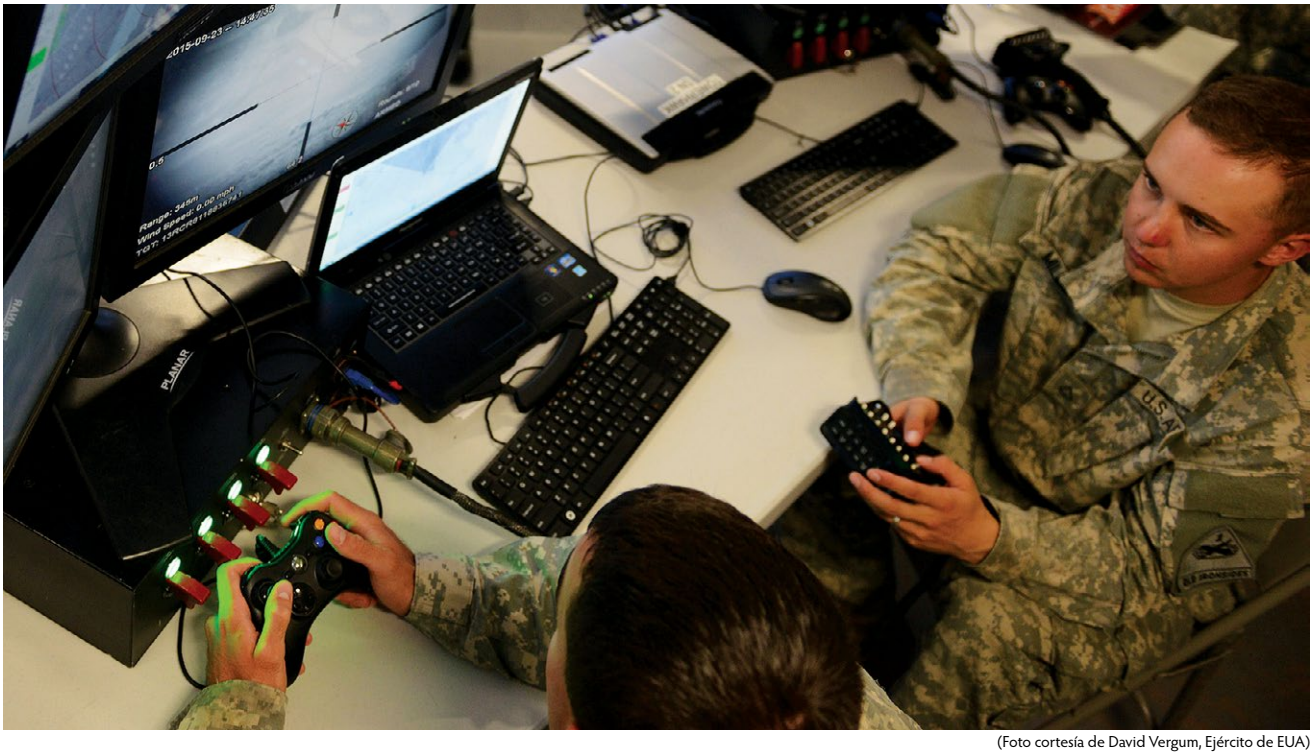
Deseo agradecerle por hacer este día necesario[4].

—Yogi Berra

Toda discusión sobre un mejor planteamiento hacia la adquisición del sistema para la SU primero tiene que comenzar probando que se necesita tal sistema, y hay suficientes pruebas para apoyarlo. En el *Concepto conjunto para el ciberespacio* del Departamento de Defensa, se estipula que el conocimiento situacional compartido del ciberespacio es uno de los 8 elementos clave para las operaciones ciberespaciales conjuntas[5]. Este concepto dio origen al Documento de Capacidades Iniciales del Conocimiento Situacional Ciberespacial Conjunto, en el que se describen los requerimientos para el conocimiento situacional ciberespacial en el escalón estratégico[6]. Por casualidad, mucha de la misma información pertinente a los escalones estratégicos conjuntos es relevante en los escalones tácticos del Ejército, donde el Ejército ha afirmado que la necesidad de un sistema para la SU ciberespacial es de suma urgencia[7].

En el *Concepto fundamental del Ejército de EUA* se afirma que para mantener una ventaja en el ciberespacio, el Ejército futuro tiene que proporcionar una capacidad para los líderes y soldados que les ayude a comprender cómo y dónde los adversarios usan las capacidades ciberespaciales y cómo responder a las mismas[8]. Además, sugiere invertir en las capacidades de mando tipo misión y sistemas que permitan que el Ejército establezca la fuerza y mejore la comprensión situacional común para ganar y mantener una ventaja en las actividades electromagnéticas ciberespaciales[9]. En el *Concepto operacional del Ejército de EUA* se identifican áreas de desarrollo de capacidades clave centradas en las iniciativas de ciencia y tecnología para proporcionar a los comandantes el conocimiento situacional necesario a través de imágenes operacionales comunes hasta la ventaja táctica. Esto, afirma, «puede ayudar a los comandantes a ganar y mantener una postura de ventaja relativa a través del dominio ciberespacial y el espectro electromagnético disputado»[10].

Las publicaciones conjuntas y del Ejército también señalan la necesidad de contar con un sistema para la SU ciberespacial. En el JP 3-12 (R), *Cyberspace Operations*, se estipula, explícitamente, que las operaciones ciberespaciales dependen del «conocimiento actual y previsible del ciberespacio y del ambiente operacional (OE, por sus siglas en inglés)»[11]. En la ADRO 6-0, *Mission Command*, se destaca la importancia de la imagen operacional común (COP, por sus siglas en inglés) en cuanto al desarrollo del conocimiento situacional[12]. En el FM 6-02, *Signal Support to Operations* se establece



(Foto cortesía de David Vergum, Ejército de EUA)

Guerreros cibernéticos defienden la red en el centro de operaciones tácticas para el 2º Equipo de combate de brigada blindada, 1ª División blindada, en el Fuerte Bliss, estado de Texas, durante una Evaluación de Integración de red 16.1 (NIE, por sus siglas en inglés). La NIE fue llevada a cabo desde el 25 de septiembre hasta el 8 de octubre de 2015.

que «mediante la integración de la información a través de todo lo ancho del área de operaciones, se puede mantener una comprensión situacional más relevante y completa... [Permitiendo] que los comandantes usen las capacidades correctas en el lugar indicado y en el momento preciso»[13]. No es de sorprender que estos documentos de doctrina reflejen el mensaje estratégico de los líderes ciberespaciales de alto nivel.

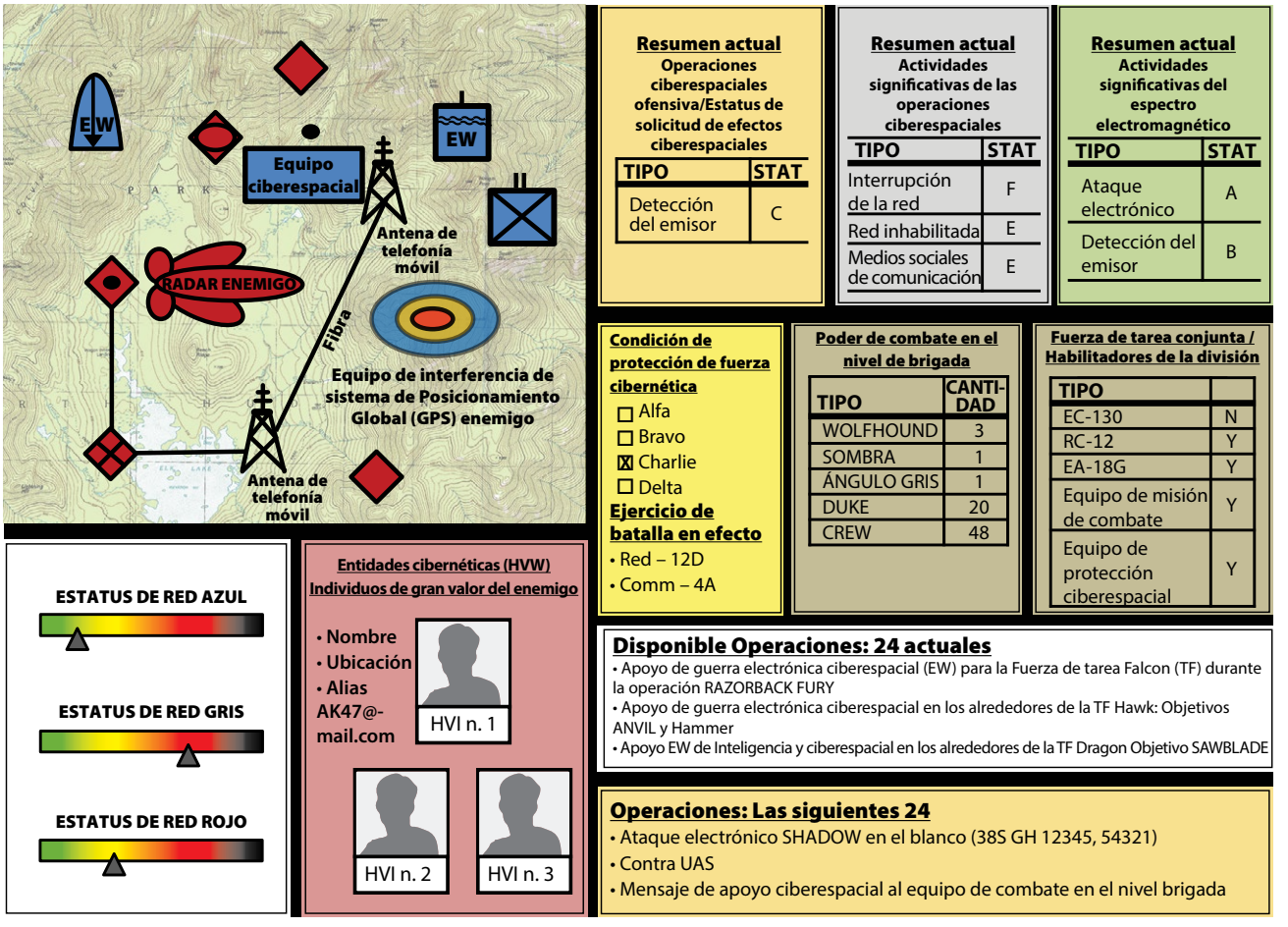
En su artículo publicado en *Joint Force Quarterly*, «Ten Propositions Regarding Cyberspace Operations», el general de división Brett Williams explica la urgencia del conocimiento situacional ciberespacial. Williams escribe lo siguiente: «El desarrollar el conocimiento situacional ciberespacial es una alta prioridad para el DoD. El desafío está en proporcionar a los comandantes, en todos los niveles, una imagen completa del dominio que sea coherente, precisa, actual y adaptable»[14]. Además, Williams concluye que los comandantes tienen que poder ver y comprender al ciberespacio para defenderlo[15]. Esta simple verdad justifica una capacidad SU ciberespacial para el Ejército. Sin embargo, las iniciativas de desarrollo de capacidad del Ejército para la SU ciberespacial actualmente están estancadas.

Por qué están estancadas las iniciativas de desarrollo de capacidad SU ciberespacial del Ejército

Si no sabe a dónde va, podría ir a parar a otro lugar[16].

—Yogi Berra

En un mundo perfecto, el Ejército podría prever sus necesidades de capacidad para permitir que el proceso de adquisición tenga éxito. Desgraciadamente, la innovación en el ciberespacio se está moviendo muy rápido para hacer que esa fecha tope sea práctica para la SU ciberespacial. El plazo típico para identificar una necesidad, redactar los requerimientos, negociar el proceso del Sistema de Integración y Desarrollo de Capacidades Conjuntas (JCIDS, por sus siglas en inglés) y, luego, producir un elemento gráfico nuevo es de 5 a 8 años. El proceso JCIDS intenta acomodar el desarrollo de softwares de sistemas de información con una opción de Caja de Tecnología de información (IT-Box Model, en inglés) más eficaz[17]. Si bien el Ejército está usando el Modelo de Caja TI, ha tomado demasiado tiempo para aprobar el primer documento de requerimiento



(Gráfico cortesía de los autores)

Figura - Ejemplo de superposición de comprensión situacional en la Imagen operacional común

relacionado al ciberespacio[18]. Uno de los desafío del Ejército podría recaer en un sistema de adquisición que esté vinculado a los viejos paradigmas.

El general David G. Perkins del Comando de Adiestramiento y Doctrina del Ejército de EUA señaló que el sistema de adquisición de defensa todavía está orientado a llenar los vacíos que nos diferencian de un enemigo conocido, en lugar de aumentar nuestro ritmo de innovación[19]. Perkins dijo que el Ejército tiene que estar dispuesto a deshacerse de los programas anticuados y, luego, invertir esos recursos en tecnologías nuevas y más transferibles[20]. Añadió que para innovar, el Ejército tiene que evitar crear requerimientos con tantos detalles que se auto limiten[21].

Es evidente que el Ejército tiene un fuerte deseo de innovación, sin embargo, un sistema de adquisición y pensamiento anticuado no son las únicas razones que lo retrasa. Otro desafío es una discordante iniciativa de desarrollo de capacidades cibernéticas. Actualmente, hay en desarrollo varios documentos de capacidad de sistema de información[22]. Todos prometen capacidades pertinentes a la comprensión situacional cibernética. Si bien el Centro de Integración de Capacidades del Ejército (ARCIC, por sus siglas en inglés) intentó coordinar estas iniciativas distintas, todavía no se han logrado ahorros significativos.

El subsecretario del Ejército para la Adquisición, Logística y Tecnología (ASA [ALT, por sus siglas en inglés]) desarrolló recientemente un planteamiento coordinado para lanzar tecnologías relacionadas al ciberespacio[23]. Sin embargo, parece estar más centrado en las operaciones defensivas y ofensivas en el ciberespacio y no en habilitar las capacidades como la SU ciberespacial[24]. A pesar de que una de las metas del ASA es crear

una capacidad de operaciones de red integrada que aumentaría la comprensión acerca de la seguridad de las redes tácticas, esa capacidad parece excluir otra información relativa a los factores fuera de las redes amigas que podría interesar a los comandantes tácticos[25]. Y, si bien en 2014 el ASA respondió a 10 declaraciones de necesidades operacionales del Comando Ciberespacial del Ejército que trataban de requerimientos de corto plazo, el interés principal ha estado centrado en reducir las vulnerabilidades en la red y no en la SU ciberespacial[26]. Esta estrategia de arriba abajo es un paso positivo, sin embargo, todavía no se ha traducido en una iniciativa de desarrollo de capacidades ciberespaciales en el último escalón de la burocracia.

Un planteamiento sencillo para los desarrolladores de capacidad SU ciberespacial del Ejército

Se puede observar bastante con solo mirar[27].

—Yogi Berra

El Ejército de EUA no necesita un sistema para la SU ciberespacial perfecto en 10 años, más bien, necesita un sistema para la SU ciberespacial lo suficientemente bueno, *ahora*. A fin de lograrlo, a los desarrolladores de capacidades se les ha aconsejado tomar un planteamiento sencillo contestando las siguientes tres preguntas básicas:

- ¿Qué información necesita el comandante?
- ¿Cómo la obtenemos y consolidamos?
- ¿Cómo debe ser presentada?

En un sentido más amplio, para adquirir exitosamente la SU ciberespacial (o cualquier otra capacidad futura), el Ejército tiene que pensar en maneras de innovar y reformar, gradualmente, un proceso de adquisición restrictivo. En primer lugar, los desarrolladores de capacidad tienen que cerciorarse de qué información referente al ciberespacio es más importante para los comandantes.

Durante las operaciones de combate, los comandantes, apoyados por sus estados mayores, vigilan y evalúan el progreso, toman decisiones para aprovechar las oportunidades y contrarrestar las amenazas, y dirigen, oportunamente, el uso del poder de combate en momentos clave[28]. El ciberespacio forma una parte significativa de ese cálculo, especialmente con respecto a sus efectos en el mando tipo misión y en las maneras sumamente establecidas del poder de combate. La información que posiblemente comprenderá el contenido básico de la SU ciberespacial presentada en las COP incluye el estado de la red de naciones amigas, anfitrionas y enemigas, amenazas cibernéticas y capacidades enemigas, infraestructura ciberespacial clave en el área de operaciones, autoridades ciberespaciales y reglas de enfrentamiento, y las tendencias del medio social por mencionar unas pocas

En segundo lugar, los desarrolladores de capacidades tienen que considerar de dónde proviene la información de la SU ciberespacial y cómo obtenerla. Actualmente, solo las fuerzas de misión ciberespacial conjuntas están autorizadas para llevar a cabo la vigilancia, reconocimiento y preparación operacional ciberespacial del ambiente. De manera que una gran cantidad de información acerca del ciberespacio se originará y residirá en las bases de datos en los niveles nacionales y estratégicos. Eso quiere decir que, los datos e información relevantes provenientes de las iniciativas de recolección de información orgánica en los escalones tácticos del Ejército pueden proporcionar un contexto importante.

Un ejemplo práctico es conectar a una entidad ciberespacial, proveniente de un recurso ciberespacial nacional o conjunto, con la identidad de una persona real (u organización) que se sabe reside en un ambiente operacional (OE, por sus siglas en inglés), según lo derivado a través de la recolección de información del lugar. El fusionar estos recursos proporciona una mejor comprensión situacional para los comandantes tácticos y ayudará a las comandancias superiores a ver más claramente al ciberespacio.

En tercer lugar, los desarrolladores de capacidades tienen que determinar la mejor manera de presentar la información. La SU ciberespacial tiene que proporcionar detalles adecuados, pero no demasiados detalles. El Ejército no puede defender a todo el ciberespacio, ni presentar todo en una COP; de lo contrario, el pensamiento de un comandante podría verse obstruido por enredos innecesarios. Los comandantes solo necesitan saber qué afecta a su misión, lo que aparte de aprovechar algunos efectos cibernéticos conjuntos consiste, principalmente, en usar formas tradicionales de poder de combate. Por consiguiente, la SU ciberespacial también tiene que permitir que la información sea presentada contextualmente para facilitar una comprensión situacional. Esto puede lograrse a través de fotografías, gráficos de semáforo, gráficos de velocímetros, cintas, diagramas de línea y bloques, y comparaciones paralelas (según lo ejemplificado en la Figura).

En cuarto lugar, los desarrolladores de capacidades tienen que evitar redactar requerimientos de sistemas que intenten reemplazar el criterio y toma de decisión humana. La SU ciberespacial tiene que proporcionar comprensión; pero depende de los comandantes tácticos y estados mayores discernir cómo actuar basados en esa comprensión.

En quinto lugar, el Ejército tiene que pensar en maneras de innovar y reformar, paulatinamente, un proceso de adquisición restrictivo. Los documentos de requerimientos ciberespaciales deben intentar fomentar la innovación al describir un marco conceptual predominante, basado en conceptos doctrinales válidos que pudan ser desarrollados con el tiempo a través del desarrollo de software sucesivos[29]. Esto es, de hecho, la meta del Modelo de la Caja TI. El desafío, por consiguiente, es identificar los aspectos de la SU ciberespacial que quedarán anticuados rápidamente y hacerlos modulares, de manera que puedan ser reemplazados rápidamente por nuevas innovaciones. Además, los desarrolladores de capacidades del Ejército tienen que decidir si la SU ciberespacial se combinará con otros sistemas sugeridos o actuales, o si permanecerá sin alterar. Al combinar varios sistemas aumenta el riesgo de que puedan quedarse atascados por años en el proceso de desarrollo. Mientras tanto, el Ejército no estará más cerca de obtener una capacidad SU ciberespacial de lo que estaba en 2013 cuando en el informe del Army Cyberspace Operations Capabilities Based Assessment se determinó que la comprensión situacional de los comandantes era su principal deficiencia[30].

Conclusión

Si ganan, los otros equipos pueden ocasionarnos problemas[31].

—Yogi Berra

Si bien varios recursos actualmente ayudan a proporcionar la SU ciberespacial, al Ejército le falta una iniciativa de desarrollo de capacidades bien coordinada para definir y agregar los requerimientos relacionados a la SU ciberespacial. Aunque el proceso JCIDS proporciona opciones de desarrollo con disponibilidades de corto tiempo, todavía parece inadecuado, según lo demostró la incapacidad del Ejército de aprobar la SU ciberespacial, o los documentos JCIDS ciberespaciales relacionados[32]. Cualquiera que sea el caso, los comandantes no pueden seguir renunciando a tomar decisiones operacionales clave acerca del OE porque no comprenden el dominio.

La SU ciberespacial puede que no resulte ser una herramienta, o sistema autónomo. O mejor dicho, la respuesta podría ser una suma de varias capacidades habilitadoras de la comprensión situacional. Por consiguiente, puede que al Ejército le vaya mejor con un sistema improvisado que le proporcione, en la actualidad, cierta SU ciberespacial, en lugar de un sistema curalotodo que prometa solucionar el mundo mañana.

Gran parte de los enemigos de Estados Unidos no tienen burocracias, ni un conducto vertical aislado que merma su capacidad de usar nuevas tecnología en el campo de batalla. De manera que, mientras los desarrolladores de capacidades del Ejército definen los requerimientos analizando las opciones y dirigiendo la orquestación de la documentación y autorización del JCIDS, los adversarios potenciales estarán jugando «pequeñas ligas» y ganando la competencia ciberespacial mediante el uso de tecnologías estándares. A fin de hacer una reaparición, el Ejército necesita una jugada que cambie el juego. Porque, enfrentémoslo, «el futuro no es lo que solía ser»[33]. ■

El teniente coronel (retirado) Jay Martin, Fuerza Aérea de EUA, es un analista militar de alto nivel de la compañía Command Decision Systems & Solutions, Inc. Cuenta a su haber con una licenciatura de la Universidad de Delaware y una maestría de Lousiana Tech University. Es egresado de la Escuela de Armamento de la Fuerza Aérea de EUA, Escuela Superior de Comando y Estado Mayor de la Fuerza Aérea y Escuela de Estado Mayor de las Fuerzas Conjuntas.

Emily Kaemmer es una analista militar de alto nivel de la compañía Command Decision Systems & Solutions, Inc. Es especialista en el desarrollo de capacidades ciberespaciales.

Referencias Bibliográficas

1. Yogi Berra, *The Yogi Book: I Really Didn't Say Everything I Said!* (New York: Workman Publishing Company, 1998).

2. Army Doctrine Publication (ADP) 5-0, *The Operations Process* (Washington, DC: U.S. Government Printing Office [GPO], mayo de 2012). La comprensión situacional es el producto de usar el análisis y criterio en la información relevante para determinar la relación que existe entre las variables operacionales y de misión para facilitar el proceso de toma de decisión. Para fines de este artículo, se pone en el mismo plano que el conocimiento situacional, el cual no está definido en la doctrina conjunta o del Ejército.

3. El término comprensión situacional ciberespacial (SU ciberespacial) se refiere a una capacidad de especulación que proporciona datos e información relevantes acerca del ciberespacio para mostrarlo en una imagen operacional común, o en el tablero de instrumento del comandante. La SU ciberespacial (capacidad) se distingue de la frase concienciación situacional ciberespacial, que según la Joint Publication (JP) 3-12(R), *Cyberspace Operations*, (Washington, DC: U.S. GPO, febrero de 2013), se refiere al requerimiento actual y conocimiento previsible del ciberespacio y del ambiente operacional del que dependen las operaciones ciberespaciales, incluso, todos los factores que afectan a las fuerzas ciberespaciales amigas y enemigas.

4. Yogi Berra, *The Yogi Book*. Said on Yogi Berra Appreciation Day, Saint Louis, Missouri, 1947.

5. Departamento de Defensa, *The Joint Concept for Cyberspace* (JCC) (agosto de 2012), pág. 9. (FOUO)

6. Joint Cyber Situational Awareness (Cyber SA) Initial Capabilities Document (ICD), 23 de abril de 2012, aprobada por el Joint Chiefs of Staff Requirements Oversight Council (JROC). Disponible en el Sistema de Administración de Conocimiento y Apoyo de Decisión JROC (KM/DS)

7. Esta declaración pertenece a la evaluación de los autores luego de comparar el Joint Cyber SA ICD con el Informe final del Army Cyber Command (ARCYBER)/2nd Army Support Element, *Army Cyberspace Operations Capabilities Based Assessment* (CBA) (Comando de Adiestramiento y Doctrina del Ejército de EUA [TRADOC], 15 de diciembre de 2013), 34. Ver Figura 9, «Priorización del análisis de necesidad funcional» y enviar solicitud de documento a ARCYBER.

8. TRADOC Pamphlet (TP) 525-3-0, *The U.S. Army Capstone Operating Concept* (Fort Eustis, VA: TRADOC 2012, pág. 28.

9. Ibíd., pág. 33.

10. TP 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World* (Fort Eustis, VA: TRADOC, 2014).

11. JP 3-12(R), *Cyberspace Operations* (Washington, DC: U.S. GPO, febrero de 2013)

12. Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: U.S. GPO. mayo de 2012, págs. 2.

13. Manual de campaña 6-02, *Signal Support to Operations* (Washington, DC: U.S. GPO. enero de 2014).

14. Brett T. Williams, «Ten Propositions Regarding Cyberspace Operations», *Joint Force Quarterly* 61 (2º trimestre, 2011): 15. General de división (retirado) Williams es el ex J3 del Comando Cibernético de EUA.

15. Ibíd.

16. Yogi Berra y Dave Kaplan, *When You Come to a Fork in the Road, Take It!: Inspiration and Wisdom From One of Baseball's Greatest Heroes* (New York: Hyperion Books, 2001).Broadway Books, 2001):

17. Joint Requirements Oversight Council, *Manual for the Operation of the Joint Capabilities Integration and Development System* (JCIDS Manual) (12 de febrero de 2015).

18. Una búsqueda del Sistema de Administración del Consejo de Vigilancia de las Capacidades y Requerimientos reveló que, hasta el momento, el Ejército no ha aprobado ningún documento relacionado al ciberespacio; mientras tanto, la Fuerza Aérea y la Armada ya tienen varios documentos aprobados.

19. David G. Perkins, «Win in a Complex World'-But How?» *Army AL&T Magazine* (enero–febrero de 2015).

20. Ibíd.

21. Ibíd.

22. Manual JCIDS. Documentos de Desarrollo de Capacidades del Sistema de Información (CDD, por sus siglas en inglés) permite que los patrocinadores describan los valores mínimos iniciales para los parámetros de rendimiento clave, características clave del sistema y otras características de rendimiento. Los patrocinadores de los sistemas de software que se benefician de la inserción de tecnología permanente, pueden aprobar el seguimiento de documentos internamente en lugar de a través del Joint Requirements Oversigh Council.

23. Matthew Maier y Jerry Cook, «Hacking Cyber Stovepipes», *Army AL&T Magazine* (edición de enero–marzo de 2015).

24. Las tres oficinas ejecutivas del programa (PEO) que desempeñan papeles clave en cuanto al apoyo de las tecnologías ciberespaciales son las siguientes: (1) Mando, Control y Comunicaciones-Táctico (PEO C3T); (2) Sistema de información empresarial (PEO EIS); y (3) Inteligencia, Guerra electrónica y Sensores (PEO IEW&S). La PEO C3T es la oficina principal de la red táctica, La PEO EIA es la oficina principal para la defensa de la red empresarial y la PEO IEW&S es la oficina principal para las iniciativas ciberespaciales de las operaciones de defensa.

25. Maier and Cook, «Hacking Cyber Stovepipes».

26. Ibíd.

27. Yogi Berra y Dave H. Kaplan, *You Can Observe a Lot by Watching: What I've Learned About Teamwork From the Yankees and Life* (Hoboken, NJ: John Wiley & Sons, 2008).

28. Field Manual (FM) 6-0, *U.S. Commander and Staff Organization and Operations* (Washington, DC: U.S. GPO. mayo de 2014, págs.

29. Department of Defense, Instruction 5000.02, Operation of the Defense Acquisition System, 7 de enero de 2015, accedido el 26 abril de 2016, http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf. Serán necesarios varios sistemas de desarrollo y despliegues de software típicamente a fin de satisfacer los requerimientos aprobados para un incremento de capacidad.

30. ARCYBER/2nd Army Support Element, *Army Cyberspace Operations*.

31. Michael J. Pellowski, *The Little Giant Book of Baseball Facts* (New York: Sterling Publishing Company, 2007).Workman Publishing Company, 2007).

32. Una búsqueda del Capabilities and Army Requirement Oversight Council Management System reveló que, hasta el momento, el Ejército no ha aprobado ningún documento relacionado al ciberespacio; mientras tanto, la Fuerza Aérea y la Armada tienen varios documentos aprobados.

33. Esta es una cita mal atribuida que Yogi Berra alega jamás haber dicho. Sin embargo, hay fuentes contrarias. Ver Berra y Kaplan, *When You Come to a Fork in the Road, Take It.*