Dans le but commun de réduire leur dépendance vis-à-vis des fournisseurs militaires et numériques étrangers, l'Iran et les pays du Golfe mettent en œuvre des stratégies divergentes qui sont en train de redessiner la région.

Sara Bazoobandi, chercheuse à l'Institut de politique de sécurité de l'université de Kiel.

SOUVERAINETÉ TECHNOLOGIQUE ET GÉOPOLITIQUE DU GOLFE

La région du golfe Persique connaît une profonde transformation dans la manière dont ses gouvernements conçoivent, développent et mettent en œuvre les connaissances. Ils ont pris des mesures pour réduire leur dépendance vis-à-vis de l'étranger et développer leurs propres capacités. Cependant, les voies choisies diffèrent considérablement, et ces différences ont des conséquences stratégiques qui s'étendent bien au-delà de la région elle-même.

Deux domaines sont au cœur de cette transformation : la défense et le cyberespace. Ce choix n'est pas le fruit du hasard. La souveraineté technologique se définit comme la capacité d'un État à développer, contrôler et maintenir de manière indépendante des technologies critiques. La capacité à produire les systèmes qui protègent l'État, projettent sa puissance et expriment ses ambitions tant à ses alliés qu'à ses adversaires est à la fois la mesure la plus claire de cette souveraineté et son catalyseur le plus déterminant. Ensemble, ces deux domaines définissent la relation de l'État avec la connaissance, la manière dont il l'organise, la contrôle et l'utilise comme une arme.

L'Arabie saoudite et les Émirats arabes unis ont favorisé le développement des connaissances dans ces deux domaines grâce à leur puissance financière, à des alliances internationales et à des programmes nationaux ambitieux. L'Iran a emprunté une voie fondamentalement différente, qui ne repose pas sur l'accès au marché ou sur des structures d'alliances, mais sur une doctrine idéologique qui considère la connaissance en soi comme une arme de l'État.

DES VOIES DIVERGENTES VERS LA SOUVERAINETÉ TECHNOLOGIQUE

Les puissances de la région partagent une ambition commune : réduire leur dépendance vis-à-vis des fournisseurs militaires et numériques étrangers. Mais les stratégies qu'elles mettent en œuvre pour atteindre cet objectif reflètent des relations fondamentalement différentes entre l'État, le savoir et la technologie.

L'Arabie saoudite et les EAU constituent un modèle de modernisation portée par les ressources. Le groupe EDGE des EAU, formé en 2019 par la fusion de plusieurs entités de défense détenues par l'État, a axé la majeure partie de son portefeuille de produits sur la fabrication nationale et a développé des capacités en matière d'armes autonomes, notamment des munitions à vol stationnaire guidées par l'intelligence artificielle. La SAMI saoudienne, lancée en 2017 dans le cadre de la Vision 2030, est passée de zéro à une entreprise d'envergure mondiale en quelques années, en recherchant des accords de transfert de technologie avec des partenaires allant des sociétés turques telles que Baykar et ASELSAN aux entreprises Lockheed Martin et Boeing des États-Unis. Ces deux États du Golfe ont également pris des engagements extraordinaires en matière d'IA. L'Arabie saoudite a consacré des centaines de milliards de dollars aux infrastructures d'IA, et les EAU ont annoncé des plans d'investissement d'une ampleur similaire. Il s'agit d'États qui achètent et bâtissent progressivement leur puissance technologique, avec le développement parallèle de l'économie de l'innovation civile et du secteur de la défense.

L'approche de l'Iran est radicalement différente. Isolé des marchés technologiques occidentaux par des décennies de sanctions, et façonné par une idéologie révolutionnaire qui considère la dépendance vis-à-vis de l'étranger comme une vulnérabilité stratégique et un échec moral, l'Iran a développé une

doctrine d'autosuffisance technologique à caractère théologique que l'on ne retrouve nulle part ailleurs dans la région. Comprendre cette doctrine est essentiel pour saisir tout ce que l'État iranien a construit par la suite.

LA PRODUCTION DE CONNAISSANCES EN IRAN : UN DEVOIR SACRÉ

Depuis les premières années de la République islamique, son approche de l'Iran en matière de science et de technologie s'inscrit dans une vision idéologique du savoir et de son lien avec la souveraineté politique. Le concept de « djihad du savoir », développé sous l'égide du défunt guide suprême, l'ayatollah Ali Khamenei, soutient que le développement scientifique de la nation est un impératif religieux, et que la dépendance vis-à-vis de la technologie étrangère est une forme d'asservissement incompatible avec le projet révolutionnaire. Dans ce cadre, le scientifique et le militaire occupent des rôles équivalents : tous deux participent à la défense de la révolution face aux ennemis extérieurs, et tous deux sont soumis aux mêmes obligations de loyauté et de sacrifice.

Les implications pratiques de ce concept pour la structure des institutions scientifiques et technologiques iraniennes ont été profondes et, dans une large mesure, négatives pour le développement général du pays. Lorsque les convictions idéologiques et la loyauté envers l'État révolutionnaire deviennent une condition préalable à la participation au secteur de la connaissance, les conséquences se propagent de manière difficile à contenir. Les programmes de recherche sont définis en fonction des priorités de sécurité plutôt que des opportunités scientifiques. Les institutions qui pourraient servir de sources de retour critique – universités, associations professionnelles, centres de recherche indépendants – se transforment, au contraire, en instruments au service des objectifs de l'État, et leur indépendance est systématiquement restreinte. Il en résulte un secteur de la connaissance idéologiquement cohérent et stratégiquement orienté, mais qui a sacrifié la diversité intellectuelle et la contestation interne dont dépend l'innovation véritable.

Ce système a permis de garantir que les priorités en matière de sécurité se reflètent non seulement dans les projets financés, mais aussi dans l'organisation des institutions et dans les promotions accordées au sein de celles-ci. Il en a résulté une militarisation de l'économie de la connaissance iranienne de l'intérieur, grâce à la mise en place d'un système dans lequel les avancées technologiques les plus importantes sont menées sous supervision militaire et conformément aux objectifs de l'appareil sécuritaire.

Selon le concept iranien de « djihad du savoir », le développement scientifique de la nation est un impératif religieux, et la dépendance vis-à-vis de la technologie étrangère est une forme d'asservissement incompatible avec le projet révolutionnaire

Les résultats sont visibles. À l'échelle nationale, ce même appareil institutionnel a mis en place l'infrastructure de surveillance, de filtrage et de contrôle que le régime utilise pour gérer sa propre population. Il ne s'agit pas de projets distincts menés en parallèle, mais d'expressions de la doctrine appliquée dans différents domaines. La dimension de projection de puissance extérieure du secteur de la connaissance, mobilisé au service des ambitions stratégiques de l'État, se manifeste dans le programme de drones de l'Iran, qui lui permet de fournir des technologies de drones à des groupes alliés et à des forces *proxies* dans de multiples zones de conflit, dans son programme de missiles balistiques et dans ses capacités cybernétiques croissantes.

LA CONSTRUCTION D'UNE CAGE NUMÉRIQUE INTERNE

L'infrastructure de contrôle d'Internet en Iran constitue l'un des systèmes les plus avancés de ce genre. Cela ne tient pas au fait qu'un composant particulier soit exceptionnellement sophistiqué, mais plutôt au fait que ces composants ont été assemblés selon une logique stratégique claire et cohérente. Cette logique ne consiste pas principalement à bloquer des contenus spécifiques, même si le blocage de contenus en fait partie. Il s'agit de construire un système dans lequel l'État conserve, à tout moment, la capacité de déterminer ce qui peut et ne peut pas être communiqué, qui peut le faire et à qui, et dans lequel les outils à la disposition des citoyens qui tentent de contourner ce contrôle sont systématiquement neutralisés.

Ceci est rendu possible grâce à une structure comportant plusieurs niveaux de soutien. De multiples mécanismes techniques indépendants régissent la manière dont les adresses internet sont attribuées, dont les données en transit sont gérées et dont les différents types de trafic internet sont structurés ou interdits. Derrière tout cela se cache également une structure qui concentre l'ensemble du trafic internet international via une seule entité étatique. Cette conception confère au gouvernement une capacité dont la plupart des systèmes de censure sont dépourvus. À savoir, la capacité de mettre en œuvre des changements de manière uniforme et instantanée pour tous les utilisateurs du pays simultanément, sans dépendre de la coopération ou de la bonne volonté de multiples opérateurs indépendants.

Outre son infrastructure de filtrage externe, l'Iran a investi dans la construction d'un réseau national parallèle : un ensemble de services hébergés localement, conçus pour remplacer les plateformes internationales bloquées ou sujettes à des interruptions. La Chine a été le principal contributeur externe à ce projet, en fournissant à la fois les systèmes techniques et les connaissances institutionnelles acquises grâce à son expérience dans la gestion d'un réseau internet national à grande échelle. Cette relation repose sur une collaboration stratégique formelle à long terme entre les deux gouvernements et a donné lieu à d'importants transferts financiers de l'Iran vers les fournisseurs de technologie chinois.

Le réseau national est promu en Iran en invoquant la souveraineté culturelle et la compatibilité religieuse, mais son importance opérationnelle est davantage stratégique que culturelle. Il assure un niveau minimal de fonctionnalité numérique nationale qui reste disponible même en cas d'interruption de la connectivité externe, ce qui signifie que le régime peut isoler ses citoyens du réseau mondial sans perturber l'activité

À la suite des manifestations de janvier, le régime a coupé l'accès à internet, un moyen de contrôler plus facilement l'information. Téhéran, janvier 2026./FATEMEH BAHRAMI/ ANADOLU VIA GETTY IMAGES

économique et administrative nationale dont dépend le gouvernement lui-même. Cette capacité a considérablement réduit le coût de l'utilisation de la connectivité comme arme politique pour l'État.

Depuis 2019, le gouvernement iranien a régulièrement utilisé les coupures d'internet comme outil de gestion politique, et l'évolution de ces interventions témoigne à la fois d'un apprentissage et d'une sophistication croissante. Le développement de cette capacité technique a été crucial pour le régime, non seulement d'un point de vue opérationnel, mais aussi politique. Lors de toute crise interne, qu'elle soit provoquée par une attaque étrangère ou un soulèvement populaire, les coupures d'internet permettent au gouvernement de manipuler plus facilement l'information. L'avantage structurel que cela génère est renforcé par le fait que les fonctionnaires du régime, les médias d'État et les communications gouvernementales peuvent continuer à fonctionner pleinement pendant toute interruption. Cette fourniture sélective d'accès à internet offre à l'État des plateformes sans égal précisément au moment où les sources indépendantes seraient, autrement, plus précieuses.

LES CONNAISSANCES, UN OUTIL AU SERVICE DE LA PROJECTION DE PUISSANCE EXTÉRIEURE

Les capacités développées grâce à l'approche technologique de l'Iran permettent également au gouvernement d'étendre son influence au-delà de ses frontières. En matière de technologie des drones, de développement de missiles et d'opérations cyber-offensives, le pays a obtenu des résultats significatifs. Cependant, ces avancées ont également mis en évidence des vulnérabilités au sein du système iranien, fortement ancré dans l'idéologie. Les systèmes conçus en privilégiant le contrôle ont tendance à être fragiles, contrairement à ceux conçus en privilégiant la résilience. Un secteur technologique organisé autour de priorités militaires a accru sa capacité destructrice de manière inédite, sans pour autant démontrer, au contraire, des qualités défensives.

Les programmes technologiques et de défense de l'Arabie saoudite et des EAU ont nécessité des investissements considérables et une collaboration étroite en matière de transfert de technologie. Ils n'ont pas non plus été épargnés par les défis qui accompagnent les grandes initiatives industrielles dirigées par l'État. Ces deux pays sont intégrés dans des réseaux de collaboration internationale qui prévoient des formes de responsabilisation externe et d'échange de connaissances absentes du modèle autonome de l'Iran. Les relations qui se construisent autour de ces collaborations ont un double objectif : elles constituent des vecteurs de connaissances techniques, mais aussi des canaux par lesquels les standards de performance, la pression concurrentielle et le contrôle externe pénètrent dans le système. Il en résulte, au sein de ces écosystèmes, un mécanisme distribué de correction des erreurs que les programmes nationaux fermés, comme celui de l'Iran, ne peuvent tout simplement pas reproduire.

La valeur de ce modèle est actuellement mise à l'épreuve dans des conditions réelles. Les conflits en cours dans la région ont mis en évidence un contraste frappant : les systèmes du Conseil de coopération du Golfe, en particulier celui des EAU, se sont révélés nettement plus efficaces pour protéger les infrastructures critiques et la population civile que leurs homologues iraniens. La défense aérienne et antimissile de l'Iran a montré des signes évidents d'effondrement face à la guerre moderne à laquelle elle est désormais confrontée. Cet écart n'est pas purement technologique. Il met en évidence les avantages cumulés d'une collaboration ouverte, d'un apprentissage itératif et d'une responsabilisation vis-à-vis de standards externes au fil du temps.

La guerre avec l'Iran a mis en évidence un fossé marqué entre l'image que le régime a de lui-même en tant que puissance technologiquement souveraine et ses vulnérabilités réelles. Les capacités offensives de l'Iran ont déployé une puissance destructrice qui, dans l'ensemble, a répondu aux attentes. Ses missiles, ses drones et ses réseaux de *proxies* ont démontré une portée réelle et la capacité de menacer la stabilité régionale. Mais les systèmes destinés à protéger l'État lui-même ont échoué. Les réseaux de renseignement et de surveillance ont été infiltrés, ce qui a permis aux adversaires de localiser et d'éliminer avec précision des hauts responsables. La doctrine du « djihad du savoir » a produit des armes capables de projeter une puissance vers l'extérieur. Elle n'a pas pu protéger les personnes qui les ont construites.

LES CONNAISSANCES SOUS LE FEU : LA CRISE DANS LE DÉTROIT D'ORMUZ

Les stratégies divergentes de l'Iran et du CCG en matière de savoir ont pris, depuis février 2026, une dimension empirique très marquée. Les attaques iraniennes contre le CCG ont remis en cause l'ensemble du modèle du CCG, fondé sur une transformation économique poussée par la technologie. Ce modèle repose sur un postulat : les États du Golfe offrent quelque chose de rare dans la région en général – stabilité politique, sécurité physique et gouvernance prévisible. C'est cette réputation qui en a fait des destinations attrayantes pour

les géants de la technologie, les fonds souverains et les investissements dans les infrastructures d'IA. Les attaques iraniennes à l'aide de drones et de missiles contre des tours de bureaux et des centres de données à travers le CCG ont été délibérément orchestrées par Téhéran pour remettre en cause la crédibilité de ce postulat, ainsi que des décennies de stratégie de diversification dans la région.

Les attaques iraniennes ont également mis en évidence une vulnérabilité structurelle dans l'ensemble du CCG, où d'importantes dépenses militaires ont été consacrées à la mise en place de systèmes de défense aérienne sophistiqués mais coûteux. Les drones iraniens Shahed, déployés en vagues massives, ont contraint le CCG à utiliser des intercepteurs coûteux contre des systèmes à faible coût. Téhéran a délibérément exploité cette asymétrie, s'en servant comme d'un moyen de guerre d'usure stratégique. Cette asymétrie est une manifestation claire de la différence doctrinale entre les stratégies de développement des connaissances et des technologies des deux côtés du golfe Persique.

L'Iran a industrialisé la production de systèmes bon marché et jetables dans le cadre de son « djihad du savoir », une doctrine qui, indépendamment de son coût pour le développement scientifique en général, s'est révélée efficace pour générer une capacité destructrice massive à grande échelle. Les États du Golfe, en revanche, continuent de dépendre de l'achat de technologies coûteuses et fabriquées à l'étranger, difficiles à produire au niveau national et trop onéreuses pour être utilisées dans les volumes requis par les tactiques de saturation de l'Iran.

Une autre dimension stratégique importante des attaques iraniennes contre le CCG réside dans le fait qu'elles visaient les infrastructures numériques. Des drones iraniens ont attaqué trois centres de données d'Amazon Web Services (deux aux EAU et un à Bahreïn), provoquant des perturbations dans les systèmes logiciels bancaires et d'entreprise. Par la suite, le Corps des gardiens de la révolution islamique a averti que les entreprises technologiques des États-Unis opérant dans le Golfe seraient considérées comme des cibles légitimes. Ces attaques révèlent l'intention de l'Iran de nuire à l'architecture institutionnelle qui sous-tend les plans de transformation économique portés par la technologie dans les États du Golfe. On s'attend à ce que les attaques contre une infrastructure clé pour l'avenir économique des États du Golfe affectent gravement la confiance des investisseurs, ce qui suscitera des doutes parmi les entreprises technologiques et les partenaires souverains dont l'engagement continu est indispensable aux ambitions de diversification de la région.

Cependant, la menace structurelle la plus grave pourrait bien être celle qui ne s'est pas encore concrétisée. L'Iran a fait part de son intention de transformer en armes les câbles sous-marins qui traversent le détroit d'Ormuz, lesquels acheminent un trafic internet et financier considérable entre l'Europe, l'Asie et le golfe Persique. Les infrastructures d'IA sont particulièrement exposées, car les centres de données du CCG dépendent des connexions à faible latence des câbles sous-marins. En raison du conflit, les opérations de réparation et de maintenance des câbles sous-marins dans le golfe Persique ont déjà été paralysées. L'impact de la crise d'Ormuz ne se limite pas à l'approvisionnement énergétique et au commerce maritime ; ses conséquences s'étendent également à la connectivité numérique mondiale.

CONCLUSION

La transformation technologique dans la région évolue de telle manière qu'elle entraîne à la fois des implications immédiates en matière de sécurité et des décisions structurelles à long terme concernant la collaboration, l'influence et les normes qui régiront les progrès de la connaissance dans toute la région. La relation entre les États et la connaissance est en train d'être renégociée d'une manière qui définira le paysage stratégique pour les décennies à venir. Les États du Golfe s'intègrent dans les réseaux technologiques mondiaux par le biais d'investissements et de partenariats. L'Iran suit une approche centrée sur lui-même, motivée par des considérations idéologiques et organisée autour de la priorité accordée au contrôle de l'État sur toutes les dimensions du développement technologique.

Les capacités offensives de l'Iran en matière de production de connaissances ont déjà démontré leur portée à l'échelle mondiale. Ces opérations sont le résultat direct du même secteur du savoir qui a mis en place l'architecture de surveillance et le programme de drones. Mais ce modèle repose sur une projection sans protection. Il s'est révélé capable de semer la destruction à l'étranger, tout en étant incapable de protéger l'État, ses infrastructures ou sa population sur son propre territoire.

Les États du Golfe offrent un autre genre d'opportunité stratégique. L'ampleur de leurs investissements dans des initiatives de développement des connaissances peut aller au-delà d'une relation purement extractive avec la technologie. Ce système reste toutefois vulnérable à une influence destructrice – comme celle de l'Iran, par exemple.

Les événements de 2026 ont rendu cette vulnérabilité tangible. Les attaques iraniennes contre des centres de données et la menace pesant sur les infrastructures de câbles sous-marins ont ébranlé l'architecture numérique dont dépend la diversification du Golfe. Elles ont également mis en évidence le fossé entre l'ambition technologique et la résilience stratégique. Ces attaques soulignent que l'investissement doit s'accompagner de stratégies solides pour défendre les infrastructures. À l'ère post-attaques iraniennes, les infrastructures de défense, de connaissance et de technologie du CCG, malgré leur envergure et leur sophistication, se trouvent dans une situation vulnérable, en partie en raison de leur dépendance continue vis-à-vis de la technologie et des partenaires étrangers.

Dans ces deux modèles, l'État cherche à projeter sa puissance, même si celle-ci revêt une signification différente dans chaque cas. Pour les États du Golfe, cela signifie une influence économique, une pertinence technologique et la capacité d'attirer des alliances mondiales qui se consolident avec le temps. Pour l'Iran, cela signifie la survie du régime, une portée idéologique et la capacité de menacer ses adversaires par la force et la déstabilisation. Il ne s'agit pas simplement de stratégies différentes ; elles reflètent des relations fondamentalement distinctes entre l'État et la connaissance elle-même. Le modèle iranien a montré ce qui se passe lorsque le développement de la connaissance est conçu pour servir ceux qui détiennent le pouvoir plutôt que ceux qui la produisent. Il en résulte un écosystème de développement des connaissances qui n'a jamais tenu la promesse du capital humain du pays, une entreprise scientifique dépouillée de l'indépendance qui la rend créative, et une population dont la relation principale avec l'infrastructure technologique construite par l'État est faite de surveillance et d'évasion./