

Capacidades espaciales iraníes y apoyo a las operaciones militares

Iranian Missile Strike:
Implications of Iran's Response

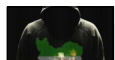
Tácticas de represalia de
el ejército iraní



EN ESTE NÚMERO



Ataque con misiles iraní:
Implicaciones de la respuesta de Irán3



Tácticas de represalia del ejército iraní7



Capacidades espaciales iraníes y apoyo
a las operaciones militares1



Previa del ATP iraní18



El pasado es presente: continuidad en la política exterior iraní
y por qué es importante20



Irán en Irak24



Actualizaciones de WTB27

Fuentes de las imágenes de portada: [derecha] Foreign CyberShafarat; [bandera inferior] Hossein Velayati / CC BY 4.0; [fondo] Google Earth.

Este número de Red Diamond incluye varios artículos centrados en Irán. Aunque nuestros lectores pueden esperar que nuestros artículos se centren en el ámbito táctico, este número amplía el contexto a un nivel más estratégico como resultado de los acontecimientos en tiempo real en el momento de su producción y de la experiencia de nuestros autores invitados. Comprender por qué Irán se comporta como lo hace facilitará la emulación fiel de los análogos iraníes en el desarrollo y la ejecución de escenarios de entrenamiento.

Son de especial interés los artículos de fondo de los renombrados expertos en la materia Joseph Fallon y Michael Rubin. Joseph Fallon, actualmente en el think tank UK Defence Forum, sitúa la política exterior iraní en su contexto histórico y sostiene que las acciones del actual régimen iraní son coherentes con los objetivos

de sus predecesores: la preservación del régimen mediante la protección de la independencia y la garantía de la integridad territorial. Michael Rubin, del American Enterprise Institute, analiza las complejidades de las relaciones entre Irán e Irak. Sostiene que el interés de Irán por dominar a su vecino occidental nunca desaparecerá, por innumerables razones culturales, económicas y estratégicas. La capacidad de Irán para ejercer influencia solo se ve frustrada por el compromiso continuo de Occidente de garantizar la independencia de Irak.

Jerry England explora cómo las fuerzas armadas iraníes, históricamente rivales, se están volviendo cada vez más expedicionarias y vengativas, y están mejorando su capacidad para coordinar sus esfuerzos. Destaca las diversas capacidades y técnicas iraníes, que van desde los misiles balísticos hasta los ciberataques. Kevin Freese ofrece una visión general de los programas espaciales iraníes y analiza la capacidad de Irán para apoyar operaciones militares a través de iniciativas espaciales y contraespaciales. Brad Marvel ofrece un avance de la próxima publicación del TRADOC G2, Army Techniques Publication (ATP) 7-100.4, *Iranian Tactics*, prevista para

lanzamiento en 2021. Por último, este número ofrece un informe de estado sobre las entradas actualizadas dentro de la *Guía mundial de equipamiento* de TRADOC G2.

Atentamente, Equipo editorial



acceso a Red Diamond a través de:

<https://community.apan.org/wg/tradoc-g2/ace-threats-integration/>

OEE Red Diamond publicado por TRADOC G-2 Dirección de Análisis de Amenazas
Entorno Operativo, Fort Leavenworth, Kansas

Consultas sobre el tema:

[Kevin Freese](#) (DAC), editor jefe

Personal de OE&TA:

Penny Mellies (DAC)
penny.j.mellies.civ@mail.mil

Director, OE&TA
913-684-7920

Teniente coronel Bryce Frederickson
bryce.e.frederickson.mil@mail.mil

913-684-7944

WO2 Rob Whalley
Robert.Whalley297@mod.gov.uk

Reino Unido LO 913-684-7994

Paula Devers (DAC)
mary.p.koontzdevers.civ@mail.mil

Especialista en inteligencia
913-684-7907

Laura Deatrick (CTR)
laura.m.deatrick.ctr@mail.mil

Editor
913-684-7925

Angela Williams (DAC)
angela.m.williams298.civ@mail.mil

Jefe de sucursal, T&S
913-684-7929

John Dalbey (CTR)
john.d.dalbey.ctr@mail.mil

Analista militar
913-684-7939

Jerry England (DAC)
jerry.j.england.civ@mail.mil

Especialista en inteligencia
913-684-7934

Rick García (CTR)
richard.l.garcia.ctr@mail.mil

Analista militar
913-684-7991

Jay Hunt (CTR)
james.d.hunt50.ctr@mail.mil

Analista militar
913-684-7960

Kris Lechowicz (DAC)
kristin.d.lechowicz.civ@mail.mil

Especialista en inteligencia
913-684-7922

Steven Sallot (CTR)
steven.m.sallot.ctr@mail.mil

Analista militar
913-684-5963

Jamie Stevenson (CTR)
james.e.stevenson3.ctr@mail.mil

Analista militar
913-684-7995

Walt Williams (DAC)
walter.l.williams112.civ@mail.mil

Especialista en inteligencia
913-684-7923

Jefe de división, A&P
913-684-7962

Jennifer Dunn (DAC)
jennifer.v.dunn.civ@mail.mil

Rick Burns (CTR)
richard.b.burns4.ctr@mail.mil

Analista militar
913-684-7987

Kevin Freese (DAC)
kevin.m.freese.civ@mail.mil

Especialista en inteligencia
913-684-7938

William Hardy (DAC)
william.c.hardy26.civ@mail.mil

Especialista en inteligencia
913-684-7901

Brad Marvel (CTR)
bradley.a.marvel.ctr@mail.mil

Analista militar
913-684-7914

Vincent Matteo (CTR)
vincent.p.matteo.ctr@mail.mil

Analista militar
913-684-7903

Matt Matthews (CTR)
matthew.m.matthews.ctr@mail.mil

Analista militar
913-684-7761

Dave Pendleton (CTR)
henry.d.pendleton.ctr@mail.mil

Analista militar
913-684-7946

Wayne Sylvester (CTR)
vernon.w.sylvester.ctr@mail.mil

Analista militar
913-684-7941

El boletín Red Diamond presenta información profesional, pero las opiniones expresadas en él son las de los autores, no las del Departamento de Defensa ni de sus elementos. El contenido no refleja necesariamente la posición oficial del Ejército de los Estados Unidos y no modifica ni sustituye ninguna información de otras publicaciones oficiales del Ejército de los Estados Unidos. Los autores son responsables de la exactitud y la documentación de las fuentes del material a los que hacen referencia. El personal de Red Diamond se reserva el derecho de editar. La aparición de hipervínculos externos no implica el respaldo del Ejército de los Estados Unidos a la información contenida en ellos.



Ataque con misiles iraníes: Implicaciones de la respuesta de Irán

Fuente: <https://www.dvidshub.net/image/6024487/ballistic-missile-attack-brings-unprecedented-amount-media-al-asad-airbase>

por Colin Christopher, TRADOC G-2

Los objetivos nacionales de Irán son ampliar el alcance y la relevancia de su marca de islam chiíta en todo Oriente Medio y asumir una posición de liderazgo regional. Irán considera que la influencia de Estados Unidos en la región es el principal obstáculo para alcanzar estos objetivos, y para asegurarlos recurre al uso global de grupos proxy, terrorismo, coacción y la amenaza y el empleo de la fuerza armada contra Estados Unidos y sus socios y aliados. Una de las principales herramientas de coacción y proyección de fuerza de Irán es su arsenal de misiles, que se caracteriza por un número cada vez mayor de sistemas relativamente sofisticados con mayor precisión, alcance y letalidad. Recientemente, Teherán empleó sus misiles balísticos en un ataque contra instalaciones estadounidenses en Irak. Aunque la operación fue claramente simbólica, la respuesta de Irán puso de manifiesto sus avanzadas capacidades, revelando a un adversario más capaz y con capacidad para desafiar al ejército estadounidense.

Resumen del ataque

El 7 de enero de 2020, Irán lanzó varios misiles balísticos de corto alcance (SRBM) desde tres ubicaciones dentro de Irán contra las fuerzas estadounidenses en Irak. Los misiles impactaron en dos bases aéreas: Ayn Al Asad, en el oeste de Irak, y una base aérea.

en Erbil, en el norte de Irak. La base aérea de Al Asad sirve como centro operativo para las operaciones militares estadounidenses en el oeste de Irak, y Erbil es un lugar de reunión para operaciones especiales, incluidas las operaciones en el norte de Irak y Siria. El ataque, cuyo nombre en clave era «Operación Mártir Soleimani», fue una represalia por el ataque con drones estadounidenses que mató al comandante de la Fuerza Qods del Cuerpo de la Guardia Revolucionaria Islámica de Irán (IRCG-QF), el general de división Qassem Soleimani.¹

Irán lanzó dieciséis misiles balísticos de corto alcance (SRBM) en dos oleadas con aproximadamente una hora de diferencia. De los dieciséis misiles lanzados, once impactaron en la base aérea de Ayn Al Asad, uno en la base aérea de Erbil y cuatro fallaron.² Irán afirma haber llevado a cabo una «guerra electrónica» durante y después del ataque, lo que probablemente indica que intentaban interferir los activos de contraataque de EE. UU.³ Los canales diplomáticos advirtieron a las fuerzas estadounidenses antes de los ataques, lo que limitó las bajas estadounidenses.⁴ El análisis posterior al ataque reveló daños en estructuras, equipos, pistas de aterrizaje craterizadas y lesiones cerebrales traumáticas a decenas de militares estadounidenses.⁵ La ausencia de víctimas mortales estadounidenses, junto con la temprana alerta política, condujo a una desescalada relativamente rápida, y desde el ataque ambas partes han mantenido una diplomacia tensa.



Figura 1. Mapa de las ubicaciones de los ataques con misiles

Fuente: TRADOC G2.

Implicaciones de la respuesta de Irán

Precisión y progresión de la escala de los misiles

El ataque contra las fuerzas estadounidenses reveló la capacidad actual de Irán para disparar diferentes tipos de misiles balísticos de corto alcance (SRBM) contra objetivos con mayor precisión. Lanzaron una lluvia de SRBM desde tres ubicaciones dentro de Irán y el 75 % de ellos alcanzaron su objetivo previsto. Se estimaba que los lanzamientos de misiles iraníes anteriores alcanzaban su objetivo previsto con una precisión de 250 metros (m). El análisis de imágenes de fuentes abiertas de este ataque con misiles sugirió una precisión de hasta 12 m.⁶ Los SRBM iraníes eran una combinación de propulsores de combustible sólido y líquido lanzados desde plataformas móviles y fijas con alcances de entre 500 y 800 kilómetros.⁷ Los misiles estaban equipados con guía por navegación satelital (SATNAV) y vehículo de reentrada maniobrable (MaRV) para mejorar la precisión.⁸

El programa nacional de misiles de Irán dedica importantes recursos al avance y desarrollo de una variedad de misiles capaces de amenazar a las fuerzas estadounidenses desplegadas, a sus aliados y socios. Además de la producción nacional de misiles, Irán se beneficia ampliamente de las adquisiciones en el extranjero. Aprovechan países como Corea del Norte y Rusia para ampliar la variedad y el alcance de sus misiles, y añaden nuevas generaciones de misiles balísticos a su arsenal.⁹ Parte del deseo de Teherán de añadir nuevas generaciones de misiles balísticos incluye la motivación de producir su propio misil balístico intercontinental (ICBM). El emergente programa espacial de Irán, la Agencia Espacial Iraní (ISA), ha creado una variedad de vehículos de lanzamiento espacial (SLV), cada uno de los cuales es más capaz de transportar cargas útiles más pesadas al espacio. Los ICBM y los SLV comparten

tecnología similar y Teherán puede utilizar la ISA para crear misiles balísticos intercontinentales. Otras ambiciones incluyen aumentar la capacidad de misiles balísticos de medio alcance (MRBM) y ampliar las capacidades de misiles de crucero.¹⁰ Irán está desarrollando rápidamente su capacidad en materia de misiles y el último ataque con misiles confirma que puede desafiar a sus enemigos con disparos más precisos y de mayor alcance.

Guerra electrónica integrada

Irán utiliza equipos modernos de guerra electrónica (EW) para proteger activos militares de gran valor. El general de brigada Amir Ali Hajizadeh, comandante de la Fuerza Aeroespacial del IRGC, afirmó que Irán empleó interferencias durante y

después de los ataques, probablemente como protocolo defensivo para protegerse de un contraataque estadounidense. El Gobierno iraní cuenta con capacidades de interferencia de las comunicaciones por satélite y del GPS, que Teherán ya demostró anteriormente al interferir los barcos que transitaban por el estrecho de Ormuz, según Según el análisis de la Agencia de Inteligencia de Defensa ¹¹. En mayo de 2019, las empresas de transporte marítimo comercial informaron de interferencias en el GPS y en las comunicaciones, que finalmente se atribuyeron a las fuerzas navales iraníes en la zona. Los barcos que navegaban por la región también informaron de falsificaciones. comunicaciones de entidades desconocidas que afirman falsamente ser buques de guerra estadounidenses o de la coalición.¹² Irán sigue buscando avances considerables en los sistemas de guerra electrónica para defender sus activos militares terrestres y navales. Las adquisiciones en el extranjero, en países como Rusia y China, han permitido a Irán reforzar y modernizar su guerra electrónica. Pudieron utilizar este suceso como prueba de las contramedidas actuales y presumir de su progreso en capacidades de guerra electrónica.

Represalias asimétricas

El líder supremo de Irán, el ayatolá Alí Jamenei, insinuó que Irán tomará medidas de represalia adicionales más allá de los ataques con misiles. Afirmó que «esto [el ataque] fue solo una bofetada anoche» ¹³. A pesar de la amenaza pública de Jamenei, es probable que Irán limite las acciones militares abiertas en favor de operaciones encubiertas tanto del IRGC-QF como de los representantes patrocinados por el Estado. Además, estas operaciones de represalia se llevarán a cabo en el momento y lugar que elija Irán, posiblemente en meses o años, en lugar de días o semanas. Acciones encubiertas podría incluir una serie de operaciones, desde ataques militares perpetrados por grupos milicianos hasta sofisticados ciberataques.

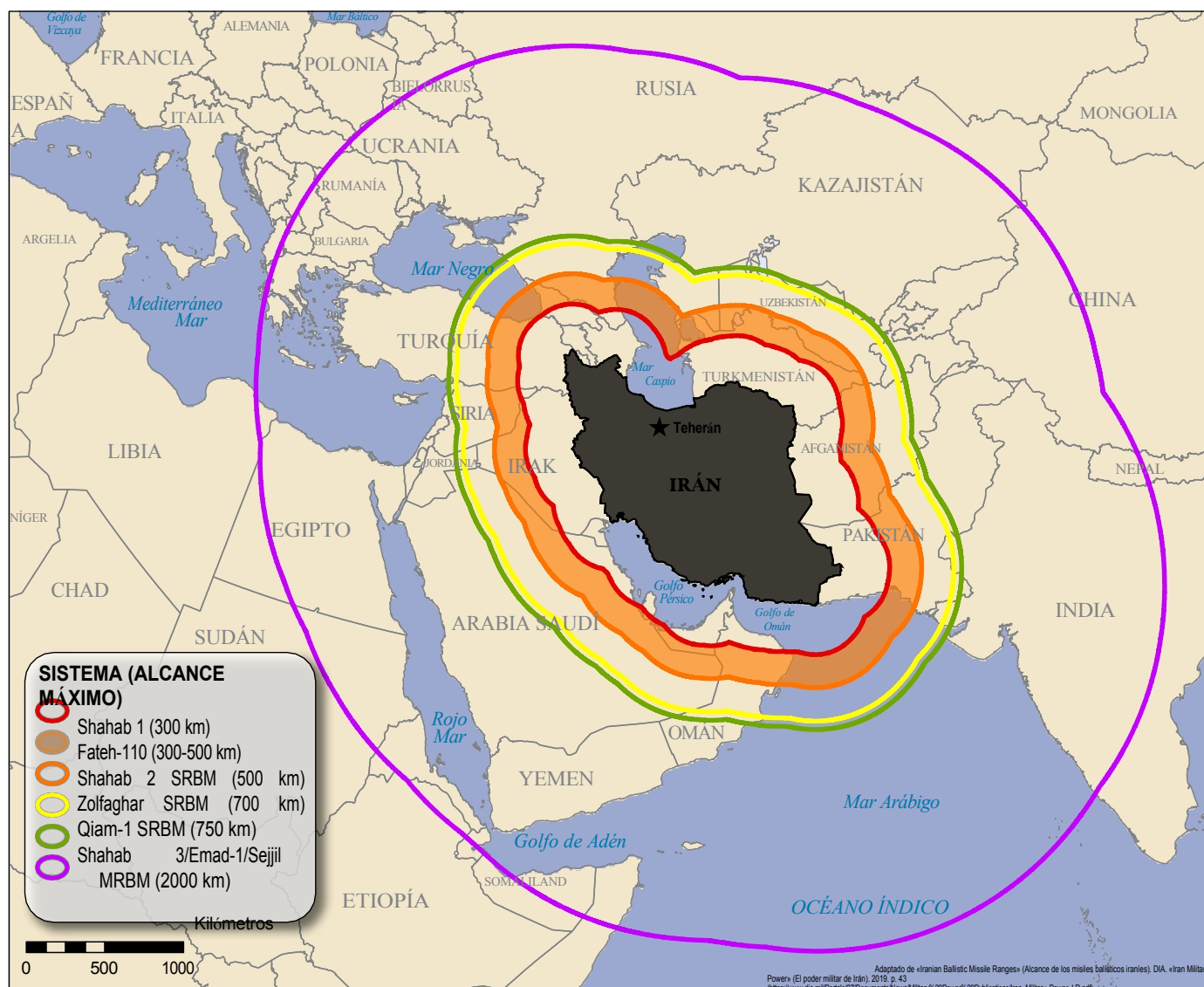


Figura 2. Tipos y alcances de los misiles iraníes

Fuente: TRADOC G2

guerra cibernética. En respuesta al ciberataque Stuxnet de 2010, Irán se centró en aumentar sus capacidades de guerra cibernética, incluyendo la ciberdefensa y los ciberataques. Cuenta con grupos cibernéticos patrocinados por el Estado capaces de lanzar ataques significativos contra infraestructuras críticas¹⁴. El uso de grupos proxy proporciona a Irán flexibilidad en el momento del ataque, negación plausible, genera distanciamiento y aprovecha la ambigüedad política y la postura estratégica.

Diplomacia iraní

Han pasado casi 30 años desde el último ataque con misiles balísticos que tuvo como objetivo las zonas de apoyo estadounidenses. En 1991, las fuerzas iraquíes atacaron con éxito a las fuerzas estadounidenses con base en Riad, Arabia Saudí, causando la muerte a 27 personas y heridas a decenas más¹⁵. En 2003, Irak volvió a atacar una zona de apoyo operativo estadounidense en Kuwait con dos misiles, pero no causó víctimas¹⁶. Durante el reciente ataque con misiles iraníes, el primer ministro iraquí confirmó que Irán había avisado a Bagdad 90 minutos antes de los ataques. La advertencia indicaba que se iba a producir un ataque contra objetivos estadounidenses en Irak.

inminente e indicó que, aunque los misiles alcanzarían objetivos en territorio iraquí, solo estarían dirigidos contra activos militares estadounidenses¹⁷. Ambas bases carecían de defensas antimisiles tierra-aire que las protegieran contra un ataque con misiles convencionales. Si no hubiera sido por las advertencias diplomáticas sobre un ataque inminente, las bajas estadounidenses podrían haber sido más numerosas. Irán hizo gala de una diplomacia hábil. Previendo una represalia segura si morían soldados estadounidenses, Irán aprovechó la oportunidad para llevar a cabo un ataque espectacular, al tiempo que se protegía diplomáticamente contra posibles represalias.

Operaciones de información

Desde el ataque contra Soleimani, Irán ha llevado a cabo una campaña de operaciones de información (IO) selectivas con el objetivo de reclutar y obtener apoyo mediante propaganda en línea que explota la muerte de Soleimani. A medida que la confrontación con Estados Unidos se intensificaba, pasando de la competencia a la crisis, la retórica se volvía cada vez más agresiva. Las operaciones de información han formado parte del arsenal de Irán desde la Revolución Islámica. Con el inicio del crecimiento exponencial de las redes sociales...

expansión, la IO de Irán se inclinó hacia Internet, convirtiéndose en una alternativa encubierta a la confrontación militar. Los representantes patrocinados por el Estado llevan a cabo campañas en las redes sociales para difundir argumentos a favor de Irán en Oriente Medio y en el extranjero. Es probable que la actual campaña de IO en línea de Irán mejore las oportunidades de reclutamiento de representantes patrocinados por el Estado y continúe intentando influir en la opinión pública regional y mundial a favor de Irán.

Conclusión

Esta crisis demostró cómo Irán puede utilizar una escala móvil de opciones para responder a lo que percibe como una agresión de Estados Unidos. También mostró cómo un adversario regional puede pasar rápidamente y sin problemas de la competencia a la

Crisis que desafía al Ejército de los Estados Unidos. Tras el ataque contra Soleimani, Irán empleó operaciones de información en un intento por controlar la narrativa tanto a nivel regional como global a su favor. El ataque con misiles balísticos de corto alcance (SRBM) de Irán contra las fuerzas estadounidenses en Irak demostró la vulnerabilidad de las instalaciones fijas ante todo el espectro de armas de mayor alcance y precisión. Para los adversarios de Estados Unidos, Irán puso de manifiesto la falta de preparación del ejército estadounidense, los detalles de las medidas de defensa pasiva que protegen a las tropas de combate y el precedente de cómo podría responder Estados Unidos cuando la competencia se convierte rápidamente en crisis. La respuesta de Irán indica claramente que se trata de un adversario regional capaz, con alcance global, que posee capacidades para las que el Ejército de los Estados Unidos no se ha entrenado durante las operaciones de contrainsurgencia o antiterrorismo.♦



Figura 3. Destrucción de la base aérea de Al Asad

Fuente: <https://www.dvidshub.net/image/6024515/ballistic-missile-attack-brings-unprecedented-amount-media-al-asad-airbase>

- Hannon, Elliot. «El ataque con misiles de Irán contra las fuerzas estadounidenses: qué ocurrió». 8 de enero de 2020. <https://slate.com/news-and-politics/2020/01/iran-missile-attack-us-forces-iraq-what-happened.html>.
- Talbot, Kyle. «El ataque de Irán contra las fuerzas estadounidenses pone de manifiesto el reto al que se enfrenta el Pentágono para detener los misiles balísticos». Stars and Stripes. 11 de enero de 2020. <https://www.stripes.com/news/middle-east/iran-s-attack-on-us-forces-exposes-pentagon-s-challenge-with-stopping-ballistic-missiles-1.614408>.
- Iran In-Depth. «Irán desactivó los sistemas de vigilancia estadounidenses durante el ataque con misiles, afirma el comandante del IRGC». Radio Farda. 9 de enero de 2020. <https://en.radiofarda.com/a/iran-disabled-us-monitoring-systems-during-missile-attack-irgc-commander-claims-30368664.html>.
- Chappell, Bill. «Lo que sabemos: el ataque con misiles de Irán contra EE. UU. en Irak». NPR. 8 de enero de 2020. <https://www.npr.org/2020/01/08/794501068/what-we-know-irans-missile-strike-against-the-u-s-in-iraq>.
- Beynon, Steve. «64 soldados estadounidenses sufrieron lesiones cerebrales traumáticas por el ataque con misiles iraní, mientras que el número total de víctimas sigue aumentando». Stars and Stripes. 30 de enero de 2020. <https://www.stripes.com/news/us/64-us-troops-suffered-traumatic-brain-injuries-from-iranian-missile-attack-as-casualty-total-continues-to-balloons-1.616914>.
- Savelsberg, Ralph. «Mejora masiva en la precisión de los misiles iraníes sobre los Scud-B». Guerra aérea, amenazas, sin categorizar. Breaking Defense. 15 de enero de 2020. <https://breakingdefense.com/2020/01/massive-improvement-in-accuracy-of-iran-missiles-over-srud-b/>.
- Taleblu, Behnam. «Irán utiliza cada vez más misiles en sus operaciones militares, y eso es un problema». The Hill. 21 de enero de 2020. <https://thehill.com/opinion/international/479076-iran-is-increasingly-using-missiles-in-its-military-operations-thats-a>.
- Amenaza de misiles. «El ataque con misiles de Irán: cómo ocurrió». Proyecto de Defensa Antimisiles del CSIS. Centro de Estudios Estratégicos e Internacionales. 9 de agosto de 2016. Última modificación: 14 de enero de 2020. <https://missilethreat.csis.org/>.
- El poder militar de Irán. «Garantizar la supervivencia del régimen y asegurar el dominio regional». Agencia de Inteligencia de Defensa. Agosto de 2019.
- Oficina del Secretario de Defensa. «Revisión de la defensa antimisiles de 2019». Departamento de Defensa. Enero de 2019.
- Agencia de Inteligencia de Defensa. «Retos para la seguridad en el espacio». DIA. Enero de 2019. <https://www.dia.mil/>.
- Joffe, Tzvi. «Estados Unidos advierte sobre interferencias en el GPS y suplantación de comunicaciones en el Golfo Pérsico». The Jerusalem Post. 8 de agosto de 2019. <https://www.jpost.com/Middle-East/US-warns-of-GPS-interference-communications-spoofing-in-Persian-Gulf-597996>.
- Smith, Patrick, Arouzi, Ali y Khodadadi Amin. «El líder supremo de Irán afirma que los ataques con misiles son una represalia insuficiente por el asesinato de Soleimani». NBC News. 8 de enero de 2020. <https://www.nbcnews.com/news/world/iran-s-supreme-leader-says-missile-strikes-insufficient-retribution-soleimani-n1112231>.
- Doffman, Zak. «La amenaza «crítica» de ciberataques de Irán: esto es lo que realmente está sucediendo ahora mismo». Ciberseguridad. Forbes. 11 de enero de 2020. <https://www.forbes.com/sites/zakdoffman/2020/01/11/irans-critical-cyberattack-threat-this-is-what-is-really-happening-right-now/#5cd42f634f78>.
- Drogin, Bob y Morrison, Patt. «Un misil iraní impacta en los barracones de los soldados estadounidenses; 27 muertos: Ataque con misiles Scud: 98 heridos en el ataque más mortífero de la guerra. Los barracones eran de la unidad de reserva de Pensilvania». Los Angeles Times. 26 de febrero de 1991. <https://www.latimes.com/archives/la-xpm-1991-02-26-mn-1889-story.html>.
- Bisney, John. «EE. UU.: Los Patriots derriban misiles iraníes». CNN. 20 de marzo de 2003. <https://www.cnn.com/2003/WORLD/meast/03/20/isrj.irq.kuwait.rockets/index.html>.
- Qiblawi, Tamara, Damon, Arwa y Laine, Brice. «Las tropas estadounidenses se refugiaron en búnkeres de la era de Saddam durante el ataque con misiles de Irán». CNN. 14 de enero de 2020. <https://www.cnn.com/2020/01/13/middleeast/iran-strike-al-asad-base-iraq-exclusive-intl/index.html>.

Retaliatory Tactics of the Iranian Military

Por Jerry England, OE&TA

La misión del ejército iraní es defender la Revolución Iraní protegiendo a los líderes de la República Islámica y manteniendo integridad territorial. Sin embargo, los renovados niveles de cooperación entre el Artesh (Ejército) y el Cuerpo de la Guardia Revolucionaria Islámica (IRGC) están haciendo que las fuerzas de combate de Irán sean cada vez más expedicionarias bajo el liderazgo actual, especialmente cuando se trata de tomar represalias contra amenazas percibidas. ¹ La doctrina de «defensa mosaico» de las Fuerzas Armadas iraníes exige que tanto el Artesh como el IRGC colaboren en tiempos de guerra, y también permite que se posicionen capacidades significativas en toda la región con el fin de impedir que los enemigos de la República Islámica establezcan una presencia duradera en Oriente Medio. Se ha renovado el énfasis en las estructuras conjuntas de mando y control, como el restablecimiento de la sede central de Khatam al-Anbiya, ha permitido a las fuerzas de combate sincronizar y coordinar mejor sus esfuerzos tanto a nivel nacional como internacional ¹.

La unión del Artesh y el IRGC, junto con una mayor tolerancia al riesgo, ha dado al régimen iraní la capacidad de responder de forma significativa a los intentos de restringir su política exterior. Las organizaciones, históricamente rivales, han logrado dejar de lado sus diferencias para preparar al ejército para el siglo XXI. Mediante tácticas y técnicas de bajo riesgo y alto rendimiento, el ejército iraní ha aumentado su alcance operativo. Esta nueva capacidad expedicionaria se mantiene en toda la región, incluso bajo estrictas sanciones internacionales. Se están probando y perfeccionando capacidades asimétricas, como los ataques de largo alcance, las operaciones de guerra no convencional y la guerra de información (INFOWAR), en un esfuerzo por establecer el régimen como protector del equilibrio tradicional de poder en Oriente Medio. ²

i. Las Fuerzas Qods, el elemento de guerra no convencional del IRGC, estuvieron bajo el mando general de brigada Esmail Qaani, continúe con el modus operandi de Soleimani.

El 2 de enero de 2020, el líder de las Fuerzas Qods del IRGC, Qasem Soleimani, murió en un ataque con misiles en el Aeropuerto Internacional de Bagdad. Conocido como el artífice de las operaciones del IRGC en Irak y Siria, Soleimani había desempeñado un papel fundamental en el perfeccionamiento de las tácticas y técnicas del ejército iraní en el siglo XXI. Tras su muerte, misiles lanzados desde Irán y sus aliados alcanzaron objetivos en la embajada estadounidense en Bagdad, así como en el Instalaciones militares estadounidenses en el desierto occidental iraquí. Además, una serie de ciberataques molestos afectaron a organizaciones de Estados Unidos y Oriente Medio ³. Aunque ambas reacciones al ataque no se consideran significativas si se comparan con la postura defensiva de Estados Unidos, el hecho de que se produjeran en un plazo relativamente corto demuestra la capacidad de Irán para responder de la misma manera cuando se ve amenazado. De hecho, la naturaleza tanto del ataque con misiles como de las actividades cibernéticas de bajo nivel ilustran cómo es probable que responda el Gobierno iraní en el futuro.

Selected Iranian Ballistic Missiles

System	Fateh-110 SRBM (and variants)	Shahab 1 SRBM	Shahab 2 SRBM	Zolfaghar SRBM	Qiam-1 SRBM	Shahab 3 MRBM	Emad-1 MRBM	Sejjil (Ashura) MRBM
Maximum Range (km)	300-500	300	500	700	At least 750	Up to 2,000	Up to 2,000	2,000
Propellant Type	Solid	Liquid	Liquid	Solid	Liquid	Liquid	Liquid	Solid
Deployment Mode	Road-mobile	Road-mobile	Road-mobile	Road-mobile	Road-mobile, Silo	Road-mobile, Silo	Road-mobile	Road-mobile

Note: This chart does not include all systems in development. All ranges are approximate.

Tres ejemplos recientes ilustran las capacidades y técnicas de represalia del régimen y son instructivos a la hora de evaluar las posibles respuestas a los intentos de control. o frenar el comportamiento contraproducente del Gobierno iraní. En primer lugar están los ataques con misiles contra la provincia de Deir ez-Zor en Siria en 2017 y 2018 tras los atentados terroristas contra instalaciones gubernamentales y militares iraníes. En segundo lugar, está el aumento de tropas iraníes en septiembre de 2015 en apoyo del Ejército Árabe Sirio en Alepo. Por último, están los ciberataques contra la gigante petrolera Saudi Aramco y el sector financiero estadounidense después de que el gusano Stuxnet dañara la instalación nuclear iraní en Nantanz. Cada uno de estos acontecimientos ha brindado a Irán la oportunidad de mostrar su capacidad militar en términos de mando y control, influencia internacional y avances tecnológicos.

Peligro lejano: 2017 y 2018 Ataques con misiles contra la provincia de Deir Ez-Zor.

El 7 de junio de 2017 se produjeron dos atentados terroristas, uno contra el edificio del Parlamento iraní y otro contra el santuario del imán Jomeini (un santuario religioso), con pocos minutos de diferencia entre ambos. Los atentados causaron aproximadamente 12 muertos y 40 heridos. El grupo terrorista Estado Islámico (ISIS) reivindicó la autoría del atentado.⁴ Las autoridades iraníes acusaron a varios actores regionales, así como a Estados Unidos. de planear el ataque.⁵ Once días después, cuatro misiles balísticos de corto alcance (SRBM) cayeron sobre la ciudad de Deir Ez-Zor, en Siria. Lanzados desde la base de misiles de Kermanshah, los misiles atravesaron el espacio aéreo iraquí y causaron daños a unos 650 km de distancia.⁶ Según se informó, era la primera vez que las fuerzas estratégicas iraníes utilizaban el misil Shahab-3 desde 1988, y el ataque se produjo solo 11 días después de que el Senado de los Estados Unidos aprobara un proyecto de ley para contrarrestar las actividades desestabilizadoras de Irán.⁷

Poco más de un año después, tras otro atentado terrorista contra un desfile militar en el cuartel general operativo del suroeste en Ahvaz, las fuerzas de misiles iraníes volvieron a responder, esta vez contra el cuartel general de facto del ISIS en la ciudad de Hajin. Del mismo modo, el ataque con misiles se lanzó desde la base de misiles de Kermanshah y alcanzó en las proximidades de los complejos del ISIS, a más de 550 km de distancia⁸. Los miembros de las milicias respaldadas por Irán en la zona comentaron que Irán había coordinado la operación con las autoridades sirias y rusas antes de llevarla a cabo⁹. Estas dos operaciones no solo pusieron de manifiesto la mejora de la capacidad balística de Irán, sino, lo que es más importante, su capacidad para sincronizar y coordinar operaciones entre sus aliados.

El ejército iraní cuenta con el arsenal de misiles balísticos más grande y diverso de Oriente Medio. La mayoría de ellos son misiles de corto alcance con un alcance máximo de 700 km. Irán dispone ahora de varios tipos de misiles de corto y medio alcance gracias

parte a la adaptación de tecnología extranjera y a un ambicioso programa espacial.¹⁰ Por ejemplo, los misiles Zolfaghar utilizados en los ataques de 2017 y 2018 emplean tecnología de motores de combustible sólido posiblemente obtenida de China.¹¹

Como parte integral de la estrategia de defensa iraní denominada «Mosaico», las fuerzas de misiles se reservan principalmente para atacar objetivos extrarregionales como parte de un plan de denegación de acceso y negación de área (A2AD) que intenta atacar las amenazas dentro de la zona de apoyo del enemigo con el fin de impedir el establecimiento de un punto de apoyo para futuras operaciones. Sin embargo, recientemente Irán ha ampliado el papel de su capacidad misilística más allá de esta función tradicional de A2AD para convertirla en un arma ofensiva y de guerra de información. Los ataques no tenían tanto que ver con causar víctimas como con transmitir el mensaje de que Irán puede competir con naciones tecnológicamente avanzadas en términos de fuego de largo alcance. Aunque las estimaciones sobre los daños reales causados en estos dos ataques varían mucho, el régimen iraní puede reivindicar su legitimidad militar ante sus aliados regionales y los ciudadanos iraníes.

Tras alcanzar una competencia relativa en tecnología de misiles, el arsenal de misiles balísticos de Irán se está convirtiendo en la mayor amenaza para la seguridad de la región y hay pruebas claras de que Irán está transfiriendo sus conocimientos a sus aliados en Oriente Medio¹². Se dice que las fuerzas de Hezbolá en el Líbano poseen más de 100 000 misiles, muchos de los cuales proceden de Irán. En Yemen, los rebeldes hutíes han lanzado misiles iraníes — entre ellos el SCAD, un misil balístico de corto alcance (SRBM) de combustible líquido— contra objetivos saudíes.¹³ En Irak, las diversas milicias respaldadas por Irán dentro de las Fuerzas de Movilización Popular (PMF) han añadido SRBM a su arsenal de cohetes no guiados desde su creación en 2014.¹⁴ Entre los sistemas se incluyen el Zelzel, el Fateh-110 y Zolfaghar, todos ellos sistemas de combustible sólido diseñados para ser fácilmente almacenados, transportados y disparados en el disputado campo de batalla iraquí.¹⁵

Las columnas voladoras del IRGC: el auge de 2015 en Siria

En otoño de 2015, según se informa, el IRGC aumentó el número de combatientes en Siria de 700 a 3000 en apoyo directo a la ofensiva siria y rusa en Alepo y sus alrededores¹⁶. En 2013, los rebeldes sirios, armados con armas recién adquiridas, habían logrado avances significativos en Alepo, incluida la toma de dos bases aéreas de la zona. Tras dos años de pérdidas territoriales en una encarnizada guerra de desgaste urbano en Alepo, los aliados de Bashar al Assad decidieron que solo una ofensiva a gran escala en múltiples frentes podría desalojar al enemigo de sus posiciones de combate en toda la ciudad.¹⁷ Con el apoyo Desde aviones de ataque terrestre rusos, el IRGC proporcionó liderazgo a un gran contingente de milicias locales y regionales, así como a las fuerzas del ejército regular sirio.¹⁸

El IRGC y el Gobierno iraní habían estado involucrados en el conflicto desde el principio, proporcionando asistencia económica y ayuda militar indirecta a través de la organización terrorista Hezbolá. Sin embargo, ante la falta de un liderazgo competente y el aumento de las deserciones de las fuerzas reclutadas del Ejército Árabe Sirio, en su mayoría suníes, el IRGC adoptó un enfoque expedicionario para los conflictos regionales. Al proporcionar comandos de la Fuerza Qods del IRGC, fuerzas especiales Artesh y combatientes milicianos de Irak y Afganistán, el IRGC ha logrado movilizar una fuerza combinada conjunta en apoyo del régimen de Assad.

Los reclutas extranjeros apoyaron al régimen con la esperanza de recibir formación y experiencia, así como salarios y prestaciones del Gobierno iraní; en algunos casos, la oportunidad de obtener la ciudadanía iraní por sus servicios en Siria.¹⁹ Las fuerzas del IRGC también han entrenado y apoyado al ejército sirio, incluyendo el establecimiento de un ejército ciudadano similar al Basij (la milicia nacional que se utiliza para controlar e intimidar a la ciudadanía iraní). El apoyo a Siria en 2015 supuso un paso significativo en el programa de ayuda militar y económica que respalda la dictadura de Bashar al Assad y representó una prueba de concepto para la estrategia de movilizar fuerzas significativas más allá del territorio iraní.

Este apoyo sin precedentes de Irán al régimen sirio se deriva de una larga historia de cooperación entre el gobierno teocrático iraní y la familia Assad, considerada miembro de una secta del chiísmo. A través de lazos religiosos y políticos, los funcionarios iraníes han podido interceder. No solo en Siria, sino también en Irak, Yemen y Líbano, utilizando eficazmente los servicios sociales para obtener apoyo para las operaciones militares. El «Movimiento de los Desposeídos», que comenzó en 1959 como una organización benéfica religiosa (para suplir la falta de servicios gubernamentales en el sur del Líbano, dominado por los chiítas), se convirtió en el movimiento Amal y finalmente fue absorbido en la década de 1980 por Hezbolá con la ayuda del Gobierno iraní.²⁰ Conocido como el «modelo Hezbolá», esta combinación de poder militar y poder blando se aprovecha para perturbar las operaciones contra las amenazas regionales y para impedir la proyección de poder de las fuerzas que tratan de detener la expansión de la influencia iraní.²¹

En las primeras etapas de la guerra civil siria, los funcionarios iraníes reconocieron el daño que causaría la pérdida de Damasco para su «anillo dorado» de seguridad. Las Fuerzas Qods iraníes, junto con el grupo terrorista Hezbolá, lograron conseguir apoyo para el régimen de Bashar al Assad mediante el reentrenamiento de las fuerzas policiales sirias y la legitimación de las milicias locales progubernamentales conocidas como «Shabiha» en la Fuerza de Defensa Nacional (NDF). La NDF y la policía recién entrenada operaban de una manera que permitía

Los ciudadanos sirios leales al régimen de Assad defienden sus hogares contra amenazas internas y externas sin alistarse en el ejército sirio y sin correr el riesgo de tener que abandonar a sus familias y propiedades. Con el asesoramiento de unidades del IRGC, las NDF aumentaron la presencia de los partidarios del Gobierno y liberaron recursos para operaciones ofensivas. Este enfoque aumentó el reclutamiento al permitir que los miembros permanecieran en sus hogares y actuaran como reserva operativa en lugar de desplegarse por todo el país.²² La capacidad de mantener las fuerzas en su lugar permitió al régimen sirio conservar el territorio una vez que fue despejado mediante acciones ofensivas.

Las técnicas de apoyo a los representantes mediante ayuda militar y armas se perfeccionaron aún más en Irak contra las fuerzas estadounidenses, mediante el entrenamiento y el asesoramiento a las milicias en el arte de la guerra de guerrillas. Este modelo seguirá exportándose a los conflictos de Oriente Medio, ya que el ejército iraní lo utiliza para mantener el control sobre su ideal del equilibrio tradicional de poder.

Otros conflictos regionales fuera de Siria influenciados por las fuerzas del IRGC de Irán incluyen Yemen, Líbano e Irak. En Yemen, el apoyo militar iraní, junto con la falta de atención occidental, ha permitido al régimen iraní apoyar ataques transfronterizos contra el ejército y la infraestructura petrolera de Arabia Saudí utilizando una combinación de acción directa y misiles tierra-tierra.²³ La transferencia de tecnología de sistemas no tripulados y otras formas de armamento de largo alcance ha permitido a Irán sostener la lucha de los hutíes contra el Gobierno de Yemen, al tiempo que le ha brindado la oportunidad de contraatacar al régimen saudí.²⁴

Los grupos de guerra no convencional iraníes también han logrado replicar el modelo de Hezbolá en Irak con el desarrollo de la Fuerza de Movilización Popular Chii (PMF), una organización paraguas que recluta y entrena milicias para operaciones contra amenazas regionales consideradas peligrosas por el IRGC.²⁵ La PMF, bajo el pretexto de ayudar al Gobierno iraquí en su lucha contra el grupo islamista suní ISIS, cerró el cuadrante noroeste de Mosul para impedir que los combatientes del ISIS entraran en Siria y continuaran la lucha contra Bashar al Assad. Se afirmó que esta estrategia no solo había acorralado al ISIS en sus complejas posiciones de combate en Mosul, sino que también había aumentado el número de bajas iraquíes y aliadas al prolongar la lucha.²⁶ Ahora que gran parte de la amenaza del ISIS ha sido destruida o dispersada, algunos grupos respaldados por Irán parecen estar centrando su atención en las fuerzas estadounidenses en la región.²⁷

Establecimiento del orden: guerra de información y gestión de la percepción

El IRGC adopta mensajes que utilizan una variedad de temas, incluyendo la persecución religiosa, la inestabilidad económica

e inestabilidad económica y corrupción gubernamental para combatir la «occidentalización» en Oriente Medio y destacar los intereses comunes con elementos potencialmente desestabilizadores entre el público objetivo. La campaña de influencia se respalda no solo con presencia sobre el terreno, sino también con una serie de actividades diseñadas para combatir la pérdida de la identidad cultural iraní. Entre estas actividades se encuentran una serie de servicios sociales y educativos, así como eventos artísticos y culturales. Programas estabilizadores, como los sistemas de bienestar que proporcionan prestaciones de supervivencia a las viudas, y los hijos de los mártires, la ayuda a la reconstrucción tras los combates, así como la asistencia a las fuerzas de seguridad para las poblaciones chiítas infrarrepresentadas, añaden legitimidad a la política exterior del régimen iraní, que busca nuevas formas de promover sus intereses²⁸.



Símbolo de la Policía Cibernética Iraní

Fuente: Wikipedia.

El uso de tecnologías en línea como Facebook, Twitter y Telegraph para informar e influir en las poblaciones objetivo es una técnica relativamente nueva para la expansión de los programas de influencia e información en toda la región. Sin embargo, las duras lecciones aprendidas de las protestas en toda la región han obligado al régimen a aprovechar los nuevos medios de comunicación para sus propios fines. Por ejemplo, la Primavera Árabe de 2011 sorprendió a los líderes iraníes en múltiples frentes, ya que se vieron directamente desafiados por el control de aliados clave en Siria, Líbano y Yemen, e indirectamente desafiados en toda la región cuando comenzaron a surgir narrativas rivales a favor del cambio revolucionario⁽²⁹⁾. La paradójica situación en la que se encontró el régimen tras el inicio de la Primavera Árabe no debería haber sido una sorpresa, ya que no habían pasado más de tres años

Antes, el Partido Verde iraní, armado con teléfonos móviles y otras plataformas de redes sociales, organizó la mayor protesta masiva en Irán desde la revolución de 1979³⁰.

En 2013, Irán había logrado integrar las redes sociales como otra plataforma para difundir su propaganda, a menudo destacando las hazañas de sus fuerzas proxy que operan en Siria y en toda la región. Además, se sabe que los líderes del régimen se han comprometido con Occidente y han inspirado a los fieles a la revolución a través de las plataformas de redes sociales.³¹

Se espera que los futuros esfuerzos del régimen iraní intenten utilizar herramientas emergentes basadas en datos, como los bots y la inteligencia artificial (IA) para seguir influyendo en los públicos objetivo de toda la región, al tiempo que censura y controla tanto los medios tradicionales como los medios en línea en Irán.³² Un informe sobre amenazas elaborado por la empresa de investigación en ciberseguridad FireEye concluyó que las operaciones de información iraníes están llevando a cabo operaciones de influencia impulsadas por las redes sociales en línea como forma de moldear los debates políticos.³³

Tecnología a medida: operaciones cibernéticas

La adopción por parte del régimen iraní de tecnologías de enfrentamiento, junto con el uso de proxies y otras entidades terceras para promover su agenda, se alinea con las operaciones cibernéticas como una propuesta de bajo riesgo y alta rentabilidad. Desde la formación del foro original de hackers Ashiyane En 2002, los piratas informáticos iraníes siguieron prosperando y desarrollaron capacidades cibernéticas para el Gobierno y el ejército, así como para milicias nacionales y extranjeras. El uso de Internet para responder a las amenazas mediante ataques a los sistemas de información políticos, económicos y de infraestructura es una herramienta de guerra de la información que constituye una táctica de represalia bastante común³⁴.

Se sabe que el IRGC participa en múltiples actividades cibernéticas, desde la falsificación de software informático hasta el desarrollo de herramientas de reconocimiento de redes, y desde 2012 ha evolucionado hasta convertirse en varios grupos de amenazas persistentes avanzadas (APT) de gran capacidad. A pesar de las estimaciones iniciales bajas sobre las capacidades cibernéticas iraníes, el régimen las desarrolló más rápidamente que otras potencias para convertirse en la amenaza creíble que es hoy en día, que ataca los sistemas de información en toda la gama de variables operativas.

En junio de 2010, se descubrió que un sofisticado ciberataque denominado «Stuxnet» había estado infectando una versión concreta de Microsoft Windows, así como la instalación iraní de enriquecimiento nuclear de Nantanz, desde 2007³⁵. El gusano Stuxnet fue diseñado para sabotear un sistema de control de supervisión y adquisición de datos (SCADA) muy específico denominado controlador lógico programable. La carga útil del gusano Stuxnet también

utilizaba cuatro vulnerabilidades previamente desconocidas en el sistema objetivo, denominadas ataques de día cero, un número sin precedentes para un solo ataque.

En el verano de 2012, tras la revelación del ataque Stuxnet a grupos ajenos a la comunidad cibernética, dos grupos, Cutting Sword of Justice e Izz ad-Din al-Qassam Cyber Fighters, lanzaron una serie de contraataques cibernéticos dirigidos al productor mundial de petróleo Saudi Aramco y al sector financiero de Estados Unidos. Los ataques contra Saudi Aramco consistieron en un gusano cibernético que se propagó como un virus por la red de la gigante petrolera. Más tarde se reveló que el malware se había infiltrado en la red utilizando un dispositivo USB infectado, similar al vector de ataque utilizado en el ataque Stuxnet. Una vez en el sistema objetivo, el gusano cibernético liberó una carga útil llamada «wiper» para borrar los datos de más de 35 000 dispositivos ³⁶.

La campaña masiva de denegación de servicio distribuido (DDoS) contra el sector financiero estadounidense fue sustancialmente mayor que los ataques DDoS anteriores, ya que los atacantes utilizaron la potencia de los centros de datos de los bancos para saturar los circuitos y provocar interrupciones en los principales bancos ³⁷. El uso de los recursos comprometidos basados en la nube como plataforma de ataque plataforma de ataque dificultó y

permitió al grupo de hackers continuar con sus operaciones a su antojo. ³⁸

Los grupos evitaron vínculos directos con el régimen, sin embargo, las pruebas de los ataques, como el código fuente y otras huellas digitales, sugerían que Irán era el responsable. En 2016, seis ciudadanos iraníes fueron detenidos por su presunta participación en los ataques al sector financiero estadounidense ³⁹. La empresa de ciberseguridad FireEye ha atribuido el nombre de usuario de uno de los desarrolladores del malware Shamoon que atacó a Saudi Aramco a la amenaza persistente avanzada (APT) iraní 33. ⁴⁰ Se desconoce cómo la experiencia iraní con Stuxnet se tradujo en un aumento de las capacidades cibernéticas de la República Islámica, pero los ataques posteriores parecieron ser más sofisticados que los anteriores, que hasta entonces consistían en actos de vandalismo en la web y la publicación de mensajes contra el régimen en foros en línea. ⁴¹

La comunidad de hackers iraníes, al igual que otras de la región, ha evolucionado de forma mayoritariamente orgánica a través de foros de hackers en línea e interacciones en toda la industria tecnológica iraní. Irán es uno de los países más conectados de Oriente Medio y cuenta con una industria tecnológica en rápido crecimiento. El uso generalizado de Internet y el pronto reconocimiento por parte del régimen iraní de la importancia



Símbolo del ejército iraní

Fuente: Wikipedia.

de las operaciones cibernéticas ha obligado a los servicios de inteligencia iraníes a buscar reclutas para sus operaciones cibernéticas. entre los grupos de hackers que podría percibir como una amenaza. En un campamento militar a las afueras de Teherán se ofreció un anuncio de un «Curso de Capacitación del Batallón Cibernético Basij», patrocinado por el gobierno, para entrenar a la próxima generación de ciber-soldados para el régimen iraní. Los cursos incluían el despliegue de contramedidas y falsedades para las fases preparatorias y operativas de los ciberataques, así como un «Curso específico sobre operaciones trollistas» ⁴². El creciente nivel de sofisticación ha dado lugar a ataques contra organismos gubernamentales estadounidenses y a ataques de denegación de servicio a gran escala contra empresas privadas, lo que indica un compromiso del gobierno iraní de explotar las vulnerabilidades cibernéticas. ⁴³

Se cree que la amenaza cibernética del Gobierno iraní está formada por múltiples organizaciones con diversos vínculos con el Gobierno, ya sea a través del ejército o por medios comerciales. Se considera que cada organización tiene su propio conjunto de objetivos y metas. Según un foro de vídeo en línea de FireEye, algunas de las herramientas e infraestructuras utilizadas por los ciberdelincuentes iraníes incluyen la implementación de técnicas sofisticadas como el rociado de contraseñas, los borradores y otras herramientas de software. El rociado de contraseñas es una forma técnicamente agresiva de seleccionar una o dos cuentas y probar metódicamente intentar contraseñas a lo largo del tiempo. Una vez que se adivina correctamente una contraseña, los datos se explotan para otras cuentas. ⁴⁴

Los actores iraníes parecen haber desarrollado una industria de ciberseguridad madura con grupos especializados en objetivos políticos, militares y económicos concretos. Por ejemplo, se dice que APT 34 (nombre dado por FireEye a un grupo iraní de amenazas persistentes avanzadas) tiene como objetivo la información de identificación personal (PII) y recopila grandes volúmenes de datos sobre personas de interés. La explotación de herramientas cibernéticas por parte de FireEye reveló que las APT gestionan sus capacidades cibernéticas con un

Un gran aparato administrativo que gestiona los datos de las empresas para contratistas o empresas ficticias, muestra que operaciones gubernamentales apoyan al gobierno y revela el proceso único de codificación y certificación de los actores maliciosos.

Otros grupos de hackers utilizan técnicas de ingeniería social que implican falsas oportunidades de empleo para conseguir que sus víctimas liberen malware. Los temas, caracterizados como señuelos laborales, utilizan la promesa de empleo y las encuestas de empleo como forma de descargar sus cargas útiles. Muchos de los objetivos son empresas de Oriente Medio del sector petrolero, hotelero, y compañías aéreas (transporte). El enfoque en la hostelería y la industria aérea tiene la ventaja añadida de descubrir los movimientos y patrones de vida de personas de interés.

La mayor parte de la información que busca APT 33 se refiere estrictamente a la obtención de inteligencia sobre empresas y entidades gubernamentales que trabajan en Oriente Medio. Los objetivos también pueden incluir a directores de TI y personas con acceso privilegiado como medio para alcanzar objetivos de alto valor. Los vínculos con las organizaciones de seguridad iraníes se han relacionado con las operaciones de APT 33 ⁴⁵.

La fuerza cibernética iraní es un actor cibernético emergente de amplio alcance que no solo utiliza técnicas cibernéticas bien conocidas, sino que también está desarrollando nuevos métodos para robar información, penetrar en infraestructuras y organizaciones públicas y perturbar la infraestructura global de información y comunicaciones.

Implicaciones

Las tácticas de represalia de Irán son letales, técnicamente avanzadas y evolucionan a un ritmo que requiere atención.

Las fuerzas del Departamento de Defensa que actualmente operan o operarán en Oriente Medio tendrán que tener en cuenta la amenaza iraní, especialmente en momentos de mayor tensión estratégica. Las técnicas desarrolladas por el IRGC se están transfiriendo a una amplia gama de actores amenazantes y ampliando la huella de la amenaza a regiones que antes no se veían afectadas por el ejército iraní.

La necesidad de Irán de construir una industria militar autosuficiente ha obligado a los fabricantes de armas iraníes a mejorar las tecnologías existentes y desarrollar nuevos medios para su producción. A medida que estas capacidades crecen, se espera que el ejército iraní las comparta con sus aliados en un intento por reducir las posibilidades de que las fuerzas del Departamento de Defensa de EE. UU. puedan operar sin obstáculos. En este contexto, la amenaza del fuego indirecto y los posibles enfrentamientos a pequeña escala son tan frecuentes como lo fueron durante el apogeo de las hostilidades en la Operación Libertad Iraquí.

Sin embargo, la capacidad cibernética de Irán también está evolucionando; a medida que el resto del mundo comienza a reconocer la amenaza que los ciberataques pueden suponer para las operaciones militares, las fuerzas cibernéticas iraníes tendrán que invertir más para mantenerse al día. Muchas empresas pueden recuperarse rápidamente de ataques molestos y desfiguraciones de sitios web, por muy embarazosos que puedan ser. La capacidad Aprovechar los sistemas de control industrial en red y otras infraestructuras puede tener un impacto mucho mayor, especialmente si las fuerzas del Departamento de Defensa operan en una región con una ciberseguridad privada deficiente. Además, un ciberataque exitoso contra un país aliado o socio puede arrastrar a las fuerzas a una situación imprevista para la que no están preparadas. El conocimiento del entorno de la información será un componente crítico de cualquier operación futura.

A medida que se reduce la presencia estadounidense en la región, Irán parece dispuesto a aprovechar finalmente la oportunidad para sacar partido de su condición de amenaza militar más desarrollada de la zona. El éxito de las operaciones militares iraníes y la falta de atención a las intenciones del Gobierno iraní en sus áreas de interés alentarán la futura participación militar iraní. El perfeccionamiento de las tácticas y técnicas del ejército iraní aumentará el riesgo de que Irán se convierta en una verdadera fuerza expedicionaria capaz de complicar aún más las posibles crisis.♦

1. Instituto Internacional de Estudios Estratégicos. «Las redes de influencia de Irán en Oriente Medio». Instituto Internacional de Estudios Estratégicos. Dossiers estratégicos. Cap. 1, noviembre de 2019.
2. Daniel R. Coats. «Evaluación mundial de amenazas de la comunidad de inteligencia». Comité Selecto del Senado sobre Inteligencia, 29 de enero de 2019.
3. Zak Doffman. «La amenaza crítica de ciberataques de Irán: esto es lo que realmente está sucediendo ahora mismo». *Forbes*, 11 de enero de 2020.
4. Amir Vahdat y Aya Batrawy. «El Estado Islámico reivindica un impactante atentado en el corazón de Irán». *Associated Press*, 7 de junio de 2017.
5. Kareem Shaheen y Nadia Khomami. «El ejército iraní culpa a los saudíes tras la muerte de 12 personas en un atentado terrorista en Teherán». *The Guardian*, 7 de junio de 2017.
6. Kyle Mizokami. «Irán lanzó una salva de misiles balísticos contra el ISIS». *Popular Mechanics*, 19 de junio de 2017.
7. Tyler Rogoway. «Irán lanzó un ataque con misiles balísticos sin precedentes contra una ciudad siria». *The War Zone*, 18 de junio de 2017; *Tehran Times*. «Irán lanza misiles contra el ISIS en Siria por los ataques de Teherán». 19 de junio de 2017.
8. ICESERVE24. «Investigación: Operación Muharram». 2019.
9. Hwaida Saad y Rof Nordland. «Irán lanza un misil balístico contra el ISIS en Siria. Vengando un ataque anterior». *New York Times*, 1 de octubre de 2018.
10. Michael Elleman. «El programa de misiles balísticos de Irán». *The Iran Primer*. Agosto de 2015.
11. Servicio de Investigación del Congreso. «Programas de misiles balísticos y lanzamientos espaciales de Irán». 6 de diciembre de 2012.
12. Shaan Shaikh. «Misiles iraníes en Irak». Centro de Estudios Estratégicos e Internacionales. Diciembre de 2019.
13. Agencia de Inteligencia de Defensa. «El poder militar de Irán». Oficina de Publicaciones del Gobierno de los Estados Unidos. 2019.
14. Shaan Shaikh. «Misiles iraníes en Irak». Centro de Estudios Estratégicos e Internacionales. Diciembre de 2019.
15. Instituto de Estudios Internacionales de Monterey. «Cronología de los misiles iraníes». Iniciativa contra la Amenaza Nuclear. Agosto de 2011.
16. Aron Lund. «No solo Rusia: el auge iraní en Siria». Centro Carnegie para Oriente Medio. 23 de mayo de 2016.
17. Aron Lund. «No solo Rusia: el auge iraní en Siria». Carnegie Middle East Center. 23 de mayo de 2016.
18. CNN. «Irán refuerza sus fuerzas en Siria». *CNN.com*. 27 de octubre de 2015.
19. Farnaz Fassihi. «Irán paga a afganos para que luchen por Siria». *Wall Street Journal*, 16 de mayo de 2014.
20. Boaz Atzil. «State of Weakness and 'Vacuum of Power' in Lebanon» (Estado de debilidad y «vacío de poder» en el Líbano), Estudios sobre conflictos y terrorismo, Escuela de Servicios Internacionales de la American University, 2010.
21. Will Fulton. «¿Hasta qué punto está involucrado Irán en Siria?». *The Iran Primer*. USIP, 6 de mayo de 2013. James B. Love. «Hezbollah: los servicios sociales como fuente de poder». Universidad Conjunta de Operaciones Especiales. Capítulo 3. Junio de 2010.
22. Aron Lund. «¿Quiénes son las milicias pro Assad?». Carnegie Middle East Center. 2 de marzo de 2015.
23. USIP. «Cronología de los ataques hufies contra Arabia Saudí». Original: 16 de septiembre de 2016.
24. Peter Brookes. «La creciente amenaza de los vehículos aéreos no tripulados iraníes requiere la intervención de EE. UU.». *Acción*. *Heritage*, 17 de septiembre de 2019.
25. Associated Press. «AP Explains: ¿Quiénes son las milicias iraquíes respaldadas por Irán?». *US News and World Report*, 31 de diciembre.
26. Dominic Evans, Maher Chmaytelli y Patrick Markey. «Cómo Irán cerró la «herradura» de Mosul y cambió la guerra de Irak». *Reuters*, 7 de diciembre de 2016.
27. Shawn Snow. «Un grupo respaldado por Irán lanza un ataque cerca de una pequeña guarnición en Siria que alberga a operadores especiales estadounidenses». *Militarytimes*, 16 de febrero de 2020.
28. Frederic Wehrey, David Thaler, Nora Bensahel, Kim Cragin y Jerrold Green. «Peligroso, pero no omnipotente: exploración del alcance y las limitaciones del poder iraní en Oriente Medio». Pág. 115. RAND, 2009.
29. Sharam Chubin. «Irán y la Primavera Árabe: ascendencia frustrada». Septiembre de 2012.
30. Abbas Milani. «El movimiento verde». *The Iran Primer*. USIP, 6 de octubre de 2010.
31. Instituto Internacional de Estudios Estratégicos. «Las redes de influencia de Irán en Oriente Medio». Instituto Internacional de Estudios Estratégicos. Dossiers estratégicos. Cap. 1 de noviembre de 2019.
32. Jessica Gynn. «Guerra de información en Facebook: dentro de las operaciones secretas de Irán para atacarte en las redes sociales». *USAToday*, 10 de enero de 2020; Alice Revelli, Lee Foster. «Una red de cuentas en redes sociales se hace pasar por candidatos políticos estadounidenses. Aprovecha los medios de comunicación estadounidenses e israelíes en apoyo de los intereses iraníes». Fireeye, 28 de mayo de 2019.
33. Equipo de inteligencia de Fireeye. «Presunta operación de influencia iraní aprovecha la red de sitios de noticias no auténticos y redes sociales dirigidas a audiencias en EE. UU., Reino Unido, Latinoamérica y Oriente Medio». Fireeye, 21 de agosto de 2019.
34. Collin Anderson y Karim Sadjadpour. «La amenaza cibernética de Irán: espionaje, sabotaje y venganza». Fundación Carnegie para la Paz Internacional. Págs. 10 y 11, 2018.
35. James Fawell y Rafal Rohozinski. «Stuxnet y el futuro de la guerra cibernética». *Survival*, Febrero marzo de 2011.
36. Fahmida Rashid. «Inside the Aftermath of Saudi Aramco Breach» (Dentro de las secuelas de la violación de Saudi Aramco). *Darkreading*, 8 de agosto de 2015.
37. Joseph Menn. «Los ciberataques contra los bancos son más graves de lo que la mayoría cree». *Reuters*, 17 de mayo de 2013.
38. Nicole Perlothy y Quentin Hardy. «El hackeo bancario fue obra de iraníes, según las autoridades». *New York Times*, 8 de enero de 2013.
39. Ellen Nakashima y Matt Zapotosky. «Estados Unidos acusa a hackers vinculados a Irán de atacar bancos y una presa en Nueva York». *Washington Post*, 24 de marzo de 2016.
40. Juha Saanen. «Fireeye identifica a un presunto grupo de hackers vinculado al Gobierno iraní». *IT News*, 21 de septiembre de 2017.
41. Collin Anderson y Karim Sadjadpour. «La amenaza cibernética de Irán: espionaje, sabotaje y venganza». Fundación Carnegie para la Paz Internacional. Págs. 10 y 11, 2018.
42. The Cyber Shafarat. «Cursos de capacitación del batallón cibernético en Abali: Basij cibernético iraní». *Treadstone* 71, 8 de enero de 2020.
43. Collin Anderson y Karim Sadjadpour. «El espionaje cibernético como amenaza de Irán. Sabotaje y venganza». Fundación Carnegie para la Paz Internacional. Págs. 10 y 11, 2018.
44. Fireeye. «State of the Hack: Spotlight Iran- from Cain & Abel to full SANDSPY» (El estado del hackeo: Irán en el punto de mira, de Cain & Abel a SANDSPY completo). YouTube. Canal Fireeye, 17 de enero de 2020.
45. Fireeye. «Estado del hackeo: Irán en el punto de mira, de Cain & Abel a SANDSPY completo». YouTube. Canal Fireeye, 17 de enero de 2020.



Fuente: Autor.

Capacidades espaciales iraníes and Support to Military Operations

Por Kevin M. Freese, OE&TA

Irán es una potencia espacial menor, pero es una potencia emergente que comprende la importancia militar del espacio y las actividades contraespaciales, y está trabajando diligentemente para mejorar sus capacidades. El

El Ejército de los Estados Unidos es el mayor usuario de capacidades espaciales del Departamento de Defensa y depende del apoyo espacial para mantener su dominio terrestre.¹ Por consiguiente, la comunidad de entrenamiento del Ejército de los Estados Unidos debería tener en cuenta las capacidades espaciales y contraespaciales de Irán al desarrollar y llevar a cabo escenarios y ejercicios que emulen los análogos iraníes o que se desarrollen dentro de Irán.

Área de influencia. En la actualidad, Irán cuenta con una importante infraestructura espacial y de misiles, así como con capacidad para lanzar misiles balísticos, una capacidad de lanzamiento espacial incipiente y poco fiable, una capacidad satelital inexistente y una capacidad antiespacial limitada. La presión internacional está ralentizando, pero no deteniendo, los avances en todas estas áreas. Los instructores y los desarrolladores de escenarios deben considerar los misiles balísticos de corto y medio alcance, ya sean empleados por fuerzas militares convencionales o por agentes irregulares, los ataques electromagnéticos y cibernéticos contra activos espaciales amigos y el acceso de segunda mano a capacidades satelitales como actividades potenciales en cualquier escenario hipotético.

Organización e infraestructura espacial

Los programas espaciales y de lanzamiento de satélites de Irán están gestionados por el Centro de Investigación Espacial de Irán (ISRC) y la Agencia Espacial de Irán (ISA), ambos dependientes del Ministerio de Comunicaciones y Seguridad de la Información del presidente iraní y del Ministerio de Defensa y Logística de las Fuerzas Armadas, que forma parte del ejército convencional de Irán (Artesh). Capacidad de misiles balísticos de Irán reside en la Fuerza de Misiles Al Ghadir, que forma parte de la Fuerza Aeroespacial del Cuerpo de la Guardia Revolucionaria Islámica de Irán (IRGCASF).² Además, el Consejo Espacial Supremo de Irán, compuesto por varios funcionarios de nivel ministerial, supervisa los programas espaciales.

Los ministerios participantes van desde los relacionados la defensa y la inteligencia hasta las carreteras y las minas.

Aunque el espacio, por su naturaleza, admite un doble uso, Irán da prioridad a la inversión en programas espaciales predominantemente militares frente a los programas civiles.³ El principal puerto espacial de Irán es el Centro Espacial Imán Jomeini, cerca de Semnan. Cuenta con dos complejos de lanzamiento, así como con instalaciones de montaje de cohetes y de pruebas de motores.⁴ La Organización Geográfica de las Fuerzas Armadas de Irán tiene una instalación para la obtención de imágenes y la cartografía en Teherán, y hay una estación terrestre de teledetección en Mahdasht.⁵ También hay ópticas y telescopios de radar en Mahdasht, que según Irán proporcionan capacidad de reconocimiento espacial, aunque dicha capacidad no está clara.⁶ Irán tiene bases de silos de misiles en Khorramabad y Tabriz, e instalaciones adicionales de misiles en Shahroud, Tabriz, Mashad, Kuhestak y



El lanzador Simorgh de Irán con el satélite Payam
photo : Tasnim News
commons.wikimedia.org/wiki/File:Simorgh_Payam_launch_04.jpg, Wikimedia Commons, 15 de enero de 2019, https://commons.wikimedia.org/wiki/File:Simorgh_Payam_launch_04.jpg, CC BY-SA 4.0

Kermanshah. Empresas del sector público y privado de todo el país suministran componentes que pueden utilizarse tanto en programas espaciales civiles como militares.⁷

Misiles balísticos

Irán mantiene el mayor arsenal de misiles balísticos de corto alcance (SRBM) y misiles balísticos de medio alcance (MRBM) de Oriente Medio y moderniza continuamente su fuerza para mejorar el alcance, la precisión y letalidad.⁸ Irán no posee ni da prioridad al desarrollo de una capacidad de misiles balísticos intercontinentales (ICBM).⁹

Los SRBM iraníes incluyen el Fateh-110, el Shahab-1 y el Shahab-2, todos ellos móviles por carretera. Se cree que Irán tiene menos de 100 lanzadores para cada uno de estos tipos de misiles, aunque el inventario de misiles puede superar en número a los lanzadores.¹⁰

- El **Fateh-100** es un cohete de combustible sólido de 8,9 m y 3450 kg capaz de transportar una carga útil de 500 kg a 300 km. Irán podría tener múltiples variantes, incluida una variante antibuque/antirradiación (el Hormuz) y una variante con un alcance de 700 km (el Zolfaghar).¹¹
- El **Shahab-1** (también conocido como Scud B/R-17/SS-1C) es un cohete de combustible líquido de 11 m y 5860 kg capaz de transportar una ojiva de 985 kg hasta 330 km. Irán los utilizó ampliamente en la guerra entre Irán e Irak.¹²
- El **Shahab-2** (también conocido como Scud C) es un cohete de combustible líquido de 11 m y 6095 kg capaz de transportar una carga útil de 770 kg a una distancia de 500 km. Irán utiliza ampliamente los Shahab-2 en ejercicios militares. El Qiam-1 es una variante ligeramente más pesada del Shahab-2 (6155 kg (6,8 t)), con una carga útil algo más ligera (750 kg) y un alcance significativamente mayor (800 km). Irán ha empleado los Qiam-1 contra objetivos del ISIS en Siria¹³ y contra objetivos estadounidenses en Irak.¹⁴

Los misiles balísticos de medio alcance iraníes incluyen el Shahab-3 y el Sejil (Ashura), ambos móviles por carretera, aunque el Shahab-3 también se lanza desde silos. Se desconoce el número de misiles de este tipo que posee Irán.¹⁵ El Shahab-3 es la variante iraní del No Dong 1 de Corea del Norte. Se trata de un

Cohete de combustible líquido de una sola etapa. Sus especificaciones exactas no están claras, pero probablemente tenga una longitud de 16,6 m, una masa de lanzamiento de 17 410 kg y sea capaz de transportar una carga útil de 1200 kg a 1300 km. Irán ha obtenido resultados dispares en las pruebas del Shahab-3 y ha desplegado menos de 50 lanzadores.¹⁶ Las variantes del Shahab-3 incluyen el Ghadr-1 y el Emad. El Ghadr-1 es un cohete de dos etapas con una etapa de combustible líquido y otra de combustible sólido. Según se informa, es ligeramente más pesado que el Shahab-3, con 19 000 kg, tiene un alcance mayor (1950 km) y una carga útil menor (800 kg). El Emad es en realidad un vehículo de reentrada sobre un Shahab-3, con una carga útil ligeramente menor (750 kg) y un alcance ligeramente más corto (1700 km) que el Ghadr-1.¹⁷ El Sejil (también conocido como Ashura) es un cohete de combustible sólido de dos etapas, de 18 m y 23 600 kg, con una capacidad de carga útil de hasta 1500 kg y un alcance de 2000 km. No se ha probado recientemente y no se sabe con certeza si está operativo.¹⁸

Lanzamiento espacial

Además de los SRBM y los MRBM, Irán cuenta con vehículos de lanzamiento espacial (SLV). A pesar de la preocupación internacional, un SLV no es un ICBM. La tecnología SLV de Irán es inferior a su tecnología de misiles, por lo que es dudoso que los SLV iraníes estén destinados a ser lanzamisiles,¹⁹ aunque las tecnologías de doble uso asociadas podrían utilizarse para facilitar y acelerar el desarrollo de ICBM.²⁰

El principal SLV de Irán es el Safir-1, un cohete de combustible líquido de dos etapas fabricado en el país. Tiene una longitud de 22 m (72 pies) y una masa de lanzamiento de entre 26 000 y 27 000 kg. El Safir-1 es capaz de colocar una carga útil de 50 kg en órbita terrestre baja (LEO).

Es una variante del misil balístico de medio alcance Shahab-3, desarrollado mediante la modificación del Shahab-3 para incluir una etapa adicional. Irán ha utilizado el Safir-1 para colocar cuatro pequeños satélites en órbita terrestre baja (LEO) y lo ha utilizado en varios intentos fallidos adicionales. La capacidad del Safir-1 lo convierte en un candidato poco probable para su conversión en un misil balístico intercontinental (ICBM).²¹ El Simorgh, o Safir-2, es el sucesor iraní del Safir. Al igual que el Safir-1, se basa en el MRBM Shahab. Tiene 27 m de largo y una masa de lanzamiento de entre 70 000 y 87 000 kg. Simorgh está diseñado para colocar cargas útiles de 250 kg en LEO, aunque aún no ha tenido éxito. Si Irán logra lanzar un Simorgh, su tecnología podría reutilizarse para apoyar un programa de misiles balísticos intercontinentales (ICBM).²²

Antisatélite (ASAT) y contraespacial

Irán cuenta con una sólida capacidad de interferencia satelital y, desde 2003, ha interferido agresivamente en las transmisiones satelitales para controlar el acceso a la información dentro de sus fronteras. Irán ha empleado con éxito interferidores terrestres desde su territorio, así como interferidores orbitales desde su propio territorio y desde el territorio de naciones aliadas. Entre los medios de comunicación afectados se encuentran la BBC, VOA, Radio Zamaneh y Rangarang.²³ Irán no solo ha reconocido su capacidad para interferir las señales de satélite, sino que promueve la proliferación de la tecnología de interferencia mediante la comercialización de interferidores de satélites a través de empresas estatales.²⁴

La capacidad de Irán para llevar a cabo ciberataques está muy por detrás de la de Rusia y China, pero ha ido creciendo desde 2010. Irán ha tenido cierto éxito al atacar a industrias del sector privado internacional utilizando diversas tácticas cibernéticas, que van desde el malware hasta los ataques distribuidos de denegación de servicio.²⁵ En caso de conflicto, los componentes orbitales o terrestres de los satélites podrían convertirse en objetivos de hackers iraníes cada vez más sofisticados.

A fecha de 2020, no hay pruebas de que Irán disponga de capacidad ASAT dirigida. Del mismo modo, las operaciones de lanzamiento y satélites iraníes son demasiado poco fiables como para considerarse amenazas ASAT coorbitales o de ascenso directo. Sin embargo, esto podría cambiar con el tiempo, a medida que mejore la capacidad espacial iraní.²⁶

Satélites

En febrero de 2020, Irán no tenía ningún satélite operativo en órbita. Sin embargo, Irán ha operado cinco satélites en órbita terrestre baja desde 2005. El conocimiento de estos satélites ilustra las capacidades, la determinación y las prioridades de Irán en el espacio. El SINA-1 fue el primer satélite de Irán, un satélite experimental de 160 kg construido por una empresa rusa y lanzado por Rusia, pero operado por Irán.

Agencia Espacial. El objetivo declarado del SINA-1 era la comunicación y la investigación ²⁷. Se lanzó en octubre de 2005 con una vida útil prevista de tres años, por lo que es poco probable que siga operativo en 2020 ²⁸. El segundo satélite de Irán, OMID, era un satélite experimental de comunicaciones de 27 kg. Fue el primer lanzamiento exitoso de un satélite nacional de Irán. Irán lo lanzó desde el Centro Espacial Jomeini a bordo de un cohete Safir-1. Funcionó durante unas semanas en febrero de 2009. ²⁹ El tercer satélite de Irán, RASAD-1, era un satélite de observación de la Tierra de 15 kg. Irán lo lanzó desde el Centro Espacial Jomeini.

Centro a bordo de un cohete Safir-1. Según se informa, tenía una resolución de 200 m. Funcionó durante tres semanas entre junio y julio.

2011. ³⁰ El cuarto satélite de Irán, NAVID, era un satélite de observación terrestre de 50 kg. Irán lo lanzó desde el Centro Espacial Jomeini a bordo de un cohete Safir-1B. Se informó de que tenía una resolución de 400 m, ⁽³¹⁾ y estaba destinado a la vigilancia meteorológica y de desastres naturales. Funcionó desde febrero hasta abril de 2012. ³² El quinto satélite de Irán, FAJR, era una versión actualizada del OMID. Supuestamente era capaz de funcionar durante 18 meses, pero salió de órbita pocas semanas después de su lanzamiento en febrero de 2015. ³³ Irán lo lanzó desde el Centro Espacial Jomeini a bordo de un cohete Safir-1B. Es posible que estuviera destinado a ser un satélite ELINT. ³⁴ Irán ha realizado múltiples intentos de lanzamiento de satélites utilizando Safir.

y cohetes Simorgh desde 2015. Ninguno ha tenido éxito ³⁵. Irán cuenta con instalaciones terrestres para satélites que podrían utilizarse para procesar imágenes y señales.

A pesar de la falta de capacidad satelital nacional, Irán sigue siendo capaz de adquirir datos satelitales de socios comerciales e internacionales.

Las sanciones y el futuro del espacio iraní

Irán tiene potencial para ser un actor espacial importante, pero es poco probable que aproveche ese potencial en un futuro previsible debido a su entorno estratégico y su enfoque. Irán es el 17º país más poblado del mundo, con

Una población que supera los 80 millones de habitantes. La población está muy urbanizada y la mitad de ella se encuentra en la edad de máxima productividad (entre 25 y 54 años). La tasa de alfabetización es del 85 % ³⁶. Más del 5 % de la población asiste a la

la universidad, pero, a diferencia de las economías más grandes, Irán es incapaz de absorber a sus graduados en los niveles adecuados de la fuerza laboral, como la ciencia de alta tecnología y la industria espacial. ³⁷ Aunque los éxitos espaciales de Irán han sido limitados, la infraestructura está en su lugar e Irán continúa invertir en el espacio. ³⁸ No obstante, el progreso de Irán se ve frenado por la presión internacional. Algunas sanciones de la ONU se levantaron en 2015, pero otras siguen vigentes. La UE tiene sus propias restricciones en vigor sobre la tecnología de doble uso, ciertos metales, equipos de transporte y actividad financiera. Al igual que las sanciones de la ONU, estas

se suavizaron en 2015, pero no se levantaron. ³⁹ Además, Estados Unidos ha restablecido muchas de las sanciones suavizadas en 2015 y ha aplicado sanciones adicionales. ⁴⁰ Algunas sanciones se dirigían específicamente a la Agencia Espacial Iraní, así como a múltiples instituciones de investigación que la apoyan. ⁴¹ La retórica y las acciones hostiles persistentes de Irán preocupan a muchos científicos y gobiernos occidentales, ⁴² y es probable que la presión internacional continúe mientras Irán apoye a las redes terroristas regionales y mundiales y amenace tanto a los países vecinos como a los lejanos. ⁴³ En consecuencia, los programas espaciales de Irán serán objeto de escrutinio y se verán obstaculizados en el futuro previsible.

Implicaciones para la comunidad de entrenamiento

Para los instructores del Ejército y los diseñadores de escenarios, las principales capacidades espaciales iraníes a tener en cuenta son los misiles balísticos de corto y que podrían utilizarse para atacar a las fuerzas militares o amenazar a los socios regionales. De hecho, es probable que los misiles balísticos sean parte integrante de cualquier Operación militar iraní. Además de las propias fuerzas iraníes, los aliados de Irán están en posesión de misiles balísticos de corto alcance iraníes y podrían emplearlos en cualquier escenario. La principal capacidad antiespacial iraní será el bloqueo electromagnético del GPS y las comunicaciones. Como capacidad secundaria, se podrían emplear ciberataques para interrumpir o degradar el apoyo espacial a las formaciones militares estadounidenses. Aunque es menos probable, no se debe descartar la capacidad de llevar a cabo ataques cinéticos contra estaciones terrestres de satélites mediante aliados.

Aunque existe una infraestructura terrestre para apoyar la explotación de imágenes y la cartografía, es poco probable que Irán cuente con un apoyo satelital significativo para las operaciones terrestres. Es probable que la capacidad existente se haya adquirido a través de socios internacionales y proveedores comerciales. Para los instructores, esto significa que las fuerzas opositoras probablemente dependerían de activos aeroturbines en lugar de ISR satelital. ♦

ACTUALIZACIÓN:

En abril de 2020, Irán anunció que el IRGC había colocado con éxito un satélite de «inteligencia estratégica», denominado NUR-1, en órbita terrestre baja. El IRGC lanzó el satélite desde Shahroud utilizando un cohete Qased y un lanzador móvil ⁴⁴. Al igual que otros SLV iraníes, el cohete Qased parece estar basado en el MRBM Shaheh-3 ⁴⁵. Las capacidades de este satélite no están claras y es posible que en realidad no sean relevantes: el mensaje estratégico del lanzamiento demuestra que el IRGC tiene capacidad de lanzamiento. Esto sugiere que la capacidad de misiles balísticos intercontinentales es un objetivo iraní y pone de relieve que Irán da prioridad a la capacidad militar sobre la exploración pacífica del espacio.

1. David Mann, «On Space Programs» (Sobre los programas espaciales), *declaración ante la Subcomisión de Fuerzas Estratégicas del Comité de Servicios Armados, Senado de los Estados Unidos*, 2.ª sesión, 113.º Congreso, 12 de marzo de 2014, http://www.armed-services.senate.gov/imo/media/doc/Mann_03-12-14.pdf.
2. Agencia de Inteligencia de Defensa, *El poder militar de Irán: garantizar la supervivencia del régimen y asegurar el dominio regional* (Washington, D.C.: Oficina de Imprenta del Gobierno, agosto de 2019); Agencia de Inteligencia de Defensa, *Retos para la seguridad en el espacio* (Washington: Oficina de Imprenta del Gobierno, enero de 2019).
3. B. Harvey, H. Smid y T. Pirard, *Potencias espaciales emergentes: los nuevos programas espaciales de Asia, Oriente Medio y Sudamérica* (Chichester, Reino Unido: Springer, 2010).
4. Iniciativa contra la Amenaza Nuclear, «Irán», julio de 2017, <https://www.nti.org/learn/facilities/313/>.
5. B. Harvey, H. Smid y T. Pirard, *Potencias espaciales emergentes: los nuevos programas espaciales de Asia, Oriente Medio y Sudamérica* (Chichester, Reino Unido: Springer, 2010); Iran Watch, «Organización geográfica de las fuerzas armadas», 24 de julio de 2019, <https://www.iranwatch.org/iranian-entities/armed-forces-geographical-organization>.
6. Space Watch, «Irán afirma tener un radar SSA capaz de detectar satélites en órbita terrestre baja», diciembre de 2018, <https://spacewatch.global/2018/12/iran-claims-to-have-ssa-radar-capable-of-detecting-satellites-in-leo/>.
7. Iniciativa contra la Amenaza Nuclear, «Irán», julio de 2017, <https://www.nti.org/learn/facilities/313/>.
8. Departamento de Defensa, 2019 *Missile Defense Review* (Washington, D.C.: Oficina de Imprenta del Gobierno, 17 de enero de 2019).
9. Proyecto de Defensa Antimisiles, «Misiles de Irán», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 14 de junio de 2018, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/country/iran/>.
10. Comité de Análisis de Misiles de la Agencia de Inteligencia de Defensa, *Amenaza de misiles balísticos y de crucero* (Washington, D.C.: Oficina de Imprenta del Gobierno, 2017).
11. Proyecto de Defensa Antimisiles, «Fateh-110», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 9 de agosto de 2016, última modificación el 14 de enero de 2020, <https://missilethreat.csis.org/missile/fateh-110/>.
12. Proyecto de Defensa Antimisiles, «Shahab-1 (Scud B-Variant)», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 28 de septiembre de 2017, última modificación el 25 de febrero de 2019, <https://missilethreat.csis.org/missile/shahab-1/>.
13. Proyecto de Defensa Antimisiles, «Shahab-2», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 9 de agosto de 2016, última modificación el 22 de enero de 2020, <https://missilethreat.csis.org/missile/shahab-2/>.
14. Geoff Brumfiel y David Welna, «Las fotos satelitales revelan el alcance de los daños causados por el ataque iraní a la base aérea en Irak», *NPR* (8 de enero de 2020), <https://www.npr.org/2020/01/08/794517031/satellite-photos-reveal-extent-of-damage-at-al-assyad-air-base>.
15. Comité de Análisis de Misiles de la Agencia de Inteligencia de Defensa, *Amenaza de misiles balísticos y de crucero* (Washington, D.C.: Oficina de Imprenta del Gobierno, 2017).
16. Proyecto de Defensa Antimisiles, «Shahab-3», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 9 de agosto de 2016, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/missile/shahab-3/>.
17. Proyecto de Defensa Antimisiles, «Emad, Ghadr (variantes del Shahab-3)», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 9 de agosto de 2016, última modificación el 21 de enero de 2020, <https://missilethreat.csis.org/missile/emad/>.
18. Proyecto de Defensa Antimisiles, «Sejjil», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 9 de agosto de 2016, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/missile/sejjil/>.
19. David Schmeidler, «El lanzamiento espacial de Irán: ¿desarrollo de un misil balístico intercontinental o de un programa espacial?», Instituto de Investigación de Política Exterior, 22 de enero de 2019, <https://www.ipi.org/article/2019/01/irans-space-launch-icbm-or-space-program-development/>.
20. Departamento de Defensa, 2019 *Missile Defense Review* (Washington, D.C.: Oficina de Imprenta del Gobierno, 17 de enero de 2019); Proyecto de Defensa Antimisiles, «Misiles de Irán», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 14 de junio de 2018, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/country/iran/>.
21. Proyecto de Defensa Antimisiles, «Safir», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 16 de octubre de 2017, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/missile/safir/>.
22. Proyecto de defensa antimisiles «Simorgh», *Amenaza de misiles, Centro de Estudios Estratégicos e Internacionales*, 28 de septiembre de 2017, última modificación el 15 de junio de 2018, <https://missilethreat.csis.org/missile/simorgh/>.
23. PBS, «Interferencia satelital en Irán: una guerra por las ondas», *Frontline Small Media Report* (noviembre de 2012), <https://www.cache.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf>.
24. Agencia de Inteligencia de Defensa, *Challenges to Security in Space* (Washington: Oficina de Imprenta del Gobierno, enero de 2019).
25. Agencia de Inteligencia de Defensa, *El poder militar de Irán: garantizar la supervivencia del régimen y asegurar el dominio regional* (Washington, D.C.: Oficina de Imprenta del Gobierno, agosto de 2019).
26. Agencia de Inteligencia de Defensa, *Retos para la seguridad en el espacio* (Washington: Oficina de Imprenta del Gobierno, enero de 2019).
27. «SINAH-1», *N2YO.com*, <https://www.n2yo.com/satellite/?s=28893>; Krebs, Gunter Dirk, «Sina 1», *Gunter's Space Page*, https://space.skyrocket.de/doc_sdat/sina-1.htm.
28. Harvey, H. Smid y T. Pirard, *Emerging Space Powers: The New Space Programs of Asia, the Middle East, and South America* (Chichester, Reino Unido: Springer, 2010).
29. Robert Christy, «Iran in Orbit», *Zarya Soviet, Russian and International Space Flight*, 9 de febrero de 2020, <https://www.zarya.info/Diaries/Iran/Iran.php>.
30. Robert Christy, «Iran in Orbit», *Zarya Soviet, Russian and International Space Flight*, 9 de febrero de 2020, <https://www.zarya.info/Diaries/Iran/Iran.php>.
31. Robert Christy, «Iran in Orbit» (Irán en órbita), *Zarya Soviet, Russian and International Space Flight*, 9 de febrero de 2020, <https://www.zarya.info/Diaries/Iran/Iran.php>.
32. «NAVID», *N2YO.com*, <https://www.n2yo.com/satellite/?s=38075#results>.
33. «FAJR», *N2YO.com*, <https://www.n2yo.com/satellite/?s=40387#results>.
34. Robert Christy, «Irán en órbita», *Zarya Soviet, Russian and International Space Flight*, 9 de febrero de 2020, <https://www.zarya.info/Diaries/Iran/Iran.php>.
35. Robert Christy, «Iran in Orbit», *Zarya Soviet, Russian and International Space Flight*, 9 de febrero de 2020, <https://www.zarya.info/Diaries/Iran/Iran.php>.
36. Agencia Central de Inteligencia, «Irán», *CIA World Factbook*, 4 de marzo de 2020, <https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html>.
37. Amin Mohseni-Cheraghlo, «Actualización desde Irán: La crisis de exceso de educación en Irán», *Banco Mundial: Arab Voices*, 6 de octubre de 2017, <https://blogs.worldbank.org/arabvoices/iran-education-crises>.

38. B. Harvey, H. Smid y T. Pirard, *Potencias espaciales emergentes: los nuevos programas espaciales de Asia, Oriente Medio y Sudamérica* (Chichester, Reino Unido: Springer, 2010).
39. Consejo Europeo, «Medidas restrictivas de la UE contra Irán», 2019, <https://www.consilium.europa.eu/en/policies/sanctions/iran/>.
40. Departamento de Estado de los Estados Unidos, «Sancciones a Irán», 2019, <https://www.state.gov/iran-sanctions/#FactSheets>.
41. Zachary Halaschak, «EE. UU. impone sanciones a la Agencia Espacial Iraní tras el fracaso del lanzamiento del cohete», *Washington Examiner*, 3 de septiembre de 2019, <https://www.washingtonexaminer.com/news/us-imposes-sanctions-on-iran-space-agency-after-failed-rocket-launch>.
42. R. Naseer y M. Amin, «Terrorismo nuclear: exageración, riesgos y realidad: el caso de Pakistán», *South Asian Studies* (2019), <http://search.proquest.com/docview/2286901691/>.
43. Agencia de Inteligencia de Defensa, *El poder militar de Irán: garantizar la supervivencia del régimen y asegurar el dominio regional* (Washington, D.C.: Oficina de Imprenta del Gobierno, agosto de 2019).
44. Marcia Smith, «Irán lanza su primer satélite militar desde una nueva base de lanzamiento», *Space Policy Online* (22 de abril de 2020), <https://spacepolicyonline.com/news/iran-launches-first-military-satellite-from-new-launch-site/>.
45. Gunter Dirk Krebs, «Qased», *Gunter's Space Page*, https://space.skyrocket.de/doc_lau/qased.htm.

El primer satélite de fabricación nacional de Irán, OMID, a bordo de un cohete Safir, lanzado el 2 de febrero de 2009.

Fuente: Mardetanha, «Omid 0654», Wikimedia Commons, 14 de mayo de 2009, https://commons.wikimedia.org/wiki/Archivo:Omid_0654.jpg
CC BY-SA 3.0.



Previa del ATP de Irán

Por Brad Marvel, OE&TA

F Siguiendo los pasos de ATP 7-100.1, *Tácticas rusas*, ATP 7-100.2, *Tácticas norcoreanas*, y ATP 7-100.3, *Tácticas chinas*, la Dirección de Integración del Entorno Operativo del TRADOC G-2 se complace en anunciar el desarrollo de ATP 7-100.4, *Tácticas iraníes. Al igual que los otros tres ATP sobre tácticas de amenazas, el 7-100.4 examina la doctrina y el enfoque táctico de las fuerzas armadas iraníes.* se complace en anunciar el desarrollo de la ATP 7-100.4, *Tácticas iraníes*. Al igual que las otras tres ATP sobre tácticas de amenazas, la 7-100.4 examina la doctrina y el enfoque táctico utilizados por una nación que representa una amenaza específica, en este caso Irán, y proporciona a los usuarios finales de todo el Ejército una descripción precisa y legible de la doctrina de la amenaza. Esto permite a los planificadores, instructores y líderes para describir con mayor precisión las posibles tácticas iraníes en centros de formación y educación de todo tipo. Al igual que otras tácticas de amenaza ATP, la 7-100.4 debe ser totalmente desclasificado. El borrador inicial del ATP 7-100.4 debería estar terminado en 2020, y su publicación final está prevista para principios de 2021.

Las tácticas descritas en el ATP 7-100.4 se han extraído principalmente de publicaciones iraníes. Entre ellas se incluyen manuales doctrinales, libros, ensayos, monografías y artículos de prensa y revistas. Estas fuentes primarias se complementan con productos de expertos en la materia de todo el campo, junto con publicaciones gubernamentales de dominio público. Las fuentes primarias iraníes no son tan fáciles de conseguir como las de otros países tratados en el ATP, en particular China, pero el entusiasmo iraní por escribir sobre teoría militar debería proporcionar datos suficientes para ofrecer una visión general completa del enfoque táctico iraní. Son muy pocas las fuentes públicas que abordan las tácticas iraníes, centrándose en su lugar en gran medida en la política iraní, la política interior y exterior y la dinámica social. Gran parte de la investigación que alimenta el ATP es original, y gran parte de su material aún no ha sido examinado en un documento de código abierto.

El primer capítulo del ATP 7-100.4 analiza los fundamentos del régimen iraní: una visión general de la estructura política de Irán, sus objetivos políticos y estratégicos, y el entorno operativo iraní. Este capítulo no pretende ser un estudio exhaustivo de la enormemente compleja estructura política y estratégica iraní, sino que pretende ofrecer al lector una comprensión práctica de los diversos factores que conforman el enfoque táctico iraní. Los capítulos 2 y 3 tratan respectivamente de la estructura de las fuerzas terrestres y de las fuerzas conjuntas, ofreciendo una visión general de la estructura y la capacidad de todas las organizaciones militares iraníes relevantes. Esta sección también incluye

Un análisis de la cadena de mando iraní, que ayuda al lector a comprender el contexto en el que se transmiten las órdenes y las interacciones entre los mandos nacionales, regionales y locales.

La inmersión profunda en el enfoque táctico iraní comienza en el capítulo 4, con una descripción de la **defensa mosaica**. Se trata del concepto operativo general iraní, comparable a la batalla aire-tierra estadounidense o las Operaciones de Espectro Completo de generaciones pasadas. La Defensa Mosaico se basa en varias hipótesis clave:

- El adversario más probable de Irán es Estados Unidos, o los aliados de Estados Unidos respaldados por el poder militar estadounidense.
- El escenario militar más probable es aquel en el que Estados Unidos y/o sus aliados inician una acción agresiva y ofensiva en territorio iraní, con el objetivo de derrocar al régimen gobernante actual.
- La potencia de fuego estadounidense, especialmente la aérea, es abrumadora.
- Estados Unidos es muy reacio a sufrir bajas importantes y es más susceptible de perder una guerra en el frente político interno que en el campo de batalla real.
- Las fuerzas armadas iraníes seguirán luchando por encontrar los recursos adecuados, especialmente en lo que se refiere a nuevos equipos y entrenamiento.
- El ejército y la población iraníes son firmemente leales al régimen iraní y lucharán con entusiasmo contra cualquier invasor, incluso si se enfrentan a una gran disparidad en cuanto a entrenamiento o calidad del equipamiento.
- El terreno de Irán es muy adecuado para una campaña defensiva.



El carro de combate principal Karrar, probablemente basado en gran medida en el T-72/T-90, es uno de los primeros programas importantes de armas autóctonas de Irán

Fuente: Agencia de noticias Tasnim / CC BY (<https://creativecommons.org/licenses/by/4.0>), [https://commons.wikimedia.org/wiki/File:Karrar_\(Iranian_tank\)_01.jpg](https://commons.wikimedia.org/wiki/File:Karrar_(Iranian_tank)_01.jpg)

Basándose en estas suposiciones, los líderes iraníes desarrollaron su doctrina en torno a cuatro principios fundamentales:

- Aprovechar las ventajas del terreno y la profundidad estratégica para maximizar la resistencia de las formaciones iraníes que, de otro modo, podrían verse muy superadas.
- Siempre que sea posible, oculte, refuerce y disperse las fuerzas iraníes para contrarrestar las ventajas del enemigo en potencia de fuego.
- Planifique el aislamiento de las unidades tanto de los escalones superiores como de otras unidades.
- Aprovecha la disposición de Irán a absorber bajas, al tiempo que explota la extrema incomodidad del enemigo con las bajas, con el fin de poner fin al conflicto mediante la discordia política en la patria del enemigo.

La Defensa Mosaico es el resultado de este conjunto de supuestos y principios rectores. La estructura de mando y control tanto del Artesh —el ejército convencional iraní— como del Cuerpo de la Guardia Revolucionaria Islámica (IRGC) se ha descentralizado en gran medida y se ha construido en torno a la defensa local. El control táctico en los escalones superiores tiene menos prioridad que la fuerte cohesión e independencia de las unidades en los niveles inferiores.

refleja la suposición de que las fuerzas iraníes pueden enfrentarse a una potencia de fuego enemiga abrumadora que perturbe su red de mando y control. Las unidades iraníes centran su entrenamiento en operaciones defensivas y atrincheramientos, en particular en métodos pasivos como el ocultamiento y el camuflaje, y hacen un uso extensivo de instalaciones subterráneas y otros activos reforzados para resistir mejor a las fuerzas poderosas y modernizadas que prefieren luchar.

en terreno abierto. El IRGC y la milicia Basij, en particular, iniciarán una resistencia popular, empleando tácticas híbridas para hostigar y desorganizar las retaguardias enemigas e infligir bajas. En otros lugares, se espera que los sistemas de defensa aérea desgasten aviones extremadamente caros y de gran valor en la batalla aérea sobre Irán, y que una variedad de sistemas de misiles, pequeñas embarcaciones de superficie y submarinos intenten degradar las fuerzas navales enemigas o interceptar embarcaciones valiosas en el golfo Pérsico y sus alrededores.

Los capítulos restantes del ATP tratan con mayor detalle el reconocimiento y la seguridad, las tácticas ofensivas y defensivas, las tácticas de guerra cibernética y de información, la participación extranjera y el terrorismo, y la seguridad interna. La mayor parte del contenido detallará cómo cada una de estas tareas tácticas respalda el concepto de defensa mosaico, lo que proporciona al lector una comprensión holística del enfoque táctico iraní.♦



Miembros de la milicia Basij asisten a la conferencia anual de Basij. Obsérvese la gran variedad en cuanto a vestimenta/uniformes, forma física, edad y probable preparación de los distintos miembros de la milicia.

Fuente: Autor desconocido / CC BY (<https://creativecommons.org/licenses/by/4.0>), https://commons.wikimedia.org/wiki/File:Great_Conference_of_Basij_members_at_Azadi_stadium_October_2018_041.jpg

El presente: la continuidad en la política del reinado iraní y su importancia

Por **Joseph E. Fallon**, Foro de Defensa del Reino Unido

La política exterior del Gobierno de Irán en Oriente Medio y el sur de Asia es racional y coherente con las acciones de política exterior de Irán emprendidas por el Sha de Irán, con la excepción de que Teherán es ahora un adversario de Estados Unidos, en lugar de un aliado.

Irán es una nación fénix. Borrado del mapa por la invasión árabe musulmana del siglo VII d. C., Irán resurgió mil años después como un Estado persa independiente gracias al sah Ismail en 1501. Para asegurar la permanencia de una identidad persa independiente, el sah Ismail, mediante el proselitismo y la violencia,² convirtió a la población al islam chií, separando así culturalmente a los iraníes de los árabes y turcos suníes y de cualquier lealtad al califa del Imperio Otomano^{3,4} o a cualquier otra potencia extranjera. (Mapa 1)

Desde entonces, la política exterior de todos los gobiernos iraníes, independientemente de la dinastía o la ideología, se ha definido por esta historia. El objetivo de un gobierno iraní es preservar el orden político existente, cuya legitimidad depende del mantenimiento de la independencia y la integridad territorial del Estado. Porque el Estado es el defensor de *Iránshahr*, el corazón de los persoparlantes. Desde el siglo XIX, este es el territorio encerrado dentro de las fronteras del Irán moderno.

Los safávidas crearon el Irán moderno. La dinastía prosperó durante dos siglos. Pero cuando no logró preservar las fronteras políticas de Irán, fue sustituida por los afsharíes. Luego vinieron los zand, los kayar, los pahlaví y los ayatolás. Los regímenes van y vienen. Pero Irán permanece independiente e intacto.

Históricamente, para proteger *Irán*, Teherán debe establecer zonas de amortiguación al oeste, Irak, y al este, Afganistán.



Mapa 1. Imperio safávida, también conocido como Persia.

Fuente: Fabienkhan / CC BY-SA 2.5 https://commons.wikimedia.org/wiki/File:Map_Safavid_persia.png

y Pakistán, asegurándose de que esos países sean aliados o neutrales. Porque cuando esas tierras no son ni lo uno ni lo otro, han sido utilizadas como base para invasiones de Irán por parte de otomanos, uzbekos, afganos, rusos, británicos y Saddam Hussein. En dos ocasiones, en 1907 y 1941, Irán estuvo a punto de desaparecer tras ser dividido por rusos y británicos. (Mapas 2 y 3)

Esta historia ha definido la política exterior de la clase política iraní, tanto secular como sectaria, en el pasado y en el presente. Por lo tanto, es un error sugerir que, al perseguir

Con este objetivo, los ayatolás de Irán pretenden restablecer el Imperio persa.

Este análisis malinterpreta la naturaleza de ambos. El Imperio Persa era una imagen invertida de la República Islámica. Cualquier intento de Teherán de emular al Imperio Persa supondría una amenaza existencial para la República Islámica.

En primer lugar, el Imperio persa era un estado no islámico basado en una fe monoteísta más antigua, el zoroastrismo.⁵

En segundo lugar, el Imperio persa permitía la libre práctica de todas las religiones en su territorio.⁶

En tercer lugar, el Imperio persa liberó a los judíos del cautiverio babilónico, fomentó su regreso a la tierra de Israel y luego concedió a Israel un alto grado de autonomía política dentro del imperio.⁷

Y en cuarto lugar, el Imperio persa fue el modelo a seguir para el Sha de Irán, némesis de los ayatolás. En una fastuosa coronación celebrada en 1967, adoptó el título de los antiguos emperadores persas, *Shāhanshāh*;⁸ en 1971 patrocinó una extravagante celebración del 2500 aniversario del Imperio persa en Persépolis, antigua capital del imperio,⁹ y en 1976 sustituyó el calendario islámico por el calendario persa de Ciro el Grande¹⁰.

Los ayatolás no están intentando resucitar el Imperio persa. Tras el fracaso de exportar la Revolución iraní a los Estados suníes en 1979, y tras la guerra entre Irán e Irak (1980-1988), Teherán se centra en la supervivencia del régimen, lo que significa garantizar la integridad territorial de Irán. Para ello, Irán busca crear una alianza islámica, dominada por Teherán, que se extiende desde el mar Mediterráneo hasta Asia Central. Una alianza de este tipo sería más duradera que el Imperio Persa, ya que no se basa en un ejército «imperial» y un soberano, sino en los lazos de una religión, una lengua y una cultura comunes.

Al oeste, «Teherán está formando un "puente terrestre" que conecta Irán a través de Irak con Siria, Líbano y la frontera israelí en el Golán. Esto es lo que se denomina la Media Luna Chií»¹¹. Esto se ve facilitado por los iraquíes,



Mapa 2. Partición de 1907.

Fuente: Fabienkhan / CC-BY-SA 2.5 https://commons.wikimedia.org/wiki/File:Map_Iran_1900-en.png



Mapa 3. Partición de 1941.

Fuente: «Segunda Guerra Mundial: invasión anglo-soviética de Irán», Iran Review, 24 de agosto de 2016 <http://www.iranreview.org/content/Documents/World-War-II-Anglo-Soviet-Invasion-of-Iran.htm>

Libaneses y un número significativo de sirios ¹² que comparten la misma fe que los iraníes: el islam chiíta. (Mapa 4)



Mapa 4. Media luna chiíta

Fuente: Adaptado de M. Izady, «Emerging Shia 'Crescent' of Power in the Core of the Middle East», Gulf/2000 Project, SIPA Columbia University, Nueva York, 2008-2009., http://gulf2000.columbia.edu/images/maps/Shia_Crescent_sm.jpg

Al este, Teherán está promoviendo los lazos culturales entre afganos, tayikos e iraníes, basándose en su lengua persa común y su herencia persa. ^{13, 14, 15} (Mapa 5)

La política exterior de Irán también tiene un componente ofensivo dirigido a su rival político y religioso, Arabia Saudita, en tres frentes.

El primero es Bahréin, un premio estratégico ¹⁶ y económico ¹⁷ situado a dieciséis millas de la costa del golfo Pérsico de Arabia Saudí. Irán defiende los derechos democráticos de los chiítas, una mayoría privada de derechos (62 %) ¹⁸ frente a los gobernantes suníes respaldados por Arabia Saudí.

En segundo lugar está Yemen, en la frontera suroeste de Arabia Saudí. Teherán está utilizando la guerra civil en Yemen como una guerra indirecta con Riad. Ante el armamento de los rebeldes chiítas (hutíes) por parte de Irán ⁽¹⁹⁾ Arabia Saudí respondió con una intervención militar para evitar la caída del gobierno pro saudí. Pero Riad no logró derrotar a los insurgentes. La guerra está agotando los recursos financieros saudíes y alejando a sus aliados tradicionales, como Estados Unidos, Egipto y Pakistán ²⁰.

En tercer lugar está la provincia oriental de Arabia Saudí. La riqueza de Riad proviene principalmente de los pozos y reservas de petróleo

situada allí. ²¹ La provincia oriental limita con el golfo Pérsico y se encuentra a unos 320 km de Irán. ²²

y está habitada por chiítas (que representan entre el 10 y el 15 % de la población saudí). ²³ Perseguidos históricamente por Riad, ²⁴ los chiítas se rebelaron en 1979. Los disturbios chiítas estallaron de nuevo en 2011 y 2012, y continúan desde 2017. ²⁵

Por qué es importante

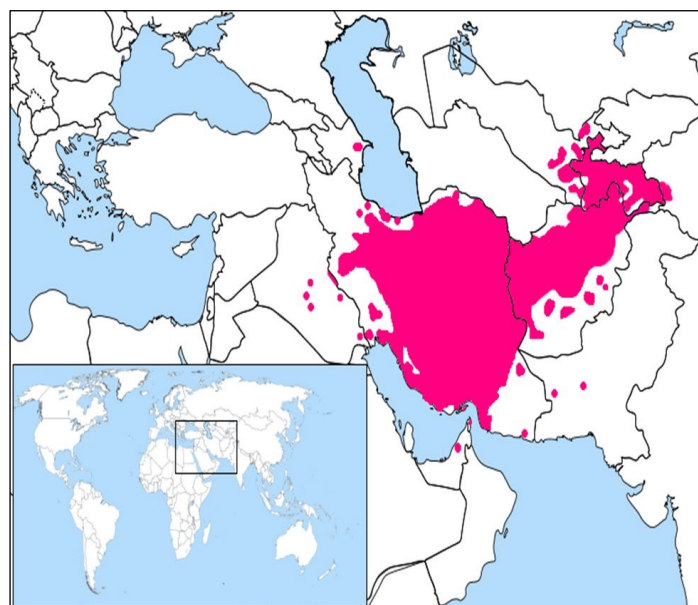
Es necesario conocer el objetivo de la política exterior de Irán si Washington quiere que Teherán deje de apoyar a los grupos terroristas y abandone su programa nuclear. Dicho conocimiento de la historia iraní permite comprender el impacto y las limitaciones de las acciones de Estados Unidos, incluidas las operaciones militares, a la hora de influir en el comportamiento de Teherán.

El nacionalismo iraní creó Irán e impulsa su política exterior, que ha logrado preservar la independencia del país durante 500 años. A este éxito contribuye el paisaje de Irán, que favorece la defensa frente al ataque. «Irán es una fortaleza».

Rodeado por tres lados por montañas y por el cuarto por el océano, con un páramo en su centro, Irán es extremadamente

difíciles de conquistar» ⁽²⁶⁾.

Un ataque militar estadounidense contra Irán para desarmar o derrocar al régimen requeriría tropas sobre el terreno. El



Mapa 5. Zonas con hablantes de persa como lengua materna

Fuente: Wikipedia, 9 de octubre de 2007, <https://commons.wikimedia.org/w/index.php?curid=3064301>

El éxito de tal invasión y ocupación estadounidense de Irán es dudoso. Washington se encontraría con una serie de obstáculos logísticos y de inteligencia.

1. Irán es cuatro veces más grande que Irak ²⁷.
2. La población de Irán es tres veces mayor que la de Irak ²⁸.
3. Irán es tres veces más grande que Afganistán ²⁹.
4. La población de Irán es dos veces y media mayor que la de Afganistán ³⁰.
5. La fuerza militar de Irán ocupa el puesto 14 de 138 países. ³¹
6. Es probable que el ejército estadounidense se enfrentara a una población mayoritaria hostil de habla persa. A diferencia de Irak, donde la mayoría árabe está dividida entre suníes y chiíes hostiles, lo que impide su colaboración política, en Irán, la solidaridad religiosa —la mayoría de habla persa es chií— promovería la solidaridad política. Esto probablemente haría más eficaz la resistencia a las fuerzas estadounidenses, utilizando el terreno como multiplicador de fuerzas.
7. Si las operaciones militares estadounidenses incluyeran ataques contra monumentos religiosos y/o culturales de Irán, esto

inflamar aún más el nacionalismo iraní. Washington probablemente perdería el apoyo de posibles aliados entre los opositores de habla persa a los ayatolás.

8. Si Washington busca debilitar al Irán persa fragmentando políticamente al país según líneas étnicas (árabes, azeries, baluchis y kurdos), también estaría fomentando involuntariamente la secesión baluchi y kurda en los Estados adyacentes, que son aliados de Estados Unidos: Irak, Pakistán y Turquía.

La mejor opción para Washington es endurecer las sanciones económicas contra Irán, con la oferta explícita de levantar todas las sanciones si concluyen con éxito las negociaciones basadas en el «gran acuerdo» propuesto por Teherán en 2003. Este documento iraní «...ponía todo sobre la mesa: el apoyo de Irán al terrorismo, su programa nuclear, incluso su hostilidad hacia Israel. A cambio, Irán pedía a Washington garantías de seguridad, el fin de las sanciones y la promesa de no presionar nunca para que se produjera un cambio de régimen» ⁽³²⁾.

La oposición de Estados Unidos se dirige contra la política de Teherán de apoyar a los terroristas y desarrollar un programa nuclear. No se dirige contra el Gobierno iraní en sí, ni contra el pueblo iraní, su religión, su historia, su cultura o su país. ♦

1. Kenneth Katzman, «Iran's Foreign and Defense Policies» (Las políticas exterior y de defensa de Irán), *Servicio de Investigación del Congreso*, actualizado el 30 de enero de 2020, p. 2, <https://fas.org/sgp/crs/mideast/R44017.pdf>
2. Francis Robinson, editor, *The Cambridge Illustrated History of the Islamic World* (Historia ilustrada del mundo islámico de Cambridge), (Cambridge University Press, 1996), p. 72
3. «Caliph/Caliphate», *The Oxford Dictionary of Islam*, *Oxford Islamic Studies Online*, 2020, <http://www.oxfordislamicstudies.com/article/opr/t125/e400>
4. William Ochsenwald, «Islam in the Ottoman Empire», *Oxford Islamic Studies Online*, última revisión, 19 de mayo de 2017, <https://www.oxfordbibliographies.com/view/document/obo-9780195390155/obo-9780195390155-0155.xml>
5. Editores de History.Com, «Imperio persa – Religión persa», *History.Com*, última actualización el 30 de septiembre de 2019, <https://www.history.com/topics/ancient-middle-east/persian-empire>
6. Ibid.
7. «Historia judía antigua: los persas», *Biblioteca Virtual Judía*, proyecto de AICE, American-Israeli Cooperative Enterprise, 1998-2020, <https://www.jewishvirtuallibrary.org/the-persians>
8. «Coronación del Sha de Irán, 1967», *The Royal Watcher*, 26 de octubre de 2017, <https://royalwatcherblog.com/2017/10/26/shah-of-irans-coronation-1967/>
9. «De Teherán a Persépolis: todo el esplendor del imperio: las celebraciones de Persépolis, 1971», <http://www.angelfire.com/empire/imperialiran/index1.html>
10. Mir M. Hosseini, «Irán cambia al calendario imperial», *Iranian History Today*, 15 de marzo de 1976, http://fouman.com/Y/Get_Iranian_History_Today.php?artid=1098
11. Patrick Clawson, Hanin Ghaddar y Nader Uskowi, «¿Qué es la media luna chií?», *The Washington Institute for Near East Policy*, 17 de enero de 2018, <https://www.washingtoninstitute.org/policy-analysis/view/middle-east-facts-volume-1-what-is-the-shia-crescent>
12. Richard Spencer, «¿Quiénes son los alauitas?», *The Telegraph*, 3 de abril de 2016, <https://www.telegraph.co.uk/news/2016/04/02/who-are-the-alawites/>
13. Akhilesh Pillalamarri, «La identidad lingüística persa de Afganistán», *The Diplomat*, 14 de noviembre de 2017, <https://thediplomat.com/2017/11/afghanistans-persian-linguistic-identity/>
14. Luciano Arvin, «Irán corteja a Tayikistán», *The Diplomat*, 31 de mayo de 2017 <https://thediplomat.com/2017/05/iran-courts-tajikistan/>
15. «Rouhani: Irán desarrollará la cooperación comercial, económica y cultural con los países de la región de Nowruz», *The Iran Project*, 28 de marzo de 2014, <https://theiranproject.com/blog/2014/03/28/rouhani-iran-to-develop-trade-economic-cultural-cooperation-with-countries-of-nowruz-region/>
16. «La importancia estratégica de Baréin para Arabia Saudí», *The Oil Drum*, 29 de junio de 2011, <https://oilprice.com/Geopolitics/Middle-East/The-Strategic-Importance-Of-Bahrain-To-Saudi-Arabia.html>

17. «El Reino de Baréin», *PNUD*, 2020, <https://www.bh.undp.org/content/bahrain/en/home/countryinfo.html>
18. David Pollock, «Sunnis and Shia in Bahrain: New Survey Shows Both Conflict and Consensus» (Suníes y chiíes en Baréin: una nueva encuesta revela tanto conflicto como consenso), *Fikra Forum*, The Washington Institute for Near East Policy, 20 de noviembre de 2017, <https://www.washingtoninstitute.org/fikraforum/view/sunnis-and-shia-in-bahrain-new-survey-shows-both-conflict-and-consensus>
19. Jonathan Saul, Parisa Hafezi, Michael Georgy, «Exclusiva: Irán intensifica su apoyo a los hutíes en la guerra de Yemen, según fuentes», *Reuters*, 21 de marzo de 2017, <https://www.reuters.com/article/us-yemen-iran-houthis-idUSKBN16S2Z2R>
20. Yoel Guzansky Ari Heistein, «La guerra de Arabia Saudí en Yemen ha sido un desastre», *The National Interest*, 25 de marzo de 2018, <https://nationalinterest.org/feature/saudi-arabias-war-yemen-has-been-disaster-25064>
21. «Provincia Oriental», *Cámara de Asharqia*, <https://www.chamber.org.sa/sites/English/AboutKingdom/AboutTheEasternRegion>
22. Graham Evans, «Golfo Pérsico», *Encyclopædia Britannica*, 2020, <https://www.britannica.com/place/Persian-Gulf>
23. Adam Coogly, «La 'guerra contra el terrorismo' de Arabia Saudí ahora tiene como objetivo a los chiíes saudíes», *Foreign Policy*, 23 de agosto de 2017, <https://www.hrw.org/news/2017/08/24/anti-shia-bias-driving-saudi-arabia-unrest>
24. Adam Coogly, «Las «reformas» de Arabia Saudí no incluyen la tolerancia hacia la comunidad chií», *Human Rights Watch*, 21 de septiembre de 2018, <https://www.hrw.org/news/2018/09/21/saudi-arabias-reforms-dont-include-tolerance-shia-community>
25. «Disturbios en Qatif entre 2017 y 2020», *Wikipedia*, https://en.wikipedia.org/wiki/2017%E2%80%932020_Qatif_unrest
26. «La geopolítica de Irán: manteniendo el centro de una fortaleza montañosa», *Stratfor*, 16 de diciembre de 2011, <https://worldview.stratfor.com/article/geopolitics-iran-holding-center-mountaint-fortress>
27. Ibid.
28. Ibid.
29. «Comparación del tamaño de los países: Irán en comparación con Afganistán», *MyLifeElsewhere.com*, 2020, <https://www.mylifeelsewhere.com/country-size-comparison/iran/afghanistan>
30. Ibid.
31. «Fuerza militar de Irán (2020)», *GlobalFirepower* (GFP), 2020, https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=iran
32. «El fax del «gran acuerdo»: una oportunidad perdida», *Showdown with Iran, PBS*, publicado el 23 de octubre de 2007, <https://www.pbs.org/wgbh/pages/frontline/showdown/themes/grandbargain.html>

Acerca del autor:

Joseph E. Fallon es un analista político internacional con más de 20 años de experiencia en asesoramiento estratégico, investigación/redacción y docencia, con conocimientos específicos en materia de defensa/seguridad nacional, terrorismo y geopolítica. En la actualidad, el Sr. Fallon es investigador asociado del think tank británico UK Defence Forum, donde proporciona a los miembros del Parlamento análisis sobre cuestiones que afectan a la seguridad y la defensa nacionales británicas; miembro del comité directivo del Grupo de Trabajo sobre Niños Reclutados por Grupos Terroristas y Extremistas Violentos; y miembro internacional del consejo editorial de la revista académica rumana *GeoPolítica*. Es autor de dos libros y más de 80 artículos publicados (por ejemplo, sobre el extremismo islámico y la política exterior de Estados Unidos). El Sr. Fallon fue profesor del Programa de Estudios Regionales de Oriente Medio del Colegio de Guerra del Ejército de los Estados Unidos, instructor sobre Afganistán y extremismo islámico en el Centro de Excelencia de Inteligencia del Ejército de los Estados Unidos, profesor invitado sobre Afganistán en el Consorcio de Conocimiento Cultural del Ejército de los Estados Unidos y profesor invitado sobre Asia Central e Irán en el Instituto de Defensa de Gestión de la Asistencia en Seguridad (DISAM).

Ir en Irak

By Michael Rubin, Ph.D., American Enterprise Institute

El 3 de enero de 2020 M. Ataque con un dron que mató al iraní Q. Q-9 Reaper jefe de la Qassem Soleimani y Fuerza y Abu Mahdi Muhandis, el subjefe de las Unidades al-puso de relieve la malignidad iraní La influencia de la Movilización Popular en Irak.

Las relaciones entre Irán e Irak son complejas. Tanto Irán como Irak son países de mayoría chiíta, pero las rivalidades étnicas y nacionales siembran profundas divisiones. Durante la guerra entre Irán e Irak de 1980-1988, la mayoría de los soldados iraquíes eran chiítas, pero se mantuvieron leales a Irak; la etnia árabe y el orgullo nacional prevalecieron sobre la solidaridad sectaria. La mayoría de los chiítas iraquíes también están en desacuerdo con la noción teológica del gobierno clerical (*velayat-e faqih*) que el difunto líder revolucionario ayatolá Ruhollah Jomeini impuso en Irán. Los intentos iraníes de imponer esta interpretación teológica a los iraquíes solo han aumentado el resentimiento iraquí hacia Irán. Los iraquíes suelen dirigir su frustración por la inestabilidad económica de Irak hacia Irán. Los iraquíes culpan a Irán de inundar el mercado con productos manufacturados baratos que socavan los frágiles sectores manufacturero y agrícola de Irak. Cuando la escorrentía agrícola causó

Tras una mortandad masiva de peces en el río Tigris, los iraquíes abrazaron la teoría conspirativa de que agentes iraníes habían envenenado el agua para obligar a los iraquíes a comprar pescado iraní.¹

Los partidarios de Irán en Irak suelen ocultar la existencia de sus milicias bajo el manto de *la fatwa* (declaración religiosa) del gran ayatolá Ali Sistani, que condujo a la creación de las *hashd al-shaabi*, las llamadas Fuerzas de Movilización Popular, que surgieron para luchar contra el Estado Islámico. En realidad, la mayoría de los grupos respaldados y dirigidos por Irán se fundaron años antes de la crisis del Estado Islámico. El Cuerpo de la Guardia Revolucionaria Islámica fundó el Cuerpo Badr en 1982. Kata'ib Hezbollah lleva activo desde octubre de 2003. Asa'ib Ahl al-Haq se fundó en julio de 2006 y Harakat Hezbollah al-Nujaba se formó

en 2013. Estos grupos reconocen abiertamente tanto su lealtad al líder supremo de Irán, Alí Jamenei, como la ayuda recibida de Irán. Los registros desclasificados de los interrogatorios de Qais Khazali, bajo custodia de la coalición entre 2007 y 2010, y hoy secretario general de Asa'ib Ahl al-Haq, detallan el entrenamiento de su grupo por parte del Cuerpo de la Guardia Revolucionaria Islámica en bases cercanas a Teherán.² Este entrenamiento se ajusta a un patrón común en el que la Guardia Revolucionaria entrena y apoya a grupos proxy.

Los *hashd al-shaabi* en su conjunto son más diversos y no todos están bajo el control de Irán. No solo los chiítas, sino también los suníes, los cristianos y los yazidíes formaron *grupos hashd*

al-shaabi. Los iraquíes también diferencian entre los grupos formados por personas procedentes de todo el país y los que tienen orígenes más locales. Durante la lucha contra el Estado Islámico, por ejemplo, Muchos chiítas de las provincias del sur de Irak se unieron a unidades del norte, lo que no solo creó un vacío de seguridad en las ciudades y pueblos del sur, sino que también generó fricciones con las comunidades locales del norte. *El wasta* (nepotismo) en la sociedad iraquí no solo tiene que ver con conseguir un trabajo, sino también con evitar conflictos. Si los iraquíes se encontraban con problemas en un puesto de control de las milicias populares (*Hashd al-Shaabi*), por ejemplo, o tenían un familiar de su familia detenidos, tenían muchas más posibilidades de resolver el problema sin violencia ni resentimientos duraderos si podían recurrir a sus contactos locales. Esto era prácticamente imposible cuando el personal de *hashd al-shaabi* procedente de fuera de su zona inmediata dominaba la seguridad. Del mismo modo, las fuerzas de seguridad locales son menos propensas a saquear propiedades en zonas donde ellos y sus familias extensas pueden ser conocidos.

El fervor antiiraní dentro de Irak alcanzó su punto álgido después de que milicias respaldadas por Irán dispararan contra la multitud durante las protestas contra la corrupción que estallaron el 1 de octubre de 2019. Altos funcionarios iraquíes, tanto del poder ejecutivo como del legislativo, afirman en privado que la violencia tomó por sorpresa al entonces primer ministro Adil Abdul-Mahdi por sorpresa, y que el error de Abdul-Mahdi fue intentar excusar y encubrir el papel de las milicias respaldadas por Irán en lugar de abordar directamente. Todos los primeros ministros iraquíes desde 2014 han reconocido en privado la amenaza que las milicias respaldadas por Irán suponen para el Estado iraquí. Los líderes iraquíes ven el papel que desempeñan el Cuerpo de la Guardia Revolucionaria Islámica y Basij en Irán y comprenden las ramificaciones de permitir que las milicias respaldadas por Irán se extiendan. ¿Por qué el Gobierno iraquí no ha tomado medidas más duras contra los abusos de *Hashd al-Shaabi*?

Hay tres razones. La primera es el poder. Tanto el líder del Cuerpo Badr, Hadi Amiri, como el ex primer ministro Nouri al-Maliki utilizan sus conexiones y su apoyo al *hashd al-shaabi* para reforzar su influencia en las turbulentas batallas políticas de Irak. Sus conexiones con el *hashd al-shaabi* también compensan la falta de apoyo de Sistani y de la clase religiosa en general en Nayaf.



La segunda es el pragmatismo. Después de que los kurdos iraquíes celebraran un referéndum sobre la eventual independencia no solo de las zonas reconocidas del Kurdistan iraquí, sino también de los territorios ricos en petróleo reclamados tanto por el Kurdistan iraquí como por el Gobierno iraquí en Bagdad, las fuerzas iraquíes y sus homólogos *del hashd al-shaabi*, respaldados por Irán, impulsaron hacia el norte, hacia zonas en disputa. Ante las quejas sobre el papel de Irán en la campaña, los funcionarios de la oficina del entonces primer ministro Haider Abadi afirmaron que utilizaron grupos respaldados por Irán porque eran más disciplinados y no se dedicarían al saqueo espontáneo como lo harían las milicias más *improvisadas* formadas a raíz del auge del Estado Islámico.

La tercera razón es el miedo. Los costes individuales de oponerse a las milicias orientadas hacia Irán son enormes. Los mismos políticos iraquíes que minimizan la influencia iraní en Irak se niegan a revertir la instalación ilegal por parte de Irán de buzones de donativos para organizaciones benéficas como el Comité de Ayuda del Imán Jomeini, con el fin de no precipitar una lucha ni antagonizar al Gobierno iraní. No es raro que el Gobierno iraní utilice este tipo de organizaciones benéficas para proyectar su influencia. El Comité de Ayuda del Imán Jomeini, por ejemplo, destaca su labor benéfica, como la distribución de alimentos, queroseno y mantas, pero también lleva a cabo actividades más encubiertas. Los mismos Las redes utilizadas para distribuir suministros humanitarios pueden distribuir armamento. Hace una década, por ejemplo, el Departamento del Tesoro de los Estados Unidos designó a su sucursal libanesa como partidaria del terrorismo «por ser propiedad o estar controlada por Hezbolá y por proporcionar apoyo financiero y material a Hezbolá» ⁽³⁾.

En lugar de tratar de consolidar el control sobre el *hashd al-shaabi*, los altos mandos iraquíes suelen eludir la responsabilidad. Cuando Najah al-Shammari, por ejemplo, asumió la cartera del Ministerio de Defensa en junio de 2019, dijo que no tenía interés en controlar al *hashd al-shaabi*, aunque técnicamente se trataba de una fuerza militar subordinada a su ministerio, ya que constitucionalmente esa era la función del jefe del Estado Mayor, y ese puesto estaba vacante en ese momento.⁴ Shammari puede haber tenido razón, pero los líderes iraquíes llevan mucho tiempo tratando la Constitución más como una sugerencia que como una ley inflexible, y la ley ofrecía suficiente flexibilidad para afirmar una mayor unidad de mando si Shammari hubiera deseado perseguir ese objetivo.

Aunque las fuerzas militares estadounidenses y los funcionarios civiles que operan en Irak están acostumbrados al delicado equilibrio con los iraquíes sobre la influencia iraní, en los últimos meses se han producido cambios significativos. Irán se ha sumido en una recesión y las sanciones estadounidenses han afectado duramente al Cuerpo de la Guardia Revolucionaria Islámica y a sus negocios asociados. Las autoridades iraquíes afirman que, mientras que la Fuerza Quds —las fuerzas especiales y el ala de operaciones externas de la Guardia Revolucionaria— subvencionaba

Las milicias iraquíes dentro de Irán, el flujo de dinero ahora se ha invertido: grupos como Kataib Hezbollah y Asa'ib Ahl al-Haq ahora desvían dinero de sus intereses comerciales en Irak hacia Irán. Esto crea un desincentivo financiero tanto para los grupos iraquíes como para Irán a la hora de permitir reformas políticas que podrían aflojar su control, y también puede explicar su disposición a utilizar la fuerza letal contra manifestantes desarmados.

Mientras el primer ministro Mohammad Allawi intenta guiar a Irak hacia unas elecciones anticipadas y llevar a cabo el cambio que exige el movimiento de protesta, otros acontecimientos podrían perturbar la relación entre Irak e Irán. El 16 de enero de 2020, Sistani fue operado de una fractura en el fémur izquierdo. Aunque el clérigo de 89 años sobrevivió a la intervención, las posibilidades de que surjan complicaciones siguen siendo elevadas dada su edad. Esto hace temer que pueda fallecer. Irak no solo perdería a una figura moderada que durante mucho tiempo se ha resistido a los dictados iraníes, sino que el líder supremo iraní Ali Jamenei y su establishment clerical intentarían presentar un candidato a *marja* más afín a las opiniones del régimen iraní; de hecho, ya lo intentaron con Mahmoud Hashemi Shahroudi, formado en Nayaf y antiguo jefe del poder judicial iraní, pero el clérigo, de 70 años, sucumbió a un cáncer cerebral en diciembre de 2018. Los esfuerzos iraníes por promover un sucesor menos independiente de Sistani no serán simplemente una batalla intelectual sobre el discurso religioso, sino que podrían también adquieren una dimensión más violenta. Es por esta razón también por la que la República Islámica se resiste a dejar de apoyar a los grupos milicianos en Irán. Al igual que estos grupos han infligido una violencia desenfrenada contra manifestantes pacíficos en Bagdad en los últimos meses, podrían ser fácilmente llamados a intimidar a otros que buscan el reconocimiento como *marja* en Nayaf.

Las relaciones entre Irán e Irak son complejas, pero, en pocas palabras, las autoridades iraníes nunca abandonarán su intento de dominar Irak. No solo comparten la frontera más larga que cualquiera de los dos países tiene con un vecino, sino que siguen estando económicamente entrelazados debido a la peregrinación chií y al turismo religioso. Mientras muchos diplomáticos expresan su esperanza de que triunfe el movimiento reformista en Irak y los partidarios de la línea dura iraní no escatiman esfuerzos para frustrar sus deseos, el verdadero talón de Aquiles del régimen iraní sigue siendo un Irak libre e independiente. La pretensión del líder supremo iraní de ser la máxima autoridad política y la autoridad religiosa significa que cualquier clérigo independiente de las ciudades santuario iraquíes de Nayaf y Karbala que contradiga al líder supremo iraní está socavando directamente su autoridad. Esto hace que el dominio iraní de Nayaf y Karbala sea importante para la supervivencia del régimen iraní. Su agresivo esfuerzo por mantener a Bagdad débil y fracturada y por hacer incursiones en Nayaf y Karbala no es un comportamiento que estén

estén dispuestos a mitigar. La muerte de Soleimani puede haber cambiado el panorama de la lucha, pero no la acabará.

¿Qué significa esto para Estados Unidos? Los intentos iraníes de dominar Irak no desaparecerán, pero el entorno operativo iraquí no siempre es tan propicio para los iraníes como suponen los analistas estadounidenses. La estrategia iraquí sigue siendo coherente. Los funcionarios iraquíes de los poderes ejecutivo y legislativo de todas las administraciones iraquíes afirman en privado que la única forma

Para contrarrestar eficazmente la influencia iraní, es necesario mantener la presencia estadounidense, de modo que las autoridades iraquíes puedan utilizar la presencia de la otra parte para vetar las exigencias de Teherán o Washington y crear un espacio independiente para la acción iraquí. Cuando las fuerzas estadounidenses se retiraron temporalmente en 2011, la influencia iraní aumentó y la estadounidense disminuyó.

Si Estados Unidos volviera a retirar sus fuerzas de Irak, las milicias respaldadas por Irán, si no la Revolución Islámica...

1. «La muerte de peces causada por la crisis del agua pone de manifiesto las graves crisis a las que se enfrenta Irak», *The Baghdad Post*, 9 de noviembre de 2018.
2. «Informe de interrogatorio táctico de la SDE chií», informe n.º 200243-008. 18 de junio de 2007, 17:30.
3. «Hoja informativa: El Departamento del Tesoro de EE. UU. apunta al apoyo de Irán al terrorismo. El Tesoro anuncia nuevas sanciones contra los líderes de la Fuerza Qods del Cuerpo de la Guardia Revolucionaria Islámica de Irán», Departamento del Tesoro de EE. UU., 3 de agosto de 2010.
4. Entrevista del autor con Najah al-Shammari, Bagdad, 1 de junio de 2019.

El propio Cuerpo de la Guardia podría volverse más agresivo. Los ataques contra Arabia Saudí sugieren que las milicias respaldadas por Irán ya disponen de misiles y vehículos aéreos no tripulados. Si los iraníes y los grupos respaldados por Irán consolidan su poder en Irak ante la ausencia de apoyo estadounidense al Estado iraquí, es probable que actúen de forma más abierta, ya que temerían menos los esfuerzos por impedir dicha agresión regional. La consolidación del control iraní sobre el territorio iraquí también permitiría la creación del llamado puente terrestre, que facilitaría el suministro de armas a los grupos aliados de Irán en Siria y Líbano. Un régimen más sectario y dominado por Irán en Bagdad también podría avivar las llamas del sectarismo e inflamar las mismas fuerzas que contribuyeron al auge del Estado Islámico. Por supuesto, la política estadounidense podría tomar varias direcciones en Irak, pero, ya sea con la presencia de tropas estadounidenses o sin ella, los planes de Irán para Irak y el éxito o el fracaso de Teherán definirán el entorno estratégico de la región en los próximos años.♦

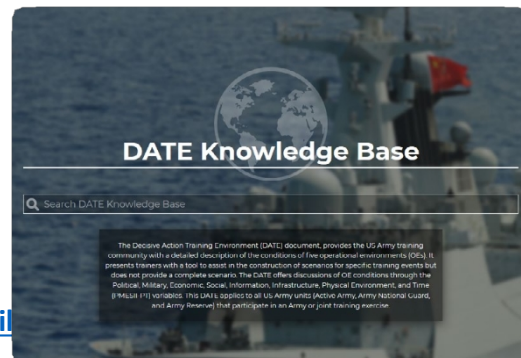
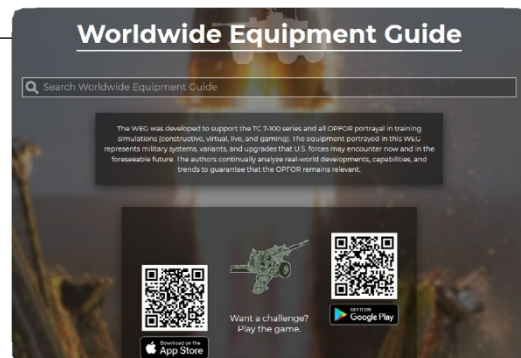
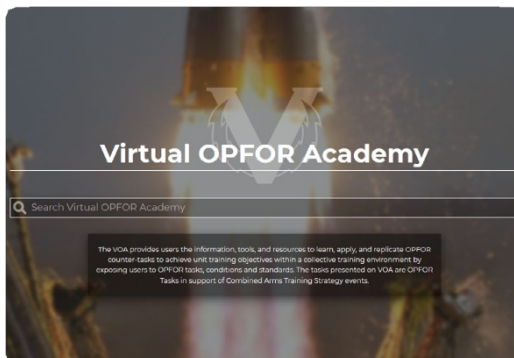
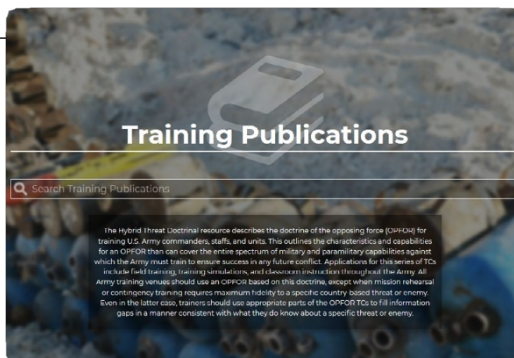
Acerca del autor:

Michael Rubin es investigador residente del American Enterprise Institute y profesor titular del departamento de Asuntos de Seguridad Nacional de la Escuela Naval Postgraduada.



Red de integración de datos del entorno operativo

ODIN es la fuente autorizada para DATES, sus estructuras de fuerzas de amenaza correspondientes, la Guía mundial de equipos (WEG) y otras publicaciones sobre doctrina de amenazas, como la serie TC 7-100.



(RS-SA-3 Goa)

Defensa puntual 136+: 50 M1097 Avenger; 50+ M48 Chaparral ARMAS 910

SP • 23 mm 230 ZSU-23-4 Shilka

REMOLCADO 680: 35 mm 80 GDF-005 con Skyguard; 57 mm 600 S-60

Gendarmería y paramilitares €397 000 en activo

Fuerzas de Seguridad Centrales €325 000

Ministerio del Interior; incluye reclutas

VEHÍCULOS BLINDADOS DE COMBATE

APC • APC (W) Walid

AUV Sherpa Light Scout

Guardia Nacional €60 000

Solo armas ligeras

FUERZAS POR FUNCIÓN

MANIOBRA

Otros

8 brigadas paramilitares (cuadro) (3 batallones paramilitares)

EQUIPO POR TIPO

VEHÍCULOS BLINDADOS DE COMBATE

APC • APC (W) 250 Walid

Fuerzas de Guardia Fronteriza €12 000

Ministerio del Interior; solo armas ligeras

FUERZAS POR FUNCIÓN MANIOBRA

Otros

18 regimientos de la Guardia Fronteriza

DESPLIEGUE

REPÚBLICA CENTROAFRICANA: ONU • MINUSCA 1023; 1 batallón de infantería; 1 compañía de transporte

REPÚBLICA DEMOCRÁTICA DEL CONGO: ONU • MONUSCO 6

SUDÁN DEL SUR: ONU • UNMISS 7

SUDÁN: ONU • UNISFA 5

SÁHARA OCCIDENTAL: ONU • MINURSO 20

FUERZAS EXTRANJERAS

Australia MFO (Operación Mazurka) 27 Canadá MFO 55

Colombia MFO 275; 1 batallón de infantería

República Checa MFO 18; 1 C295M Fiyi

MFO 170; elm 1 batallón de infantería

Francia MFO 1

Italia MFO 75; 3 PB

Nueva Zelanda MFO 26; 1 unidad de entrenamiento; 1 unidad

de transporte Noruega MFO 3

Reino Unido MFO 2

Estados Unidos MFO 465; batallón de infantería de la ARNG; batallón de apoyo de la ARNG (1 compañía de desactivación de explosivos, 1

compañía médica, 1 compañía de helicópteros)

Uruguay MFO 41 1 unidad de ingeniería/transporte

Irán IRN

Rial iraní IRR	2023	2024	2025
PIB	IRR 143qrn	198 qrn	262qrn
	USD 373 000	434 000	464 000
	millones		millones
Crecimiento real del PIB	% 5,0	3,7	3,1
Presupuesto de defensa [a]	TIR 3,19 qrn	3,67 qrn	
	USD [b] 8330	8040	
	millones	millones	

[a] Excluye las fuerzas del orden (NAJA)

[b] Conversiones utilizando el tipo de cambio NIMA



Población	88 386 937					
Edad	0-14	15-19	20-24	25-29	30-64	Más de 65
Hombres	11,9	3,6	3,3	3,3	25,4	3,2
Mujeres	11,4	3,5	3,1	3,1	24,5	3,7

Capacidades

La ambición de Irán es convertirse en la potencia regional dominante y controlar el poder de Israel y Estados Unidos. Los esfuerzos iraníes para alcanzar este objetivo se han centrado en una doctrina asimétrica que combina la defensa territorial mediante la movilización nacional, un arsenal de vehículos aéreos no tripulados (UAV) de ataque unidireccional (OWA), misiles de crucero y balísticos, así como una alianza de actores no estatales equipados con armamento de largo alcance. Estas ambiciones se han visto cuestionadas tras la guerra entre Israel y Hamás. Un inventario de misiles balísticos de corto y medio alcance, misiles de crucero de ataque terrestre y UAV permite a Irán llevar a cabo ataques de largo alcance sin necesidad de contar con una fuerza aérea capaz. Sin embargo, los ataques de Irán contra Israel en abril y octubre de 2024 revelaron las limitaciones de estos sistemas tanto para penetrar las defensas antimisiles avanzadas como para alcanzar la precisión necesaria para dañar significativamente la infraestructura militar. El resto de las fuerzas armadas convencionales se enfrentan a equipos cada vez más obsoletos que el ingenio y las técnicas asimétricas solo pueden compensar en parte. El envejecimiento de los equipos es evidente en toda la fuerza aérea. Aunque la fuerza naval de Irán se centra en enfoques asimétricos, como el uso de minas, misiles antibuque, lanchas rápidas y pequeños submarinos, el servicio ha mostrado interés en las operaciones en aguas profundas y la proyección de poder. Existen problemas de C2 entre las fuerzas regulares y el IRGC. Aunque no puede satisfacer las necesidades nacionales de todas las armas importantes, la industria nacional ha alcanzado un alto grado de competencia en la producción de ciertos tipos de armas avanzadas. Irán también ha desarrollado amplias técnicas de evasión de sanciones para apoyar a su industria de defensa. El aumento de la cooperación militar con Moscú podría ofrecer a Irán una vía de acceso a armamento y tecnología más modernos.

ACTIVOS 610 000 (Ejército 350 000 Guardia Revolucionaria Islámica

Cuerpo de la Guardia Revolucionaria Islámica 190 000

Armada 18 000 Fuerza Aérea 37 000 Defensa Aérea 15 000)

Gendarmería y Paramilitares 40 000

El Estado Mayor de las Fuerzas Armadas coordina dos organizaciones paralelas: las fuerzas armadas regulares y el Cuerpo de la Guardia Revolucionaria Islámica

Servicio militar obligatorio de 18 a 21 meses (según se informa, con variaciones dependiendo del lugar en el que se preste el servicio)

RESERVA 350 000 (Ejército 350 000, exmilitares voluntarios)

ORGANIZACIONES POR SERVICIO

Espacio

EQUIPO POR TIPO

SATÉLITES • **ISR** 1 *Khayam* (según informes)

Ejército 130 000; 220 000 reclutas (total 350 000)

FUERZAS POR FUNCIÓN

5 cuarteles generales regionales a nivel de cuerpo de ejército

MANDO

- 1 cuartel general de división de mando
- 4 cuarteles generales de divisiones blindadas 2 cuarteles generales de divisiones mecanizadas 4 cuarteles generales de divisiones de infantería

FUERZAS ESPECIALES

- 1 división de comando (3 brigadas de comando)
- 6 brigadas de comando
- 1 brigada de fuerzas especiales

MANIOBRA

- Blindada**
- 8 brigadas blindadas
- Mecanizadas** 14 brigadas mecanizadas
- Ligeras**
- 12 brigadas de infantería
- Maniobra aérea** 1 brigada aerotransportada
- Aviación**
- Algunos grupos aéreos

APOYO DE COMBATE

- 5 grupos de artillería

EQUIPO POR TIPO

Totales, incluidos los que están en poder de las Fuerzas Terrestres del IRGC. La operatividad de parte del equipo es dudosa.

VEHÍCULOS BLINDADOS DE COMBATE

- MBT** 1513+: 100 *Chieftain* Mk3/Mk5; 168 M47/M48; 150 M60A1; 540 Safir-74/T-54/T-55/ZTZ-59; 75+ T-62; 480 T-72S
- LT TK** 80 *Scorpion* **RECCE** 35
- EE-9** *Cascavel*
- IFV** 610+: 210 BMP-1; 400 BMP-2 con 9K111 *Fagot* (RS-AT-4 *Spigot*); BMT-2 *Cobra* **APC** 640+
 - APC (T)** 340: 140 *Boragh* con 9K111 *Fagot* (RS-AT-4 *Spigot*); 200 M113
 - APC (W)** 300+: 300 BTR-50/BTR-60; *Rakhsh*
 - PPV** *Toofan*

VEHÍCULOS DE INGENIERÍA Y MANTENIMIENTO

- ARV** 20+: BREM-1 reportado; 20 *Chieftain* ARV; M578; T-54/55 ARV reportado

VLB 15 *Chieftain* AVLB
MW *Taftan* 1

ANTITANQUE/ANTIINFRAESTRUCTURA

MSL • **MANPATS** 9K11 *Malyutka* (RS-AT-3 *Sagger*); 9K111 *Fagot* (RS-AT-4 *Spigot*); 9K111-1 *Konkurs* (RS-AT-5 Spandrel/Towsan-1); *Almaz*; *Dehlavieh* (Kornet); *I-Raad*; *Saeqhe* 1; *Saeqhe* 2; *Toophan*; *Toophan* 2
RCL 200+: 75 mm M20; 82 mm B-10; 106 mm ε200 M40; 107 mm B-11

ARTILLERÍA 6.798+

SP 292: 122 mm 60 2S1 *Gvozdika*; 155 mm 150 M109A1; 170 mm 30 M-1978; 175 mm 22 M107; 203 mm 30 M110
REMOLCADAS 2030+: 105 mm 150: 130 M101A1; 20 M-56; 122 mm 640: 540 D-30; 100 Tipo 54 (M-30); 130 mm 985 M-46; 152 mm 30 D-20; 155 mm 205: 120 GHN-45; 70 M114; 15 Tipo 88 WAC-21; 203 mm 20 M115
MRL 1476+: 107 mm 1300: 700 Tipo 63; 600 HASEB
Fadjr 1; 122 mm 157: 7 BM-11; 100 BM-21 *Grad*; 50 *Arash*/*Hadid/Noor*; 240 mm 19+: ε10 *Fadjr* 3; 9 M-1985; 330 mm *Fadjr* 5
MOR 3000: 81 mm; 82 mm; 107 mm M30; 120 mm HM-15; HM-16; M-65

LANZADORES DE MISILES SUPERFICIE-SUPERFICIE

SRBM • **Convencional** ε30 CH-SS-8 (175 msl); Fateh-360; Shahin-1/Shahin-2; *Nazeat*; *Oghab*

AERONAVES • **TPT** 17 **Light** 16: 10 Cessna 185; 2 F-27 *Friendship*; 4 *Turbo Commander* 690; **PAX** 1 *Falcon* 20

HELICÓPTEROS

ATK 50 AH-1J *Cobra*
TPT 167: **Pesado** ε20 CH-47C *Chinook*; **Medio** 69: 49 Bell 214 (algunos armados); 20 Mi-171; **Ligero** 78: 68 Bell 205A (AB-205A); 10 Bell 206 *Jet Ranger* (AB-206)

VEHÍCULOS AÉREOS NO TRIPULADOS

CISR • **Medio** *Ababil* 3; *Ababil* 4; *Mohajer* 6 **ISR** • **Medio** *Mohajer* 4; **Ligero** *Mohajer* 2; *Yasir* **OWA** *Ababil* T; *Akhgar*; *Arash*; *Omid*

MISILES LANZADOS DESDE EL AIRE

ASM *Almas* (según informes); Heydar-1; *Qaem* 114; *Shafaq* (mod)

BOMBAS

Qaem guiado por láser
Qaem 5 guiado por electroóptica

SISTEMA DE

DEFENSA AÉREA

SAM

Corto alcance FM-80 (CH-SA-4)
Defensa puntual 9K36 *Strela*-3 (RS-SA-14 *Gremlin*); 9K32 *Strela*-2 (RS-SA-7 *Grail*)†; *Misaq* 1 (QW-1); *Misaq* 2 (QW-18); 9K338 *Igla*-S (RS-SA-24 *Grinch*) (según informes); HN-5A (CH-SA-3)

ARMAMENTOS 1122

SP 180: 23 mm 100 ZSU-23-4; 57 mm 80 ZSU-57-2
REMOLCADOS 942+: 14,5 mm ZPU-2; ZPU-4; 23 mm 300 ZU-23-2; 35 mm 92 GDF-002; 37 mm M-1939; 40 mm 50 L/70; 57 mm 200 S-60; 85 mm 300 M-1939

Cuerpo de la Guardia Revolucionaria Islámica 190 000

Cuerpo de la Guardia Revolucionaria Islámica Fuerzas Terrestres 150 000

Controla las fuerzas paramilitares Basij. Cuenta con poco personal en tiempos de paz. Función principal: seguridad interna; función secundaria: defensa externa, en colaboración con las fuerzas armadas regulares.

FUERZAS POR FUNCIÓN

MANDO

31 cuarteles generales provinciales (2 en Teherán)

FUERZAS ESPECIALES

3 divisiones de operaciones especiales 1 brigada aérea

MANIOBRA

Blindada

2 divisiones blindadas 3 brigadas blindadas

Ligera

8+ divisiones de infantería 5+ brigadas de infantería

EQUIPO POR TIPO

SRBM • Convencional algunos Fateh-360 VEHÍCULOS

AÉREOS NO TRIPULADOS

CISR • Medio Mohajer 6 ISR • Ligero Meraj 313 OWA Meraj 532

BOMBAS

Guiadas por láser Qaem Guiadas electroópticamente Qaem 5

Cuerpo de la Guardia Revolucionaria Islámica Fuerzas Navales Más de 20 000 (incluidos 5000 marines)

FUERZAS POR FUNCIÓN

APOYO AL COMBATE

Algunas baterías de artillería Algunas baterías ASHM con HY-2 (CH-SSC-3 Seersucker)

EQUIPO POR TIPO

Además de los buques enumerados, el IRGC opera un número considerable de lanchas patrulleras con un desplazamiento a plena carga de menos de 10 toneladas, entre los que se incluyen buques de la clase Boghammar y pequeños vehículos aéreos de efecto suelo de la clase Bavar.

PATRULLAS Y COMBATIENTES COSTEROS 131

PCGM 3 Shahid Soleimani con 2 lanzadores gemelos con Ghader ASHM, 2 lanzadores individuales con C-704 (Nasr) ASHM, 2 VLS de 3 celdas y 4 VLS de celda única (probablemente equipados con SAM), 1 plataforma de aterrizaje para helicópteros

PBFG 56:

5 C14 con 2 lanzadores gemelos con C-701 (Kosar)/C-704 (Nasr) ASHM 10 Mk13 con 2 lanzadores simples con misiles antiaéreos C-704 (Nasr), 2 tubos lanzatorpedos simples de 324 mm 10 Thondor (PRC Houdong) con 2 lanzadores gemelos con C-802A (Ghader) ASHM, 2 AK230 CIWS

25 Peykaap II (IPS-16 mod) con 2 lanzadores simples con C-701 (Kosar) ASHM/C-704 (Nasr), 2 TT simples de 324 mm 6 Zolfaghar (Peykaap III/IPS-16 mod) con 2 lanzadores simples con C-701 (Kosar)/C-704 (Nasr) ASHM

PBG 1 Shahid Rouhi con 2 lanzadores gemelos con C-704 (Nasr) ASHM

PBFT 15 Peykaap I (IPS -16) con 2 lanzadores simples de 324 mm TT

PBF 35: 15 Kashdom II; 10 Tir (IPS-18); ε10 Pashe (MIG-G-1900)

PB 21: ε20 Ghaem; 1 Shahid Nazeri ANFIBIOS

BUQUES DE DESEMBARCO • LST 3 Hormuz 24 (diseño Hejaz para uso comercial)

EMBARCACIONES DE DESEMBARCO • LCT 2 Hormuz 21 (capacidad para tender minas)

LOGÍSTICA Y APOYO 5

AP 3 Naser

ESB 2: 1 Shahid Mahdavi (portahelicópteros y UAV polivalente) con 2 lanzadores gemelos con C-802A (Ghader) ASHM; 1 Shahid Roudaki con 4 lanzadores gemelos con C-802A (Ghader) ASHM

PLATAFORMAS MARÍTIMAS NO HABITADAS

UUV • ATK Algunos

DEFENSA COSTERA • ASHM C-701 (Kosar); C-704 (Nasr); C-802 (Noor); HY-2 (CH-SSC-3 Seersucker)

HELICÓPTEROS

MRH 5 Mi-171 Hip

TPT • Light some Bell 206 (AB-206) Jet Ranger VEHÍCULOS

AÉREOS NO TRIPULADOS

CISR • Medio Ababil 3; Ababil 5; Mohajer 6

ISR • Mohajer 4 mediano; Yasir ligero

OWA Ababil T; Shahed 131; Shahed 136

MISILES LANZADOS DESDE EL AIRE

ASHM CM-35A Nasr (C-704)

BOMBAS

Guiadas por láser Qaem

Guiado electroóptico Qaem

Cuerpo de la Guardia Revolucionaria Islámica Marines 5000+

FUERZAS POR FUNCIÓN

MANIOBRA

Anfibia 1 brigada de maniobra

Fuerza Aeroespacial del Cuerpo de la Guardia Revolucionaria Islámica 15 000

Controla la fuerza de misiles estratégicos de Irán

FUERZAS POR FUNCIÓN CAZA/ATAQUE

TERRESTRE

1 escuadrón con Su-22M4 Fitter K; Su-22UM-3K Fitter G

ENTRENAMIENTO

1 escuadrón con EMB-312 Tucano*

EQUIPOS POR TIPO

LANZADORES DE MISILES TIERRA-TIERRA

MRBM • Convencionales 100+: Dezful (Zolfaghar mod);

Emad-1 (Shahab-3 mod); Fattah-1; Ghadr-1/-2 (Shahab-3 mod); *Kheibar Shekan*; *Khorramshahr*; *Rezvan* (*Qiam* mod); Sajjil-2;
SRBM • Convencional 100+: Fateh-110; Fateh-313; Hormuz-1/-2 (Fateh-110 mod); *Khalij Fars* (Fateh-110 mod ASBM); Qiam-1; *Zelzal*; *Zolfaghar* (IR-SS-1) **GLCM • Convencional** *Paveh*; Quds-2; Quds-3

SATÉLITES Véase *Espacio*

AERONAVES 22 con capacidad de combate

FGA 7: hasta 6 Su-22M4 *Fitter* K; 1+ Su-22UM-3K *Fitter* G

TRG 15 EMB-312 Tucano* **VEHÍCULOS AÉREOS**

NO TRIPULADOS

CISR • Pesado *Shahed* 129; **Medio** *Ababil* 3; *Shahed* 133; *Shahed* 141; *Shahed* 181; *Shahed* 191

ISR • *Shahed* 123 **mediano**

OWA *Shahed* 131; *Shahed* 136

MISILES LANZADOS DESDE EL

AIRE

ASM Almas (según informes); *Qaem* 114 (según informes) **BOMBAS**

Sadid guiado por láser

Sadid guiado por electroóptica

DEFENSA AÉREA

SAM

De medio alcance 3.º *Khordad*; 15.º *Khordad*; *Talash* **Defensa** puntual *Misag* 1 (QW-1); *Misag* 2 (QW-18)

Fuerza Revolucionaria Islámica Quds 5000

Armada 18 000

Cuartel general en Bandar Abbas

EQUIPO POR TIPO

Además de los buques enumerados, la Armada iraní opera un número considerable de lanchas patrulleras con un desplazamiento a plena carga inferior a 10 toneladas.

SUBMARINOS • TÁCTICOS 19

SSK 1 *Taregh* (RUS *Paltus* (Proyecto 877EKM (*Kilo*))) (2 más fuera de servicio) con 6 tubos lanzatorpedos simples de 533 mm

SSC 1 *Fateh* con 4 TT simples de 533 mm con C-704 (Nasr-1) *AShM/Valfajr* HWT

SSW 17: 16+ *Ghadir* ((DPRK *Yeono* mod) con 2 TT simples de 533 mm con Jask-2 (C-704 (*Nasr*)) *AShM/Valfajr* HWT (buques adicionales en construcción); 1 *Nahang*

PATRULLERAS Y BUQUES DE COMBATE COSTEROS 69

CORVETAS 8

FSGM 3 *Jamaran* (derivado del Vospet Mk 5 del Reino Unido) con 2 lanzadores gemelos con C-802 (*Noor*) (CH-SS-N-6) ASHm, 2 lanzador simple con SM-1 SAM, 2 triples 324 mm SVTT Mk 32 ASTT, 1 cañón de 76 mm, 1 plataforma de aterrizaje para helicópteros (1 más†) **FSG** 5:

2 *Alvand* (UK Vospet Mk 5) con 2 gemelos Inchr con C-802 (CH-SS-N-6) ASHm, 2 triples SVTT de 324 mm Mk 32 ASTT, 1 cañón de 114 mm

1 *Alvand* (UK Vospet Mk 5) con 2 lanzadores gemelos con C-802 (CH-SS-N-6) ASHm, 2 triples 324 mm SVTT

Mk 32 ASTT, 1 AK630M CIWS, 1 cañón de 114 mm

1 *Bayandor* (PF-103 estadounidense) (1 más fuera de servicio) con 2 lanzadores gemelos con C-802 (CH-SS-N-6) ASHm, 2 triples SVTT de 324 mm Mk 32 ASTT, 1 cañón de 76 mm

1 *Hamzah* con 2 lanzadores simples con C-802 (*Noor*) (CH-SS-N-6) ASHm

PCFG 15: hasta 10 *Kaman* (FRA *Combattante* II) con 1 lanzador doble con C-802 (*Noor*) (CH-SS-N-6) ASHm, 1 cañón de 76 mm; 5+ *Sina* con 1 lanzador doble con C-802 (*Noor*) (CH-SS-N-6) ASHm, 1 cañón de 76 mm

PBG 9:

3 *Hendijan* con 2 lanzadores gemelos con C-802 (*Noor*) (CH-SS-N-6) ASHm

3 *Kayvan* con 2 lanzadores simples con C-704 (*Nasr*) ASHm 3

Parvin con 2 lanzadores simples con C-704 (*Nasr*) ASHm

PBFT 3 *Kajami* (semisumergible) con 2 TT de 324 mm

PBF 1 MIL55

PB 33: 9 C14; 8 *Hendijan*; 6 MkII; 10 MkIII

GUERRA DE MINAS • CONTRAMEDIDAS CONTRA MINAS 1

MCC 1 *Shahin*

BUQUES DE DESEMBARCO

ANFIBIO 12

LST 3 *Hengam* con 1 plataforma de aterrizaje para helicópteros (capacidad para 9 tanques y 225 soldados)

LSM 3 *Farsi* (ROK) (capacidad para 9 tanques y 140 soldados)

LSL 6 *Fouque*

LANCHA DE DESEMBARCO 11

LCT 2

LCU 1 *Liyan* 110

UCAC 8: 2 *Wellington* Mk 4; 4 *Wellington* Mk 5; 2 *Tondar* (UK *Winchester*)

LOGÍSTICA Y APOYO 15

AE 2 *Delvar*

AKL 3 *Delvar*

ESB 1 *Makran*

AO 2 *Bandar Abbas*

AWT 5: 4 *Kangan*; 1 *Delvar*

AXL 2 *Kialas*

DEFENSA COSTERA • ASHm C-701 (*Kosar*); C-704

(*Nasr*); C-802 (*Noor*); C-802A (*Ghader*); *Ra'ad* (según informes)

Marines 2600

FUERZAS POR FUNCIÓN

MANIOBRA

Anfibia

2 brigadas de maniobra

Aviación naval 2.600

EQUIPO POR TIPO

AERONAVES

TPT 16: **Luz** 13: 5 Do-228; 4 F-27 *Friendship*; 4 *Turbo*

Comandante 680; **PAX** 3 *Falcon* 20 (ELINT) **HELICÓPTEROS**

ASW ε10 SH-3D *Sea King*

MCM 3 RH-53D *Sea Stallion*

TPT • Ligero 17: 5 Bell 205A (AB-205A); 2 Bell 206 *Jet Ranger* (AB-206); 10 Bell 212 (AB-212) **VEHÍCULOS AÉREOS NO TRIPULADOS**
CISR • Pesado *Shahed* 129 **BOMBAS**
Sadid guiadas por láser
Sadid guiado electroópticamente

Fuerza Aérea 37 000

FUERZAS POR FUNCIÓN

Incluye el equipamiento de la Fuerza Aérea del IRGC

CAZA

- 1 escuadrón con F-7M *Airguard*; JJ-7*
- 2 escuadrones con F-14 *Tomcat*
- 2 escuadrones con MiG-29A/UB *Fulcrum*

CAZA/ATAQUE TERRESTRE

- 5 escuadrones con F-4D/E *Phantom*
- II 4 escuadrones con F-5E/F *Tiger II*
- 1 escuadrón con *Mirage* F-1B/E

ATAQUE TERRESTRE

- 1 escuadrón con Su-24MK *Fencer D*

PATRULLA MARÍTIMA

- 1 escuadrón con P-3F *Orion*

ISR

- 1 escuadrón (detachado) con RF-4E *Phantom II**

BÚSQUEDA Y RESCATE

- Algunos vuelos con Bell 214C (AB-214C)

AVIÓN CISTERNA/TRANSPORTE

- 1 escuadrón con B-707; B-747; B-747F

TRANSPORTE

- 1 escuadrón con B-707; *Falcon* 50; L-1329 *Jetstar*; Bell 412
- 2 escuadrones con C-130E/H *Hercules*
- 1 escuadrón con F-27 *Friendship*; *Falcon* 20
- 1 escuadrón con Il-76 *Candid*; An-140 (Iran-140 *Faraz*)

ENTRENAMIENTO

- 1 escuadrón con Beech F33A/C *Bonanza* 1 escuadrón con F-5B *Freedom Fighter*
- 1 escuadrón con PC-6
- 1 escuadrón con PC-7 *Turbo Trainer*
- Algunas unidades con MFI-17 *Mushshak*; TB-21 *Trinidad*; TB-200 *Tobago*

HELICÓPTERO DE TRANSPORTE

- 1 escuadrón con CH-47 *Chinook*
- Algunas unidades con Bell 206A *Jet Ranger* (AB-206A); *Shabaviz* 2-75; *Shabaviz* 2061

EQUIPO POR TIPO

AERONAVES 265 aptas para el combate

FTR 138: 15 F-5B *Freedom Fighter*; 54 F-5E/F *Tiger II*; 18 F-7M *Airguard*; ε10 F-14 *Tomcat*; 35 MiG-29A/UB *Fulcrum*; hasta 6 *Azarakhsh* (según informes)
FGA 73: 55 F-4D/E *Phantom II*; 2 *Mirage* F-1BQ; 10 *Mirage* F-1EQ; hasta 6 *Saegheh* (según informes)
ATK 29 Su-24MK *Fencer D*

ASW 3 P-3F *Orion*

ISR: 6+ RF-4E *Phantom II** **TKR/TPT** 4: 2 B-707; ε2 B-747

TPT 116: **Pesados** 12 Il-76 *Candid*; **Medianos** ε19 C-130E/H *Hercules*; **Ligeros** 75: 11 An-74TK-200; 5 An-140 (Iran-140 *Faraz*); 10 F-27 *Friendship*; 1 L-1329 *Jetstar*; 10 PC-6B *Turbo Porter*; 8 TB-21 *Trinidad*; 4 TB-200 *Tobago*; 3 *Turbo Commander* 680; 14 Y-7; 9 Y-12; **PAX** 10: ε1 B-707; 1

B-747; 4 B-747F; 1 *Falcon* 20; 3 *Falcon* 50

TRG 128: 25 Beech F33A/C *Bonanza*; 14 JJ-7*; 25 MFI-17 *Mushshak*; 12 *Parastur*; 15 PC-6; 35 PC-7 *Turbo Trainer*; 2 Yak-130 *Mitten**

HELICÓPTEROS

MRH 2 Bell 412

TPT 38+: **Pesados** 2+ CH-47 *Chinook*; **Medianos** 30 Bell 214C (AB-214C); **Ligeros** 6+: 2 Bell 206A *Jet Ranger* (AB-206A); 4 Bell 212 (AB-212) (VIP); algunos *Shabaviz* 2-75; algunos *Shabaviz* 2061

VEHÍCULOS AÉREOS NO TRIPULADOS

CISR • Pesado *Kaman* 22 (según informes); **Medio** *Ababil* 4/5; *Kaman* 12; *Kaman* 22 (según informes); *Mohajer* 6

MISILES LANZADOS DESDE EL AIRE

AAM • IR AIM-9J *Sidewinder*; PL-2A‡; PL-7; R-60 (RS-AA-8 *Aphid*); R-27T (RS-AA-10B *Alamo*) (según informes); R-73 (RS-AA-11A *Archer*); **SARH** AIM-7E-2 *Sparrow*; R-27R (RS-AA-10A *Alamo*); **ARH** AIM-54 *Phoenix*†

ASM AGM-65A *Maverick*; Kh-25 (RS-AS-10 *Karen*); Kh-25ML (RS-AS-10 *Karen*); Kh-29L/T (RS-AS-14A/B *Kedge*) **AShM** C-801K; CM-35A *Nasr* (C-704); CM-200A *Ghader* (C-802A)

ARM Kh-58 (RS-AS-11 *Kilter*)

LACM *Asef* (estado incierto)

BOMBAS

GBU-87/B guiadas electroópticamente; *Qassed*

Fuerza de Defensa Aérea 15 000

FUERZAS POR FUNCIÓN

DEFENSA AÉREA

16 bn con MIM-23B *I-Hawk/Shahin*
4 batallones con S-300PMU2 (RS-SA-20 *Gargoyle*)
5 escuadrones con FM-80 (CH-SA-4); *Rapier*; HQ-2 (CH-SA-1); S-200 *Angara* (RS-SA-5 *Gammon*); 9K331 *Tor*-M1 (RS-SA-15 *Gauntlet*) **EQUIPO**

POR TIPO DEFENSA AÉREA

SAM 410

Largo alcance 42+: 10 S-200 *Angara* (RS-SA-5 *Gammon*); 32 S-300PMU2 (RS-SA-20 *Gargoyle*); *Bavar*-373

Medio alcance 59+: ε50 MIM-23B *I-Hawk/Shahin*; 9 HQ-2 (CH-SA-1); *Talash/15° Khordad*

Corto alcance 279: 250 FM-80 (CH-SA-4); 29 9K331 *Tor*-M1 (RS-SA-15 *Gauntlet*)

Defensa puntual 30+: 30 *Rapier*; *Misag* 1 (QW-1); *Misag* 2 (QW-18)

ARMAMENTOS • REMOLCADOS 23 mm ZU-23-2; 35 mm GDF-002

Gendarmería y fuerzas paramilitares 40 000-60 000

Fuerzas del orden 40 000-60 000 (tropas fronterizas y de seguridad); 450 000 en caso de movilización (incluidos los reclutas)

Parte de las fuerzas armadas en tiempo de guerra

EQUIPO POR TIPO

PATRULLAS Y COMBATIENTES COSTEROS • PB €90

AERONAVES • TPT • Ligeras 2+: 2 An-140; algunas Cessna 185/Cessna 310

HELICÓPTEROS • TPT • Ligeros €24 AB-205 (Bell 205)/

AB-206 (Bell 206) *Jet Ranger*

Fuerza de Resistencia Basij €600 000 en movilización

Milicia paramilitar con una membresía declarada de 12,6 millones; €600 000 con capacidad de combate

Irak IRQ

Dinar iraquí IQD		2023	2024	2025
PIB	IQD	332 billones	343 billones	352 billones
	USD	252 000 millones	264 000 millones	271 000 millones
Crecimiento real del PIB	%	-2,9	0,1	4,1
Presupuesto de defensa [a]	IQD	13,8 billones	16,5 billones	
	USD	10 500	12 700 millones	
FMA (EE. UU.)	USD	250 millones	75,5 millones	90,0 millones

[a] Excluye el presupuesto del Ministerio del Interior y del Consejo de Seguridad Nacional



Población 42 083 436

Edad	0-14	15-19	20-24	25-29	30-64	Más de 65
Hombres	17,7	5,4	4,8	4,1	16,7	1,6
Mujeres	16,9	5,2	4,7	4,0	16,8	2,0

Capacidades

Las fuerzas armadas iraquíes han tenido éxito en la lucha contra el ISIS, aunque la amenaza no ha sido eliminada. Las fuerzas estadounidenses han permanecido en el país como asesores en el marco de la Fuerza Operativa Conjunta Combinada - Operación Inherent Resolve (OIR) y el Pentágono lleva a cabo actividades bilaterales de cooperación en materia de seguridad, aunque un acuerdo a finales de 2024 anunciaba una reducción del número de tropas estadounidenses. El presupuesto de Irak prevé una ampliación considerable de las Fuerzas de Movilización Popular (PMF), una agrupación de unas 50 facciones, algunas de ellas vinculadas a Irán. Bagdad depende del Servicio Antiterrorista (CTS) para las operaciones ofensivas. La Policía Federal Iraquí también opera como fuerza militar. Turquía tiene como objetivo al Partido de los Trabajadores del Kurdistan en el norte de Irak y mantiene bases allí. La región kurda mantiene dos divisiones bajo el control nominal del Ministerio de Asuntos Peshmerga, pero las dos principales facciones kurdas mantienen fuerzas separadas más numerosas. Irak cuenta con una mezcla de plataformas de la era soviética, rusas, europeas y estadounidenses, pero tiene importantes deficiencias en materia de apoyo logístico, fuego conjunto y

Planificación de misiones. Irak está tratando de modernizar sus fuerzas armadas y reducir su dependencia de Estados Unidos, para lo cual ha encargado helicópteros europeos, radares franceses y sistemas de defensa aérea surcoreanos. La industria de defensa iraquí es limitada y se centra en armas ligeras y municiones, así como en algunas tareas de mantenimiento.

ACTIVOS 193 000 (Ejército 180 000 Armada 3000 Fuerza Aérea 5000 Defensa aérea 5000) Gendarmería y paramilitares 266 000

ORGANIZACIONES POR SERVICIO

Ejército €180 000

Incluye el Servicio Antiterrorista

FUERZAS POR FUNCIÓN

FUERZAS ESPECIALES

- 3 brigadas de fuerzas especiales
- 1 brigada de rangers (3 batallones de rangers)

MANIOBRA

Blindada

- 1 (9.ª) división blindada (2 brigadas blindadas, 2 brigadas mecanizadas, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada logística)

Mecanizada

- 3 (5.ª, 8.ª y 10.ª) divisiones mecanizadas (4 brigadas de infantería mecanizada, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada de intendencia)
- 1 (7.ª) división mecanizada (2 brigadas de infantería mecanizada, 1 brigada de infantería, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada de intendencia)

Ligera

- 1 (6.ª) división motorizada (3 brigadas de infantería motorizada, 1 brigada de infantería, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada de intendencia)
- 1 (14.ª) división motorizada (2 brigadas de infantería motorizada, 3 brigadas de infantería, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada de intendencia)
- 1.ª División de Infantería () 1.ª División de Infantería () (2.ª División de Infantería () División de Infantería () 1.ª División de Infantería (11th) (3 brigadas de infantería ligera, 1 batallón de ingenieros, 1 regimiento de transmisiones, 1 brigada de intendencia) 1.ª División de Infantería (15th) (5 brigadas de infantería)
- 1 (16.ª) div inf (2 brigadas inf)
- 1 (17.ª Cdo) inf div (4 inf bde, 1 engr bn, 1 sigs regt, 1 log bde)
- 1 brigada de infantería

Otros

- 1 (PM SF) división sinónimo (3 brigadas de infantería)

HELICÓPTERO

- 3 escuadrones de helicópteros de ataque con Bell T407; H135M 1 escuadrón de helicópteros de ataque con Mi-28NE *Havoc*
- 1 escuadrón de helicópteros de ataque con Mi-35M *Hind* 1 escuadrón ISR con SA342M *Gazelle*
- 1 escuadrón con Bell 205 (UH-1H *Huey* II) 3 escuadrones con Mi-17 *Hip* H; Mi-171Sh
- 2 escuadrones de entrenamiento con Bell 206; OH-58C *Kiowa* 1 escuadrón de entrenamiento con Bell 205 (UH-1H *Huey* II) 1 escuadrón de entrenamiento con Mi-17 *Hip*

VEHÍCULO AÉREO NO TRIPULADO

- 1 escuadrón con CH-4; CH-5

EQUIPO POR TIPO

VEHÍCULOS BLINDADOS DE COMBATE

- MBT 401+: €100 M1A1 *Abrams*; 178+ T-72M/M1; €50

El entorno operativo 2024-2034



A gran escala
Operaciones de combate

Dejado en blanco intencionadamente

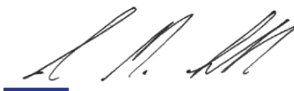
Prólogo

El Ejército de los Estados Unidos se enfrenta a retos nuevos y cada vez más peligrosos en comparación con hace solo unos años, debido a una amenaza en rápida modernización y a una amenaza aguda que participa en operaciones de combate prolongadas a gran escala en las puertas de la OTAN. Durante dos décadas de contrainsurgencia y contraterrorismo, estos adversarios tradicionales han observado cómo nuestras Fuerzas se enfrentaban a organizaciones extremistas violentas que tenían objetivos y recursos limitados y utilizaban armas y tácticas improvisadas. Ahora, muchas de estas amenazas han remitido, mientras que nuestros adversarios tradicionales, con presupuestos de defensa sustanciales y ambiciones globales, se han reafirmado. Nos han estudiado mientras ejecutábamos operaciones y están utilizando esas lecciones en su defensa y planificación estratégica. Para alcanzar la victoria en el entorno operativo del siglo XXI, el Ejército de los Estados Unidos debe conocer a estos enemigos como conocía a los soviéticos en el siglo XX.

China, la amenaza que marca el ritmo, está construyendo sistemas de defensa para alcanzar sus ambiciones globales. Cuenta con el ejército más grande del mundo en cuanto a personal y con la capacidad de ejecutar un enfoque nacional integral ante los conflictos que puede movilizar rápidamente su base industrial. El proceso de modernización de China ha experimentado una rápida transformación tecnológica hacia su visión de una guerra «informatizada» e «inteligente». También está impulsando un ambicioso sistema de educación militar profesional con el objetivo de crear un cuerpo de suboficiales fuerte.

Mientras tanto, Rusia, la amenaza más grave, se ha visto envuelta en una invasión de Ucrania desde 2022. Aunque no ha obtenido el éxito que esperaba inicialmente, Rusia está adquiriendo experiencia en operaciones de combate a gran escala y demostrando que el simple hecho de aguantar más que el enemigo es una opción militar potencialmente válida. La guerra en Ucrania ha demostrado que la próxima contienda se caracterizará por la guerra de la información y se centrará en los efectos multidominio. Los incendios serán el centro de gravedad, lo que hará que la protección sea una prioridad y las maniobras resulten difíciles.

En su misión de evaluar el entorno operativo, el Comando de Transformación y Entrenamiento del Ejército de los Estados Unidos debe sintetizar todas sus observaciones e investigaciones en conocimientos que el Ejército pueda aplicar. Eso es lo que este documento se propone hacer, pero es solo un primer paso. La información aquí contenida debe transmitirse y ser comprendida por los soldados del Ejército de los Estados Unidos de todos los rangos y niveles. Nuestros soldados, nuestra gente, son nuestra mayor fortaleza y debemos hacer todo lo posible para fortalecer la profesión de la guerra. La competencia como profesional del Ejército comienza con la comprensión de la amenaza, pero no termina ahí. Todo líder tiene la obligación de ser un aprendiz continuo y reflexivo fuera de la educación y el entrenamiento militar profesional tradicional.



Ian M. Sullivan

Jefe de Integración de Personal de Inteligencia

Comando de Transformación y Entrenamiento del Ejército de los Estados Unidos

«Para alcanzar la victoria, debemos conocer al enemigo. Conocer al enemigo comienza por el entorno operativo».

De la visión a la victoria

Contenido

Prólogo	ii
Resumen ejecutivo	1
Introducción	3
Condiciones de LSCO	5
Implicaciones de LSCO	21
Conclusión	28
Apéndice	29

Resumen ejecutivo

El Comando de Transformación y Entrenamiento del Ejército de los Estados Unidos (T2COM) G-2, a través de su observación y evaluación continua del Entorno Operacional (OE), identificó 12 condiciones que probablemente influirán en la forma en que el Ejército de los Estados Unidos se entrena y opera en operaciones de combate a gran escala (LSCO) durante el período 2024-2034. Dadas estas condiciones de las LSCO, el T2COM G-2 también identificó cinco implicaciones de las LSCO modernas que probablemente afectarán a la forma en que el Ejército de los Estados Unidos adapta sus capacidades relacionadas con la doctrina, la organización, el entrenamiento, el material, el liderazgo y la educación, el personal, las instalaciones y la política (DOTMLPF-P). Estas implicaciones son relevantes, pero no se limitan a la forma en que el Ejército aplica el OE al entrenamiento y al desarrollo de líderes para establecer las mejores condiciones para tener éxito en las LSCO. Este documento se centra en las LSCO y no cubre la totalidad de las operaciones del Ejército en el OE durante los próximos 10 años.

Las condiciones clave que probablemente impulsarán la LSCO en los próximos 10 años incluyen:

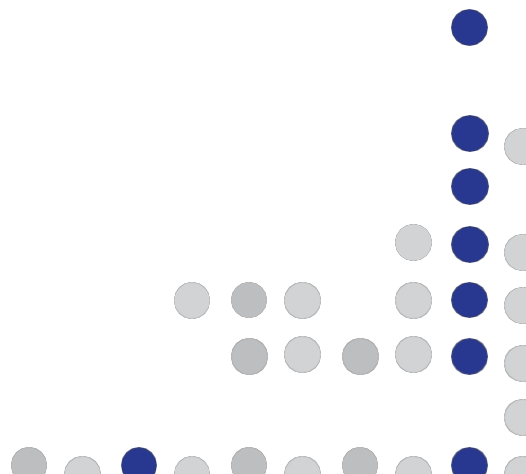
- El LSCO se caracterizará por **la competencia y la guerra en todos los ámbitos**, ya que la competencia y los conflictos se extienden más allá de las batallas físicas e implican cada vez más múltiples ámbitos y dimensiones interconectados.
- **La masa y la precisión** se complementan entre sí en la LSCO, y los combatientes tendrán que identificar la combinación adecuada de estos factores para obtener ventajas.
- El aumento de la producción, el empleo y el éxito de **los sistemas no tripulados** significa que el Ejército puede esperar encontrarse con estos sistemas en toda la amplitud y profundidad de la LSCO.
- La LSCO requerirá disparar y mantener cantidades masivas de municiones contra adversarios que probablemente disfruten de la ventaja inicial de las líneas interiores, lo que supondrá un reto para **la profundidad y el alcance de los depósitos** del Ejército.
- LSCO se caracterizará por la democratización y la proliferación de tecnologías avanzadas y comunicaciones globales hiperconectadas, lo que creará un **campo de batalla** cada vez más **transparente** que dificultará esconderse del enemigo.
- LSCO será **cada vez más letal** debido a la intersección de la ubicuidad de los sensores, la automatización del campo de batalla, los ataques de precisión y los fuegos masivos.
- En LSCO, las fuerzas estadounidenses se enfrentarán a los esfuerzos **de denegación de acceso/denegación de área** (A2/AD) de los adversarios, centrados en impedir nuestro despliegue en el teatro de operaciones y en impedir nuestra libertad de acción una vez desplegados.
- El aumento de los requisitos **logísticos** de la LSCO supondrá un reto para las operaciones de sostenimiento del Ejército, y los adversarios atacarán esas mismas operaciones desde el territorio nacional hasta el campo de batalla.
- La LSCO contará con requisitos **de defensa del territorio nacional**, ya que los adversarios dispondrán de capacidades convencionales, híbridas e irregulares para llevar a cabo operaciones contra el territorio nacional.
- Un entorno operativo cada vez más urbano significa que la LSCO incluirá **una densa guerra urbana** en entornos con condiciones de combate difíciles.
- La capacidad de los adversarios para influir rápidamente en las dimensiones informativa y humana supondrá un reto para la capacidad del Ejército de lograr **la ventaja informativa** en la LSCO.

- Los adversarios consideran **las armas de destrucción masiva** (ADM) como una ventaja asimétrica que tiene un impacto desmesurado en las operaciones estadounidenses y es probable que intenten emplearlas en un conflicto armado a gran escala.

Estas condiciones e implicaciones ilustran la complejidad de la LSCO en un entorno operativo dinámico. Proporcionan al Ejército de los Estados Unidos mucho que considerar a la hora de adaptar su doctrina, entrenar a sus soldados y desarrollar a sus líderes para ejecutar la LSCO en apoyo de los objetivos de seguridad nacional.

Estas condiciones de LSCO tendrán varias implicaciones probables en la forma en que el Ejército de los Estados Unidos aborda un futuro conflicto LSCO:

- Es probable que la LSCO exija a los combatientes comprender la dicotomía entre el **arte y la ciencia de la guerra** para lograr un equilibrio que aproveche al máximo las vulnerabilidades del adversario y minimice sus puntos fuertes.
- Los costes humanos y materiales de la LSCO sugieren que los combatientes se beneficiarán de una comprensión clara de cómo ven **la aniquilación frente al desgaste** como objetivo de la LSCO antes de que comiencen las hostilidades.
- El aumento de la transparencia, la letalidad y los retos para el movimiento en la LSCO pueden requerir una reevaluación de nuestro enfoque de **las maniobras, los disparos y la protección**.
- **Las personas son la ventaja** de LSCO, y el Ejército de los Estados Unidos deberá mantener su superioridad en el reclutamiento, entrenamiento y desarrollo eficaz de soldados y líderes de clase mundial.
- El combatiente en LSCO que haga de **la rápida adaptación** una parte fundamental de su enfoque de la guerra estará en mejores condiciones de aprovechar las oportunidades fugaces en el campo de batalla.



La OE y la LSCO () en el FM 3-0 y el ADP 3-0 del Ejército de los Estados Unidos

El conocimiento de la OE es el precursor de una acción eficaz.

El nuevo modelo del entorno operativo ayuda a los líderes a visualizar los cinco ámbitos y comprender su interrelación a través de las dimensiones física, informativa y humana.

Las fuerzas del Ejército deben verse a sí mismas, al enemigo o al adversario con precisión y comprender su OE antes de poder identificar o explotar las ventajas relativas.

El complejo entorno operativo en el que el

Ejército de los Estados Unidos llevará a cabo la LSCO contiene condiciones que no son necesariamente nuevas, pero que pueden ser de mayor relevancia para sobrevivir y tener éxito en la guerra terrestre.

Los comandantes terrestres deben tener en cuenta estas condiciones al preparar sus fuerzas y planificar la ejecución de las operaciones.

El enfoque de la preparación del Ejército se centra en las LSCO. Estas operaciones son operaciones de combate conjuntas de gran envergadura en cuanto a su alcance y el tamaño de las fuerzas comprometidas, y se llevan a cabo como una campaña destinada a alcanzar objetivos operativos y estratégicos.

Durante las LSCO, las fuerzas del Ejército se centran en la derrota y destrucción de las fuerzas terrestres enemigas como parte del equipo conjunto, y contribuyen a la derrota de las fuerzas en otros ámbitos.

Introducción

En 2021, el Ejército de los Estados Unidos publicó *El entorno operativo (2021-2030): competencia entre grandes potencias, crisis y conflictos*. En ese momento, China se había convertido recientemente en la principal amenaza para los Estados Unidos. El desarrollo y la transformación militar de China, junto con los de otros adversarios clave, llevaron a los Estados Unidos a reflexionar sobre cómo debían modernizarse y transformarse para mantener su ventaja. Además, la pandemia de COVID-19 estaba en pleno apogeo y desafiaba el statu quo mundial en materia de gobierno, economía, calidad de vida y guerra.

Ese documento se centraba en la modernización y el empleo militar de China y Rusia en situaciones de competencia, crisis y conflicto; el impacto de la COVID-19 y cómo China y Rusia podrían salir de la pandemia; y cómo la modernización china y rusa estaba desafiando el dominio del Ejército de los Estados Unidos a la hora de proporcionar la fuerza mejor entrenada y equipada para ejecutar la guerra de maniobras.

En 2024, las cambiantes condiciones globales exigieron una reevaluación de la caracterización del Ejército de los Estados Unidos del OE. El resultado es este documento, T2COM OE Threat Assessment 1.0, *The Operational Environment 2024-2034: Large-Scale Combat Operations* (Evaluación de amenazas T2COM OE 1.0, El entorno operativo 2024-2034: Operaciones de combate a gran escala), que se centra en las condiciones y las implicaciones de las LSCO modernas que el Ejército de los Estados Unidos tendrá que afrontar en los próximos 10 años. El objetivo es informar al Ejército sobre aspectos de LSCO y

su impacto en las operaciones, apoyando así la toma de decisiones de los altos mandos del Ejército y la planificación y ejecución de la formación del Ejército de los Estados Unidos, de modo que este pueda contribuir con éxito a los objetivos de seguridad nacional. Esta publicación tiene en cuenta los principales actores que representan una amenaza identificados en la *Estrategia de Defensa Nacional de los Estados Unidos de América de 2022*, así como los conceptos clave del *Manual de Campo del Ejército de los Estados Unidos 3-0: Operaciones*. Aunque el Ejército de los Estados Unidos puede operar en una amplia gama de contingencias y entornos, debe mantener su enfoque en la preparación para la LSCO. Este documento se centra en la LSCO y no cubre la totalidad de las operaciones del Ejército en el OE durante los próximos 10 años.

Este documento es el resultado del estudio continuo realizado por los analistas de T2COM G-2 sobre las actividades de estos principales actores amenazantes y las observaciones de conflictos recientes y en curso. Este trabajo también se deriva de la colaboración rutinaria entre la Empresa de Inteligencia y Seguridad del Ejército, así como con la Comunidad de Inteligencia. T2COM G-2 desea expresar su especial agradecimiento al Centro Nacional de Inteligencia Terrestre por su apoyo en esta iniciativa.

El carácter complejo e incierto de las LSCO y las capacidades de los adversarios requieren que este documento se base en las siguientes hipótesis para enmarcar la evaluación de OE para 2024-2034:

- Aunque LSCO representa el tipo de operaciones más exigentes y peligrosas que el Ejército de los Estados Unidos debe estar preparado para llevar a cabo durante la próxima década, la mayoría de sus operaciones se desarrollarán por debajo del umbral del conflicto armado.
- Las amenazas constantes, agudas y persistentes seguirán sin cambios.

- Es poco probable que se produzcan acontecimientos geopolíticos que modifiquen de forma fundamental es poco probable que se produzcan cambios fundamentales en el enfoque de los adversarios de EE. UU. respecto a las LSCO.

- Es poco probable que se produzcan cambios tecnológicos revolucionarios que afecten a las LSCO.

Todos los principales adversarios de Estados Unidos poseen o están desarrollando capacidades que aumentan el potencial de conflicto. China, nuestra amenaza principal, busca convertirse en un ejército altamente moderno capaz de derrotar a Estados Unidos a nivel regional y, eventualmente, a nivel mundial en una guerra conjunta y multidominio. La modernización del Ejército Popular de Liberación de China (EPL) no está diseñada solo para lograr una superioridad tecnológica. En cambio, está diseñada para desafiar al Ejército de los Estados Unidos y a la Fuerza Conjunta mediante el dominio en materia de material, soldados y líderes, y enfoque de la guerra, tres áreas que han sustentado

El poderío militar estadounidense desde 1991. Rusia, nuestra grave amenaza, continúa su campaña de agresión contra Ucrania, al tiempo que sigue representando un riesgo constante en áreas clave.

Entre ellas se incluyen amenazas a la patria; misiles de crucero de largo alcance; cibernéticas, informáticas y espaciales; armas nucleares, químicas y biológicas; y amplias campañas en la zona gris. Corea del Norte, Irán y las organizaciones extremistas violentas siguen siendo amenazas persistentes, lo que genera incertidumbre y subraya la necesidad de que el Ejército de los Estados Unidos esté preparado para llevar a cabo operaciones multidominio en todo el mundo a diferentes escalas. Además, la aparición de una colusión autoritaria cada vez más frecuente, en la que los actores que representan una amenaza colaboran de forma transaccional para contrarrestar los intereses occidentales, probablemente planteará nuevos retos en el ámbito de la guerra. La reciente colaboración entre Rusia y Corea del Norte pone de relieve la voluntad y la necesidad de los regímenes autoritarios de unir fuerzas contra las alianzas de naciones democráticas.

Comprensión

Estos avances y su papel en el OE, en constante evolución, establecen las condiciones básicas para mantener la preparación del Ejército frente a todos los enemigos.

El T2COM está formando hoy a los soldados y líderes de las futuras formaciones del Ejército. Los soldados rasos y tenientes que lleguen este año a los puestos del T2COM serán los jefes de pelotón y comandantes de compañía que se enfrentarán a los adversarios de Estados Unidos en el futuro. Todos los soldados y líderes deben tener un conocimiento práctico del OE y de nuestros principales adversarios: la amenaza creciente, la amenaza aguda y las amenazas persistentes.





LSCO se caracterizará por la competencia y la guerra en todos los ámbitos, ya que la competencia y el conflicto se extienden más allá de las batallas físicas e implican cada vez más múltiples ámbitos y dimensiones interconectados.

LSCO

Condiciones

Competencia y guerra en todos los ámbitos

Durante gran parte de su existencia, Estados Unidos solo tuvo que enfrentarse a rivales en un ámbito: el terrestre. Estados Unidos disfrutó de un apoyo aéreo y marítimo sin rival y, más tarde, de un apoyo espacial y cibernético sin rival. Sin embargo, la democratización de la tecnología y los avances en los sistemas robóticos y cibernéticos permitirán a los adversarios enfrentarse al Ejército de los Estados Unidos y a la Fuerza Conjunta en todos los ámbitos —tierra, aire, mar, espacio y ciberespacio— y en las dimensiones física, informativa y humana.

Algunos adversarios emplearán sofisticados sistemas de defensa aérea terrestres que el Ejército deberá derrotar para crear oportunidades para los activos aéreos amigos y permitir la plena aplicación de las capacidades de combate conjunto de los Estados Unidos. Es probable que los elementos de la Armada de los Estados Unidos dependan de los fuegos y la protección terrestres para permitir la libertad de acción marítima que, a su vez, respalda las operaciones del Ejército. Mientras tanto, nuestros adversarios atacarán cada vez más

las defensas aéreas, los puertos, las bases y el sostenimiento de los Estados Unidos que contribuyen a la

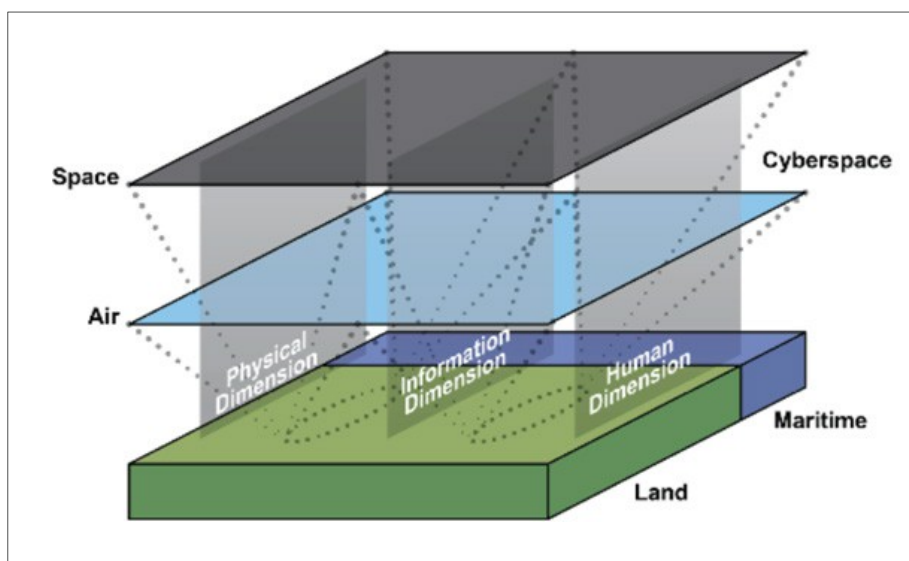


Figura 1: El FM 3-0 describe cómo las fuerzas del Ejército de los Estados Unidos llevan a cabo operaciones multidominio a lo largo de un OE que consta de cinco dominios y tres dimensiones.

Operaciones conjuntas. Las amenazas cada vez mayores para las formaciones procedentes de sistemas no tripulados en todos los dominios, como se ha visto en el conflicto de Ucrania, se suman a esta complejidad.

La convergencia de las capacidades cibernéticas con las terrestres, aéreas, marítimas y espaciales puede producir un efecto mayor que la suma de sus partes. Las armas cibernéticas pueden negar o degradar la preparación y la cohesión de las unidades, al tiempo que proporcionan inteligencia. Por ejemplo, un arma cibernética podría activar un activo espacial para transmitir información a los activos de inteligencia, vigilancia y reconocimiento (ISR) y proporcionar al adversario información sobre la situación y los objetivos.

Para China, el espacio es un ámbito importante, aunque congestionado. Cuenta con casi 300 satélites ISR en órbita y recientemente ha lanzado el satélite óptico de teledetección de órbita alta Yaogan-41, que tiene una resolución estimada de 2,5 metros, lo que permite al EPL identificar vehículos individuales. Para 2034, es probable que China alcance la paridad con las capacidades espaciales de Estados Unidos, o incluso las supere.

China y Rusia tienen la capacidad de denegar o degradar dominios enteros durante un conflicto LSCO con Estados Unidos y sus aliados. Estos adversarios también cuentan con sofisticadas operaciones cibernéticas que pueden perturbar a Estados Unidos tanto durante el LSCO

y en la fase de competencia sin llegar al conflicto. Comprender, aprovechar y resolver los conflictos de información en todos los ámbitos y desde todas las dimensiones, en tiempo real, será clave para la victoria.



La masa y la precisión se complementan entre sí en LSCO, y los combatientes deberán identificar la combinación adecuada de estos factores para obtener ventajas.

Masa frente a precisión

En Ucrania, Rusia sigue prefiriendo los ataques masivos contra objetivos que no se pueden ver, en lugar de los ataques de precisión contra objetivos identificados. Por el contrario, Ucrania se ha centrado en analizar los datos de los sensores, priorizar los objetivos, aplicar la economía de esfuerzo, automatizar la asignación de objetivos a la munición más cercana disponible y llevar a cabo ataques de precisión para aislar los sistemas clave y las cadenas de suministro. Encontrar la combinación adecuada entre fuego masivo y precisión proporcionará oportunidades aprovechables en LSCO. La supervivencia y el éxito requerirán la flexibilidad necesaria para culminar, dispersar y ocultar rápidamente. Será necesario un uso flexible del equipo existente, lo que permitirá efectos entre dominios contra una gama más amplia de objetivos. En LSCO, el combatiente que pueda desplegar grandes cantidades de municiones de precisión de bajo coste y proteger al mismo tiempo sus redes de sostenimiento tendrá una ventaja en el campo de batalla.

En LSCO, los combatientes compensarán el desgaste de los sistemas de alta gama empleando capacidades heredadas, como ha hecho Rusia en Ucrania, al tiempo que dotarán a sus ejércitos de una profundidad de munición abrumadora, como ha hecho China. Los adversarios seguirán invirtiendo en capacidades de alta gama y combinarán ese enfoque con ciclos rápidos de innovación y adaptación. La velocidad de innovación, adquisición e integración de tecnologías nuevas y emergentes con los equipos existentes será decisiva.

Los disparos de precisión seguirán estando sujetos a efectos entre dominios. Dependen en gran medida de los satélites para la detección, el posicionamiento, la navegación y la sincronización, que son vulnerables a las interferencias y al bloqueo. Las plataformas espaciales también son vulnerables

a los ataques cinéticos, los ataques con energía dirigida, las interferencias por encuentro o aproximación cercana de otros satélites, así como a las colisiones con desechos espaciales u otros objetos en órbita.

Proliferación de sistemas no tripulados

Se ha producido un aumento en la producción, el empleo y el éxito de los sistemas no tripulados en el campo de batalla en las LSCO modernas. Los sistemas aéreos no tripulados (UAS) fueron fundamentales para la victoria de Azerbaiyán contra Armenia en la Segunda Guerra de Nagorno-Karabaj en 2020. Más recientemente, la siguiente evolución de los UAS —los sistemas de visión en primera persona (FPV) y de ataque unidireccional (OWA)— está demostrando ser fundamental en las guerras en curso entre Rusia y Ucrania e Israel y Hamás.

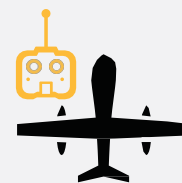
Los UAS están transformando la adquisición y el ataque de objetivos. Los UAS ISR se están empleando para detectar e informar sobre objetivos, mientras que las municiones merodeadoras están reduciendo la latencia en la selección de objetivos y superando los retos relacionados con el tiempo de vuelo para los sistemas de ataque de mayor alcance. Los UAS también pueden tener un potente efecto cognitivo debido a la amenaza persistente que suponen para los elementos terrestres. El bajo coste de adquisición y la amplia disponibilidad de la tecnología necesaria para construir UAS significa que los actores estatales y no estatales más pequeños y con recursos limitados pueden ser capaces de construir fuerzas aéreas facsímiles para desafiar a los estados poderosos con grandes presupuestos de defensa y robustas fuerzas aéreas tripuladas. China, por ejemplo, se ha convertido en líder mundial en la exportación de UAS de combate. Al menos 17 países poseen inventarios de UAS de combate fabricados en China, y estos sistemas se han empleado en conflictos en todo el mundo.

Los sistemas no tripulados que pueden atravesar zonas urbanas y subterráneas serán ventajosos en LSCO. Por ejemplo, en agosto de 2022, los zapadores rusos utilizaron pequeños vehículos terrestres no tripulados en Ucrania para inspeccionar edificios en busca de explosivos. Hamás creó una red integral de almacenamiento,

logística y túneles de ataque que condujeron a su ataque del 7 de octubre de 2023 contra Israel. LSCO implicará sistemas terrestres no tripulados con sensores y comunicaciones que podrían atravesar estas áreas primero, manteniendo a los soldados fuera de peligro hasta que sea necesario. Estos sistemas no tripulados podrían proporcionar audio y vídeo en tiempo real a un nodo de mando y control (C2) con cámaras multispectrales, extremidades controladas a distancia o autónomas para interrogar objetos y cargas útiles para producir efectos cinéticos.

Del mismo modo, los buques submarinos o de superficie no tripulados desempeñarán un papel cada vez más importante en la LSCO. Por ejemplo, en febrero de 2023, las fuerzas rusas podrían haber utilizado un buque de superficie no tripulado para atacar un puente entre Ucrania y Moldavia, a juzgar por las informaciones difundidas en las redes sociales. Mientras tanto, China se centra en desarrollar software de colaboración que pueda utilizarse para embarcaciones submarinas y de superficie no tripuladas en múltiples configuraciones. Está financiando la investigación en colaboración tripulada-no tripulada, lo que podría proporcionar importantes ventajas en el campo de batalla, ya que ni los humanos ni las máquinas actúan por sí solos con la misma eficacia que cuando trabajan en tándem.

Los soldados estadounidenses deben estar preparados para hacer frente a la amenaza que supone la proliferación generalizada de los UAS. Los soldados de todo tipo de unidades y rangos deben estar tan familiarizados con el uso de tecnologías contra los UAS como con el manejo de sus propias armas. Las tácticas y el entrenamiento contra los UAS deben abordar el refuerzo y otros preparativos de las posiciones de combate contra los drones armados, desarrollando la conciencia de las capacidades de un sistema para vigilar a un soldado.



El aumento de la producción, el empleo y el éxito de los sistemas no tripulados significa que el Ejército puede esperar encontrarse con estos sistemas en toda la extensión y profundidad de LSCO.



Figura 2: La proliferación de sistemas no tripulados aumenta la amenaza y exige requisitos de protección en el OE.

Fuente: Estrategia contra los sistemas aéreos no tripulados pequeños del Departamento de Defensa de los Estados Unidos, <https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf>.

en cualquier espectro, incluidos el visible, el infrarrojo y las frecuencias de radio, y métodos para neutralizarlos.

Profundidad y alcance de la revista

Como se señala en el *FM 3-0*, la LSCO puede consumir las reservas de municiones del cuerpo y la división en 72-96 horas, especialmente en el caso de cañones, cohetes y morteros. El gasto masivo de municiones en la guerra entre Rusia y Ucrania pone de manifiesto las posibles limitaciones de las cifras de producción en tiempos de paz en la LSCO. El reabastecimiento de municiones requeriría un esfuerzo considerable, y cualquier problema en la cadena de suministro podría agravar un calendario ya de por sí ajustado. La guerra entre Rusia y Ucrania es un claro recordatorio de que no siempre se puede contar con suficientes reservas de municiones. Estados Unidos depende en gran medida de la industria privada para muchos sistemas de armas clave, y muchos sistemas sofisticados cuentan con ordenadores a bordo que funcionan con microchips, la mayoría de los cuales se fabrican fuera de Estados Unidos, en lugares como China y Taiwán. Un conflicto que involucrara a cualquiera de estos países podría detener la fabricación de microchips y obstaculizar la producción de municiones.

Es probable que el conflicto con China o Rusia tenga lugar en los teatros de operaciones del Indo-Pacífico o Europa, respectivamente. Ambos adversarios disfrutarán de una clara ventaja al operar con líneas interiores, lo que les garantizará un acceso relativamente rápido y fácil al equipo, las municiones y el personal. En cualquiera de los dos teatros, Estados Unidos contará con una red logística que se extiende a lo largo de varios miles de kilómetros desde el territorio nacional hasta el teatro de operaciones, lo que la hace vulnerable a ataques, A2/AD o accidentes.



LSCO requerirá disparar y mantener cantidades masivas de municiones contra adversarios que probablemente disfruten de la ventaja inicial de las líneas interiores, lo que supondrá un reto para la profundidad y el alcance de los depósitos del Ejército.



LSCO se caracterizará por la democratización y proliferación de tecnologías avanzadas y de las comunicaciones globales hiperconectadas, creando un campo de batalla cada vez más transparente campo de batalla que hace difícil esconderse del enemigo.

Campo de batalla transparente

El campo de batalla moderno es cada vez más transparente debido a la proliferación de tecnologías avanzadas (dispositivos inteligentes, sensores, emisores, etc.), así como a la aparición de comunicaciones globales hiperconectadas y redes sociales. Históricamente, los datos de alta calidad para la localización de objetivos y la vigilancia generalizada se han limitado a los actores estatales con grandes recursos. Sin embargo, la disponibilidad cada vez más universal de tecnologías emergentes y disruptivas ha permitido a combatientes menos poderosos utilizar tecnologías y datos comerciales para localizar, fijar y eliminar objetivos de alto valor. Por ejemplo, Ucrania ha tenido un gran éxito en la localización, el ataque y la destrucción de fuerzas rusas basándose en las señales no autorizadas de los teléfonos móviles de los soldados rusos, incluido un ataque con cohetes contra un cuartel ruso que causó la muerte de 63 personas.

Si bien la confusión y la fricción seguirán siendo complejidades inherentes a la guerra, la transparencia en el campo de batalla seguirá aumentando con el crecimiento de otras tecnologías, como las plataformas espaciales comerciales, el Internet de las cosas, los sistemas autónomos y la fusión de datos en tiempo real. Los adversarios con capacidades y capacidades anteriormente limitadas de mando, control, computación, comunicaciones, cibernéticas, inteligencia, vigilancia, reconocimiento y selección de objetivos utilizarán tecnologías comerciales disponibles en el mercado, datos de acceso público y aplicaciones y conocimientos de inteligencia artificial/aprendizaje automático de código abierto para alcanzar una paridad relativa con los Estados Unidos. Imágenes, vídeos y transmisiones en directo aparentemente benignos desde dispositivos personales a redes sociales y aplicaciones de mensajería alertarán a los adversarios de las operaciones en curso y les proporcionarán la ubicación de las tropas y las instalaciones.

Estos adversarios podrán entonces examinar miles de publicaciones en redes sociales, señales de teléfonos móviles e imágenes satelitales para corroborar los datos con transmisiones en directo desde UAS y refinar sus objetivos de forma rápida y precisa.

El LSCO moderno será una competición entre los que se esconden y los que buscan, con oportunidades de explotación fugaces para ambos. Si un objetivo puede verse, puede ser eliminado. La capacidad del Ejército para protegerse en este campo de batalla transparente será fundamental para su supervivencia y éxito. La capacidad de esconderse a plena vista cobra aún mayor importancia con la masa y la precisión de los sistemas de armas modernos.

Mayor letalidad

El OE es cada vez más letal gracias a la omnipresencia de sensores y a la proliferación de la automatización del campo de batalla, lo que facilita una precisión eficaz y capacidades de ataque masivo. La integración de los UAS ISR con artillería de tubo y cohetes permite lanzar fuego convencional masivo preciso y oportuno desde posiciones de disparo dispares, así como ataques precisos contra objetivos de alto valor con municiones guiadas de precisión (PGM). Estos disparos tienen efectos en toda la profundidad del campo de batalla, lo que facilita el ataque a fuerzas de maniobra, fuerzas atrincheradas en defensas estáticas y zonas urbanas, y C2, nodos logísticos y principales rutas de suministro en zonas de retaguardia.

Las Fuerzas Armadas de Ucrania han utilizado grandes cantidades de sistemas portátiles de defensa antiaérea (MANPADS), misiles guiados antitanque y UAS FPV, combinados con fuego, con gran eficacia. En julio de 2024, Rusia había perdido 3197 carros de combate principales —más que todo su inventario en servicio activo al inicio del conflicto— y 6160 vehículos blindados de combate, lo que la ha obligado a sacar del almacén sistemas cada vez más obsoletos. El coste humano asociado a la destrucción de este equipo refleja directamente la letalidad de la LSCO. Las bajas rusas superan las 300 000 en dos años, mientras que las estimaciones de bajas ucranianas sugieren al menos 200 000 víctimas. Del mismo modo, las estimaciones de bajas de la Segunda Guerra de Nagorno-Karabaj en 2020 reflejan la letalidad de la LSCO en términos de pérdidas de personal y equipo. Durante un período de 44 días, Armenia sufrió unas 2800 muertes, mientras que Azerbaiyán perdió aproximadamente 3400 efectivos. Además, Armenia perdió hasta el 50 % de su defensa aérea.

sistemas y el 40 % de su artillería a los ataques de Azerbaiyán durante el primer día de combate.

China está observando y aprendiendo de la experiencia de Rusia en Ucrania para planificar cualquier posible contingencia en Taiwán. Las pérdidas de personal y equipo rusos en el campo de batalla debido al avistamiento y los ataques de los UAS probablemente llevarán al EPL a desarrollar o mejorar los sistemas de defensa aérea de corto alcance y a proporcionar mayores capacidades de protección a las unidades de maniobra. El gran número de muertos y heridos también probablemente impulsará al EPL a examinar cómo lleva a cabo las operaciones médicas tácticas y a tratar de mejorar la atención y la evacuación de las víctimas. Por último, es probable que el EPL examine su avanzada doctrina de asalto con fuego debido a la ineficacia de los ataques masivos con fuego de largo alcance rusos al principio de la invasión de Ucrania.



LSCO será cada vez más letal debido a la intersección de la ubicuidad de los sensores, la automatización del campo de batalla, los ataques de precisión y los fuegos masivos.

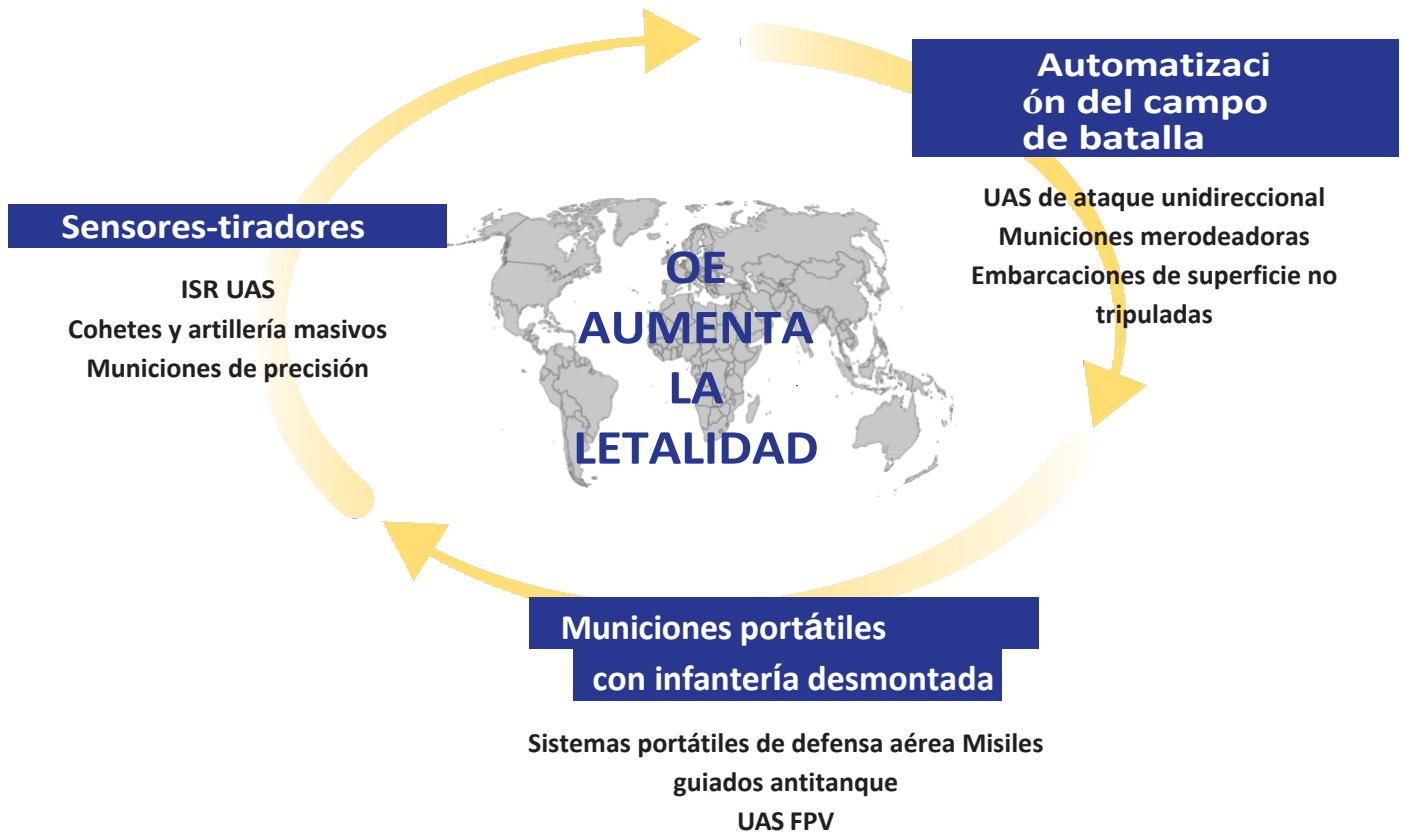


Figura 3: La intersección de las opciones de detección, automatización y ataque en LSCO aumenta la letalidad de las operaciones.

Antiacceso/denegación de área

Las fuerzas estadounidenses se enfrentarán a los esfuerzos A2/AD de sus adversarios, centrados en impedir el despliegue en el teatro de operaciones, negar la libertad de acción una vez desplegados y provocar una desincronización significativa de la Fuerza Conjunta. Es probable que el impacto de las capacidades A2/AD, tanto en el entorno físico como en el ciberespacio, ponga a prueba la capacidad del Ejército de los Estados Unidos para llegar al campo de batalla y mantener la lucha. La capacidad de proporcionar la logística necesaria para mantener la LSCO probablemente se verá cuestionada desde el territorio nacional hasta el campo de batalla.

La guerra entre Rusia y Ucrania refuerza la importancia de la A2/AD en un campo de batalla cada vez más transparente. Se requiere una infraestructura significativa para desplegar y emplear fuerzas modernas: puertos aéreos de desembarco, puertos marítimos de desembarco, redes de carreteras y ferrocarriles e infraestructura de comunicaciones. Cada uno de estos elementos representa una superficie de ataque para los sistemas cinéticos y no cinéticos de la A2/AD, y la mayor capacidad de los adversarios para detectar y atacar con precisión en profundidad amplía drásticamente el campo de batalla. Desde el punto de vista táctico, la guerra de minas es el mejor ejemplo de los esfuerzos de denegación de área en la guerra entre Rusia y Ucrania. Las pérdidas ucranianas al intentar romper las defensas preparadas por Rusia ponen de relieve el peligro que supone un adversario al que se le da tiempo, espacio y recursos para preparar el campo de batalla con obstáculos, incendios y vigilancia.

La estrategia anti-acceso incluye las actividades de un adversario en los ámbitos diplomático, informativo, militar y económico del poder nacional para impedir que Estados Unidos entre en la zona de conflicto. Los adversarios llevarán a cabo actividades no cinéticas para influir, coaccionar y amenazar a los aliados y socios potenciales de Estados Unidos para que no cooperen

con la Fuerza Conjunta. También utilizarán la amenaza de ataques cinéticos mediante demostraciones, disparos reales y ejercicios para mostrar su capacidad de castigar el apoyo a las operaciones estadounidenses.

La denegación de área también puede interrumpir o desorganizar las capacidades del adversario, lo que afecta a la capacidad de apoyar funciones clave. El aumento de la profundidad de los objetivos puede hacer que los sistemas adversarios se desplacen con más frecuencia o se alejen más de lo óptimo. Es probable que los puestos de mando se vean obligados a retroceder más, lo que complicará las comunicaciones y obligará a los comandantes a desplegar su grupo de mando más lejos de su puesto de mando principal. Los radares de contraataque tendrán que desplazarse con frecuencia, lo que reducirá el número y la densidad de los sistemas que rastrean los disparos enemigos en un momento dado. Los nodos de sostenimiento estarán más atrás y muy distribuidos, lo que disminuirá la eficiencia.



En LSCO, las Fuerzas Armadas de los Estados Unidos se enfrentarán a los esfuerzos de denegación de acceso/área de los adversarios, centrados en impedir nuestro despliegue en el teatro de operaciones y en limitar nuestra libertad de acción una vez desplegados.

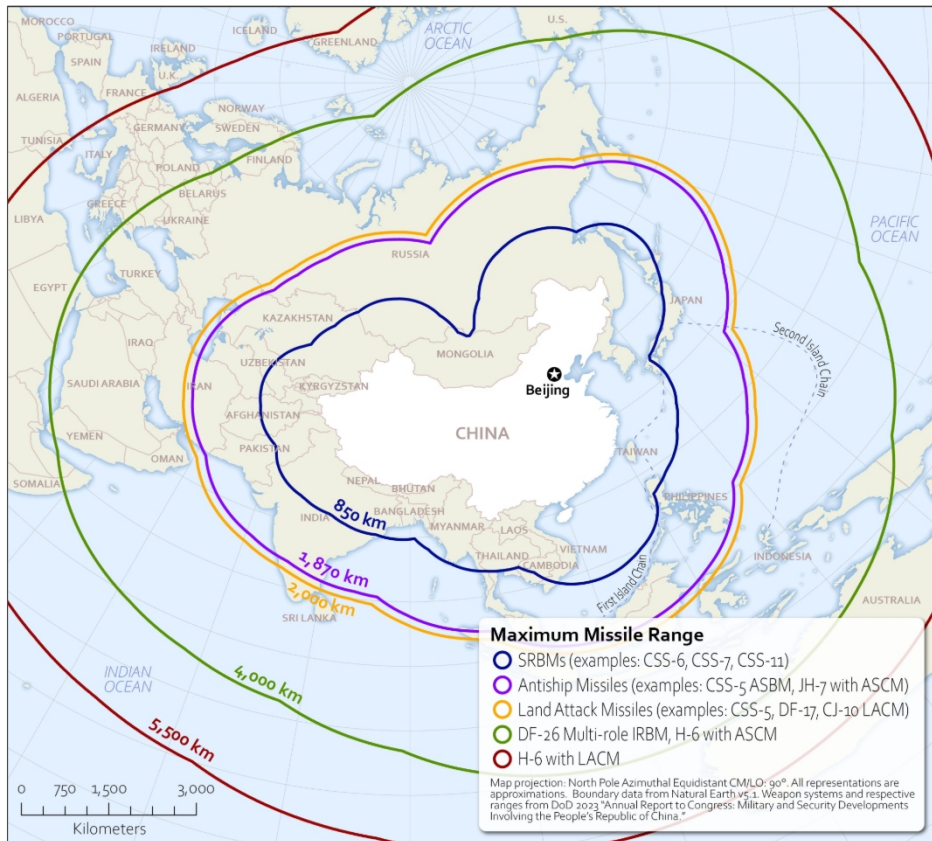


Figura 4: El EPL intentará aprovechar todos los ámbitos y dimensiones para impedir la entrada de las Fuerzas Conjuntas de EE. UU. en el teatro de operaciones y amenazar las operaciones una vez en el teatro.

Ataque convencional

La mejora de las capacidades de fuego terrestre del Ejército Popular de Liberación significa que la Fuerza de Cohetes del Ejército Popular de Liberación, la Armada del Ejército Popular de Liberación y la Fuerza Aérea del Ejército Popular de Liberación pueden centrarse en la lucha contra la intervención, mientras que el Ejército Popular de Liberación se encarga de la lucha cuerpo a cuerpo.

Guerra electrónica/ataque cibernético

Las fuerzas de guerra electrónica y cibernética disuaden, retrasan, interrumpen y degradan las operaciones del Departamento de Defensa antes y durante un conflicto.

Guerra de la información

El EPL lleva a cabo operaciones en el ámbito cognitivo para obtener el dominio en las dimensiones informativa y humana con el fin de ejercer una influencia desmesurada sobre la opinión pública y la moral militar.

Logística disputada

El suministro de formaciones de combate preparadas es una prioridad para los altos mandos del Ejército. Esto incluye galvanizar el

La base industrial estadounidense debe desarrollar la profundidad de la revista Nation necesaria para respaldar el LSCO duradero. Las cadenas de suministro y el apoyo de mantenimiento para respaldar el LSCO serán objetivos de gran valor para nuestros adversarios, lo que sugiere que deben protegerse y mantenerse operativos. En el punto álgido de la guerra entre Rusia y Ucrania a finales de 2022, Rusia gastaba 20 000 proyectiles de artillería al día. A medida que los nodos logísticos y las principales rutas de suministro rusas eran blanco activo de los ataques ucranianos, esa tasa diaria de fuego se redujo drásticamente a 5000 proyectiles al día. Las tasas sostenidas de fuego ruso y el desgaste causado por los ataques ucranianos obligaron a Rusia a ampliar su producción nacional de municiones a aproximadamente 3 millones de proyectiles al año y a buscar ayuda externa de Corea del Norte e Irán.

Los adversarios tratarán de interrumpir las principales rutas de suministro en puntos clave, como terrenos restringidos, puentes, túneles y cruces ferroviarios. Proteger estas rutas será vital para mantener las operaciones. Dada la transparencia del campo de batalla, los vehículos y convoyes de suministro

serán identificados y rastreados hasta los puntos de reabastecimiento para ser atacados y posteriormente destruidos por fuego, lo que desgastará tanto la logística como los medios de transporte y distribución asociados.

Los adversarios mantienen la capacidad de atacar la infraestructura logística de los Estados Unidos, lo que afectará los procesos de despliegue durante la escalada hacia el conflicto. Además, la fase de competencia puede dar paso inmediatamente al conflicto, sin dejar un período de crisis para iniciar el flujo de fuerzas. Una vez en el teatro de operaciones, los complejos A2/AD, cibernéticos, de información, contraespaciales y de reconocimiento/ataque sofisticados desafiarán tanto la maniobra como el sostenimiento en todos los escalones.



El aumento de las necesidades logísticas de la LSCO supondrá un reto para las operaciones de sostenimiento del Ejército, y los adversarios atacarán esas mismas operaciones desde el territorio nacional hasta el campo de batalla.

Ucrania logra el éxito al dar prioridad a la interrupción de la logística en invierno

En el invierno de 2023-2024, el Mando de las Fuerzas Terrestres de Ucrania declaró públicamente su intención de atacar las líneas de suministro, los depósitos y los centros de mando para causar un impacto psicológico en los soldados rusos. Los ucranianos dejaron a los soldados rusos abandonados al frío, sin provisiones suficientes, y luego lanzaron ataques contra sus posiciones. Las fuerzas rusas también subestimaron las necesidades logísticas, lo que aumentó el número de bajas y agravó los efectos psicológicos de las operaciones ucranianas.



La LSCO incluirá requisitos de defensa de la patria, ya que los adversarios dispondrán de capacidades convencionales, híbridas e irregulares para llevar a cabo operaciones contra la patria.

Defensa nacional

Es probable que la patria deje de ser un santuario durante un futuro conflicto LSCO. China, Rusia y otros adversarios están invirtiendo fuertemente en capacidades híbridas e irregulares, como operaciones informáticas y cibernéticas, para atacar objetivos y sistemas vulnerables dentro del territorio de los Estados Unidos y sus aliados. Estos ataques pueden tener efectos desmesurados con un coste y un esfuerzo relativamente bajos y con menos riesgo de escalada que los ataques cinéticos tradicionales.

Rusia y China creen que ya están en conflicto activo con Estados Unidos. Están trabajando para establecer puntos de apoyo dentro de redes críticas —sistemas gubernamentales reforzados, industria privada y redes sociales— con el fin de reforzar sus capacidades de recopilación de información contra nosotros, interrumpir nuestras funciones críticas y retrasar nuestra capacidad de proyectar fuerza. Probablemente ocultarán su participación e intentarán mantener los efectos por debajo del umbral de escalada a LSCO. La mejora de las capacidades tecnológicas de la información permite a los actores estatales y no estatales desafiar al Ejército en múltiples ámbitos simultáneamente.

Es probable que los adversarios de Estados Unidos se centren en las funciones de apoyo y aprovechen las divisiones entre civiles y militares. Tanto Rusia como China han establecido medios para sembrar narrativas disruptivas en el espacio informativo. Los actores maliciosos podrán recopilar información aparentemente sin importancia de diversas fuentes abiertas o de usuarios de Internet inconscientes y convertirla en inteligencia útil, incluyendo datos sobre altos mandos del Ejército, soldados y familiares de soldados. El

Ejército de los Estados Unidos es un objetivo atractivo para las operaciones de influencia digital de los adversarios, ya que ofrece un grupo grande y

grupo diverso de personas altamente motivadas y respetadas cuyas acciones y creencias pueden tener un impacto desmesurado en la nación en su conjunto.

Al inicio de la LSCO, es probable que los adversarios pasen de operaciones cibernéticas y de información no atribuibles a efectos físicos más destructivos. Es probable que los adversarios intensifiquen sus acciones utilizando sistemas de alcance ultralargo con cargas útiles convencionales, plataformas asimétricas, UAS comerciales y sabotajes para amenazar infraestructuras y operaciones clave. Probablemente será necesario perfeccionar los procesos de movilización para responder rápidamente a amenazas complejas. Aumentar la concienciación sobre las amenazas en todos los ámbitos y reforzar la infraestructura militar podría ayudar a mejorar la preparación.

Guerra urbana densa

Las Naciones Unidas prevén que, para 2050, el 68 % de la población mundial vivirá en zonas urbanas, lo que aumentará la posibilidad de que las operaciones del Ejército de los Estados Unidos se desarrollen en entornos urbanos densamente poblados. La guerra urbana plantea varios retos, como se ha visto en la guerra entre Rusia y Ucrania, el conflicto entre Israel y Hamás y la derrota del ISIS en Irak. El vaivén de la guerra en Ucrania, en particular, demuestra que no basta con atacar las zonas urbanas. La clave estará en mantener y defender el terreno. Los ejércitos que puedan alternar entre el ataque y la defensa rápidamente y sin previo aviso tendrán ventaja sobre los que no puedan hacerlo. Los defensores pueden aprovechar la infraestructura existente y la densidad de población para atrincherarse en edificios, metros y otras redes subterráneas.

Los retos habituales de la guerra se verán agravados, ya que las zonas urbanas y subterráneas dificultarán las maniobras. Las condiciones de las carreteras, el tráfico, la población civil y la densidad de edificios limitarán la libertad de movimiento y la capacidad de reunir

grandes formaciones. Las manzanas de las ciudades crearán puntos de estrangulamiento naturales, los vehículos civiles se convertirán en obstáculos y los cañones urbanos dificultarán el vuelo de la mayoría de las plataformas aéreas. La búsqueda y el despeje se verán obstaculizados por la cobertura y el ocultamiento que proporcionan los rascacielos, los túneles y las infraestructuras subterráneas. La densidad de población reducirá la eficacia de la artillería, ya que aumentará el riesgo de víctimas entre la población no combatiente. Es posible que Estados Unidos tenga que crear condiciones que obliguen a sacar las batallas de las zonas urbanas para llevar a cabo una LSCO eficaz, lo que probablemente no será factible en algunos casos.



Una OE cada vez más urbana significa que la LSCO incluirá una densa guerra urbana en entornos con condiciones de combate difíciles.

La liberación de Mosul pone de relieve la dificultad de la guerra urbana

La liberación de Mosul, la segunda ciudad más grande de Irak, del Estado Islámico de Irak y Siria (ISIS) en 2016 es instructiva en cuanto a la dificultad que enfrenta una fuerza grande, bien armada y altamente entrenada para desalojar incluso a un oponente inferior de un entorno urbano. El ISIS mantenía una fuerza de infantería ligera de solo entre 3000 y 5000 efectivos con ametralladoras pesadas, lanzagranadas, fusiles sin retroceso, morteros y cohetes. Sin embargo, el ISIS construyó una elaborada defensa dentro de la ciudad fortificando edificios, bloqueando vías de acceso, creando obstáculos y construyendo refugios subterráneos y túneles. Como resultado, el ISIS fue capaz de mantener Mosul durante nueve meses frente a las fuerzas de seguridad iraquíes, superiores en número (aproximadamente 94 000 efectivos), y al apoyo de las fuerzas de la coalición.



La capacidad de los adversarios para influir rápidamente en las dimensiones informativa y humana pondrá a prueba la capacidad del Ejército para lograr la ventaja informativa en las LSCO.

Ventaja informativa

La capacidad de influir en las dimensiones informativa y humana ya no se limita a las naciones poderosas y a las organizaciones de noticias tradicionales.

Los adversarios de Estados Unidos están desarrollando métodos para utilizar capacidades emergentes como los deepfakes o los contenidos multimedia sintéticos (fotos, vídeos o clips de audio que han sido manipulados digitalmente o fabricados íntegramente para engañar) con el fin de desafiar la capacidad del Ejército de Estados Unidos para obtener y mantener información y ventaja humana dentro y fuera del campo de batalla. En LSCO, es probable que las redes de información sean objetivos críticos en los que un solo ataque pueda tener efectos desmesurados sobre la capacidad de las fuerzas armadas para acceder a la información y tomar decisiones. A medida que los adversarios buscan métodos modernos para aumentar su información y mejorar los procesos de toma de decisiones, también es probable que se encuentren cada vez más vulnerables a la influencia.

China reconoce que la información y el ámbito cognitivo serán clave en cualquier conflicto, y su búsqueda del dominio en las dimensiones de la información y los recursos humanos es una parte integral de su enfoque de la guerra. Las operaciones del ámbito cognitivo de China tienen como objetivo aprovechar la tecnología de la información avanzada y los sistemas de comunicaciones para obtener ventajas operativas y facilitar las operaciones psicológicas con el fin de manipular la forma en que un adversario recibe y procesa la información. El EPL busca evolucionar la guerra informatizada hacia una guerra inteligente, cuyo objetivo es integrar la IA y otras tecnologías emergentes para aumentar las capacidades de procesamiento de la información, acelerar la toma de decisiones, facilitar el uso de enjambres y ayudar a las operaciones en el ámbito cognitivo.

China pondrá en práctica estos conceptos atacando redes centralizadas para ralentizar o detener el flujo de información; combinando efectos físicos y psicológicos; y dirigiéndose a individuos con narrativas propagandísticas basadas en intereses, demografía, región o nación.

El pensamiento militar ruso hace hincapié en que las operaciones informativas, psicológicas y cognitivas pueden abarcar distintos ámbitos y son un aspecto esencial de la guerra híbrida. Las operaciones informativas y técnicas rusas buscan manipular o destruir los sistemas y redes de información, mientras que las operaciones de confrontación informativa y psicológica se centran en la toma de decisiones y la percepción del adversario. Durante los conflictos, ambas formas de guerra informativa se utilizan para confundir al enemigo y obtener ventajas estratégicas con un coste mínimo. A lo largo del conflicto de Rusia con Ucrania, ha llevado a cabo amplias campañas de influencia dirigidas tanto a Ucrania como a sus aliados occidentales. A medida que la conectividad y la tecnología sigan mejorando, es probable que Rusia perfeccione sus técnicas para utilizar operaciones que afecten a los sistemas y redes de información, así como para elaborar narrativas que influyan en la percepción de los públicos objetivo.

Armas de destrucción masiva

La amenaza de armas de destrucción masiva más probable a la que se enfrentarán los combatientes en la zona de operaciones es la de las armas químicas. Las Fuerzas Armadas de Ucrania han registrado miles de casos de uso de municiones que contienen sustancias químicas tóxicas por parte de las fuerzas rusas, incluyendo más de 750 casos en un solo mes. El Estado Mayor de las Fuerzas Armadas de Ucrania informa de que Rusia ha utilizado con mayor frecuencia granadas llenas de agentes antidisturbios lanzadas desde UAS. Además de los agentes antidisturbios, las fuerzas rusas han utilizado cloropicrina, una sustancia química cuyo uso en la guerra está prohibido por la Convención sobre Armas Químicas (CAQ). Los objetivos tácticos de Rusia al emplear estos agentes químicos son reducir la eficacia de las tropas en posiciones defensivas confinadas y expulsarlas de sus posiciones defensivas para exponerlas al fuego.

Aparte de su uso táctico en Ucrania, en los últimos años Rusia ha utilizado armas químicas al menos en dos ocasiones en intentos de asesinato, mantiene un programa de armas químicas no declarado y incumple sus obligaciones en virtud de la Convención sobre Armas Químicas (CAQ). Rusia tampoco ha cumplido sus obligaciones en virtud de la Convención sobre Armas Biológicas (CAB) de desmantelar su programa de guerra biológica. Desde el punto de vista nuclear, el arsenal de Rusia incluye casi 6000 ojivas nucleares estratégicas y no estratégicas, tres cuartas partes de las cuales probablemente estén operativas. Además, Rusia ha estado trabajando para modernizar sus fuerzas nucleares mediante el desarrollo de misiles hipersónicos y vehículos planeadores, misiles de crucero de propulsión nuclear, sistemas submarinos autónomos y misiles balísticos intercontinentales (ICBM) con capacidad para ojivas múltiples.

Aunque China es signataria de la CAQ, científicos de un instituto de investigación militar chino han expresado su interés en las aplicaciones militares de agentes farmacéuticos, como el fentanilo. A pesar de su participación en la CAB, China sigue desarrollando su infraestructura biotecnológica y buscando la cooperación científica con países que son motivo de preocupación. Los estudios realizados en instituciones médicas militares chinas abordan la identificación, el análisis y la caracterización de diversas familias de potentes toxinas con aplicaciones de doble uso. Además, China está ampliando y modernizando su arsenal nuclear. Para 2033, China probablemente contará con más de 1000 ojivas nucleares, capacidad para patrullas submarinas con misiles balísticos persistentes, bombarderos nucleares especializados y cientos de instalaciones reforzadas para misiles balísticos intercontinentales.

Es probable que tanto Rusia como China consideren el uso de armas de destrucción masiva como una ventaja asimétrica que les ayude a superar sus debilidades percibidas, al tiempo que tiene un impacto desmesurado en las operaciones estadounidenses. Es probable que los futuros conflictos LSCO impliquen el uso de armas químicas en el campo de batalla, y es probable que aumente la amenaza del uso de armas biológicas y nucleares.



Los adversarios consideran que las armas de destrucción masiva constituyen una ventaja asimétrica que tiene un impacto desmesurado en las operaciones estadounidenses y es probable que intenten emplearlas en LSCO.



Es probable que el LSCO exija a los combatientes que comprendan la dicotomía entre el arte y la ciencia de la guerra para lograr un equilibrio que aproveche al máximo las vulnerabilidades del adversario y minimice sus puntos fuertes.

LSCO

Implicaciones

El arte frente a la ciencia de la guerra

El esfuerzo de modernización militar de China se propone transformar sus fuerzas armadas en unas que adopten la ciencia de la guerra, como lo demuestra la doctrina del Ejército Popular de Liberación (EPL) sobre la guerra informatizada e inteligente. La guerra informatizada sugiere que China cree que obtener ventaja en materia de información es un componente necesario para la victoria. La guerra inteligente demuestra la importancia que China concede a la integración de la inteligencia artificial en su toma de decisiones militares con el fin de alcanzar el dominio decisorio en todos los aspectos de la guerra. Los dirigentes chinos están preocupados por la corrupción dentro de las filas del EPL, especialmente en los niveles inferiores, y, en la medida de lo posible, quieren eliminar al soldado individual del proceso de toma de decisiones en favor de una orientación impulsada por máquinas.

Esto contrasta radicalmente con la forma de guerrear del Ejército de los Estados Unidos, que se basa en gran medida en la guerra como una forma de arte. El Ejército de los Estados Unidos considera que sus soldados son su mayor ventaja en la batalla y confía en su intuición, improvisación y adaptación para alcanzar la victoria. La autoridad para tomar decisiones se delega a menudo a los niveles inferiores, como lo demuestra el énfasis que se pone en cultivar un cuerpo de suboficiales fuerte en el Ejército de los Estados Unidos.

Para muchos otros adversarios, la aplicación del arte y la ciencia de la guerra es más situacional, impulsada por el OE. Por ejemplo, un adversario que generalmente enfatiza el arte de la guerra puede ser propenso a dar más importancia a la ciencia en un entorno en el que hay más transparencia y, por lo tanto, una menor capacidad para engañar, lograr la sorpresa o emplear tácticas asimétricas.

Para el Ejército de los Estados Unidos, comprender esta dicotomía ayudará a inculcar la empatía estratégica y evitar la proyección especular. Una descripción precisa de las fortalezas y debilidades del enemigo, junto con una comprensión profunda de sus tendencias y formas preferidas de guerra, será vital para el éxito en el campo de batalla.

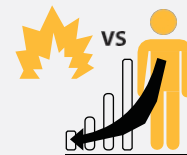
Aniquilación frente a desgaste como objetivos de LSCO

A lo largo de la historia, los beligerantes casi siempre han buscado una aniquilación rápida y decisiva para poner fin a un conflicto con éxito. Esto se ha logrado principalmente mediante la sorpresa y el uso abrumador de la fuerza, lo que presenta al oponente un *hecho consumado* y minan su voluntad de luchar. Sin embargo, la aniquilación rápida en las fases iniciales de una guerra es poco probable en un conflicto LSCO con un adversario casi igual que opera en su periferia. Tal escenario conduciría a un conflicto prolongado que podría poner a prueba todas las facetas del poder nacional.

La capacidad del Ejército de los Estados Unidos para reparar, regenerar o reemplazar grandes cantidades de material mientras participa activamente en la lucha será fundamental para ganar un conflicto prolongado y a gran escala. Es probable que haya poco tiempo y capacidad para transportar grandes cantidades de material dañado a las zonas de retaguardia o al territorio nacional para su reparación. Aunque la capacidad de poner rápidamente en funcionamiento los almacenes de guerra probablemente compensará en cierta medida el desgaste, las unidades desplegadas en un teatro de operaciones avanzado podrían ver sus capacidades materiales mermadas a un ritmo muy superior a la producción de la base industrial de defensa estadounidense. Incluso si la industria puede mantener el ritmo, es probable que el Ejército tenga que hacer frente a las necesidades de formación de los nuevos soldados y líderes para que aprendan estos sistemas en combate.

Es probable que los conflictos relacionados con el cambio climático obliguen a volver a la movilización de toda la sociedad que se dio en la era industrial. Los posibles adversarios de Estados Unidos plantearán desafíos únicos al intentar lograr una victoria rápida. Por ello, pueden ser necesarias diferentes estrategias para resistir y derrotarlos.

. Si bien tanto Rusia como Ucrania han trabajado para estimular la producción tradicional de defensa, cada una de ellas también ha aprovechado a desarrolladores independientes, pequeñas empresas y productos comerciales listos para usar que actúan como multiplicadores de fuerza y compensan las pérdidas de material. Ambas partes han incorporado rápidamente sistemas de bajo costo, fáciles de fabricar o listos para usar que son cada vez más capaces de dañar o destruir plataformas de gran valor y sofisticación.



Los costes humanos y materiales de la LSCO sugieren que los combatientes se benefician de una comprensión clara de cómo ven la aniquilación frente al desgaste como objetivo de una LSCO antes de que comiencen las hostilidades.



El aumento de la transparencia, la letalidad y los retos para el movimiento en LSCO pueden requerir una reevaluación de nuestro enfoque de la maniobra, los incendios y la protección.

Maniobras, fuego y protección

El aumento de la letalidad y la transparencia del campo de batalla, junto con el carácter cada vez más global de la guerra, pueden requerir una reevaluación del enfoque del Ejército respecto a funciones de combate como las maniobras, los disparos y la protección. Los ejemplos contemporáneos de LSCO sugieren nuevas formas de localizar, fijar y acabar. Rusia y Ucrania están proporcionando ejemplos de disparos como pieza central de la capacidad de ataque y defensa de sus ejércitos.

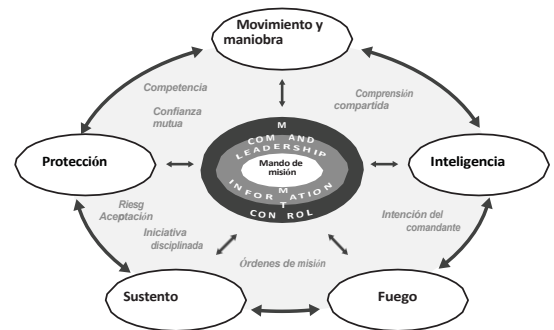


Figura 5: Las LSCO pueden requerir que el Ejército de los Estados Unidos reexamine la interacción de los procesos actuales de mando y control.

En ese conflicto, los incendios han sido la principal causa de víctimas mortales.

Los incendios se han vuelto más letales y eficaces gracias a los nuevos sistemas y tecnologías que amplían su alcance y mejoran su precisión. El GPS ha mejorado la precisión de las municiones y los puntos de disparo. La detección en el campo de batalla, los incendios de largo alcance y las capacidades de posicionamiento, navegación y sincronización han permitido una capacidad de ataque más rápida y precisa. Como resultado, también ha aumentado la amenaza de la contraartillería. Los incendios deben poder mantenerse móviles y dispersarse rápidamente para evitar el contraataque. Se requiere un movimiento constante y es necesario ocultar los planes para evitar ser detectados o seguidos por ISR.

Es probable que las condiciones actuales de la OE afecten a la capacidad del Ejército de los Estados Unidos para moverse, disparar y sobrevivir. Las formaciones de maniobra deberán ser metódicas para garantizar que no sean descubiertas antes de llegar al combate, pero también deberán ser rápidas y decisivas para evitar ser detectadas por el ISR. Para sobrevivir a los disparos y a la contrabatería se requieren tácticas, técnicas y procedimientos (TTP) eficaces combinados

con personal altamente capacitado, disciplinado y fuerzas organizadas. Las complejas barreras de obstáculos en capas con campos de minas mixtos vigilados por fuego complican enormemente las ya peligrosas operaciones de brecha. La protección requerirá que las capacidades de los sistemas en desarrollo sean más móviles, ágiles y letales, al tiempo que emitan menos señales.

Las personas son la ventaja

El Ejército de los Estados Unidos se enorgullece de su capacidad para reclutar, entrenar y desarrollar de manera eficaz soldados y líderes de talla mundial con el fin de mantener una ventaja en términos de personal. Es probable que el reto de las incorporaciones al Ejército ponga a prueba la capacidad del Ejército de los Estados Unidos para generar fuerzas y reconstituir la mano de obra en caso de un conflicto LSCO prolongado y de alta intensidad con un coste humano significativo. Para reconstituir suficientemente las formaciones, los ejércitos tendrán que preparar y movilizar rápidamente toda la fuerza y regenerar la mano de obra antes y durante la hora de necesidad.

Es probable que nuestro reto de reclutamiento se mantenga como una cuestión de seguridad nacional. Se ha producido un descenso constante en las incorporaciones al Ejército de los Estados Unidos en los últimos años; para 2034, habrá aún menos personas disponibles, aptas y físicamente accesibles para el reclutamiento. La generación más joven utiliza la tecnología a una edad mucho más temprana, lo que conforma su

percepciones del Ejército de los Estados Unidos en un entorno virtual segmentado que seguirá siendo cada vez más inmersivo. Es casi seguro que aumentará la competencia del Ejército de los Estados Unidos con la industria privada por el talento, que ofrece una mayor remuneración y otras ventajas.

La guerra entre Rusia y Ucrania ilustra que las tasas de desgaste en los conflictos prolongados probablemente superarán las estimaciones de bajas previas al conflicto, reduciendo las formaciones preexistentes —en particular las que cuentan con más entrenamiento y experiencia— por debajo del nivel de preparación para el combate. Podría resultar fundamental sustituir unidades completas o reforzar eficazmente otras unidades en función de las necesidades y funciones. En LSCO, la lucha en el teatro de operaciones solo será una parte del conflicto. Para luchar y ganar probablemente se necesitará la capacidad de mantener una fuerza competente en múltiples teatros de operaciones y en el territorio nacional simultáneamente.



Las personas son la ventaja de LSCO, y el Ejército de los Estados Unidos necesitará mantener su superioridad en reclutar, entrenar y desarrollar de manera eficaz soldados y líderes de clase mundial.

Rusia no estaba preparada para la magnitud de las pérdidas de tropas en Ucrania

Al comienzo de la invasión de Ucrania en 2022, las Fuerzas Armadas rusas carecían de suficiente personal para un conflicto prolongado y a gran escala. Durante un período de un año, las Fuerzas Armadas rusas sufrieron entre 40 000 y 55 000 bajas mortales y 78 000 soldados heridos de forma permanente, con un promedio de 400 bajas al día. Los oficiales subalternos y las unidades altamente entrenadas, incluidas las Spetsnaz y las aerotransportadas, se encontraban entre las fuerzas rusas más diezmadas entre la primavera y el otoño de 2022. Para satisfacer las necesidades inmediatas de mano de obra, los estándares de reclutamiento, los requisitos y los plazos de entrenamiento rusos han disminuido constantemente desde que comenzó la invasión. El entrenamiento ruso también se ha visto afectado por el agotamiento del personal de entrenamiento que presta servicio en las unidades de combate. Las Fuerzas Armadas rusas, aunque capaces de adquirir continuamente nuevas tropas, son ahora un «ejército masivo de baja calidad y alta cantidad», en palabras del Ministerio de Defensa británico.



Figura 6. Cadetes del EPL recibiendo instrucción política como parte de la intención de China de profesionalizar mejor su ejército.

Fuente: Informe sobre el poder militar de China de 2019 de la Agencia de Inteligencia de Defensa, https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf

El EPL reconoce la importancia de la dimensión humana en las operaciones militares y está profesionalizando su cuerpo de oficiales y suboficiales en consecuencia. En el caso de los oficiales, está desarrollando y reforzando las cualidades de liderazgo, entre las que se incluyen la lealtad política al Partido Comunista Chino, la conciencia estratégica, la destreza en asuntos militares, la adhesión a la cultura militar, la capacidad de adaptación y otros aspectos intangibles. Para mejorar sus suboficiales, el EPL ha establecido dos tipos diferentes de suboficiales. Los primeros se ocupan de las tareas tradicionales de liderazgo de los suboficiales, mientras que los segundos son expertos técnicos con experiencia en ingeniería, tecnología de la información y ciencia de datos.

Adaptación rápida

Para obtener ventajas competitivas en LSCO es necesario adaptar de forma rápida y continua las organizaciones, la tecnología y las tácticas con el fin de aprovechar oportunidades fugaces. Para lograrlo, los líderes deben esforzarse por alcanzar una flexibilidad orgánica, aprendiendo y adaptándose constantemente, adoptando innovaciones y superando la resistencia institucional inherente al cambio. Los líderes también deben sincronizar deliberadamente las adaptaciones y comprender que estas producen efectos fugaces, ya que el oponente inevitablemente se adaptará en respuesta.

Al principio de la invasión, Rusia relegó los UAS al apoyo de los complejos de fuego de reconocimiento, con un número limitado de UAS Orlan-10 ISR que proporcionaban apoyo para la localización de objetivos. Sin embargo, los civiles ucranianos se unieron a las Fuerzas Armadas de Ucrania para adaptar rápidamente los UAS comerciales al apoyo de las operaciones de combate,

innovando con capacidades ad hoc y expedientes sobre el terreno para localizar y atacar a las fuerzas rusas. Desde entonces, la proliferación de UAS ISR, repetidores, OWA, de ataque superior y FPV en ambos bandos ha dado lugar a constelaciones de drones que operan sobre y detrás de las líneas del frente.

Las crecientes bajas en combate causadas por los disparos de artillería dirigidos por UAS y los ataques de precisión con UAS FPV obligaron a algunas unidades rusas a adaptar sus tácticas, técnicas y procedimientos (TTP) de infantería, pasando de asaltos blindados montados a asaltos desmontados «en oleadas humanas» con Storm-Z contra las defensas ucranianas atrincheradas. Algunas unidades aerotransportadas y de fusileros motorizados rusas han demostrado una tasa de adaptación e innovación táctica relativamente acelerada en comparación con otras unidades rusas, incluida la voluntad de aprender de las mejores prácticas exhibidas por las empresas militares privadas rusas.



El combatiente en LSCO que haga de la rápida adaptación una parte fundamental de su enfoque de la guerra estará en mejores condiciones de aprovechar las oportunidades fugaces en el campo de batalla.

Adaptaciones rápidas del empleo de UAS en Campos de batalla contemporáneos

Los conflictos de Nagorno-Karabaj y Ucrania ilustran la importancia de la rápida adaptación, concretamente en lo que respecta al uso de UAS, en la búsqueda de la ventaja en el campo de batalla del siglo XXI. Durante la Segunda Guerra de Nagorno-Karabaj, Azerbaiyán empleó biplanos An-2 «Colt» de la era soviética controlados a distancia para penetrar en el espacio aéreo armenio, lo que activó los radares de defensa aérea armenios y permitió a las fuerzas azerbaiyanas localizarlos, apuntarlos y suprimirlos rápidamente. Ucrania integró UAS, misiles de crucero lanzados desde el aire, misiles antibuque y embarcaciones no tripuladas para saturar las defensas rusas y atacar las principales defensas aéreas, aeródromos, puertos y puentes de la Crimea ocupada. Rusia y Ucrania han incorporado la fabricación aditiva y la realidad aumentada para transformar drones adquiridos comercialmente en PGM. Al carecer de las cadenas de suministro necesarias para mantener su equipo de 60 años de antigüedad, las unidades de apoyo técnico material rusas han empleado impresoras 3D para fabricar nuevas piezas cerca de la línea del frente en Ucrania, devolviendo rápidamente el equipo al combate.

El tractor Wagner Group y las Fuerzas Armadas de Ucrania. Las escuadras desmontadas de estas unidades, junto con sus vehículos de combate de infantería, maniobraron para proporcionar fuego de apoyo mutuo y explotaron el terreno de cerca, algo que no se vio en otras unidades rusas. La incapacidad de Rusia para adaptar y estandarizar las TTP en todas sus fuerzas subraya la

importancia de ser capaz de comprender, difundir e inculcar rápidamente la adaptación en LSCO para aprovechar las oportunidades tácticas.

China, observando la experiencia de Rusia en Ucrania, está incorporando las lecciones aprendidas al EPL. Esforzándose por construir un «sistema» militar superior

de sistemas», el EPL está transformando su educación y cultura militar profesional para formar líderes adaptables e innovadores. En concreto, el EPL quiere que sus líderes aprendan nuevos métodos militares de otros países, incorporen tecnologías futuras y sean más creativos.

Conclusión

Para prepararse para los escenarios de reemergencia de LSCO, el Ejército de los Estados Unidos necesita comprender las condiciones que más probablemente lo impulsarán, así como su impacto en las operaciones. Es probable que el OE de 2024-2034 se caracterice por 12 condiciones clave que darán forma a la LSCO y tendrán amplias implicaciones para el Ejército. Comprender la complejidad de estas condiciones e implicaciones impulsará las decisiones del Ejército sobre doctrina, entrenamiento de soldados y desarrollo de líderes para tener éxito en la guerra multidominio.

El Ejército puede esperar que la LSCO se caracterice por amenazas multidominio en un campo de batalla cada vez más transparente y letal en múltiples teatros. Nuestros adversarios aprovecharán la democratización de la tecnología y los avances en los sistemas robóticos y cibernéticos para enfrentarse al Ejército de los Estados Unidos en todos los ámbitos: tierra, aire, mar, espacio y ciberespacio. Las áreas que el Ejército consideraba antes seguras o garantizadas, como el territorio nacional, la logística, la superioridad aérea, el control marítimo y el acceso al teatro de operaciones, ya no podrán darse por sentadas. El Ejército tendrá que luchar a largas distancias para proporcionar protección, tiempo y recursos para mantener la LSCO. El papel cada vez más importante de la información, los sistemas no tripulados y el posible empleo de armas de destrucción masiva aumentarán la complejidad de los conflictos armados. Los adversarios de Estados Unidos desafiarán continuamente la capacidad del Ejército de Estados Unidos para obtener y mantener la ventaja informativa en

y fuera del campo de batalla. Los sistemas no tripulados, cada vez más económicos y ampliamente disponibles, proporcionarán a los adversarios una serie de capacidades, desde la localización de objetivos ISR hasta el apoyo a operaciones urbanas y subterráneas.

Para alcanzar la victoria, el Ejército de los Estados Unidos debe conocer al enemigo. Conocer al enemigo comienza con la OE.

Nuestra amenaza principal, China, busca transformarse de una fuerza centrada en la defensa territorial a un ejército moderno, inteligente y con capacidad conjunta, capaz de derrotar a la Fuerza Conjunta de los Estados Unidos en LSCO. El EPL está haciendo esto a través de la modernización militar en todas las partes del marco DOTMLPF-P del ejército estadounidense. La amenaza aguda, Rusia, ve a Estados Unidos y a la OTAN como sus enemigos eternos, especialmente dada la respuesta de Occidente al conflicto en Ucrania y la expansión de la OTAN a lo largo de la periferia de Rusia. Para hacer frente a esta amenaza percibida, y basándose en las lecciones aprendidas en Ucrania, Rusia mantendrá su enfoque en una fuerza masiva centrada en el fuego, capaz de llevar a cabo una LSCO prolongada y desgastante, con una guerra de información para la que cree que las democracias occidentales no están preparadas. Las amenazas persistentes de los actores regionales y las organizaciones extremistas violentas seguirán añadiendo complejidad a las operaciones del Ejército, desafiando nuestras fortalezas y explotando nuestras vulnerabilidades cuando y donde puedan. Para estar preparados para una serie de misiones operativas, incluida la LSCO, nuestros soldados y

Los líderes deberán estar preparados para pensar y adaptarse rápidamente a las condiciones cambiantes para mantener la superioridad. Esta OE establece las condiciones básicas para mantener la preparación, entrenar y operar contra todo tipo de enemigos, y lograr la victoria en el campo de batalla.



Apéndice

Condiciones de LSCO



Competencia y guerra en todos los ámbitos:

Las LSCO se caracterizarán por la competencia y la guerra en todos los ámbitos, ya que la competencia y los conflictos se extienden más allá de las batallas físicas e implican cada vez más múltiples ámbitos y dimensiones interconectados.



Masa frente a precisión: La masa y la precisión se complementan entre sí en LSCO, y los combatientes deberán identificar la combinación adecuada de estos factores para obtener ventajas.



Proliferación de sistemas no tripulados: El aumento en la producción, el empleo y el éxito de los sistemas no tripulados significa que el Ejército puede esperar encontrarse con estos sistemas en toda la extensión y profundidad de la LSCO.



Profundidad y alcance de los depósitos: La LSCO requerirá disparar y mantener cantidades masivas de municiones contra adversarios que probablemente disfruten de la ventaja inicial de las líneas interiores, lo que supondrá un reto para la profundidad y el alcance de los depósitos del Ejército.



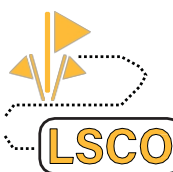
Campo de batalla transparente: El LSCO se caracterizará por la democratización y proliferación de tecnologías avanzadas y comunicaciones globales hiperconectadas, lo que creará un campo de batalla cada vez más transparente en el que será difícil esconderse del enemigo.



Mayor letalidad: El LSCO será cada vez más letal debido a la intersección de la ubicuidad de los sensores, la automatización del campo de batalla, los ataques de precisión y los fuegos masivos.



Denegación de acceso/área: En LSCO, las fuerzas estadounidenses se enfrentarán a los esfuerzos de denegación de acceso/área de los adversarios, centrados en impedir nuestro despliegue en el teatro de operaciones y en impedir nuestra libertad de acción una vez desplegados.



Logística disputada: El aumento de los requisitos logísticos de LSCO supondrá un reto para las operaciones de sostenimiento del Ejército, y los adversarios atacarán esas mismas operaciones desde el territorio nacional hasta el campo de batalla.



Defensa nacional: El LSCO contará con requisitos de defensa nacional, ya que los adversarios dispondrán de capacidades convencionales, híbridas e irregulares para llevar a cabo operaciones contra el territorio nacional.



Guerra urbana intensa: Un entorno operativo cada vez más urbano significa que la LSCO incluirá la guerra urbana intensa en entornos con condiciones de combate difíciles.



Ventaja informativa: La capacidad de los adversarios para influir rápidamente en la información y en las dimensiones humanas pondrá a prueba la capacidad del Ejército para lograr una ventaja informativa en el LSCO.



Armas de destrucción masiva: Los adversarios consideran que las armas de destrucción masiva constituyen una ventaja asimétrica que tiene un impacto desmesurado en las operaciones estadounidenses y es probable que intenten emplearlas en LSCO.

Implicaciones para las LSCO



El arte frente a la ciencia de la guerra: Es probable que la LSCO exija a los combatientes que comprendan la dicotomía entre el arte y la ciencia de la guerra para lograr un equilibrio que aproveche al máximo las vulnerabilidades del adversario y minimice sus puntos fuertes.



Las personas son la ventaja: Las personas son la ventaja en LSCO, y el Ejército de los Estados Unidos deberá mantener su superioridad en el reclutamiento, entrenamiento y desarrollo eficaz de soldados y líderes de clase mundial.



Aniquilación frente a desgaste: Los costes humanos y materiales de la LSCO sugieren que los combatientes se beneficiarán de una comprensión clara de cómo ven la aniquilación frente al desgaste como objetivo de la LSCO antes de que comiencen las hostilidades.

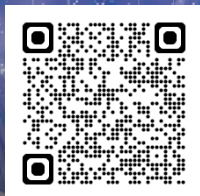


Adaptación rápida: El combatiente en la LSCO que haga de la adaptación rápida una parte fundamental de su enfoque de la guerra estará en mejores condiciones de aprovechar las oportunidades fugaces en el campo de batalla.



Maniobras, disparos y protección: El aumento de la transparencia, la letalidad y las dificultades para desplazarse en LSCO pueden requerir una reevaluación de nuestro enfoque respecto a las maniobras, los disparos y la protección.

Dejado en blanco intencionadamente



Resumen del entorno operativo



Panorama estratégico y problemas que el enemigo plantea y que deben resolverse

China como amenaza creciente; Rusia, Irán, Corea del Norte, VEO/TCO persistentes; potencial de colusión

- 1. Guerra de sistemas/destrucción de sistemas:** los adversarios atacan el C2, el ISR y los fuegos para interrumpir/destruir la toma de decisiones de EE. UU., sus aliados y socios
- 2. RSOI disputado:** los adversarios y sus representantes están desarrollando capacidades cada vez mayores para interrumpir las operaciones de fortaleza a puerto
- 3. Mayor letalidad:** la masa y la precisión en todos los ámbitos hacen que la protección sea cada vez más difícil en un campo de batalla altamente transparente y automatizado
- 4. Logística disputada:** los adversarios utilizarán ataques antiacceso/denegación de área, cibernéticos y asimétricos para atacar el sostenimiento desde el territorio nacional hasta el campo de batalla
- 5. Superioridad del adversario en el ámbito cognitivo:** influencia generalizada, desinformación y operaciones de información contra EE. UU., sus aliados y socios antes, durante y después de las operaciones cinéticas.
- 6. Otras amenazas para el territorio nacional:** amenazas cinéticas y no cinéticas para las infraestructuras críticas (militares/civiles) y la industria.
- 7. Uso químico, biológico, radiactivo y nuclear:** los adversarios amplían las amenazas y capacidades, al tiempo que reducen el umbral para su uso como elemento disuasorio.



Los adversarios explotarán sistemáticamente las vulnerabilidades para ampliar sus capacidades de ataque en todo el teatro de operaciones, incluida la patria