

La guerra de nueva generación de Rusia

Disuadir y ganar en el nivel táctico

Dr. James Derleth

En el siglo XXI ha surgido una tendencia a confundir las líneas entre los estados de guerra y de paz...

Incluso las propias «reglas de la guerra» han cambiado. El papel de los medios no militares para alcanzar objetivos políticos y estratégicos es mayor y, en muchos casos, estos superan el poder de las armas en su eficacia...

Los enfrentamientos frontales entre grandes formaciones a nivel estratégico y operacional se están convirtiendo gradualmente en algo del pasado...

El empleo de acciones asimétricas se ha difundido y esto permite anular las ventajas del enemigo en los conflictos armados. Entre esas acciones figuran el empleo de fuerzas de operaciones especiales y oposición interna para crear un frente permanente en todo el territorio del Estado enemigo, así como acciones, dispositivos y medios basados en la información que son perfeccionados constantemente...

Las diferencias en los niveles estratégico, operacional y táctico, así como entre las operaciones ofensivas y defensivas, están desapareciendo.

—General Valery Gerasimov, jefe del
Estado Mayor General de Rusia

Para los rusos, la disuasión se basa en el uso integrado de instrumentos no militares, convencionales y nucleares¹. En cambio, para Occidente, la disuasión tradicionalmente se basa en el despliegue y el empleo de fuerzas convencionales y nucleares². Una diferencia crucial es que, para Rusia, la disuasión no se detiene tras el estallido de un conflicto y los instrumentos se seguirán aplicando en

todas las etapas de una crisis político-militar para intentar controlar la escalada y garantizar condiciones favorables. Por lo tanto, para fomentar la disuasión y prevalecer, en caso de que fracase, Estados Unidos debe ser capaz de contrarrestar los instrumentos en cualquier ámbito (no militar, convencional, nuclear), nivel (táctico, operacional, estratégico) y fase de conflicto³. Si bien el Ejército de EUA se enfrenta a desafíos complejos, dinámicos y multidominio en el actual ambiente operacional (AO), el entrenamiento y la formación se concentran principalmente en la disuasión y derrota de adversarios con capacidades similares en operaciones de combate a gran escala (*large scale combat operations* – *LSCO*). Sin embargo, como los acontecimientos en Crimea y Georgia demuestran, la disuasión basada en fuerzas convencionales y nucleares no ha sido una estrategia acertada ya que Rusia ha podido alcanzar sus objetivos nacionales mediante otros instrumentos no letales.

Si bien en los centros de formación y entrenamiento del Ejército se estudian las fuerzas convencionales y nucleares, es importante señalar que los instrumentos no letales, como la guerra de información (*information warfare* — *IW*) no son abordados y esto afecta considerablemente la capacidad de las formaciones tácticas para disuadir o ganar en caso de producirse un conflicto⁴. Tradicionalmente, en la doctrina militar de Estados Unidos, las actividades de información cumplen una función de apoyo para facilitar y posibilitar las operaciones de combate. En cambio, Rusia siempre ha tenido un enfoque holístico e integrado de la IW⁵. Los rápidos avances en la tecnología de la información no han hecho sino reforzar esta perspectiva. Los líderes militares



«Tomé esta foto durante una misión en Georgia que coincidió con el aniversario del Día de los Veteranos. En ruso, les pregunté a los pensionistas si hablaban inglés. No lo hablaban. Luego les pregunté cómo podían escribir un cartel en inglés si no lo hablaban. Dijeron que sus “amigos” los escribieron por ellos. Esto, para mí, es una imagen muy poderosa que demuestra la omnipresencia de la guerra de información rusa. ¿Qué harían nuestras fuerzas si tuvieran que enfrentarse a este grupo mientras apoyan a Georgia en un conflicto contra Rusia?».

—James Derleth

rusos creen que las batallas decisivas de un conflicto se libran en el dominio de la información y que las operaciones de información en las fases iniciales son más decisivas que la guerra convencional posterior. En la IW, una de las maniobras decisivas es atacar las vulnerabilidades y el centro de gravedad del adversario con operaciones letales para producir efectos de información en lugar de efectos letales⁶. De esta manera, los roles de los dos dominios se invierten. En lugar de ser una operación de apoyo, las campañas de información se han convertido en la operación que necesita apoyo⁷. Como consecuencia, la superioridad en materia de información es fundamental para aumentar la utilidad de los instrumentos en

Una manifestación prorrusa y anti-OTAN en el Día de la Victoria en Europa (VE) el 9 de mayo de 2019 frente al Museo Joseph Stalin en Gori, Georgia. (Foto del autor)

todos los ámbitos y fases de un conflicto⁸. Sin ella, es imposible prevalecer en el combate. La información puede generar o aprovechar el apoyo militar y político local, desacreditar el liderazgo, ralentizar la adopción de decisiones, alimentar la disensión, configurar la opinión pública, fomentar o manipular las fuentes locales de inestabilidad y movilizar a las poblaciones locales contra las fuerzas extranjeras. Todo esto disminuye la probabilidad de que se produzcan enfrentamientos letales y mejora las posibilidades de éxito⁹. En resumen, la IW puede ser el preludio de un conflicto armado, una preparación del campo de

batalla que precede el despliegue de fuerzas, o un fin en sí mismo, a través del cual Rusia y otros adversarios debilitan las fuerzas superiores de Estados Unidos sin disparar un solo tiro.

Aunque en la doctrina del Ejército se señala que «en los conflictos modernos, la información se ha convertido en algo tan importante como la acción letal a la hora de determinar el resultado de las operaciones», los soldados de las formaciones tácticas tienen una capacidad limitada para comprender o influir en el ambiente de información (AI)¹⁰. En particular, la doctrina se basa en el supuesto de que la IW solo se ejecutará en el nivel operacional y estratégico. Esto es cuestionable dado el actual ambiente de amenazas¹¹. Como las formaciones tácticas se verán considerablemente afectadas por la IW enemiga en cualquier fase del conflicto, necesitan ser capaces de comprender y configurar el AI. De lo contrario, los adversarios seguirán determinando las condiciones de la competencia y los conflictos futuros.

La amenaza: una viñeta

En las elecciones nacionales de Estonia, un partido nacionalista proestonio se hizo con el control del Gobierno¹². Frustrada por el resultado de las elecciones y la falta de ciudadanía, la minoría étnica rusa —el 20 % de la población— se manifestó en contra. El Gobierno ruso, por su parte, emitió declaraciones de apoyo; lanzó una campaña encubierta para condicionar las percepciones con más de doscientas mil cuentas de Twitter en las que enviaron 3.6 millones de tuits utilizando la etiqueta #proteggerrusosenEstonia; y llevó a cabo ejercicios militares con la participación de sus fuerzas terrestres, navales y aéreas en la región.

Una semana después, un grupo de manifestantes se reunió en la plaza de Narva, un pueblo al este de Estonia en la frontera con Rusia. Al quejarse de que sus derechos humanos habían sido violados, los manifestantes exigieron autonomía para Narva, estatuto oficial para el idioma ruso y ciudadanía estonia. Cuando la policía llegó para disolver la manifestación, se enfrentó a un grupo armado de hombres en edad militar que hablaban ruso. Temiendo la pérdida de vidas inocentes, la policía abandonó el lugar. Al mismo tiempo, un grupo de manifestantes armados atacó el puesto fronterizo de Estonia con Rusia y obligó a que fuera abandonado. Un tercer grupo

de manifestantes se apoderó del centro de telecomunicaciones local (cortaron el tráfico de Internet, radio, teléfono y televisión hacia y desde Narva), rodeó la comisaría de policía y asaltó el ayuntamiento y de esta manera hicieron que el alcalde, Tarmo Tammiste, dimitiera. Georgi Zhukov, portavoz de los manifestantes, declaró el establecimiento de la República Popular de Narva y pidió ayuda a Rusia «para garantizar la paz y el orden público contra los nacionalistas y los fascistas». Estas acciones fueron apoyadas por una serie de ciberataques que abrumaron al Gobierno estonio, la economía, las noticias, las telecomunicaciones y las redes militares en todo el país. Los ciberataques neutralizaron la capacidad de mando y control del Gobierno, así como su capacidad para comunicarse con su población y aliados. Los ciberataques incluyeron la publicación de videos que supuestamente mostraban a las fuerzas de seguridad estonias masacrando a residentes estonios de ascendencia rusa. Las imágenes circularon en Internet por medio de *bots*, lo cual afectó negativamente la opinión pública de Estonia y Estados Unidos entre las poblaciones simpatizantes y no simpatizantes de Rusia en toda Europa. El Gobierno de Estonia declaró ilegal el establecimiento de la República Popular de Narva y exigió que se devolviera el control a los funcionarios.

Una semana después de que el puesto fronterizo fuera abandonado, la inteligencia estonia estimó que cientos de personas con uniformes militares sin insignia entraron en la región desde Rusia. En respuesta, el Gobierno de Estonia convocó una reunión de emergencia del Consejo del Atlántico Norte (*North Atlantic Council* — *NAC*) para

El Dr. James Derleth es el asesor sénior de entrenamiento interagencial en el Centro de Apresto Conjunto Multinacional en Hohenfels, Alemania. Sus responsabilidades incluyen formar y entrenar al personal civil y militar en la guerra rusa de nueva generación, operaciones de estabilidad y operaciones cívico-militares; integrar los desafíos de seguridad contemporáneos en los ejercicios; e interactuar con las misiones diplomáticas, las organizaciones internacionales y las no gubernamentales para integrarlas en el entrenamiento. Obtuvo una maestría de The American University y un doctorado de la Universidad de Maryland en 1990.

invocar la disposición de defensa colectiva (Artículo 5) del Tratado del Atlántico Norte. El NAC rechazó la solicitud de Estonia debido a la falta de claridad en cuanto a la nacionalidad del grupo armado y el origen de los ciberataques. A pesar de la negativa de la CNA, Estados Unidos aceptó desplegar el 2º Regimiento de Caballería (*2nd Cavalry Regiment* — 2CR) en Estonia. Su misión era apoyar al ejército estonio, a las fuerzas de seguridad locales y al Gobierno local en la consecución de los siguientes cuatro objetivos:

- preservar la integridad territorial de Estonia,
- apoyar la legitimidad del Gobierno estonio,
- fomentar la seguridad interna, y
- evitar que el conflicto escale.

Cuando el 2CR se preparaba para salir de la guarnición en Vilseck, Alemania, en los medios sociales aparecieron varios videos que supuestamente mostraban a personal estadounidense agrediendo sexualmente a varios menores de edad alemanes. Los vídeos parecían implicar a jefes del regimiento, por lo que las autoridades alemanas iniciaron una investigación. Varias protestas ocurrieron a las puertas de la guarnición y el despliegue de la unidad se retrasó.

Cuando el 2CR llegó a Estonia, trasladó su área de acantonamiento a Jõhvi, a 50 kilómetros al noroeste de Narva. Al día siguiente, un vehículo aéreo no tripulado sin identificación fue visto sobrevolando la base del 2CR. Poco después, los teléfonos celulares de los soldados perdieron acceso a la red celular local y comenzaron a recibir mensajes de texto diciéndoles que abandonaran la zona para evitar su «destrucción».

En resumen, *antes* de que el 2CR llegara a su área de acantonamiento, el enemigo ya había conseguido ejecutar operaciones multidominio para dominar el espacio de la información, generar oposición local e internacional, limitar la capacidad del regimiento para comunicarse con el Gobierno local o sus propias formaciones, fomentar disturbios civiles y controlar infraestructura clave.

Rusia comenzó a realizar operaciones de IW decisivas inmediatamente después de que el 2CR llegara con sus formaciones, las cuales, si bien eran letales, contaban con capacidades limitadas en términos de entrenamiento y formación sobre la IW. En otras palabras, el 2CR ya había perdido la iniciativa antes de que el primer Stryker saliera por la puerta. Este escenario limitó considerablemente el poder de combate del comandante del 2CR y su capacidad para llevar a cabo su misión.



Los roles de los dos dominios se invierten [operaciones letales vs. operaciones de información]. En lugar de ser una operación de apoyo, las campañas de información se han convertido en la operación que necesita apoyo.



Durante el desplazamiento del 2CR, hubo ataques de guerra electrónica contra su red de comunicaciones que limitaron la capacidad de los soldados para comunicarse entre ellos y con las fuerzas de seguridad locales. En medios sociales «patrióticos» se publicaron videos de fuentes desconocidas dirigidos a grupos antibélicos de Estados Unidos y Europa que mostraban cómo el ganado y los cultivos de la población local de origen ruso sufrieron daños y cómo los servicios esenciales (agua, electricidad, saneamiento) fueron interrumpidos en Narva. Tales mensajes transformaron la opinión pública estadounidense y europea de oponerse a la agresión a apoyar la ciudadanía y el uso del idioma ruso para los residentes minoritarios de Estonia.

¡Esto no es una amenaza hipotética! La relación entre la guerra contemporánea y la IW puede verse claramente en cómo Rusia capturó Crimea en febrero de 2014. Las operaciones de IW incluyeron la participación de la población local a través de entrevistas, «encuestas», mítines de referéndum y reuniones prorrusas; la diseminación masiva de carteles, folletos, volantes y mensajes de texto; la interrupción de cables de fibra óptica; control del punto de intercambio de Internet en Simferópolis; la sustitución de canales ucranianos por canales rusos; ataques de guerra electrónica contra sistemas de comunicación militar ucranianos; ataques cibernéticos contra sitios web de Ucrania y de la OTAN; la publicación de correspondencia, correos electrónicos



Los «hombrecitos verdes» de Rusia facilitando la anexión de la península ucraniana de Crimea en febrero de 2014. Armados con armas pequeñas y equipo ruso modernos, este personal era una combinación de fuerzas especiales rusas y otras unidades de élite que llevaban uniformes verdes sin insignia. Rusia al principio afirmó que estos hombrecitos verdes eran milicias patrióticas ucranianas locales que simpatizaban con las reivindicaciones de Rusia sobre Crimea. Se apoderaron y ocuparon el Parlamento de Simferópol y numerosas bases militares de Crimea, y bloquearon el Aeropuerto Internacional de Simferópol para impedir la llegada de las fuerzas gubernamentales ucranianas. Simultáneamente, Rusia emprendió una amplia campaña mundial de guerra híbrida utilizando una gran variedad de instrumentos, entre ellos la diplomacia, la guerra económica, la guerra electrónica, los ataques cibernéticos, la propaganda y la violencia enfocada para lograr sus objetivos. Las contramedidas y respuesta de Occidente han sido ineficaces en gran parte contra el *fait accompli* de Rusia. (Captura de pantalla de Hromadske.tv)

y grabaciones telefónicas entre funcionarios ucranianos, de la Unión Europea y de Estados Unidos; la creación de sitios web falsos en los que Rusia atacó a unidades militares ucranianas utilizando las cuentas de medios sociales de los soldados; el uso de sitios web reales (Facebook, Twitter, Odnklassniki, V Kontakte) para sembrar el pánico y los rumores; ataques de negación de servicio en los que se enviaron miles de mensajes de texto y llamadas telefónicas a los teléfonos celulares de líderes militares y civiles para impedir que se comunicaran y respondieran a las acciones rusas. El dominio del espacio de la información permitió que solo se divulgara información de origen ruso, lo que dio lugar a que un porcentaje importante de la población acogiera a las tropas rusas. Estas acciones, combinadas con acciones no letales de reconocimiento y desestabilización de

la *Spetsnaz*, socavaron la moral y la eficacia de combate del ejército ucraniano, lo que llevó a la rendición de dieciséis mil soldados¹³. Este escenario es un excelente ejemplo de operaciones multidominio que abarcaron todo el espectro de la información. Como consecuencia, Rusia pudo manipular la percepción de la población ucraniana, impedir una respuesta militar, influir en el proceso de toma de decisiones, fomentar la desconfianza en el Gobierno y limitar su comportamiento estratégico minimizando el uso de la fuerza letal.

Desafíos

El Ejército se ha dado cuenta, aunque un poco tarde, del desafío que la guerra de próxima generación representa y está reorganizando el Comando Cibernético para sincronizar sus capacidades y

«cambiar la forma en que llevamos a cabo la guerra de información»¹⁴. Para ello, «se integrarán y emplearán las secciones de inteligencia, las operaciones de información, el ciberespacio, la guerra electrónica y las capacidades espaciales para proporcionar a los comandantes de combate opciones para competir por debajo del nivel de conflicto armado»¹⁵. Si bien estos objetivos son importantes, hay muchos desafíos que dificultan su implementación en el nivel táctico. Entre ellos figuran, según algunas observaciones realizadas en el Centro de Apresto Conjunto Multinacional (*Joint Multinational Readiness Center — JMRC*) en Hohenfels, Alemania, la falta de comprensión del AI; la incapacidad de integrar el AI en el proceso de las operaciones; la incapacidad de integrar los multiplicadores de fuerza; la ineficacia de la coordinación de los socios civiles; la renuencia a reconocer que las acciones físicas afectan el espacio de la información; y la falta de doctrina, educación y capacitación que permita a las formaciones mitigar las acciones del enemigo a fin de recuperar la iniciativa táctica y operacional.

Falta de entendimiento del AI. Aunque las unidades son capaces de identificar amenazas letales, su entendimiento limitado de las no letales puede tener un impacto incluso mayor en la maniobra. Los conflictos se producirán en poblaciones interconectadas que son parte de un AI complejo. Si la conciencia situacional no es adecuada, el poder de combate se degradará a la larga. Si bien los comandantes deberían comprender e intentar configurar el AI, las secciones de inteligencia del estado mayor, las encargadas de facilitarles esta información para llevar a cabo tales actividades, por lo general se centran en los grupos enemigos y en las acciones que podrían tener consecuencias letales, por lo que el AI queda relegado a un segundo plano. Como consecuencia, los comandantes no establecen requisitos de inteligencia ni utilizan plantillas estándar para comprender el AI. Justifican esto simplificando el espacio de batalla y aplicando una visión estrecha del peor de los casos en el que las fuerzas enemigas superan a sus formaciones. Desafortunadamente, los conflictos modernos no son un simple «todo o nada». Las formaciones que no entienden el AI son «ciegas» en cuanto a la forma en que son percibidas por la población y cómo son retratadas por el enemigo. Esto limita la capacidad de una formación para obtener información sobre las

fuerzas y posiciones enemigas y para identificar a los partidarios del enemigo o a las fuerzas de operaciones especiales que se encuentran detrás del espacio donde operan las tropas terrestres. A modo de ilustración, para proteger sus comunicaciones, una unidad de rotación (*rotational unit — RTU*) en un reciente ejercicio de entrenamiento en el JMRC decidió utilizar la Red Secreta de Routers de Protocolo de Internet (*SIPRNet*) como su principal medio de comunicación. El resultado fue que, si bien la unidad pudo comunicarse internamente de manera segura, debido a que se habían descuidado los sistemas de información no clasificados, la RTU no tenía conocimiento del entorno local. Esta falta de comprensión dio lugar a manifestaciones locales que restringieron las principales rutas de suministro de la unidad, a que desplazados internos interfirieran en sus maniobras y a que se perdiera gran cantidad de información importante de desplazados internos que huían del enemigo. Esta falta de visibilidad y comprensión del AI afectó directamente el poder de combate de la RTU.

No integrar el AI en el proceso de operaciones. El objetivo del proceso de operaciones, según la Publicación Doctrinal del Ejército 5-0, *El proceso de operaciones* (ADP 5-0, *The Operations Process*), es comprender, visualizar y describir el ambiente operacional; tomar y articular decisiones; y dirigir, liderar y evaluar las operaciones militares¹⁶. Los entrenamientos en el JMRC siguen demostrando que las formaciones tácticas no están integrando el AI en las operaciones. Esto ocurre porque los comandantes no entienden el AI o solo ven sus acciones desde una perspectiva física¹⁷. Esta falta de entendimiento también es exacerbada por el estado mayor y su enfoque en la letalidad de las plataformas y los sistemas de armas del enemigo. Por ejemplo, un estado mayor puede atacar fácilmente una formación de tanques enemiga, pero tiene dificultades para lidiar con los medios sociales del enemigo que instigan a realizar manifestaciones en las principales rutas de suministro. Por consiguiente, las formaciones no pueden identificar o apoyar las capacidades relacionadas con la información (*information-related capabilities — IRC*) amigas, identificar y atacar las IRC enemigas, o integrar esta información en las operaciones y planes. Esto forma parte de un desafío institucional más amplio, a saber, que la «victoria» solo puede obtenerse mediante operaciones de combate letales.

Incapacidad para integrar los multiplicadores de fuerza. En la doctrina del Ejército de EUA se enfatiza que los comandantes tienen la responsabilidad de operar en todos los dominios, incluyendo el AI. Sin embargo, las formaciones tácticas carecen de muchas capacidades orgánicas relacionadas con la información. Cuando se despliegan, las formaciones tácticas reciben multiplicadores de fuerza como unidades de asuntos civiles (*civil affairs — CA*) y operaciones psicológicas (*psychological operations — PSYOP*). Sin embargo, estos y otros multiplicadores de fuerza (oficiales de asuntos públicos [*public affairs officers — PAO*], oficiales de guerra electrónica [*electronic warfare officers — EWO*], etc.) a menudo no influyen en el AI. Hay varias razones para esta situación, pero dos se destacan:

1. Los multiplicadores de fuerza no trabajan con las formaciones tácticas antes de un ejercicio o despliegue. Como no son elementos orgánicos

del estado mayor y la interacción entre ambos es limitada, es difícil para ellos integrar sus conocimientos del AO en las operaciones. Esto ocurre en parte porque las áreas y campos de entrenamiento en las estaciones de origen no reproducen los AI multifacéticos y dinámicos que se encuentran en los conflictos modernos. Típicamente, los comandantes crean sus propias fuerzas contrarias y estas no cuentan con las capacidades de guerra de información que un enemigo real sí posee. Por ello, las formaciones no entienden cómo los multiplicadores de fuerza pueden facilitar sus operaciones y, en consecuencia, las unidades, acostumbradas a la letalidad en los entrenamientos de sus guarniciones de origen, llegan a ejercicios y despliegues drásticamente diferentes de lo que han experimentado. Por eso no pueden ganar en ellos, ya que tienen un entrenamiento limitado.



La sargento Camille Coffey (izquierda) y los especialistas Victorious Fuqua (centro) y Mark Osterholt, todos analistas en operaciones cibernéticas del Destacamento Expedicionario de Apoyo Cibernético, 782º Batallón de Inteligencia Militar (Ciber), llevan a cabo operaciones cibernéticas ofensivas durante la Rotación 18-03 en el Centro Nacional de Entrenamiento en Fort Irwin, California. (Foto de Steven Stover, 780ª Brigada de Inteligencia Militar de Asuntos Públicos)

2. Los multiplicadores de fuerza no crean productos vinculados a la intención y objetivos operacionales del comandante. Muchas veces, los productos de los multiplicadores de fuerza están más vinculados a su estrecha especialidad operacional militar que a los estados finales del comandante¹⁸. Por ejemplo, en el anexo de asuntos civiles que debería «describir la forma en que las operaciones de asuntos civiles, en coordinación con otras organizaciones militares y civiles, apoyan el concepto de operaciones descrito en el plan u orden básico» a menudo se enumeran simplemente aspectos de la situación civil (zonas, estructuras, capacidades, organizaciones, personas y acontecimientos)¹⁹. Como los comandantes no ven la relación entre esta información y su intención, a los multiplicadores de fuerzas se les suelen asignar otras tareas como la vigilancia del centro de operaciones tácticas o la instalación de obstáculos. Otro desafío relacionado es la incapacidad de los multiplicadores de fuerza para salir de su «burbuja». En el JMRC, a menudo notamos que como las IRC (CA, PAO, PSYOP, etc.) definen sus misiones de forma estrecha, no sincronizan sus actividades, por lo que limitan su efecto. En cambio, la 77ª Brigada, del Reino Unido, combina estas capacidades en equipos de información, actividades y divulgación que «apoyan los objetivos militares de los comandantes [...] utilizando actividades no letales y palancas no militares legítimas como medio para moldear el comportamiento de las fuerzas opositoras y los adversarios»²⁰.

Coordinación ineficaz con socios civiles. La IW de los rusos se centra en deslegitimar las estructuras militares y políticas de los adversarios. Sin embargo, debido a plazos operacionales, competencia técnica limitada y falta de autoridad legal, las formaciones tácticas de EUA a menudo no pueden mitigar los efectos de la IW enemiga porque para ello se requiere un enfoque intergubernamental. Las organizaciones internacionales, las organizaciones no gubernamentales, los Gobiernos locales, los medios de comunicación y las agencias de publicidad pueden apoyar y/o ejecutar actividades de información táctica. El fracaso de las formaciones tácticas para identificar a los socios civiles e integrar sus conocimientos y experiencia en las operaciones limita

su capacidad de maniobrar y consolidar los logros. Aunque existen numerosas razones para esta situación, entre los factores clave se encuentran el hecho de no identificar a los socios civiles en el ambiente operacional y el hecho de no comprender las capacidades y ventajas que estos brindan.

Renuencia a reconocer que la IW afecta la maniobra. Ha habido un cambio dramático en las operaciones militares contemporáneas como resultado de la globalización, la difusión de tecnologías relacionadas con las Fuerzas Armadas y la revolución de la información. A pesar de ello, el énfasis actual en las LSCO ha hecho que los comandantes se centren en los aspectos de las maniobras de las operaciones ofensivas y defensivas. Aunque la manipulación de la información puede crear efectos de negación y es doctrinalmente una forma de fuegos, los comandantes no están utilizando los recursos de estado mayor necesarios ni enfatizando el aspecto cognitivo de las operaciones²¹. Esta falta de recursos aplicados puede tener numerosas consecuencias que limitan la capacidad de llevar a cabo operaciones multidominio. Esto incluye permitir que el enemigo establezca condiciones primero, neutralice la superioridad militar, limite la capacidad de emplear la fuerza y construya una imagen pública negativa tanto para el público amigo como para el enemigo.

Falta de educación y entrenamiento en la guerra de nueva generación (*new generation warfare* — NGW). La educación y el entrenamiento tradicional y contemporáneo en el Ejército se centra en las principales operaciones de combate contra las Fuerzas Armadas de un Estado con capacidades similares o casi similares. No obstante, a pesar de la falta de éxito en Vietnam, Afganistán, Iraq, Libia, Mindanao, Siria y el Sahel, existe la creencia de que, si el Ejército puede ejecutar eficazmente las LSCO, puede ganar cualquier conflicto. Esta creencia tiene tres errores significativos. En primer lugar, como demostraron los conflictos mencionados, aplicar la educación y el entrenamiento de las LSCO en operaciones que no son de LSCO invariablemente obliga a una adaptación generalizada y costosa, poniendo en peligro el éxito de la misión. Segundo es la suposición común de que el próximo enfrentamiento será un conflicto entre grandes potencias. Como el ex secretario de Defensa James Mattis solía señalar, el enemigo también «tiene



opciones». Conscientes de que sus fuerzas no pueden ganar una batalla convencional contra Estados Unidos, adversarios como China, Irán y Rusia están invirtiendo considerablemente en recursos asimétricos para explotar las vulnerabilidades estadounidenses. En tercer lugar, el deseo del Ejército de centrarse en amenazas tradicionales no cambia la realidad de que una serie de actores no estatales sigue fomentando el descontento en todo el mundo, socavando la estabilidad regional y amenazando los intereses de Estados Unidos. Los datos muestran que la mayoría de los conflictos armados actuales son conflictos civiles o subestatales internacionalizados y no guerras interestatales convencionales²².

Para ganar los conflictos futuros, el Ejército debe replantear su educación y entrenamiento. Aunque algunos centros de entrenamiento de combate han creado e integrado AI complejos y dinámicos en sus ejercicios, muchas veces se ignoran o se les resta importancia para que no «interfieran con otros objetivos de entrenamiento». Como consecuencia, las RTU no están recibiendo una experiencia de entrenamiento

Estudiantes de la Escuela de Comando y Estado Mayor (*Command and General Staff College — CGSC*) en Fort Leavenworth, Kansas, planifican operaciones de combate a gran escala el 14 de mayo de 2019. Muchos creen, equivocadamente, que el Ejército puede ganar cualquier conflicto siempre y cuando ejecute las operaciones de combate a gran escala eficazmente. (Foto: M. Shane Perkins, instructor de la CGSC)

realista. Una buena regla general para medir el progreso sería evaluar si una RTU dedica la misma cantidad de recursos o más a las operaciones de AI que a las operaciones físicas. Si bien esto sería una medida de rendimiento más que una evaluación del efecto, obligaría por lo menos a los comandantes a tratar de integrar las operaciones de EI en la planificación²³.

Otro desafío es la falta de formación con respecto a la NGW y cómo entrenar a los líderes militares para ganar en operaciones multidominio (la anexión de Crimea por parte de Rusia es un ejemplo de este tipo de operaciones). Aparte de un curso creado en el JMRC, desconozco de algún otro curso en Estados Unidos o la OTAN que prepare a las formaciones tácticas para derrotar las tácticas de NGW.

Entender e influir en el AI

Si bien muchos de estos desafíos son resultado de decisiones y políticas tomadas a niveles más altos, las formaciones tácticas tendrán que hacer frente a sus ramificaciones. Por consiguiente, ¿qué pueden hacer para ganar en el ambiente de información contemporáneo? Muchas cosas se pueden hacer, como, por ejemplo, preparar a las formaciones en sus estaciones de origen, integrar los multiplicadores de fuerza en el Programa de Formación de Líderes (*Leadership Training Program* — *LTP*), analizar el AI antes del despliegue, modificar la organización de tareas, integrar a los socios civiles en los procesos de estado mayor, poner a un líder sénior a cargo de la integración de los multiplicadores de fuerza y los socios civiles, y fomentar la participación de los comandantes.

Prepararse en la estación de origen. Al darse cuenta de que las RTU carecían de entrenamiento de NGW, el JMRC creó un programa de instrucción de tres días y un equipo de entrenamiento móvil para impartirlo en las estaciones de origen. Desafortunadamente, la mayoría de las RTU rechazan la oportunidad, lo que significa que tienen poca o ninguna experiencia entendiendo el ambiente operacional o derrotando amenazas no letales antes de ir a centros de entrenamiento o misiones reales. Las formaciones que no se entrenan para contingencias realistas tienen una gran desventaja. Como ocurrió en las guerras de Afganistán e Iraq (en las que se envió un equipo de entrenamiento de contra-insurgencia móvil a cada brigada desplegada), una simple solución sería hacer obligatorio que todas las RTU tomen un curso de NGW o un curso regional relacionado antes de ir a un centro de entrenamiento de combate. Esto es importante ya que la NGW se basa en un estado de conflicto permanente.

Fomentar la integración de habilitadores (*enablers*) en el Programa de Formación de Líderes. Dado que muchos de los multiplicadores de fuerza son reservistas, a menudo no son incluidos en los LTP de la unidad de rotación. Por ello, no empiezan a trabajar con la unidad a la que apoyan hasta después de ser desplegados. Sincronizarse con los estados mayores de las brigadas y demostrar su importancia a los comandantes, que generalmente se concentran en amenazas letales, se dificulta. Para mitigar este desafío, el 353° Comando de Asuntos

Civiles ordenó que todas sus formaciones (1) debían tomar el curso de NGW ofrecido por el JMRC antes de desplegarse al teatro de operaciones del Comando Europeo y (2) los representantes del batallón desplegado deben asistir a las conferencias de planificación de las unidades de rotación y al LTP. Esto les permitirá empezar a trabajar temprano con la unidad a la que apoyarán y demostrar su importancia al equipo.

Analizar el AI antes del despliegue. Así como las unidades deben identificar las formaciones enemigas en su AO antes del despliegue, también deberían identificar las operaciones de información enemigas que han estado configurando el AO antes de su llegada. Como mínimo, este análisis debería incluir las principales IRC amigas y enemigas, información sobre la forma en que el enemigo está influyendo en el AO, posibles cursos de acción para negar las actividades enemigas que podrían afectar las operaciones de combate y medidas de efecto que demuestren el éxito de las operaciones de contrainformación.

Modificar la organización de tareas. Dado que el AI es global y está en constante evolución, comprenderlo es un desafío más complejo que comprender el entorno físico. Por lo tanto, se deben dedicar más recursos del estado mayor para la comprensión del AI. Al centrarse en el «efecto» que debe lograrse (por ejemplo, degradar el poder de combate del enemigo, fomentar la libertad de maniobra y dar prioridad a los requisitos de inteligencia relacionados con la información), el cambio será más fácil. Durante una revisión después de la acción del AI, el comandante de la RTU que utilizó el SIPRNet como medio de comunicación se dio cuenta de que esta herramienta tenía numerosas consecuencias imprevistas que limitaban su poder de combate. Para mitigar este problema, el comandante creó una «célula de ataque» que incluía no solo a multiplicadores de fuerza comunes (PAO, CA, EWO, PSYOP), sino también a secciones de inteligencia y operaciones. La célula de ataque incluía a miembros del estado mayor para garantizar que la información generada por los multiplicadores de fuerza se incluyera en la planificación y la selección de objetivos. Para fomentar la integración y mejorar la capacidad para actuar ante amenazas no letales, el comandante trajo al equipo de entrenamiento móvil del JMRC para que impartiera el curso de NGW a la célula.

Integrar a los socios civiles en los procesos de estado mayor. Dado que los socios civiles tendrán tiempo operando en las zonas en las que se desplegará la unidad, ya contarán con contactos locales, conocimientos especializados y capacidades para configurar el AI. Sin embargo, muchas veces esta oportunidad se desperdicia porque las formaciones no identifican a los socios civiles y nos los integran en las operaciones. Una forma sencilla de mitigar este desafío es asegurarse de que se incluyan en los procesos de estado mayor. Por ejemplo, doctrinalmente, debería haber un Grupo de Trabajo de Operaciones de Información en la brigada. Integrar a los socios civiles en este grupo permitiría identificar la narrativa del enemigo y desarrollar mensajes para derrotarlo, así como identificar objetivos no letales para el proceso de selección de objetivos. La participación de los socios civiles en las operaciones también puede facilitarse mediante la arquitectura de fuegos existente. Cuando los comandantes quieren producir efectos letales, simplemente le dicen a su coordinador de fuegos el efecto que quieren lograr. El sistema entonces ejecuta esta tarea. Si los comandantes proporcionaran la misma orientación para efectos no letales/de información, y puesto que las brigadas carecen de capacidad en el espacio de la información, el coordinador de fuegos tendría que utilizar a los socios civiles y a los multiplicadores de fuerza para lograr el efecto deseado.

Designar un líder sénior para las actividades no letales. Las RTU que han tenido más éxito en las operaciones multidominio han designado a un líder sénior —generalmente el subcomandante o el oficial ejecutivo de la brigada— para supervisar la integración de la información en las operaciones. Aunque otros oficiales de estado mayor son sin duda capaces de desempeñar esta tarea, carecen del rango necesario para integrar a los multiplicadores de fuerza y a los socios civiles en las operaciones de la brigada.

Involucrar a los comandantes. La forma más importante de ganar la guerra de información es garantizando que los comandantes en cualquier nivel sean conscientes de que la información es una «prioridad». Los líderes deben entender que el AI puede facilitar —o limitar— su capacidad para llevar a cabo las operaciones multidominio necesarias para lograr los estados finales deseados. Un buen punto de partida sería evaluar a los comandantes no solo por su puntuación en artillería sino también por su capacidad para ejecutar operaciones multidominio en un AI realista.

Resumen

La dicotomía entre la guerra y la paz ya no es un concepto útil para pensar en la seguridad nacional o en las operaciones tácticas. Estamos en un estado de competencia y conflicto que es continuo y dinámico. Como ha quedado demostrado, varios adversarios pueden lograr sus intereses nacionales sin entrar en conflicto con operaciones no letales basadas en la guerra de información. En un artículo publicado por la revista rusa *Pensamiento Militar*, I. Vorobyev y V. Kiselyov señalaron: «La información ahora es un arma. No solo complementa los ataques y las maniobras de fuego, sino que los transforma y los une». Por ello, «la información se está convirtiendo en una lucha armada por derecho propio [énfasis en el original]»²⁴. Para derrotar las amenazas multidimensionales, las formaciones tácticas de EUA deben ser capaces de entender e influir en el AI. Aunque el Ejército ha empezado un poco tarde a darse cuenta de la existencia de una competencia de información y conflicto continuo, ha centrado su atención y recursos para apoyar las LSCO²⁵. Sin embargo, la naturaleza de las amenazas emergentes (p. ej., fuegos de precisión de largo alcance, sistemas de defensa aérea de múltiples capas, drones, guerra electrónica, ciberataques, etc.) sugiere que las futuras operaciones militares serán llevadas a cabo por unidades tácticas. Por eso, en contraste con la política de Estados Unidos, Rusia ha estado modificando su estructura de fuerzas, pasando de divisiones a formaciones de nivel inferior (brigada y batallón). Rusia cree que el éxito en el ambiente operacional contemporáneo requiere que las formaciones de nivel inferior tengan cierto grado de autonomía y capacidad para realizar una variedad de misiones, ya que los factores mencionados anteriormente limitarán gravemente la capacidad de los niveles superiores para apoyarlas. Esto incluye «subunidades de guerra psicológica y de confrontación informativa»²⁶. Hasta que el Ejército no reconozca que el espacio de información no solo es un dominio de conflicto sino también el centro de gravedad, nos enfrentaremos a dos alternativas muy duras: tolerar desafíos no convencionales o escalarlos a un conflicto armado. Esto deja a Estados Unidos en una tremenda desventaja frente a los adversarios que utilizan la información como arma para influenciar y configurar las interacciones en todos los dominios para apoyar las maniobras tácticas integradas de las armas combinadas. ■

Notas

Epígrafe. Valery Gerasimov, «The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations», *Voyenno-Promyshlenny Kurier* (Correo Militar-Industrial), 26 de febrero de 2013, accedido 12 de mayo de 2020, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

1. Ministerio de Defensa de la Federación Rusa, *Military-Encyclopedic Dictionary* (2015), accedido 28 de mayo de 2020, http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14206@morfDictionary, citado en K. Ven Bruusgaard, «Russian Strategic Deterrence», *Survival: Global Politics and Strategy* 58, nro. 4 (2016). Véase también Okke Geurt Lucassen, «In Between War and Peace: The Conceptualization of Russian Strategic Deterrence», UPTAKE Working Paper No. 16/2018 (Tartu, Estonia: University of Tartu Press, 2018), 10, accedido 28 de mayo de 2020, http://www.uptake.ut.ee/wp-content/uploads/2019/03/Okke_Lucassen_WP2.pdf. La disuasión estratégica «es el conjunto de instrumentos que utilizan el poder blando y el poder duro, empleando herramientas (des)informativas, cibernéticas, económicas, militares y políticas, tanto ofensivas como defensivas, de forma continua, independientemente de tiempos de paz o de guerra, con el fin de disuadir el conflicto violento, la desescalada (o la cesación temprana) del conflicto militar o la estabilización de situaciones político-militares en (posibles) estados adversarios (coaliciones) de intereses en condiciones favorables para la Federación de Rusia».

2. Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

3. Gerasimov, «El valor de la ciencia está en la previsión». Gerasimov señala que las operaciones contemporáneas siguen una proporción aproximada de 4:1 de medidas no militares y militares con competencia no militar bajo el control de formaciones militares que utilizan operaciones de información, organizaciones militares privadas, fuerzas de operaciones especiales y el potencial de protestas internas. Este punto de vista tiene dos ramificaciones significativas: primero, Occidente considera las medidas no militares como formas de evitar la guerra mientras que Rusia las considera armas de guerra (véase Charles Bartles, «Getting Gerasimov Right», *Military Review* 96, nro. 1 [2016]: 34); y segundo, las formaciones tácticas se enfrentarán a un sinnúmero de desafíos no letales que afectarán su poder de combate y su capacidad de maniobra.

4. Véase Catherine Theohary, «Information Warfare: Issues for Congress», Congressional Research Service (CRS) Report No. R45142 (Washington, DC: CRS, 2018), accedido 28 de mayo de 2020, <https://crsreports.congress.gov/product/pdf/R/R45142/5>. A diferencia de las operaciones de información, la guerra de información no está definida en la doctrina militar de Estados Unidos. Este artículo utiliza la guerra de información para describir la ejecución de acciones ofensivas y defensivas en el dominio de la información para obligar a los oponentes a sucumbir a la voluntad de uno a través del uso de operaciones cibernéticas, operaciones psicológicas, guerra electrónica, seguridad de operaciones y engaño militar.

5. «Convention on International Information Security», Ministry of Foreign Affairs of the Russian Federation, 27 de septiembre de 2011, accedido 20 de mayo de 2020, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCkB-6BZ29/content/id/191666. Véase también *On Russia's Information War Concepts before the House Armed Services Subcommittee on Emerging Threats and Capabilities*, 115º Cong., 1ª ses. (2017) (declaración de Timothy Thomas), accedido 20 de mayo de 2020, <https://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf>. Un documento de estrategia ruso de 2011 llamado «Convención sobre la seguridad de la información a nivel internacional» define la IW como un «conflicto entre dos o más Estados en el espacio de la información con el objetivo de infligir daños a los sistemas, procesos y recursos de información, así como a estructuras de importancia crítica, entre otras; socavar los sistemas políticos, económicos y sociales; llevar a cabo campañas psicológicas masivas contra la población de un Estado con el fin de desestabilizar a la sociedad y el Gobierno; así como obligar a un Estado a tomar decisiones que favorecen a sus oponentes». En el ámbito militar, el objetivo de la IW es: 1) lograr objetivos políticos sin el uso de la fuerza militar y 2) generar una respuesta internacional favorable al despliegue de sus fuerzas militares o fuerzas aliadas a Moscú. Las «armas» de información son la tecnología, los medios y los métodos utilizados en la guerra de información.

6. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 2012, incorporando Change 1, 2014), ix. Según la doctrina, las operaciones de información son «el empleo integrado, durante las operaciones militares, de capacidades relacionadas con la información en concierto con otras líneas de operación para influir, perturbar, corromper o usurpar la toma de decisiones de los adversarios y posibles adversarios mientras protegemos la nuestra». Según esta definición, las operaciones de información se centran en la coordinación y sincronización solo durante las operaciones militares y dependen de otras capacidades para producir efectos. Monica Ruiz, «Impacts of Russian Information Operations: Technical and Psychological Aims», International Centre for Defence and Security, 24 de octubre de 2017, accedido 13 de mayo de 2020, <https://icds.ee/impacts-of-russian-information-operations-technical-and-psychological-aims/>. Por otro lado, el enfoque holístico de Rusia en relación con la IW se divide en dos componentes: «informativa-técnica», que se ajusta a la definición occidental de guerra electrónica y cibernética y se centra en las capacidades técnicas; e «informativa-psicológica», que se asemeja al concepto de la OTAN de comunicaciones estratégicas y operaciones psicológicas, centrado en las operaciones de influencia.

7. Keir Giles, «Delivery of Information Effects by Russian Special Forces and Intelligent Agencies» (borrador de trabajo).

8. Sergei Modestov, «Strategicheskoe soderzhanie na teatre informatsionnogo protivoborstva», *Vestnik Akademii Voennykh Nauk*, nro. 1 (2009): 26, citado en Dmitry (Dima) Adamsky, «Cross-Domain Coercion: The Current Russian Art of Strategy», *Proliferation Papers* 54 (Paris: Institut français des relations internationales [ifri], noviembre de 2015), accedido 13 de mayo

de 2020, <https://www.ifri.org/sites/default/files/atoms/files/pp54a-damsky.pdf>. Para Rusia, la campaña de información difumina la línea entre guerra y paz, frente y retaguardia, niveles de guerra (técnico, operacional, estratégico), formas de guerra (ofensiva y defensiva) y formas de coerción (disuasión y compulsión).

9. Véase Adamsky, «Cross-Domain Coercion», 24; Gerasimov, «The Value of Science Is in the Foresight»; Margarita Jaitner, «Russian Information Warfare: Lessons from the Ukraine», en *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cyber Defence Centre of Excellence, 2015), 91, accedido 13 de mayo de 2020, https://ccd-coe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf. Esto se puede lograr con desinformación, ciberataques, sabotaje digital, etc. La importancia de lograr la superioridad en materia de información en la guerra puede verse en el tiempo y los recursos que se han invertido en la creación de fuentes oficiales, semioficiales y extraoficiales de información relacionadas con la guerra, incluyendo canales de YouTube dedicados.

10. Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2017), párr. 2-113. Para más información, véase JP 3-13, *Information Operations*, ix-x.

11. No está claro cómo los ciberataques, la guerra electrónica, los fuegos de precisión de largo alcance, los drones, etc., permitirían a los escalones superiores comunicarse con, y mucho menos ejecutar, operaciones de guerra de información tácticamente relevante.

12. Adaptado de «Weaponized Information: One Possible Vignette», *Mad Scientist Laboratory* (blog), U.S. Army Training and Doctrine Command, 7 de noviembre de 2019, accedido 13 de mayo de 2020, <https://madsciblog.tradoc.army.mil/190-weaponized-information-one-possible-vignette/>.

13. Véase Vladimir Sazonov, Kristiina Müür e Igor Kopõtin, «Methods and Tools of Russian Information Operations Used Against Ukrainian Armed Forces: The Assessment of Ukrainian Experts», ENDC Occasional Papers No. 6/2017 (Tartu, Estonia: Estonian National Defence College [ENDC], 2017): 59; Oscar Jonsson y Robert Seely, «Russian Full Spectrum Conflict: An Appraisal After Ukraine», *Journal of Slavic Military Studies* 28, nro. 1 (2015): 15; Jaitner, «Russian Information Warfare: Lessons from the Ukraine», 91; Gleb Pakharensky, «Cyber Operations at Maidan: A First-Hand Account», en Geers, *Cyber War in Perspective*, 61; Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2017), 5-31, accedido 13 de mayo de 2020, https://www.rand.org/pubs/research_reports/RR1498.html.

14. Una nota sobre las definiciones. Las amenazas contemporáneas emergentes y un tanto ambiguas, muchas de las cuales no alcanzan el umbral que históricamente se considera «guerra», han sido denominadas guerra híbrida (Estados Unidos y OTAN), guerra de nueva generación (Rusia), guerra sin restricciones (China) y competencia en la zona gris (otras fuentes). La falta de una definición común permite a varias entidades elegir una definición que se ajuste a su visión del mundo o perspectiva burocrática. Esto permite la racionalización de las nociones preconcebidas y, lo que es más importante, limita nuestra comprensión de las amenazas reales. En un intento por mitigar este desafío, este artículo utiliza las siguientes definiciones:

Amenaza híbrida. ADP 3-0, *Operations*, describe una amenaza híbrida como «una combinación diversa y dinámica de fuerzas regulares, fuerzas irregulares, elementos criminales, o una

combinación de estas fuerzas y elementos, todos unificados, para lograr efectos mutuamente beneficiosos». Es importante señalar que este punto de vista se centra en las amenazas militares, no en un tipo de guerra, y que las amenazas híbridas pueden ser derrotadas mediante la aplicación del poder militar. Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. GPO, 2019), 1-3.

Guerra de nueva generación (NGW). La NGW busca lograr resultados políticos o militares sin recurrir a medios militares convencionales abiertos, aunque este último no está excluido. En la NGW, el principal espacio de batalla es la mente. Como resultado, el conflicto contemporáneo está dominado por la guerra de información para lograr la superioridad desmoralizando moral y psicológicamente al personal militar y a la población civil del enemigo antes y, si es necesario, durante las hostilidades. Esto reduce la necesidad de desplegar un poder militar letal, haciendo que la población militar y civil del adversario apoye al agresor en detrimento de su propio Gobierno. En consecuencia, los rusos han colocado el concepto de *influencia* en el centro de su planificación operacional. Esto es relevante para entender su significado estratégico ya que la operacionalización de la NGW no puede ser caracterizada como una estrategia militar en el sentido tradicional occidental. Por ejemplo, la guerra híbrida puede ser parte de la NGW sin necesariamente definirla. Esta descripción se basa en las acciones rusas en Ucrania, así como en los discursos y escritos de los líderes e investigadores militares rusos. Véase Jānis Bērziņš, «Not 'Hybrid' but New Generation Warfare», en *Russia's Military Strategy and Doctrine*, ed. Glen E. Howard y Matthew Czekaj (Washington, DC: Jamestown Foundation, 2019), accedido 13 de mayo de 2020, <https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Docctrine-web.pdf?x30898&x87069>; véase Gerasimov, «The Value of Science is in the Foresight»; S. G. Chekinov y S. A. Bogadanov, «On the Nature and Content of a New-Generation War», *Voennaya Mysl [Pensamiento Militar]*, nro. 10 (2013), accedido 13 de mayo de 2020, <https://pdfs.semanticscholar.org/c887/4593b1860de12fa40dadcae8e96861de8ebd.pdf>.

Guerra irrestricta. La guerra irrestricta se basa en la creencia de que la globalización actúa como un multiplicador de fuerzas para métodos no militares menos tradicionales como la guerra diplomática (creación de alianzas), la guerra económica (sanciones comerciales), la guerra cibernética (ataques de piratería informática) o la guerra ambiental (desastres naturales causados por el hombre). Por consiguiente, para alcanzar los objetivos estratégicos, China debe ir más allá del espectro de poder de fuerza puramente militar y operar en múltiples dominios. En 2003, China publicó unas «Directrices de trabajo político del Ejército Popular de Liberación». En estas se describen «tres guerras» que deben librarse en tiempo de paz y en las operaciones militares. La primera, «guerra psicológica», es la aplicación de presión militar, diplomática y económica para debilitar la voluntad de los adversarios. La segunda, «guerra de opinión pública», se centra en la manipulación abierta y encubierta de la información para influir en el público internacional y nacional. La tercera, «guerra legal», se refiere a la explotación de las normas internacionales para lograr los objetivos de China. Véase Nan Li, «Unrestricted Warfare and Chinese Military Strategy» (Singapur: Institute of Defence and Strategic Studies, 2002), accedido 28 de mayo de 2020, <https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO02022.pdf>; Sergio Miracola, «Chinese Hybrid Warfare», Italian International Institute for Political Studies, accedido 13 de mayo de 2020, <https://www.ispionline.it/en/publicazione/chinese-hybrid-warfare-21853>.

Competencia en la zona gris. Se define como «las actividades encubiertas o ilegales no tradicionales del Estado que están por debajo del umbral de la violencia armada organizada; e incluye la alteración del orden, la subversión política de organizaciones gubernamentales y no gubernamentales, las operaciones psicológicas, el abuso de los procesos legales y la corrupción financiera como parte de un diseño integrado para lograr una ventaja estratégica. Esta competencia entre y dentro de los agentes estatales y no estatales se sitúa entre la dualidad tradicional de la guerra y la paz y se caracteriza por la ambigüedad sobre la naturaleza del conflicto, la opacidad de las partes implicadas y la incertidumbre sobre los marcos políticos y jurídicos pertinentes». En particular, las tres descripciones se caracterizan por la competencia en la zona gris. Véase Frank Hoffman, «Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges», *Prism* 7, nro.4 (2018): 36; Philip Kapusta, «The Gray Zone», *Special Warfare* 28, nro. 4 (octubre-diciembre de 2015): 18–25, accedido 13 de mayo de 2020, <https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf>.

Resumen. A diferencia de las descripciones rusas y chinas de la guerra contemporánea, que se basan en operaciones multidominio facilitadas por una guerra de información que ocurre simultáneamente de forma encubierta y abierta por debajo del umbral tradicional de la guerra, la opinión de Estados Unidos se centra en las amenazas militares manifiestas que pueden ser derrotadas mediante la aplicación del poder militar. Como señala Frank Hoffman, adoptar esta estrecha concepción convencional del conflicto no prepara a los futuros líderes para la gama de amenazas emergentes. Tampoco es propicio para el desarrollo de la doctrina y el entrenamiento: «Un enfoque miope de las amenazas convencionales oscurece la complejidad de los fenómenos y simplifica en exceso los desafíos. También puede ser una forma de poner demasiado énfasis en una misión preferida para un paradigma convencional de gran guerra, lo que reduce nuestra comprensión cognitiva del conflicto». Frank G. Hoffman, «Hybrid Warfare and Challenges», *Joint Force Quarterly*, nro. 52 (2009, 1^{er} trimestre): 34–59, accedido 13 de mayo de 2020, <https://smallwarsjournal.com/documents/jfqhoffman.pdf>.

15. Sydney Freedberg Jr., «The Golden 5 Minutes: The Need for Speed in Information War», *Breaking Defense*, 21 de octubre de 2019, accedido 13 de mayo de 2020, <https://breakingdefense.com/2019/10/the-golden-five-minutes-the-need-for-speed-in-information-war/>.

16. Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 2019), v.

17. «Information Warfare Foundational Study (borrador de trabajo)» (Fort Gordon, GA: U.S. Army Cyber Command, 10 de julio 2019), 8.

18. Jen Judson, «Army Learning How Cyber Support Plays Role in Tactical Operations», *DefenseNews*, 10 de noviembre de 2015, accedido 13 de mayo de 2020, <http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/>.

Durante un ejercicio piloto, en el que se intentó incorporar apoyo cibernético en una brigada de infantería, un observador señaló que «aunque proporcionamos algunas personas muy inteligentes desde un punto de vista técnico, estas no pudieron comunicar al comandante de la brigada y el estado mayor, en términos que pudieran comprender fácilmente, las capacidades que brindaban y la mejor manera de integrarlas».

19. FM 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Printing Office, 2014), Anexo D.

20. «77th Brigade Influence and Outreach», Ejército Británico, accedido 13 de mayo de 2020, <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/>. La 77ª Brigada es una unidad combinada de la reserva y las fuerzas regulares del Ejército Británico formada en 2015. Sus misiones incluyen análisis de audiencia, actores y adversarios; actividades de información y divulgación; actividades de información contra el adversario; apoyo a socios civiles; recopilación de contenido de medios de comunicación; difusión de medios de comunicación; supervisión del AI; evaluación del AI; asesoramiento y capacitación en materia de seguridad humana (haciendo hincapié en la seguridad de las personas y su ámbito social y económico más que en la seguridad del Estado); y apoyo a las operaciones en curso.

21. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense [DOD], 2020), accedido 13 de mayo de 2020, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>. Las medidas adoptadas en el ciberespacio que crean efectos de negación notables (p. ej., degradación, perturbación o destrucción) o la manipulación que conduce a la negación del dominio físico son consideradas una forma de fuegos.

22. Alexandra Evans y Alexandra Stark, «Bad Idea: Assuming the Small Wars Era is Over», *Defense 360*, Center for Strategic and International Studies, 13 de diciembre de 2019, accedido 14 de mayo de 2020, <https://defense360.csis.org/bad-idea-assuming-the-small-wars-era-is-over/>.

23. «Information Warfare Foundational Study», 35.

24. I. Vorobyov y V. Kiselyov, «Russian Military Theory: Past and Present», *Pensamiento Militar* 22, nro. 1 (2013): 56.

25. Por ejemplo, el Ejército de EUA está planeando crear dos nuevos batallones integrados de inteligencia, información, cibernética, guerra electrónica y espacial para ayudar a configurar el ambiente operacional, supervisar los flujos de información y realizar operaciones de información o misiones cibernéticas.

26. «В Белоруссии начались учения 'Нерушимое братство-2016'» [Comienza en Bielorrusia el ejercicio Hermanidad Inquebrantable 2016], RIA, 23 de agosto de 2016, accedido 14 de mayo de 2020, <https://ria.ru/world/20160823/1475032583.html>, citado en Giles, «Delivery of Information Effects by Russian Special Forces and Intelligent Agencies». Los ejercicios en 2016 incluyeron el uso de «subunidades de guerra psicológica y de confrontación informativa».