Soldados de la 56ª Brigada de Combate Stryker en una maniobra de armas combinadas el 11 de junio de 2019 durante el ejercicio Decisive Strike 2019 en el Centro de Apoyo al Entrenamiento en Krivolak, Macedonia del Norte. (Foto: Sargento segundo Frances Ariele L. Tejada, Ejército de EUA)

El engaño militar multidominio para exponer al enemigo en 2035

Teniente coronel Stephan Pikner, Ejército de EUA

El problema operacional al que se enfrentará el Ejército en el año 2035 será fundamentalmente diferente de los problemas a los que se ha enfrentado anteriormente. El antiguo desafío, para el que las plataformas y la doctrina actuales del Ejército siguen estando optimizadas, era un problema que se resolvía rompiendo el segundo escalón de las fuerzas de asalto soviéticas con fuegos de precisión de largo alcance, interdicción aérea de ala fija y ataques profundos de la aviación de ataque de ala rotatoria. Hoy en día, y todavía más en 2035, las grandes potencias adversarias de Estados Unidos plantean un reto totalmente diferente. Al amenazar el acceso a un teatro de operaciones y negar las áreas de reunión necesarias para preparar un contraataque decisivo, los adversarios de Estados Unidos han socavado el modo de guerra expedicionario preferido. Este enfoque de antiacceso/negación de área (A2/AD) dificulta la capacidad de responder eficazmente a una agresión rápida y limitada, lo que deja a los aliados y socios vulnerables a una amplia gama de actividades coercitivas y subversivas[1]. El elemento central del A2/AD es una red bien defendida, redundante y en gran medida oculta compuesta de sensores y tiradores que pueden localizar y atacar a las fuerzas amigas que se desplazan y se preparan en un teatro de operaciones[2]. Para hacer frente a este reto, el Ejército debe adoptar un enfoque novedoso que localice y fije los componentes críticos del A2/AD del adversario para así garantizar la libertad de acción en 2035.

Este argumento a favor del engaño militar multidominio como elemento central para encontrar al enemigo en los campos de batalla de 2035 se desarrolla en tres partes. En primer lugar, se abordan brevemente los antecedentes doctrinales del engaño militar en la actualidad. En segundo lugar, y de forma más exhaustiva, se analiza la probable evolución de los sistemas A2/AD del adversario, en particular los puntos fuertes y los posibles puntos débiles de la inteligencia artificial (IA) en la selección de objetivos. La tercera parte es una serie de recomendaciones que el Ejército debería considerar para emplear mejor el engaño multidominio y encontrar al enemigo, con ejércitos de campaña como integradores de estas actividades.

Antecedentes doctrinales del engaño militar

Los antecedentes doctrinales e históricos del engaño militar están bien establecidos. En términos generales, las actividades de engaño militar «se planifican y se ejecutan para hacer que los adversarios realicen, o dejen de realizar, acciones que favorecen los objetivos del comandante»[3]. En el contexto específico de alertar un sistema A2/AD adversario, esto implica amplificar las huellas de las unidades señuelo y sustituir continuamente las huellas de las unidades reales por otras simuladas, sobrecargando así al adversario con un número abrumador de falsos positivos[4]. Este enfoque de generar un gran número de falsos positivos —la impresión de que hay objetivos cuando en realidad no los hay— contrasta con la noción tradicional de camuflaje, que intenta crear un falso negativo enmascarando las huellas de las fuerzas amigas. El éxito de los esfuerzos de engaño radica en su carácter multidominio. En una era en la que los sensores son cada vez más utilizados, sofisticados y variados, la suplantación de un solo tipo sirve de poco contra un adversario capaz de fusionar rápidamente múltiples fuentes de información. El «engaño multidominio», como propone Christopher Rein, «requiere una estrecha y cuidadosa coordinación entre los dominios de la guerra para garantizar que los fallos en uno de ellos no anulen los esfuerzos en otras áreas»[5].

Un técnico de eliminación de artefactos explosivos controla un robot TALON el 17 de abril de 2019 durante un entrenamiento en la Base Expedicionaria Conjunta Little Creek-Fort Story, en Virginia. (Foto: Contramaestre Jeff Atherton, Armada de EUA)

La probable evolución de los sistemas A2/AD adversarios

Conocer con precisión la arquitectura A2/AD del adversario implica integrar la información recopilada mediante diversos medios. La dependencia excesiva de un solo método, como las comunicaciones electrónicas interceptadas o las imágenes aéreas, puede dar lugar a lagunas insalvables en la comprensión. Estados Unidos ha sido durante mucho tiempo inigualable en su conocimiento del campo de batalla, pero grandes potencias adversarias están ganando terreno rápidamente debido a un par de acontecimientos interrelacionados. En primer lugar, el aumento de la sofisticación, fidelidad, asequibilidad y variedad de los sensores ha facilitado y abaratado la obtención de información militar relevante. Sin embargo, convertir esa información en conocimiento requiere un segundo paso, y su inminente automatización puede resultar revolucionaria. La promesa de que el aprendizaje automático pueda fusionar la información bruta con rapidez y precisión en objetivos procesables complicará enormemente las tareas de ocultación —y supervivencia— en el futuro campo de batalla.

Los avances generales en plataformas y sensores de bajo costo en el mercado, como los drones y las cámaras de alta resolución, junto con la información de fuente abierta en tiempo casi real, como las publicaciones en las redes sociales y las imágenes por satélite comercialmente disponibles, han transformado tanto la escala y la fidelidad de la información como el número de actores internacionales que tienen acceso a ella. Estos sensores, que antes solo estaban al alcance de las principales potencias, han proliferado ampliamente en las últimas décadas. Esta tendencia no da señales de disminuir. A medida que los medios de detección se vuelvan más baratos, más fiables y capaces de recopilar información de alta calidad, la ventaja informativa de la que ha disfrutado Estados Unidos durante las últimas décadas se erosionará aún más[6].

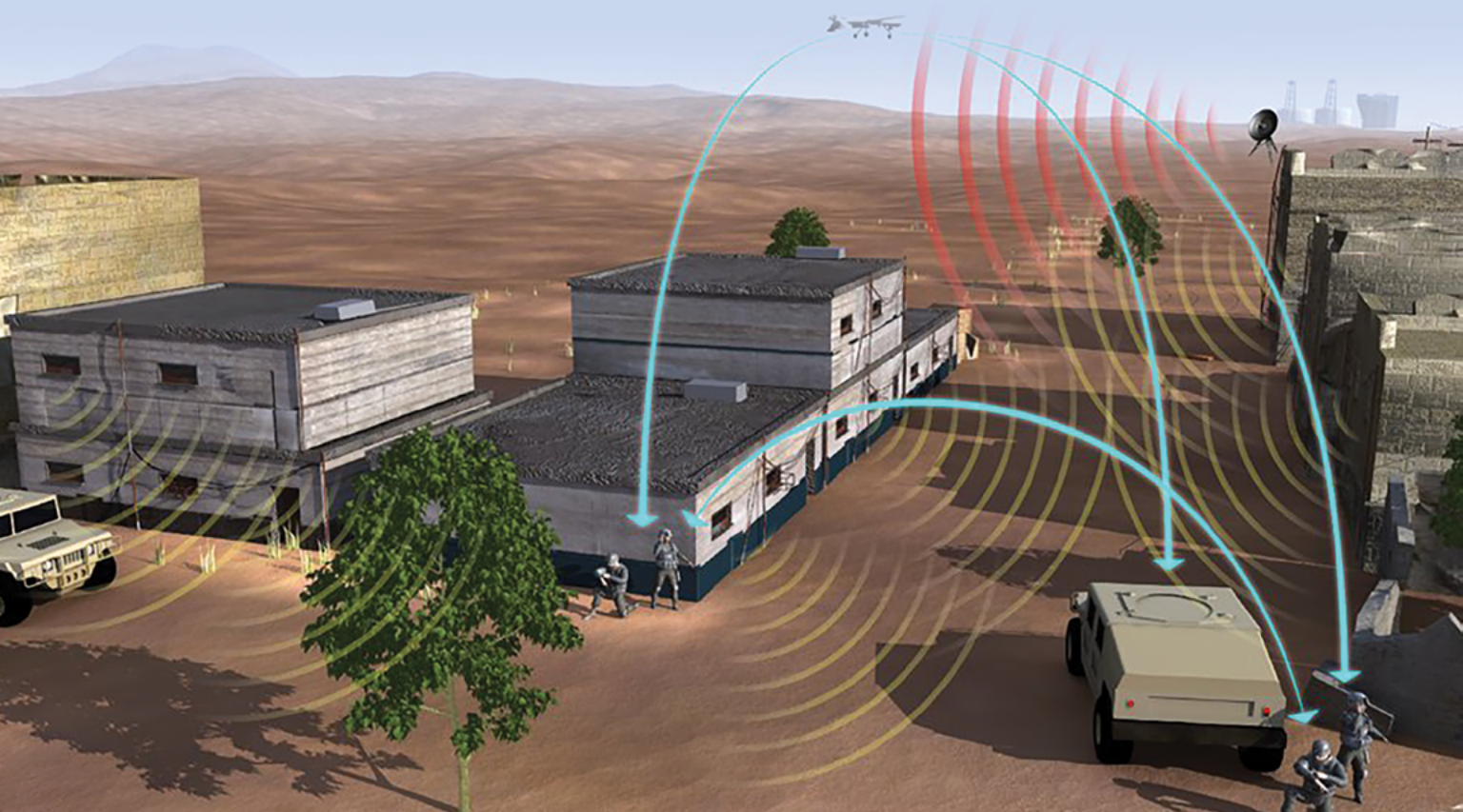
El aumento de la diversidad y calidad de los medios de recopilación es solo la mitad del desafío. La otra mitad —la fusión de la información procedente de múltiples fuentes para trazar un retrato completo de un objetivo— es una tarea más difícil. En la actualidad, se trata de un proceso muy laborioso en el que participan equipos multifuncionales de analistas que examinan minuciosamente grandes cantidades de datos captados por sensores de resolución cada vez mayor. Según algunos estimados, se necesitarían «ocho millones de personas para analizar todas las imágenes del mundo que se generarán en los próximos veinte años»[7]. Sin embargo, los avances en el aprendizaje

automático pueden mejorar y acelerar considerablemente la fusión de la información recopilada. Los clasificadores de aprendizaje automático, que «toman una muestra de entrada y la identifican como una de varias clases de salida», son especialmente adecuados para la fusión y la selección de objetivos[8]. En el contexto de apoyo de la IA a los objetivos A2/AD, la muestra de entrada serían los datos recopilados a través de una serie de sensores, y las clases de salida serían una clasificación del objetivo. Un algoritmo de aprendizaje automático adecuadamente entrenado y con acceso a una amplia gama de datos precisos podría entonces encontrar la proverbial aguja en el pajar y clasificar con precisión un objetivo, acelerando y mejorando en gran medida el hasta ahora laborioso proceso de fusión de información[9].

Al igual que su ventaja decreciente en materia de sensores, Estados Unidos no tendrá el monopolio de estas técnicas de fusión automatizada. Para 2035, es probable que sus adversarios hayan aprovechado las técnicas de aprendizaje automático para fusionar la información obtenida de una amplia gama de sensores contra sus armas A2/AD. Esto supondrá una nueva serie de retos con respecto a la forma en la que las fuerzas amigas se ocultan. La recopilación masiva de una amplia gama de huellas de las fuerzas amigas puede anular los esfuerzos de estas por camuflarse de forma monodimensional. Por ejemplo, minimizar las emisiones electromagnéticas puede tener un efecto insignificante contra un adversario que aún puede detectar la huella térmica, civil o de medios sociales de una unidad. En términos más generales, crear un falso negativo cohesivo contra un sistema de sensores multidominio altamente sensible será casi imposible. El adversario detectará algo y una IA bien entrenada podrá extrapolar una imagen precisa del objetivo a partir de lo detectado.

Aunque es inquietante, esta posible revolución en las técnicas de recopilación y fusión de información de los adversarios de Estados Unidos representa una oportunidad para que las fuerzas amigas encuentren al enemigo en los campos de batalla de 2035. Si se hace de forma cohesionada, el novedoso engaño militar multidominio puede distorsionar los algoritmos del adversario y aprovechar las tensiones organizativas y de procedimiento entre las propuestas

Las nuevas tecnologías convertirán e integrarán las señales electromagnéticas procedentes de múltiples fuentes en datos digitales. Estos podrán ser procesados a una velocidad sin precedentes para mejorar la capacidad del combatiente de ver a través de las medidas de engaño del enemigo para identificar y neutralizar las amenazas en el campo de batalla moderno. Los avances tecnológicos también mejorarán drásticamente la capacidad de las fuerzas amigas para engañar los esfuerzos de recopilación de inteligencia del enemigo a través de medidas de guerra electrónica mejoradas. (Ilustración: DARPA)



producidas por el aprendizaje automático y los responsables humanos. Este engaño no es un fin en sí mismo; para aclarar información incompleta y contradictoria de la selección de objetivos, un adversario se verá obligado a exponer su arquitectura A2/AD utilizando medios cada vez más expuestos que emiten huellas inequívocas. Engañar a un adversario para que exponga nodos críticos de su arquitectura A2/AD es fundamental para encontrar fuerzas enemigas bien ocultas en 2035.

El aprendizaje automático no es inmune a la falsificación, puesto que depende más en datos fácilmente cuantificables como entradas que en los procesos existentes en los que los humanos pueden incorporar pruebas ambiguas en su contexto. Los sensores centrados en la detección de datos electromagnéticos, acústicos, térmicos, gravitacionales, visuales, vibratorios, de redes sociales geoetiquetados o de análisis de texto asistido por computadora deben alimentar cuidadosamente, de forma limpia, un algoritmo de aprendizaje automático. Este algoritmo, a su vez, se entrena formando correlaciones entre huellas similares y características conocidas del objetivo[10]. Su precisión depende de la riqueza de los datos de entrenamiento, en el que los verdaderos positivos y las covariables válidas asociadas constituyen la base para el ajuste y la actualización del algoritmo. En un contexto militar, los verdaderos positivos serían casos reales del objetivo, y las covariables asociadas serían toda la gama de huellas medibles en todos los dominios. En la actualidad, la fusión de la información multidominio se lleva a cabo a través de células de personal militar que requieren mucha mano de obra. El aprendizaje automático ofrece la oportunidad de que este mismo proceso se lleve a cabo de forma rápida, automática y mediante el reconocimiento de patrones de correlación que pueden eludir la cognición humana. Enturbiar deliberadamente las aguas mediante operaciones de engaño militar que ofusquen el aspecto de un verdadero objetivo puede socavar este proceso de aprendizaje, engañando a un sistema A2/AD asistido por la IA para que busque en el lugar equivocado las huellas equivocadas. O, como señalan Edward Geist y Marjory Blumenthal, las fuerzas amigas pueden emplear «máquinas de niebla de guerra» para confundir los sensores de los adversarios y los procesos de aprendizaje automático asociados[11].

Esta mayor dependencia de flujos de datos cuantificables para alimentar un algoritmo de selección de objetivos basado en el aprendizaje automático también puede abrir una vulnerabilidad crítica dentro de la organización de un adversario que se puede producir a expensas de la experiencia y la intuición humana, lo que hace que todo el sistema sea vulnerable al engaño multidominio. El desarrollo desigual y vacilante de la IA en las últimas décadas está plagado de ejemplos de máquinas aparentemente inteligentes que, cuando se les plantean retos de la vida real que van más allá del estrecho alcance de su entrenamiento, son completamente inutiles[12]. A diferencia de los sistemas programados de forma convencional, no hay un equipo de ingenieros que pueda ajustar fácilmente el código para apoyar mejor a los responsables humanos del sistema, sino una caja negra en la que los resultados son generados por capas ocultas de enlaces ponderados dentro de una red neuronal formada por la iteración de los datos de entrenamiento[13]. Esta falta de claridad sobre el modo en que la máquina aprende puede causar fricciones en un sistema de toma de decisiones humano mejorado por la IA. Antes de que se produzca un fallo en el mundo real, la supuesta omnisciencia de un algoritmo de aprendizaje automático puede disminuir el valor relativo de la toma de decisiones humana, creando el dilema de que cuando más se necesita el sistema de aprendizaje automático es cuando menos se confía en él, mientras que la alternativa humana se ha atrofiado en cuanto a su estatus y capacidad[14].

Engañar al sistema de selección de objetivos basado en el aprendizaje automático puede hacer que el adversario active sensores que dejan una gran huella o ataque objetivos fantasma. En un futuro conflicto terrestre, esto abre una importante ventana de oportunidad para realizar

El teniente coronel Stephan Pikner, Ejército de EUA, es estratega (FA59) y graduado del Programa Avanzado de Política y Planificación Estratégica. Es licenciado por la Academia Militar de EUA, tiene una maestría en Administración Pública por la Harvard Kennedy School of Government y un doctorado por la Universidad de Georgetown. Su destino más reciente fue como G5 adjunto (planes) del Comando Terrestre Aliado de la OTAN en Izmir, Turquía.

fuegos conjuntos de contrabatería contra la «cadena de muerte» del enemigo, compuesta por sensores, nodos de mando y control, y plataformas de armas[15]. Lo que el engaño militar multidominio aporta a la guerra del futuro es la posibilidad de confundir a la máquina —llevándola a cometer errores en la cadena de selección de objetivos— y exponer sus medios de reconocimiento y ataque.

Recomendaciones

El desarrollo y el despliegue de las organizaciones, la doctrina, el adiestramiento y el equipo necesarios para el empleo eficaz del engaño militar multidominio requiere un enfoque deliberado y coordinado[16]. En esta sección se exponen cuatro consideraciones específicas para una fuerza capaz de aprovechar el engaño multidominio para encontrar al enemigo en 2035. En primer lugar, los componentes de una postura integrada de engaño multidominio deben ser flexibles y adaptables para mantener un efecto de engaño sostenido contra un adversario que aprende. En segundo lugar, el engaño multidominio de espectro completo no puede comenzar en una crisis, sino que debe basarse en las condiciones de base establecidas durante la competencia por debajo del umbral del conflicto armado. En tercer lugar, como es muy probable que en las operaciones terrestres participen aliados y socios que lucharán junto a las fuerzas terrestres estadounidenses, el engaño multidominio se verá reforzado si se les incluye en un esquema que abarque todo el teatro. Por último, el engaño multidominio no debe verse como un fin en sí mismo, sino como un medio para incitar al adversario a «mostrar sus cartas». Al provocar que la cadena de muerte A2/AD del enemigo busque formaciones fantasma, el engaño multidominio puede activar —y, por lo tanto, exponer— componentes críticos de la red enemiga que pueden ser destruidos.

La primera consideración al desarrollar el engaño multidominio es la dinámica interactiva, competitiva y evolutiva del engaño militar. El éxito del engaño depende tanto de las percepciones e interpretaciones del adversario sobre las huellas amigas como de las emisiones que generan las formaciones. Además de los aspectos técnicos de la creación de apariencias creíbles, existe un elemento organizativo crítico que se basa en la cultura militar del adversario: lo que puede engañar a los estadounidenses puede no engañar a un adversario, y los métodos que pueden ser eficaces contra un rival pueden ser descartados por otro. Los esfuerzos de engaño deben adaptarse continuamente a medida que evolucionan los prejuicios, las capacidades y la doctrina del adversario.

En segundo lugar, el éxito del engaño en un conflicto debe construirse sobre una base establecida en tiempos de paz. La competencia persistente por debajo del umbral del conflicto armado debe incluir esfuerzos deliberados para vigilar, enmascarar y simular todo el espectro de huellas de las fuerzas terrestres amigas. El objetivo es doble: en primer lugar, «analizarnos» de forma exhaustiva y, en segundo lugar, influir en los conjuntos de datos de entrenamiento que los adversarios de Estados Unidos están construyendo sobre las fuerzas amigas en tiempo de paz para entrenar a sus sistemas de selección de objetivos asistidos por la IA. Para lograr estos objetivos, las operaciones de las formaciones amigas en tiempos de paz deben ser supervisadas exhaustivamente por equipos encargados de construir un perfil completo de las huellas de una unidad. Este perfil será la línea de base de lo que puede ser detectado y explotado por los sensores A2/AD del adversario. Estos equipos vigilarían a las fuerzas amigas tanto en enfrentamientos tácticos simulados como durante despliegues en posiciones avanzadas reales. A partir de estos datos, recopilados durante despliegues, ejercicios y rotaciones, se puede elaborar una imagen completa de cómo aparecen las formaciones terrestres ante toda la gama de sensores de un adversario.

Esa huella completa de las fuerzas amigas catalogada en tiempo de paz puede utilizarse de dos maneras. La primera es enmascarar la huella de formaciones reales minimizando sus emisiones. En contra de la sabiduría convencional de «entrenar como se lucha», muchas de las medidas que se tomarían para enmascarar la huella de una unidad solo deberían tomarse en una crisis del mundo real. Practicarlas de forma rutinaria durante la competencia en tiempos de paz permitiría al adversario conocer otros «indicadores» de la ubicación y disposición de una unidad que son más difíciles (o imposibles) de enmascarar durante un conflicto. Por ejemplo, minimizar la huella electromagnética de una unidad durante un despliegue rotacional puede llevar a un adversario a

buscar más de cerca otras huellas menos fáciles de ocultar como indicadores clave de fuerzas amigas.

Además de informar sobre la mejor manera de enmascarar la verdadera posición de una unidad amiga en crisis, la huella global de las fuerzas amigas puede reproducirse como técnica de engaño. Esta huella no solo incluye el equipo militar de una formación amiga, sino también las emisiones de medios sociales y civiles que produce el despliegue de dicha fuerza. Las unidades de engaño amigas que pueden simular las características de formaciones de combate completas pueden actuar como «señuelos» que desvían la atención de las formaciones reales y engañan al enemigo para que exponga componentes críticos de su cadena de muerte.

En tercer lugar, está casi garantizado que la futura guerra en el dominio terrestre tendrá lugar en un contexto de coalición. Para maximizar la eficacia táctica del engaño militar multidominio, las huellas de las formaciones terrestres aliadas y asociadas deben medirse e imitarse de forma similar a las fuerzas terrestres estadounidenses. En el ámbito del teatro de operaciones, esto incluye las operaciones de engaño militar que afectan los puertos de desembarco, los centros de fuerzas estratégicas y otras infraestructuras críticas que permiten a las fuerzas amigas entrar en una zona de operaciones. Como estas instalaciones suelen estar cerca de centros de población y suelen tener una doble función civil y militar, hay que tener especialmente en cuenta las preocupaciones de los aliados y las limitaciones de las actividades de engaño militar. Deben trazarse líneas claras que refuercen el estatus de protección de ciertas instalaciones y personal (por ejemplo, hospitales, centros religiosos, personal médico) y establecer la comunicación con los aliados de EUA para evitar cualquier percepción de que estos esfuerzos violan el Derecho de los Conflictos Armados[17].

Por último, el objetivo general de este esfuerzo de engaño militar multidominio es encontrar al enemigo en los campos de batalla. Es en la presentación de un objetivo irresistible, pero falso, para el adversario donde el engaño militar multidominio facilita la búsqueda del enemigo. Activar el sistema integrado de sensores y tiradores del enemigo simulando la presencia de objetivos lucrativos, pero fantasmas, puede poner al descubierto medios de alto valor y la capacidad de supervivencia de su cadena de muerte. Un engaño eficaz puede desencadenar la activación de toda la gama de sensores del adversario: equipos de reconocimiento, sistemas de ataque electrónico, satélites, vehículos aéreos no tripulados, radares de vigilancia terrestre y medios cibernéticos en busca de una quimera. Las armas A2/AD del enemigo, como los misiles balísticos de teatro de operaciones, la artillería de largo alcance y las fuerzas especiales, se desplegarían igualmente desde lugares seguros y camuflados para atacar lo que creen que son concentraciones amigas reales. Anticipando esta activación, los sistemas de inteligencia, vigilancia y reconocimiento amigos, sincronizados con el plan de engaño militar multidominio, pueden anticipar, percibir y explotar esta actividad enemiga abierta y activa. En lugar de una búsqueda ineficaz y costosa contra los componentes reforzados y camuflados de un sistema A2/AD, el engaño militar multidominio lleva a que nuestros futuros adversarios se expongan prematuramente.

La aplicación de estas recomendaciones requiere un conocimiento detallado de la potencia adversaria, el nivel adecuado de autoridades y capacidades amigas, y una buena disposición durante la competencia por debajo del umbral del conflicto armado para mantener y modular una campaña de engaño duradera. En la estructura actual del Ejército, esta tarea recaería muy probablemente entre un cuerpo de ejército y el Mando del Componente de Servicio del Ejército. A medida que el Ejército se adapta a la competencia entre grandes potencias, la recomendación final de este artículo es que un ejército de campaña, centrado en la competencia contra un adversario específico, debería ser el proponente e integrador de las operaciones de engaño militar multidominio[18]. Sin la carga de las responsabilidades de todo el teatro del Mando del Componente de Servicio del Ejército, y a diferencia de un cuerpo de ejército orientado a un adversario específico, un ejército de campaña estaría mejor posicionado para diseñar y llevar a cabo una campaña de engaño militar duradera, cohesiva y adaptable. A través del engaño, el Ejército puede obligar a sus adversarios a atacar a ciegas contra las sombras, exponiendo los componentes críticos de su arquitectura A2/AD a la detección, destrucción y, en última instancia, a la derrota. ■

Notas

1. Andrew J. Duncan, «New 'Hybrid War' or Old 'Dirty Tricks'? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment», *Canadian Military Journal* 17, nro. 3 (verano de 2017): 6–11.

2. Wilson C. Blythe Jr. *et al*., *Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study* (Fort Leavenworth, KS: Army University Press, 2020), accedido 20 de octubre de 2020, https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?-ver=2020-03-25-122734-383.

3. Field Manual 3-13.4, *Army Support to Military Deception* (Washington, DC: U.S. Government Publishing Office, 2019), 1-2.

4. *Ibid*., 1-8.

5. Christopher M. Rein, ed., «Multi-Domain Deception», en *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press: 2018), 2.

6. Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).

7. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (Nueva York: Hatchette, 2020), 59.

8. Patrick McDaniel, Nicolas Papernot y Z. Berkay Celik, «Machine Learning in Adversarial Settings», *IEEE Security & Privacy* 14, nro. 3 (mayo de 2016): 68–72.

9. Stephan Pikner, «Training the Machines: Incorporating AI into Land Combat Systems», Landpower Essay Series (Washington, DC: Institute of Land Warfare, enero de 2019), accedido 20 de octubre de 2020, https://www.ausa.org/sites/default/files/publications/LPE-19-1-Training-the-Machines-Incorporating-AI-into-Land-Combat-Systems.pdf.

10. Gary Marcus, «Deep Learning, a Critical Appraisal» (ensayo, New York University, 2018), accedido 20 de octubre de 2020, https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf.

11. Edward Geist y Marjory Blumenthal, «Military Deception: AI's Killer App?», War on the Rocks, 23 de octubre de 2019, accedido 20 de octubre de 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

12. Marcus, «Deep Learning, a Critical Appraisal».

13. McDaniel, Papernot y Celik, «Machine Learning in Adversarial Settings».

14. Peter Hickman, «The Future of Warfare Will Continue to Be Human», War on the Rocks, 12 de mayo de 2020, accedido 20 de octubre de 2020, https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/.

15. Brose, *The Kill Chain*.

16. «Para cambiar un ejército—ganar en el futuro», *Military Review* Tomo 75, nro. 4, (Cuarto Trimestre de 2020): 48-60.

17. «Geneva Convention (IV): Relative to the Protection of Civilian Persons, Part I», Infoplease, 12 de agosto de 1949, accedido 2 de noviembre de 2020, https://www.infoplease.com/primary-sources/government/united-nations/convention-relative-protection-civilian-persons-time-war.

18. Amos C. Fox, «Getting Multi-Domain Operations Right: Two Critical Flaws in the U.S. Army's Multi-Domain Operations Concept», Land Warfare Paper 133 (Washington, DC: Association of the United States Army, junio de 2020), accedido 20 de octubre de 2020, https://www.ausa.org/sites/default/files/publications/LWP-133-Getting-Multi-Domain-Operations-Right-Two-Critical-Flaws-in-the-US-Armys-Multi-Domain-Operations-Concept.pdf.