

En su objetivo común de reducir la dependencia de proveedores militares y digitales extranjeros, Irán y los países del Golfo aplican estrategias divergentes que están reconfigurando la región.

Sara Bazoobandi es investigadora del Instituto de Política de Seguridad de la Universidad de Kiel.

SOBERANÍA TECNOLÓGICA Y GEOPOLÍTICA DEL GOLFO

La región del golfo Pérsico está experimentando una profunda transformación en la forma en que sus gobiernos conciben, construyen y despliegan el conocimiento. En toda la región, los Estados han tomado medidas agresivas para reducir la dependencia del extranjero y desarrollar capacidades propias. Sin embargo, los caminos que han elegido difieren notablemente, y esas diferencias conllevan consecuencias estratégicas que se extienden mucho más allá de la región.

Dos ámbitos ocupan el centro de esta transformación: la defensa y el ciberespacio. No se trata de elecciones fortuitas. La soberanía tecnológica se define como la capacidad de un Estado para desarrollar, controlar y mantener tecnologías críticas de forma independiente. La capacidad de producir los sistemas que protegen al Estado, proyectan su poder y señalan sus ambiciones tanto a aliados como a adversarios es a la vez la medida más clara de esa soberanía y su facilitador más trascendental. En conjunto, estos dos ámbitos definen la relación del Estado con el conocimiento, cómo se organiza, controla y utiliza como arma.

Arabia Saudí y Emiratos Árabes Unidos han impulsado el desarrollo del

conocimiento en ambos ámbitos mediante el poder financiero, las alianzas internacionales y ambiciosos programas nacionales. Irán ha tomado una ruta fundamentalmente diferente: una basada no en el acceso al mercado o en estructuras de alianzas, sino en una doctrina ideológica que enmarca el conocimiento en sí mismo como un arma del Estado.

CAMINOS DIVERGENTES HACIA LA SOBERANÍA TECNOLÓGICA

Como se ha indicado, las potencias de la región comparten una ambición común: reducir la dependencia de proveedores militares y digitales extranjeros. Pero las estrategias mediante las cuales persiguen esa ambición muestran relaciones fundamentalmente diferentes entre el Estado, el conocimiento y la tecnología.

Arabia Saudí y EAU representan un modelo de modernización impulsada por los recursos. El grupo EDGE de Emiratos Árabes Unidos, formado en 2019 mediante la fusión de múltiples entidades de defensa de propiedad estatal, ha localizado la mayor parte de su cartera de productos en la fabricación nacional y ha desarrollado importantes capacidades en materia de armas autó-

nomas, incluidas municiones de vuelo estacionario guiadas por Inteligencia Artificial (IA). La SAMI de Arabia Saudí, puesta en marcha en 2017 en el marco de la Visión 2030, ha pasado de la nada a convertirse en una empresa de escala mundial en pocos años, al buscar acuerdos de transferencia de tecnología con socios que van desde compañías turcas como Baykar y ASELSAN hasta las estadounidenses Lockheed Martin y Boeing. Ambos Estados del Golfo también han asumido compromisos extraordinarios con la IA. En los últimos años, Arabia Saudí ha destinado cientos de miles de millones de dólares a infraestructuras de IA, y EAU ha anunciado planes de inversión de una magnitud similar. Se trata de Estados que compran y avanzan hacia la relevancia tecnológica, con el desarrollo paralelo de la economía de la innovación civil y el sector de la defensa.

El enfoque de Irán es categóricamente diferente. Aislado de los mercados tecnológicos occidentales por décadas de sanciones, y moldeado por una ideología revolucionaria que considera la dependencia extranjera como una vulnerabilidad estratégica y un fracaso moral, Irán desarrolló una doctrina

de autosuficiencia tecnológica con un carácter teológico que no se encuentra en ningún otro lugar de la región. Comprender esa doctrina es esencial para entender todo lo que el Estado iraní construyó posteriormente.

LA PRODUCCIÓN DE CONOCIMIENTO EN IRÁN: UN DEBER SAGRADO

El enfoque de Irán respecto a la ciencia y la tecnología desde los primeros años de la República Islámica se rige por una afirmación ideológica sobre el significado del conocimiento y su relación con la soberanía política. El concepto de "yihad del conocimiento", desarrollado bajo el mandato del difunto líder supremo, el ayatolá Alí Jameneí, sostiene que el desarrollo científico de la nación es un imperativo religioso, y que la dependencia de la tecnología extranjera es una forma de subyugación incompatible con el proyecto revolucionario. En este marco, el científico y el soldado ocupan roles equivalentes: ambos participan en la defensa de la revolución frente a enemigos externos, y ambos están sujetos a las mismas obligaciones de lealtad y sacrificio.

Las implicaciones prácticas de este concepto para la estructura de las instituciones científicas y tecnológicas de Irán han sido profundas y, en gran medida, negativas para el desarrollo general del país. Cuando las convicciones ideológicas y la lealtad al Estado revolucionario se convierten en un requisito previo para participar en el sector del conocimiento, las consecuencias se propagan de una forma difícil de contener. Las agendas de investigación se configuran en función de las prioridades de seguridad más que de las oportunidades científicas. Las instituciones que podrían servir como fuentes de retroalimentación crítica —universidades, asociaciones profesionales, centros de investigación independientes— se transforman, en cambio, en instrumentos de los objetivos estatales, y su independencia se ve restringida sistemáticamente. El resultado es un sector del conocimiento coherente ideológicamente y dirigido estratégicamente, pero que ha sacrificado la diversidad intelectual y la contestación interna de las que depende la verdadera innovación.

Este sistema ha garantizado que las prioridades de seguridad se reflejen no solo en lo que se financia, sino también en cómo se organizan las instituciones

Según el concepto de 'yihad del conocimiento' iraní, el desarrollo científico de la nación es un imperativo religioso, y la dependencia de la tecnología extranjera es una forma de subyugación incompatible con el proyecto revolucionario

y a quién se le permite ascender dentro de ellas. El efecto ha sido militarizar la economía del conocimiento iraní desde dentro, al crear un sistema en el que el desarrollo tecnológico más trascendental se produce bajo supervisión militar y de acuerdo con los objetivos del aparato de seguridad.

Los resultados de este sistema son visibles. A nivel nacional, la misma maquinaria institucional ha producido la infraestructura de vigilancia, filtrado y control que el régimen utiliza para gestionar a su propia población. No se trata de proyectos separados que se desarrollan en paralelo, sino de expresiones de la doctrina aplicada en diferentes ámbitos. La dimensión de proyección de poder exterior del sector del conocimiento, reclutado para servir a las ambiciones estratégicas del Estado, se manifiesta en el programa de drones de Irán, que le permite suministrar tecnología de drones a grupos aliados y fuerzas *proxies* en múltiples zonas de conflicto, en su programa de misiles balísticos y en sus crecientes capacidades cibernéticas.

LA CONSTRUCCIÓN DE UNA JAULA DIGITAL INTERNA

La infraestructura de control de Internet de Irán representa uno de los sistemas más avanzados de su tipo. Esto no se debe a que ningún componente concreto sea excepcionalmente sofisticado, sino a que los componentes se han ensamblado siguiendo una lógica estratégica clara y coherente. Esa lógica no consiste en bloquear contenidos específicos, aunque el bloqueo de contenidos forma parte de ella. Se trata de construir un sistema en el que el Estado conserve, en todo momento, la capacidad de determinar qué se puede y qué no se puede comunicar, quién puede hacerlo y a quién, y en el que las herramientas a disposición de los ciudadanos que intentan eludir ese control sean neutralizadas sistemáticamente.

Esto se consigue mediante una estructura con varios niveles de apoyo. Múltiples mecanismos técnicos independientes manipulan cómo se asignan las direcciones de Internet, cómo se gestionan los datos en tránsito y cómo se estructuran o prohíben los diferentes tipos de tráfico de Internet. Detrás de todo esto hay también una estructura que concentra todo el tráfico internacional de Internet a través de una única entidad estatal. Este diseño otorga al gobierno una capacidad de la que carecen la mayoría de los sistemas de censura. Es decir, la capacidad de implementar cambios de manera uniforme e instantánea para todos los usuarios del país simultáneamente, sin depender de la cooperación o el cumplimiento de múltiples operadores independientes.

Además de su infraestructura de filtrado externo, Irán ha invertido durante muchos años en la construcción de una red nacional paralela: un conjunto de servicios alojados localmente diseñados para sustituir a las plataformas internacionales que están bloqueadas o sujetas a interrupciones (por ejemplo, aplicaciones de mensajería, sistemas de pago en línea, aplicaciones de transporte compartido). China ha sido el contribuyente externo más importante a este proyecto, al proporcionar tanto los sistemas técnicos como los conocimientos institucionales acumulados a través de su propia experiencia en la gestión de una red nacional de Internet a gran escala. La relación se basa en una colaboración estratégica formal a largo plazo entre los dos gobiernos y ha implicado importantes transferencias financieras de Irán a los proveedores de tecnología chinos.

La red nacional se promociona dentro de Irán utilizando el discurso de la soberanía cultural y la compatibilidad religiosa, pero su importancia operativa es estratégica más que cultural. Proporciona un nivel mínimo de funcionalidad



Tras las protestas de enero, el régimen cortó el acceso a Internet, un medio de controlar la información con mayor facilidad. Teherán, enero de 2026./FATEMEH BAHRAMI/ANADOLU VIA GETTY IMAGES

digital nacional que permanece disponible incluso cuando se interrumpe la conectividad externa, lo que significa que el régimen puede aislar a sus ciudadanos de la red global sin interrumpir la actividad económica y administrativa nacional de la que depende el propio gobierno. Esta capacidad ha reducido considerablemente el coste que supone para el Estado utilizar la conectividad como arma política.

El gobierno iraní ha utilizado repetidamente las interrupciones de Internet como herramienta de gestión política desde 2019, y la evolución de esas intervenciones refleja tanto un aprendizaje como una sofisticación creciente. El desarrollo de dicha capacidad técnica ha sido crucial para el régimen, no solo desde el punto de vista operativo, sino también político. Durante cualquier tipo de crisis interna, ya sea causada por un ataque extranjero o un levantamiento popular, los cortes de internet permiten al gobierno moldear la información con mayor facilidad. La ventaja estructural que esto genera se ve reforzada por el hecho de que los funcionarios del régimen, los medios de comunicación estatales y las comunicaciones gubernamentales pueden seguir funcionando plenamente durante cualquier interrupción. Esta provisión selectiva de acceso a Internet está proporcionando al Estado plataformas sin rival precisamente en los momentos en que las fuentes independientes serían, de otro modo, más valiosas.

EL CONOCIMIENTO, UNA HERRAMIENTA PARA LA PROYECCIÓN DE PODER EXTERIOR

Las capacidades que ha generado el enfoque tecnológico de Irán también permiten al gobierno proyectar su poder más allá de sus fronteras. En materia de tecnología de drones, desarrollo de misiles y operaciones cibernéticas ofensivas, el país ha logrado resultados significativos. Sin embargo, estos avances también han puesto de manifiesto vulnerabilidades dentro del sistema iraní, fuertemente impulsado por la ideología. Los sistemas diseñados dando prioridad al control tienden a ser frágiles, a diferencia de los sistemas diseñados dando prioridad a la resiliencia. Un sector tecnológico organizado en torno a prioridades militares ha ampliado su capacidad destructiva de una forma sin precedentes, sin llegar a demostrar, por el contrario, cualidades defensivas.

Los programas tecnológicos y de defensa de Arabia Saudí y EAU han supuesto una inversión y una colaboración sustanciales para la transferencia de tecnología. Tampoco han estado exentos de los retos que acompañan a las grandes iniciativas industriales dirigidas por el Estado. Ambos países están integrados en redes de colaboración internacional que contemplan formas de rendición de cuentas externa e intercambio de conocimientos ausentes en el modelo autónomo de Irán. Las relaciones que se construyen en torno

a tales colaboraciones tienen un doble propósito: son conductos de conocimiento técnico, pero también canales a través de los cuales los estándares de rendimiento, la presión competitiva y el escrutinio externo entran en el sistema. Como resultado, se genera en tales ecosistemas un mecanismo distribuido de corrección de errores que los programas nacionales cerrados, como el de Irán, simplemente no pueden replicar.

El valor de este modelo se está poniendo ahora a prueba en condiciones reales. Los conflictos en la región han puesto de manifiesto un marcado contraste: los sistemas del CCG, en particular el de EAU, han demostrado ser mucho más eficaces a la hora de proteger las infraestructuras críticas y la población civil que sus homólogos iraníes. La defensa aérea y antimisiles de Irán ha mostrado claros signos de colapso frente a la guerra moderna a la que se enfrenta ahora. Esta brecha no es meramente tecnológica. Evidencia las ventajas acumuladas de la colaboración abierta, el aprendizaje iterativo y la rendición de cuentas ante estándares externos a lo largo del tiempo.

La guerra con Irán ha puesto de manifiesto una marcada brecha entre la imagen que el régimen tiene de sí mismo como potencia tecnológicamente soberana y sus vulnerabilidades reales. Las capacidades ofensivas de Irán desplegaron un poder destructivo que, en líneas generales, se ajustó a lo esperado. Sus misiles, drones y redes de *proxies* demostraron un alcance real y la capacidad de amenazar la estabilidad regional. Pero los sistemas destinados a proteger al propio Estado fallaron. Las redes de inteligencia y vigilancia fueron infiltradas, lo que permitió a los adversarios localizar y eliminar a altos mandos con precisión. La doctrina del yihad del conocimiento produjo armas capaces de proyectar poder hacia el exterior. No pudo proteger a las personas que las construyeron.

EL CONOCIMIENTO BAJO FUEGO: LA CRISIS EN EL ESTRECHO DE ORMUZ

Las estrategias divergentes en materia de conocimiento entre Irán y el CCG han adquirido, desde febrero de 2026, una dimensión empírica muy marcada. Los ataques iraníes contra el CCG no solo pusieron a prueba las defensas aéreas de los Estados del Golfo, sino que también desafiaron todo el modelo del CCG de transformación económica impulsada

por la tecnología. Ese modelo se basa en una premisa fundamental: que los Estados del Golfo ofrecen algo escaso en la región en general –estabilidad política, seguridad física y gobernanza predecible. Es precisamente esta reputación la que los ha convertido en destinos atractivos para los gigantes tecnológicos, los fondos soberanos y las inversiones en infraestructura de IA. Los ataques con drones y misiles iraníes contra torres acristaladas y centros de datos en todo el CCG han sido diseñados deliberadamente por Teherán para cuestionar la credibilidad de esa premisa, junto con décadas de estrategia de diversificación en la región.

Los ataques iraníes también han puesto de manifiesto una vulnerabilidad estructural en todo el CCG, donde se han destinado cuantiosos gastos militares a la construcción de sistemas de defensa aérea sofisticados pero costosos. Los drones iraníes Shahed, desplegados en oleadas masivas, han obligado al CCG a emplear costosos interceptores contra sistemas de bajo coste. Teherán ha explotado deliberadamente esta asimetría, como una forma de desgaste estratégico. Dicha asimetría es una clara manifestación de la diferencia doctrinal entre las estrategias de desarrollo del conocimiento y la tecnología a ambos lados del golfo Pérsico.

Irán ha industrializado la producción de sistemas baratos y desechables a través de su "yihad del conocimiento", una doctrina que, independientemente de sus costes para el desarrollo científico en general, ha demostrado ser eficaz a la hora de generar capacidad destructiva masiva a gran escala. Los Estados del Golfo, por el contrario, siguen dependiendo de la compra de tecnología cara y fabricada en el extranjero, difícil de producir a nivel nacional y demasiado costosa para ser utilizada en el volumen que requieren las tácticas de saturación de Irán.

Otra dimensión estratégicamente relevante de los ataques iraníes contra el CCG es el hecho de que se dirigieran contra la infraestructura digital. Drones iraníes atacaron tres centros de datos de Amazon Web Services (dos en EAU y uno en Baréin), provocando interrupciones en los sistemas de *software* bancario y empresarial. Posteriormente, la Guardia Revolucionaria (IRGC) advirtió de que las empresas tecnológicas estadounidenses (por ejemplo, Microsoft, Google, Apple, Meta y Oracle) que operaran en el Golfo serían consideradas objetivos legítimos. Estos ataques ponen de mani-

fiesto la intención de Irán de dañar la arquitectura institucional que sustenta los planes de transformación económica impulsados por la tecnología de los Estados del Golfo. Se prevé que los ataques contra una infraestructura clave para el futuro económico de los Estados del Golfo afecten gravemente a la confianza de los inversores, lo que suscitará dudas entre las empresas tecnológicas y los socios soberanos cuyo compromiso continuado es indispensable para las ambiciones de diversificación de la región.

Sin embargo, la amenaza estructural más profunda podría ser aquella que aún no se ha materializado. Irán ha manifestado su intención de convertir en armas los cables submarinos que discurren bajo el estrecho de Ormuz, los cuales transportan un vasto tráfico de Internet y financiero entre Europa, Asia y el golfo Pérsico. La infraestructura de IA está especialmente expuesta, ya que los centros de datos del CCG dependen de las conexiones de baja latencia de los cables submarinos. Debido al conflicto en curso ya han paralizado las operaciones de reparación y mantenimiento de los cables submarinos en el golfo Pérsico. El impacto de la crisis en el estrecho de Ormuz no se limita al suministro energético y al comercio marítimo, sus consecuencias se extienden también a la conectividad digital global.

CONCLUSIÓN

La transformación tecnológica en la región se está desarrollando de tal forma que genera tanto implicaciones inmediatas para la seguridad como decisiones estructurales a largo plazo sobre la colaboración, la influencia y las normas que regirán el avance del conocimiento en toda la región. La relación entre los Estados y el conocimiento se está renegotiando de formas que definirán el panorama estratégico durante décadas. Los Estados del Golfo se están integrando en las redes tecnológicas globales a través de la inversión y las alianzas. Irán está siguiendo un enfoque centrado en sí mismo, impulsado ideológicamente y organizado en torno a la prioridad del control estatal sobre todas las dimensiones del desarrollo tecnológico.

Las capacidades ofensivas de Irán en materia de producción de conocimiento ya han demostrado su alcance a nivel mundial. Estas operaciones son un producto directo del mismo sector del conocimiento que ha construido la ar-

quitectura de vigilancia y el programa de drones de Irán. Pero este modelo es de proyección sin protección. Ha demostrado ser capaz de causar destrucción en el extranjero, al tiempo que no logra proteger al Estado, su infraestructura o su población en el país.

Los Estados del Golfo presentan un tipo diferente de oportunidad estratégica. La escala de su inversión en compromisos de desarrollo del conocimiento puede ir más allá de una relación puramente extractiva con la tecnología. Sin embargo, este sistema sigue siendo vulnerable a un alcance destructivo –por ejemplo, el de Irán.

Los acontecimientos de 2026 han hecho tangible esta vulnerabilidad. Los ataques iraníes contra centros de datos y la amenaza a la infraestructura de cables submarinos han sacudido la arquitectura digital de la que depende la diversificación del Golfo. También han puesto de manifiesto la brecha entre la ambición tecnológica y la resiliencia estratégica. Estos ataques subrayan que la inversión debe combinarse con estrategias sólidas para defender la infraestructura. En la era posterior a los ataques de Irán, la infraestructura de defensa, conocimiento y tecnología del CCG, a pesar de su envergadura y sofisticación, se encuentra en una situación vulnerable, en parte debido a su continua dependencia de la tecnología y los socios extranjeros.

En ambos modelos, el Estado busca proyectar poder, aunque este signifique algo diferente en cada caso. Para los Estados del Golfo, significa influencia económica, relevancia tecnológica y la capacidad de atraer alianzas globales que se consolidan con el tiempo. Para Irán, significa la supervivencia del régimen, el alcance ideológico y la capacidad de amenazar a los adversarios mediante la fuerza y la desestabilización. No se trata simplemente de estrategias diferentes; reflejan relaciones fundamentalmente distintas entre el Estado y el propio conocimiento. El modelo de Irán ha dejado constancia de lo que ocurre cuando el desarrollo del conocimiento se diseña para servir a quienes detentan el poder en lugar de a quienes lo producen. El resultado es un ecosistema de desarrollo del conocimiento que nunca ha cumplido la promesa del capital humano del país, una empresa científica despojada de la independencia que la hace generativa, y una población cuya relación principal con la infraestructura tecnológica construida por el Estado es de vigilancia y evasión./