La aplicación de visualización digital, o DVA, proporciona al Ejército una solución de conmutación de vídeo basada en software y permite al personal del puesto de mando conectarse a la red de área local para compartir toda o parte de su pantalla con otras personas o en el sistema de visualización más grande de puesto de mando. (Simulación de foto cortesía del Ejército de EUA)

Localizar al enemigo en el campo de batalla saturado de datos en 2035

Capitán T. S. Allen, Ejército de EUA

Para localizar al enemigo hoy en día, las fuerzas armadas apuntan a los recursos de recopilación de información, que pueden identificar cualquier cosa, desde un indicio visual hasta una frecuencia de radio única, en la dirección que creen que está el enemigo hasta que determinan la ubicación del mismo. Este modelo es anticuado porque el crecimiento del ciberespacio en una red de control global

que conecta dispositivos ha creado un nuevo campo de batalla saturado de datos, cubierto por miles de millones de dispositivos en red que comparten constantemente información y pueden ser explotados para localizar al enemigo de manera más eficiente[1].

Para 2035, en el campo de batalla saturado de datos las fuerzas armadas normalmente localizarán al enemigo explotando los datos en el ciberespacio y en el entorno de información más amplio, en lugar de observar a las fuerzas enemigas directamente con sus propios medios de recopilación de información[2]. Sencillamente, el enemigo va a emitir donde está, o terceros van a emitir donde está el enemigo, tan a menudo como las fuerzas armadas van a apuntar una cámara o antena al enemigo para encontrarlo. Las fuerzas armadas consultarán constantemente una amplia variedad de bases de datos con información del ciberespacio, tanto de acceso público como adquirida con sensibilidad, para obtener indicadores de dónde se encuentra el enemigo. En lugar de buscar al enemigo visual o electrónicamente, las fuerzas armadas más eficaces lo buscarán en Google, utilizando herramientas de inteligencia que explotan el ciberespacio.

En el campo de batalla digital, la fuerza armada mejor posicionada para aprovechar el ciberespacio y encontrar al enemigo tendrá una ventaja significativa. El Ejército de EUA necesita romper y rehacer su modelo de inteligencia táctica con el fin de prepararse para ganar en estas condiciones.

Localizar blancos en el campo de batalla de 2035

Ya está en marcha la transformación de la inteligencia táctica para centrarse en el ciberespacio[3]. Los enemigos de Estados Unidos han estado atacando a sus fuerzas basándose en mensajes en los medios sociales después de que hubiera brechas de seguridad operacional por lo menos desde 2007[4]. Por su parte, las Fuerzas Armadas de EUA han bombardeado a terroristas que cometieron el error de publicar autofotos que revelaban su ubicación[5]. A medida que siga aumentando el número de dispositivos conectados a la red y la frecuencia con que las personas los utilizan para difundir información de manera intencional o no intencional, también seguirá aumentando la utilidad de las actuales corrientes de datos cibernéticos para identificar la ubicación de cualquier cosa, ya sea un consumidor o un vehículo de combate blindado[6]. Con el tiempo, el ciberespacio y el ambiente de información más amplio se convertirán, casi con toda seguridad, en la principal fuente de inteligencia de Estados Unidos, incluyendo la inteligencia táctica sobre la ubicación y la disposición de las fuerzas enemigas. Si bien las fuerzas de EUA seguirán utilizando los medios tradicionales de recopilación de información para determinar la ubicación de las unidades enemigas y localizarlas con exactitud, también dependerán cada vez más de la información del ciberespacio para determinar dónde deben apuntar esos sensores en primer lugar. Después de todo, no hay necesidad de patrullar toda una provincia en busca de una columna de tanques enemigos cuando alguien publica una autofoto que muestra los tanques en el fondo o cuando el movimiento de una columna de tanques a lo largo de una autopista causa una perturbación masiva en las pautas de tráfico civil bien establecidas que pueden ser fácilmente identificadas en los datos de tráfico recogidos por las aplicaciones de navegación en los teléfonos celulares.

Hasta la fecha, la transformación de la inteligencia táctica por el ciberespacio ha sido más evidente en la disciplina de la inteligencia de fuente abierta (OSINT). Desde el establecimiento de la «Web Social», también conocida como «Web 2.0», a finales de los 90, el contenido generado por el usuario en los medios sociales ha sido fundamental en la cultura de Internet. Además, los teléfonos inteligentes, que permiten a los usuarios cargar contenidos desde casi cualquier lugar para capturar y difundir imágenes con rapidez, han pasado a funcionar como miles de millones de dispositivos de recopilación de información en red que comparten públicamente muchas de sus conclusiones en los medios sociales. El resultado ha sido la proliferación de

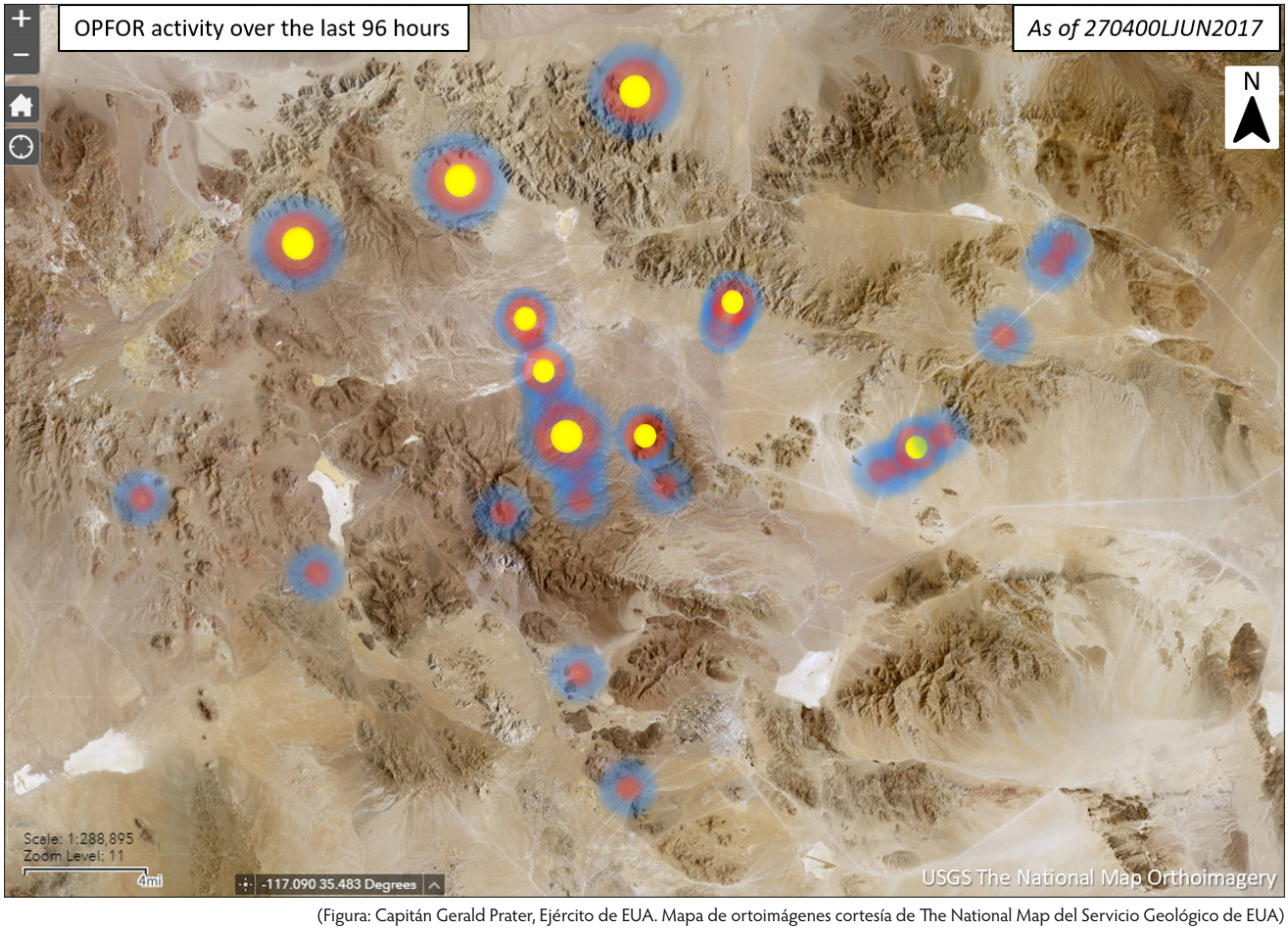
El capitán T. S. Allen, Ejército de EUA, es un oficial de inteligencia militar que sirve en el Grupo de Guerra Asimétrica en Fort George G. Meade, Maryland. Anteriormente sirvió en Afganistán y Corea del Sur, y está calificado para planificar operaciones ciberespaciales y de información. Allen tiene una licenciatura en Ciencias Políticas e Historia Militar de la Academia Militar de EUA en West Point, Nueva York, y una maestría en Estudios de Guerra del King's College en Londres.

Los soldados configuran el entorno de computación táctica en modo extensivo, que junta varios puntos en un mapa digital para crear un mapa grande similar al que está disponible en puestos de mando más grandes. Esta tecnología puede ayudar a los soldados a colaborar y aumenta la conciencia situacional en toda la formación al compartir una imagen operativa común casi en tiempo real del «campo de batalla saturado de datos». (Fotografía cortesía del Ejército de EUA)

información disponible públicamente de valor operacional y de inteligencia[7]. Incluso las organizaciones civiles hoy en día tienen la capacidad de llevar a cabo evaluaciones de inteligencia con un alto grado de precisión utilizando estos datos. En un ejemplo notable, el Consejo Atlántico y Vice News pudieron identificar a soldados rusos individuales que luchaban encubiertamente en Ucrania basándose en su actividad en los medios de comunicación social en 2014[8]. Del mismo modo, el sitio web de periodismo de investigación Bellingcat ha podido ofrecer consistentemente evaluaciones de inteligencia de alta calidad basadas casi exclusivamente en lo que denomina «inteligencia de fuente abierta» derivada de los medios de comunicación social. Como señala el analista civil de fuentes abiertas Cameron Colquhoun, «Entre los miles de millones de mensajes, cargas de archivos y acciones de compartir y gustar, las personas una y otra vez traicionan sus intereses a los observadores minuciosos»[9].

Sin embargo, según mi experiencia como oficial de inteligencia, la OSINT no se ha convertido en la fuente principal de inteligencia táctica. En primer lugar, depende en gran medida de que los usuarios, que no están controlados o investigados, compartan libremente información sobre eventos de interés. En segundo lugar, estos usuarios tienen fuertes razones para no monitorear a las fuerzas militares, porque estas fuerzas están armadas y son peligrosas. Incluso cuando los usuarios lo hacen, rara vez lo hacen de manera persistente, y como la inteligencia táctica es rápidamente perecedera, la OSINT solo es rara vez útil para encontrar al enemigo a nivel táctico.

De aquí al 2035, el ciberespacio completará otra transformación masiva como la que se ha visto anteriormente con los teléfonos inteligentes y los medios de comunicación social, y sus en la inteligencia táctica serán aún más significativos. La nueva transformación está impulsada por el auge de la «Internet de



(Figura: Capitán Gerald Prater, Ejército de EUA. Mapa de ortoimágenes cortesía de The National Map del Servicio Geológico de EUA)

Mapa de calor de la ubicación de fuerzas opuestas en el Centro Nacional de Entrenamiento en 2017

Dos innovadores tenientes reprodujeron el mapa utilizando datos de localización de los medios sociales, que podrían haberse producido desde cualquier parte del mundo, sin necesidad de un equipo especial de inteligencia.

las cosas» (IoT). El ciberespacio ya ha pasado de ser una red de comunicación mundial que conecta a las personas a una red de control mundial que conecta los dispositivos, como sostiene Laura DeNardis en *The Internet in Everything: Freedom and Security in a Network World* (La Internet en todo: Libertad y seguridad en un mundo de redes)[10]. Actualmente, los dispositivos son responsables de más actividad en el ciberespacio que las personas, y el ciberespacio se utiliza para controlar todo, desde los termostatos en los hogares privados hasta los sistemas de control industrial en las fábricas. Debido a que la IoT está en gran medida automatizada, los usuarios cuyo comportamiento incontrolable limitó la utilidad táctica de la OSINT derivada de la Web 2.0 ahora son irrelevantes. «Si los humanos desaparecieran repentinamente de la tierra», escribe DeNardis, «el mundo digital seguiría vibrando»[11]. La doctrina del ciberespacio del Ejército probablemente cambiará para reflejar esto. Mientras que las características doctrinales actuales del ciberespacio enfatizan que el ciberespacio es «socialmente habilitante», el Ejército ya tiene amplias razones para caracterizar el ciberespacio como «automatizado en su mayor parte»[12].

La IoT presenta emocionantes oportunidades de inteligencia táctica. Si la inteligencia y las operaciones cibernéticas se integran de manera eficaz, la IoT podría convertirse en una mina de oro sin precedentes de inteligencia, dando a los recopiladores de inteligencia acceso a un sinnúmero de sensores para encontrar al

enemigo. Mientras que durante la guerra de Vietnam Estados Unidos trató de monitorear amplias zonas lanzando desde el aire miles de sensores en la selva, en el futuro se podrían alcanzar objetivos similares explotando los sensores civiles que ya están en uso[13]. Los dispositivos tales como las cámaras de seguridad doméstica tienen información de valor de inteligencia si se apuntan al lugar correcto; dado lo común que se han vuelto, es seguro que algunos sensores de IoT estarán apuntando a áreas de interés al menos en algún momento. Además, los dispositivos de IoT son infamemente inseguros, como lo demuestran regularmente los *hackers*[14]. A principios de 2020, el 98 % del tráfico de IoT no estaba encriptado, lo que facilitaba enormemente su explotación[15]. Las principales desventajas importantes de la explotación de sensores de IoT son que no pueden controlarse técnicamente y que son vulnerables al engaño y manipulación, pero estas debilidades se comprobarán por la enorme escala de datos disponibles, que pueden utilizarse para añadir cada vez más información con la que hacer evaluaciones.

A medida que se desarrolla la IoT, una práctica común emergente y significativa es que la mayoría de los vehículos transmiten datos sobre su ubicación. Aunque el Ejército no encontrará principalmente al enemigo dentro de Estados Unidos, las prácticas cibernéticas de EUA suelen proliferar en todo el mundo, por lo que son un indicador importante. Hoy en día, en Estados Unidos, todas las aeronaves ya emiten sus ubicaciones a través del Sistema de Vigilancia Dependiente Automática-Difusión (ADS-B), y la mayoría de los buques hacen lo mismo a través del sistema de identificación automática. El Departamento de Transporte de EUA también aboga por el empleo de sistemas de comunicaciones de seguridad de vehículo a vehículo para la mayoría de los automóviles privados que emitirían datos de localización[16]. Para 2035, sistemas como el ADS-B, el sistema de identificación automática, y el de vehículo a vehículo, casi seguro que proliferarán en todo el mundo. Si bien estos sistemas están diseñados para garantizar la seguridad y un mínimo de privacidad,

Un mapa de calor de 2018 que muestra el movimiento de soldados basado en los datos de localización recogidos por la aplicación de preparación física Strava en la Base Aérea de Bagram en Afganistán. (Captura de pantalla cortesía de Strava Labs)

ya que siguen compartiendo datos de localización, en la práctica harán posible que cualquier dispositivo automatizado debidamente equipado pueda monitorear fácilmente todos los movimientos de los vehículos. Además, si el ADS-B sirve de guía, es probable que los sensores fijos que monitorean la actividad de movimiento y la comparten automáticamente en el ciberespacio se conviertan en algo común para satisfacer la demanda pública de datos sobre el tráfico. Como descubrió la Oficina de Contabilidad del Gobierno de EUA en una evaluación del ADS-B realizada en 2018, estos sistemas plantean graves riesgos para la seguridad operacional de las fuerzas militares, incluyendo las nuestras, porque podrían exigirnos que transmitiéramos la localización de actividades militares delicadas[17].

También hay una norma emergente pero controvertida de que los seres humanos compartan datos sobre su ubicación en el ciberespacio a través de sus teléfonos y dispositivos portátiles de IoT. El Departamento de Defensa recibió un sorprendente recordatorio de esto en 2018 cuando Strava, una empresa de dispositivos de acondicionamiento físico, publicó un mapa de calor basado en los usuarios que destacaba las rutas de carrera en las bases militares de todo el mundo[18]. Recibió otro en 2019, cuando el *New York Times* informó de que utilizaba datos de localización de teléfonos celulares para rastrear los movimientos de un alto funcionario del Departamento de Defensa[19]. Es probable que el compartir de datos de localización continúe porque, como sostiene Shoshanna Zuboff, las corporaciones se benefician de la explotación de los datos de localización de los usuarios y la mayoría de los usuarios están dispuestos a proporcionarlos. Si bien muchas personas se sienten incómodas con la idea de ser rastreadas individualmente, a menudo tienen pocas objeciones a que se compartan datos que se etiquetan como «agregados» o «anónimos»[20]. La pandemia de COVID-19 ha atraído mucho más la atención del público hacia los rastreadores de localización de teléfonos celulares[21]. Durante la pandemia, Google utilizó su base de datos de ubicaciones de usuarios de teléfonos inteligentes para proporcionar informes detallados a los funcionarios de salud pública sobre los patrones de vida en todo el mundo y los publicó[22]. En un caso de uso más pertinente, una empresa de análisis geoespacial del sector privado informó de que las fábricas de armas rusas estaban ralentizando la producción aprovechando datos similares para ver cuántos empleados de la fábrica se presentaban a trabajar durante la pandemia[23]. Curiosamente, solo cinco días después, el Gobierno ruso prohibió al personal militar llevar teléfonos inteligentes que rastrean la ubicación de los usuarios[24].

Para el 2035, entonces, viviremos en un mundo en el que la mayoría de los movimientos generan una huella en el ciberespacio.

Para el 2035, entonces, viviremos en un mundo en el que la mayoría de los movimientos generan una huella en el ciberespacio. El movimiento vehicular será fácil de rastrear, y como mínimo, se podrán ver las tendencias generales del movimiento humano individual. Es probable que nadie instale sistemas de rastreo en los vehículos militares, pero eso no reducirá el valor de inteligencia de esta enorme fuente de datos. Las fuerzas militares maniobrarán a través de un campo de batalla saturado de datos, donde cada acción «oculta» que realicen provocará una reacción fácilmente observable. Aunque no emitan nada, estas fuerzas serán indirectamente visibles en el ciberespacio cuando interrumpan las pautas normales de vida, cuando causen atascos al conducir por las autopistas, cuando la gente publique información sobre sus actividades en los medios sociales y cuando entren en el campo de visión de dispositivos de IoT explotables como las cámaras de seguridad. En muchos casos, los analistas podrán localizar al enemigo identificando las alteraciones de las pautas normales de vida que muestren una *inactividad atípica* en un área determinada. Lo llamo «inteligencia negativa», similar al vacío significativo del «espacio negativo» en los medios visuales. Si bien las organizaciones militares

no necesariamente pueden lanzar fuegos letales contra objetivos identificados solo en el ciberespacio, el ciberespacio proporcionará la capa de base de inteligencia en la que las fuerzas de inteligencia encontrarán al enemigo. Los medios tradicionales de recopilación de información seguirán desempeñando un papel importante, pero se centrarán en la localización de las fuerzas enemigas que se encuentran en el ciberespacio. La fuerza que esté mejor preparada para acceder a la amplia variedad de información de valor de inteligencia en el ciberespacio tendrá una ventaja decisiva sobre otra fuerza que se limite a menos medios de recopilación de información técnicamente controlados que solo podrá recopilar una cantidad de datos exponencialmente menor.

Este no es el campo de batalla tradicional

El campo de batalla saturado de datos de 2035 presenta interesantes oportunidades de inteligencia, como también enormes desafíos para el Ejército de EUA. Para lograr una ventaja decisiva, el Ejército debe hacer cambios fundamentales en su modelo de inteligencia táctica, incluso más allá de los cambios señalados en *The U.S. Army in Multi-Domain Operations 2028*, que describe su visión futura pero no menciona la IoT[25]. Estos cambios son imperativos porque si no se implementan, el Ejército podría encontrarse con una sobrecarga crónica de información, incapaz de llevar a cabo el mando tipo misión, y luchando en futuras guerras sin muchas de sus ventajas históricas.

En primer lugar, y lo más importante, el Ejército debe prepararse para explotar la información del ciberespacio en instalaciones de inteligencia centralizadas y altamente automatizadas que se centran en el apoyo a la toma de decisiones tácticas que identificarán la información de valor táctico, la procesarán, la explotarán y la difundirán a las formaciones tácticas para la acción. Históricamente, tenía sentido que el Ejército esperara que los comandantes encontraran

El especialista Nathaniel Ortiz, Equipo Expedicionario de Actividades Cibernéticas y Electromagnéticas (CEMA), 781° Batallón de Inteligencia Militar, lleva a cabo operaciones en el ciberespacio el 9 de mayo de 2017 en el Centro Nacional de Entrenamiento, Fort Irwin, California. Más recientemente, el 915° Batallón de Apoyo de Guerra en el Ciberespacio, activado el 1° de enero de 2019, es la primera capacidad expedicionaria orgánica escalable que cumple con los requisitos tácticos actuales y previstos del Ejército en materia de CEMA. (Foto de Bill Roche, Comando Cibernético del Ejército de EUA)

Integrantes del 6º Escuadrón de Operaciones Especiales utilizan una tableta para cargar las coordenadas el 17 de diciembre de 2019 durante un ejercicio que demuestra las capacidades del sistema avanzado de gestión de combate (ABMS) en Duke Field, Florida. Durante la primera demostración del ABMS, los operadores de la Fuerza Aérea, Ejército, Armada y la industria probaron múltiples herramientas y tecnología de intercambio de datos en tiempo real en un escenario basado en la defensa nacional promulgado por el Comando Norte de EUA y posibilitado por los altos líderes de la Fuerza Aérea. (Fotografía: Sargento Técnico Joshua J. García, Fuerza Aérea de EUA)

muchos de sus propios objetivos porque podían hacerlo con los medios de recopilación de información de acceso cercano en sus formaciones. El campo de batalla saturado de datos cambiará esto ya que la mayoría de los dispositivos de IoT están diseñados para ser conectados en red y compartir información a nivel mundial, haciendo que el acceso cercano sea menos importante. Los dispositivos de IoT comparten datos a través de un ciberespacio que será cada vez más «centralizado», con corporaciones masivas como TenCent en China y Yandex en Rusia controlando una parte sin precedentes de todos los datos[26].

Si bien la centralización de Internet requerirá la centralización de la recopilación de información de inteligencia, la toma de decisiones del Ejército debe seguir siendo ampliamente distribuida para mantener la flexibilidad táctica. Como resultado, los nuevos centros de inteligencia tendrán que mejorar la difusión de lo que saben hasta el nivel táctico, principalmente a través de las existentes brigadas de inteligencia militar de teatro de operaciones asignadas a los ejércitos de campo, para aumentar los sensores de acceso cercano[27]. Debido a la enorme cantidad de datos que deben ser procesados, la inteligencia artificial y aprendizaje automatizado se convertirán en la clave del procesamiento y explotación. Los encargados de la recopilación de inteligencia en el campo de batalla de 2035 modificarán los algoritmos para responder a sus necesidades de información. De lo contrario, es casi seguro que se enfrentarán a una sobrecarga de información y a fallos de la inteligencia[28]. La ampliación de las capacidades de la inteligencia y el aprovechamiento de las economías de escala en los niveles superiores ayudarán a evitar la creación de una sobrecarga de información en los escalones inferiores.

En segundo lugar, para explotar adecuadamente el campo de batalla saturado de datos, el Ejército debe

romper la canalización de información entre las comunidades cibernéticas y de inteligencia. Las capacidades excelentes que se utilizan actualmente para la inteligencia, vigilancia y reconocimiento en el ciberespacio tendrán que volver a utilizarse para responder a los requisitos de inteligencia de los comandantes de maniobra[29]. En lugar de limitarse a lograr un conocimiento de la situación del ciberespacio, como afirma la doctrina actual, las fuerzas cibernéticas tendrán que habilitar a las fuerzas de inteligencia logrando un conocimiento de la situación de todos los dominios a través del ciberespacio[30]. Esto requerirá que las fuerzas cibernéticas y de inteligencia compartan información fluidamente en apoyo de los comandantes tácticos, como parte de la «convergencia», el objetivo del Ejército de lograr la «integración rápida y continua de todos los dominios a través del tiempo, espacio y capacidades para superar al enemigo»[31].

En tercer lugar, el Ejército necesita prepararse para que sus propias acciones a nivel táctico sean visibles en el ciberespacio. Cada nueva oportunidad de inteligencia es también una potencial amenaza a la seguridad operacional. El modelo de seguridad operacional del Ejército corre el riesgo de quedarse obsoleto; sigue centrado en el control de las emisiones, pero para 2035 tendrá que controlar u ofuscar las emisiones de los dispositivos civiles que monitorearán constantemente a las fuerzas del Ejército en el campo de batalla saturado de datos. Dado que es imposible controlar todos esos dispositivos, la ofuscación y el engaño adquirirán mayor importancia, incluso en los niveles tácticos[32]. Los planificadores de seguridad operacional del Ejército también deben pensar cada vez más «de cara al futuro» y prepararse para luchar y ganar incluso después de que sus actividades sean divulgadas al mundo entero. El Ejército tendrá que impulsar las capacidades mejoradas de ofuscación y engaño a niveles más bajos que nunca, muy por debajo del nivel de cuerpo de ejército, que es actualmente el nivel más bajo en el que se prevén desplegar capacidades militares de engaño[33]. En el campo de batalla saturado de datos, incluso las pequeñas unidades tácticas necesitarán el equivalente cibernético de máquinas de niebla.

En cuarto lugar, el Ejército debe tomar medidas deliberadas para conservar el mando tipo misión cuando la tecnología permita la microgestión. Como escribió el mariscal de campo McLuhan en 1964, «A largo plazo, el contenido de un medio importa menos que el propio medio para influir en la forma en que pensamos y actuamos»[34]. La tecnología avanzada de

Para aquellos interesados en leer más sobre la defensa cibernética, la redacción de *Military Review* recomienda la edición de primavera de 2020 de *The Cyber Defense Review* (CDR). La revista CDR es un esfuerzo académico del Instituto Cibernético del Ejército en West Point, Nueva York. La CDR genera un diálogo intelectual multidisciplinario a través de artículos y ensayos académicos que invitan a la reflexión sobre los aspectos estratégicos, operacionales y tácticos del dominio cibernético. La CDR rompe las barreras y fomenta soluciones innovadoras para los desafíos de la seguridad cibernética mundial. La CDR recopila perspectivas de pensadores preeminentes en todo el gobierno, industria y el mundo académico con respecto a los potenciales desafíos, impactos e iniciativas para consideración mientras resolvemos los problemas futuros para el Ejército y la Nación. Para ver la edición de primavera de 2020 de la CDR, visite https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Summer%202000/CDR%20V5N2%20Summer%202020-r8-1.pdf.

mando y control casi siempre socava el mando tipo misión porque facilita la microgestión. Cuando el telégrafo se utilizó por primera vez en las operaciones militares en la guerra de Crimea en 1855, el comandante general francés descubrió inmediatamente que «el extremo paralizante de un cable eléctrico» facilitaba a sus dirigentes en París la tarea de darle órdenes sin la información adecuada y le dificultaba responder a las situaciones sobre el terreno a medida que estas se desarrollaban[35]. En el futuro, cuando el comandante de un batallón en un centro de operaciones tenga más información sobre el lugar donde se encuentra una fuerza enemiga que el líder de un pelotón en contacto con esa misma fuerza enemiga, el comandante del batallón estará tentado de microgestionar al líder del pelotón. Sin embargo, la flexibilidad del mando tipo misión sigue dando a las fuerzas de EUA una ventaja decisiva[36]. Como resultado, debemos tomar medidas cuidadosas para conservar el mando tipo misión centrado en el ser humano dentro de nuestras fuerzas a medida que avanza la tecnología.

En quinto lugar, el Ejército debe ser sensible a las preocupaciones técnicas civiles-militares que surgirán en el campo de batalla saturado de datos. Los «datos» son casi todos propietarios y controlados por la industria privada. Si bien las empresas privadas con acceso a esos datos participan en un próspero mercado de datos sobre las actividades de los ciudadanos particulares en todo el mundo, los intermediarios de datos pueden ser reacios a compartir información con las fuerzas armadas que la utilizarán con fines militares o de inteligencia. Las relaciones con estos intermediarios de datos serán más importantes que nunca (y también probablemente más tensas). Habida cuenta de los derechos de privacidad y otras preocupaciones legítimas en materia de protección de datos, la explotación de datos sobre objetivos extranjeros que son propiedad de empresas situadas en Estados Unidos o en naciones aliadas seguirá siendo una cuestión espinosa. Además, la explotación de dispositivos civiles probablemente planteará nuevas cuestiones de derecho de la guerra.

En último lugar, el Ejército debe reconocer que hay una posibilidad real de que sus adversarios tengan una ventaja en la lucha de inteligencia táctica del ciberespacio. Muchas de las ventajas materiales que ofrecen excelentes recursos de recopilación de información existentes del Ejército serán menos importantes en el campo de batalla saturado de datos y, como resultado, se tendrán que desarrollar nuevas ventajas no materiales. El hecho de que Estados Unidos haya liderado la revolución de la información no significa que el Ejército de EUA esté en las mejores condiciones para dominar los futuros campos de batalla[37].

Muchos adversarios de Estados Unidos pueden ser superiores en este campo. Como David Kilcullen demuestra en su libro *The Dragons and the Snakes: How the Rest Learned to Fight the West*, publicado en 2020, los adversarios de Estados Unidos ha conseguido sacar ventaja explotando sistemas que fueron puestos a disposición de la población en general, como la Internet y el GPS[38]. Dado que muchas actividades en el ciberespacio tienen necesidades de recursos relativamente bajas y, sobre todo, requieren una adaptación a un entorno cibernético en constante cambio, los agentes no estatales ágiles y sin restricciones tienen una ventaja sobre las grandes burocracias estatales como el Ejército[39]. Hay señales prometedoras de que el Ejército también puede innovar, como los ejemplos de soldados que descubrieron cómo localizar a las fuerzas enemigas explotando aplicaciones sociales como Tinder y Snapchat que revelan datos de localización[40]. Si bien los innovadores de abajo hacia arriba no pueden construir las soluciones centralizadas y escalables que necesita el Ejército, este debe hacer más para habilitar a los innovadores *hackers* en sus filas[41].

Conclusión

Los datos que se extenderán en todo el campo de batalla de 2035 y cambiarán fundamentalmente la inteligencia táctica ya se están acumulando lentamente en las bases de datos de todo el mundo. En los futuros campos de batalla, los medios tradicionales de recopilación de información seguirán desempeñando un papel fundamental para permitir a las fuerzas armadas localizar las fuerzas enemigas, pero debido a la proliferación de dispositivos en red que difunden automáticamente cantidades asombrosas de datos en la IoT, la fase de *localización* en el proceso de selección de blancos tendrá un enfoque cibernético. Para mantener sus ventajas en los futuros campos de batalla, el Ejército debe mejorar su capacidad para localizar al enemigo en el ciberespacio en apoyo de la inteligencia táctica, a partir de ahora.

Notas

1. Para ver una discusión de un campo de batalla saturado de fuegos, véase Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 30. El término «campo de batalla saturado de datos» es propio del autor y original en el presente artículo. Es una referencia al «campo de batalla saturado de fuegos», que caracteriza al combate terrestre contemporáneo.

2. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, desde junio de 2020), 55 y 104, accedido 15 de septiembre de 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727. El «ciberespacio» se define como «un dominio mundial dentro del entorno de información que consta de las redes interdependientes de infraestructuras de información de tecnología y datos residentes, incluyendo la Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados». El «entorno de información» se define como «el conjunto de personas, organizaciones y sistemas que recolectan, procesan, difunden o actúan basado en la información».

3. T. S. Allen y Robert A. Heber Jr., «Where Posting Selfies on Facebook Can Get You Killed», *Wall Street Journal* (sitio web), 26 de julio de 2018, accedido 15 de septiembre de 2020, https://www.wsj.com/articles/where-posting-selfies-on-facebook-can-get-you-killed-1532642302.

4. «Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq», Military.com, 15 de marzo de 2012, accedido 15 de septiembre de 2020, https://www.military.com/defense-tech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq.

5. Walbert Castillo, «Air Force Intel Uses ISIS "Moron" Post to Track Fighters», CNN, 5 de junio de 2015, accedido 15 de septiembre de 2020, https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html?mod=article_inline.

6. Stuart A. Thompson y Charlie Warzel, «Twelve Million Phones, One Dataset, Zero Privacy», *New York Times* (sitio web), 19 de diciembre de 2019, accedido 15 de septiembre de 2020, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

7. Heather J. Williams y Ilana Blum, «Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise» (Santa Monica, CA: RAND Corporation, 2018), accedido 15 de septiembre de 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

8. «Selfie Soldiers: Russia Checks in to Ukraine», VICE News, 16 de junio de 2015, accedido 15 de septiembre de 2020, https://www.vice.com/en_us/article/bjk9na/selfie-soldiers-russia-checks-in-to-ukraine.

9. Cameron Colquhoun, «A Brief History of Open Source Intelligence», Bellingcat, 14 de julio 2016, accedido 15 de septiembre de 2020, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

10. Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, CT: Yale University Press, 2020).

11. *Ibid*., 3.

12. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 11 de abril de 2017), párrafo 1-64, accedido 15 de septiembre de 2020, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002097.

13. Matt Novak, «How the Vietnam War Brought High-Tech Border Surveillance to America», Gizmodo, 24 de septiembre de 2015, accedido 15 de septiembre de 2020, https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillan-1694647526.

14. Joseph Cox y Samantha Cole, «How Hackers Are Breaking into Ring Cameras», VICE News, 11 de diciembre de 2019, accedido 15 de septiembre de 2020, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

15. Unit 42, «2020 Unit 42 IoT Threat Report», Palo Alto Networks, 10 de marzo de 2020, accedido 15 de septiembre de 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

16. T. S. Allen, «Open-Source Intelligence: A Double-Edged Sword», Proceedings 144, nro. 8 (agosto de 2018), accedido 15 de septiembre de 2020, https://www.usni.org/magazines/proceedings/2018/august/open-source-intelligence-double-edged-sword.

17. U.S. Government Accountability Office (GAO), *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft* (Washington, DC: U.S. GAO, January 2018), accedido 15 de septiembre de 2020, https://www.gao.gov/assets/690/689478.pdf.

18. Patrick Tucker, «Strava's Just the Start: The US Military's Losing War Against Data Leakage», Defense One, 31 de enero de 2018, accedido 15 de septiembre de 2020, https://www.defenseone.com/technology/2018/01/stravas-just-start-us-militarys-losing-war-against-data-leakage/145632/.

19. Thompson y Warzel, «Twelve Million Phones, One Dataset, Zero Privacy».

20. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Nueva York: Hachette Book Group, 2019), 242–45.

21. Sara Morrison, «The Hidden Trackers in Your Phone, Explained», Vox, 8 de julio de 2020, accedido 15 de septiembre de 2020, https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

22. «COVID-19 Community Mobility Reports», Google, modificada por última vez 13 de septiembre de 2020, accedido 15 de septiembre de 2020, https://www.google.com/covid19/mobility/.

23. Patrick Tucker, «Russian Arms Production Slowed by Coronavirus, Analysts Find», Defense One, 1 de mayo de 2020, accedido 15 de septiembre de 2020, https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

24. «Putin Bans Armed Forces Members from Carrying Electronic Devices, Gadgets», Radio Free Europe/Radio Liberty, 7

de mayo de 2020, accedido 15 de septiembre de 2020, https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

25. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 de diciembre de 2018), accedido 15 de septiembre de 2020, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

26. Prem Tummalacherla, «The Top 3 Issues of the Centralized Internet», Medium, 14 de junio de 2019, accedido 15 de septiembre de 2020, https://medium.com/@IamPremt/the-top-3-issues-of-the-centralized-internet-1db59d5e495e.

27. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

28. Tom Lamont, «Can We Escape from Information Overload?», *The Economist* (sitio web), 29 de abril de 2020, accedido 15 de septiembre de 2020, https://www.economist.com/1843/2020/04/29/can-we-escape-from-information-overload.

29. FM 3-12, *Cyberspace and Electronic Warfare Operations*, párrafo 1-41.

30. Ibid., párrafo 1-71.

31. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, iii.

32. Edward Geist y Marjory Blumenthal, «Military Deception: Ai's Killer App?», War on the Rocks, 23 de octubre de 2019, accedido 15 de septiembre de 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

33. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

34. Marshall McLuhan, citado en Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), 3.

35. Gordon Wright, «Soldiers and Statesmen in 19th Century France», en *Soldiers and Statesmen: The Proceedings of the 4th Military History Symposium*, ed. Monte D. Wright y Lawrence J. Paszek (Washington, DC: Office of Air Force History, Headquarters USAF; and United States Air Force Academy, 1973), 28.

36. B. A. Friedman y Olivia A. Garard, «Technology-Enabled Mission Command», War on the Rocks, 9 April 2020, accedido 15 de septiembre de 2020, https://warontherocks.com/2020/04/technology-enabled-mission-command-keeping-up-with-the-john-paul-joneses/.

37. Kenneth Pollack, «Society, Technology, and Future Warfare», American Enterprise Institute, 6 de noviembre de 2019, accedido 15 de septiembre de 2020, https://www.aei.org/research-products/report/society-technology-and-future-warfare/.

38. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 38–65.

39. Stephen Rodriguez, «The Fox in the Henhouse: How Bureaucratic Processes Handicap US Military Supremacy and What to Do about It», Atlantic Council, 26 de febrero de 2020, accedido 15 de septiembre de 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fox-in-the-henhouse-how-bureaucratic-processes-handicap-us-military-supremacy-and-what-to-do-about-it/.

40. Curt Taylor, «It's Time for Cavalry to Get Serious about Cyber Reconnaissance», eArmor, otoño de 2018, accedido 15 de septiembre de 2020, https://www.benning.army.mil/Armor/eArmor/content/issues/2018/Fall/4Taylor18.pdf; Gina Harkins, «A Lance Corporal's Phone Selfie Got His Marine Unit "Killed" at 29 Palms», Military News, 7 de enero 2020, accedido 15 de septiembre de 2020, https://www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

41. James Long, «Shoot, Move, Communicate, and Innovate: Harnessing Innovative Capacity in the Ranks», Modern War Institute at West Point, 16 de marzo de 2020, accedido 15 de septiembre de 2020, https://mwi.usma.edu/shoot-move-communicate-innovate-harnessing-innovative-capacity-ranks/.