شـــبكة الأنبـاء الأكاديميـة أكـابـــرس
ACADEMIC PRESS NETWORK

عسكرة الفضاء الافتراضي وأثرها على أمن الطاقة في الخليج العربي: قراءة نقديّة للعمليات المعلوماتية والسيبرانية الإيرانية لعام 2026

The Digital Militarization of Virtual Space and its Impact on Energy Security in the Arabian Gulf: A Critical Reading of Iranian Information and Cyber Operations in 2026

Authors: / أسماء الباحثين

محمد زيدان عواد عبد الحميد خفاجي[1] | Mohamed Zidan Awwad Abdelhamid Khafagy[1]

Affiliations: / الانتماءات المؤسسية

باحث في العلاقات الخليجية-الإيرانية والسياسات الدولية، جامعة إفريقيا الفرنسية العربية – مالي

[1] – Researcher in Gulf-Iranian Relations and International Politics, Université Privée Africaine Franco-Arabe (UPAFA) Mali

الباحث المراسل | Corresponding Author: محمد زيدان عواد عبدالحميد خفاجي

البريد الإلكتروني | Email: mohammedzidan89@gmail.com

ORCID ID: 0009-0007-8265-8250

تاريخ الاستلام: 24 / 06 /2026 تاريخ القبول: 26 / 06 / 2026 تاريخ النشر: 03 / 06 / 2026

Abstract | الملخص

تأتي هذه الدراسة لتفكيك طبيعة التحول البنيوي الذي يشهده التنافس الجيوسياسي في منطقة الخليج العربي لعام 2026، والمتمثل في انتقال أدوات الصراع الإقليمي من الأنماط العسكرية والجيواقتصادية الصلبة إلى "عسكرة الفضاء الافتراضي" كآلية محورية لإنتاج الردع غير المتماثل. تنطلق الدراسة من إشكالية رئيسية تبحث في أثر ونطاق التهديدات الهجينة والعمليات المعلوماتية والسيبرانية التي تديرها إيران ضد البنية التحتية الحيوية لمنشآت النفط والغاز التابعة لدول مجلس التعاون الخليجي، لاسيما في ظل الطفرة التكنولوجية التكاملية لنظم التحكم الصناعي وعمليات الأتمتة الكاملة الحاكمة لإمدادات الطاقة العالمية. وبتطبيق مقترب تحليل النظم وأداة التحليل الجيوسياسي، تسعى الدراسة

إلى تقديم قراءة نقدية تعيد تفكيك العقيدة الهجومية السيبرانية الإيرانية، مع تقييم موضوعي لكفاءة ومخرجات السياسات الأمنية الحالية لدول الخليج في حماية سيادتها الرقمية والنفطية. وقد خلصت الدراسة إلى أن الفضاء السيبراني قد تحول من مجرد بيئة دعم تقني إلى ساحة معركة جيوسياسية مستقلة بذاتها أفرزت ما يُمكن تسميته بـ "معركة المضيق الرقمية"، وهو ما يفرض على دول مجلس التعاون الخليجي بناء معايير متقدمة في حوكمة الدفاع السيبراني المشترك للانتقال من عقيدة الدفاع الوقائي المنفرد إلى نموذج الردع الجماعي الملزم القادر على رفع كلفة الاختراقات الافتراضية وحماية عصب الاقتصاد الدولي.

الكلمات المفتاحية: عسكرة الفضاء الافتراضي؛ أمن الطاقة؛ العمليات المعلوماتية؛ السيادة الرقمية؛ توازنات الردع؛ العلاقات الخليجية-الإيرانية.

This study analyzes the structural shift characterizing geopolitical competition in the Arabian Gulf region in 2026, defined by the transition of regional conflict dynamics from conventional military and geoeconomic hard power to the "militarization of virtual space" as a pivotal mechanism for asymmetric deterrence. The research addresses a core problem centered on investigating the impact and scope of hybrid threats, along with cyber and information operations conducted by Iran against the critical oil and gas infrastructure of the Gulf Cooperation Council (GCC) states. This is especially critical given the accelerating integration of Industrial Control Systems (ICS/SCADA) and the comprehensive automation governing global energy supplies. Utilizing the Systems Approach and Geopolitical Analysis, the study provides a critical reading that deconstructs Iran's offensive cyber doctrine while objectively evaluating the efficiency and outcomes of current Gulf security policies in safeguarding digital and resource sovereignty. The study concludes that cyber space has evolved from a mere technical support environment into an independent geopolitical battlefield, conceptualized as the "Digital Strait Battle." Consequently, this requires GCC states to establish advanced standards in joint cyber defense governance, transitioning from isolated preventive defense models to a binding collective deterrence framework capable of raising the cost of virtual intrusions and securing the core of the international economy.

Keywords: Digital Militarization; Energy Security; Information Operations; Digital Sovereignty; Deterrence Dynamics; Gulf-Iranian Relations.

1. المقدمة

تشهد البيئة الأمنية الدولية والإقليمية مع انتصاف عام 2026 تحولاً جيوسياسياً بنيوياً أعاد صياغة المفاهيم الكلاسيكية للقوة والردع وتوازنات النفوذ في العلاقات الدولية. فلم تعد التهديدات الأمنية محصورة في الأبعاد الفيزيائية الصلبة، بل تداخلت بشكل عضوي مع جيل جديد من الحروب الهجينة التي تتخذ من الفضاء السيبراني

والافتراضي ساحة قتالية وعملياتية مباشرة. هذا التحول أعاد تعريف مفهوم "المجال الحيوي" للدول؛ إذ لم يعد هذا المجال مقيداً بحدود الجغرافيا السياسية المرئية، بل امتد ليشمل مساحات برمجية غير مرئية قادرة على إحداث تأثيرات مادية وتدميرية ملموسة تعادل نتائج الضربات العسكرية التقليدية (Gray, 2012).

وفي قلب هذا المشهد، تقبع منطقة الخليج العربي بوصفها الشريان الحيوي الأهم لعصب الاقتصاد العالمي وسلاسل إمداد الطاقة الدولية. ومع تسارع وتيرة التحول الرقمي وتبني دول مجلس التعاون الخليجي لتطبيقات الذكاء الاصطناعي والحوكمة البرمجية المتكاملة لإدارة منشآتها النفطية وشبكات التوزيع والتحكم الصناعي، تضاعفت مساحات "الانكشاف الاستراتيجي" (التقرير الاستراتيجي الخليجي، 2026). في المقابل، طوّرت طهران عقيدة هجومية بالغة الديناميكية، ترتكز على "عسكرة الفضاء الافتراضي" والتوظيف الكثيف للعمليات المعلوماتية والهجمات السيبرانية ذات الصبغة الاستراتيجية (Cyber Defense Review, 2026). إن هذا التموضع يسعى لإدارة صراع موازٍ يُمكن تسميته بـ"معركة المضيق الرقمية"، وهي معركة تهدف إلى الالتفاف على أوراق الضغط التقليدية المترتبة على الاختناقات المائية الجغرافية الصلبة كمضيقي هرمز وباب المندب، وخلق معادلات ردع جديدة تمكنها من الضغط على القرار الاقتصادي والسياسي فرضاً لشروط تفاوضية مستجدة لعام 2026 (ربيع، 2026).

1.2 مشكلة الدراسة

تتبلور المشكلة البحثية في الفجوة البنيوية المتسعة بين اندفاع دول مجلس التعاون الخليجي نحو الرقمنة الشاملة والأتمتة العميقة لمنشآت الطاقة الحيوية كخيار اقتصادي وتنموي حتمي لعام 2026، وبين تصاعد وتطور العقيدة السيبرانية الهجومية لإيران التي باتت تعتمد على الفضاء الافتراضي كأداة رئيسية للردع غير المتماثل والمناورة الجيوسياسية. وثمة نقص في الدراسات السياسية والنقدية التي تقيم أثر هذا التحول على أمن البنية التحتية الحيوية في سياق العلاقات الخليجية-الإيرانية المعاصرة. بناءً عليه، يسعى البحث للإجابة على السؤال الجوهري الآتي: ما هي طبيعة وأبعاد التأثير الاستراتيجي الذي تحدثه عسكرة الفضاء الافتراضي والعمليات المعلوماتية الإيرانية لعام 2026 على أمن وحصانة البنية التحتية الحيوية للطاقة في دول الخليج؟

1.3 أهداف الدراسة

- الهدف الرئيسي: تقييم الأثر المباشر والجيوسياسي لعسكرة الفضاء الافتراضي والعمليات المعلوماتية الإيرانية لعام 2026 على أمن البنية التحتية الحيوية للطاقة في دول مجلس التعاون الخليجي.
- الأهداف الفرعية:

1. تفكيك المحددات العقائدية للاستراتيجية السيبرانية الهجومية لإيران وطبيعة العمليات الموجهة لشبكات التحكم الصناعي (ICS/SCADA) الخليجية.
2. تقييم كفاءة ومخرجات الاستجابة الدفاعية وحوكمة السيادة التكنولوجية بدول مجلس التعاون الخليجي في مواجهة التهديدات الهجينة الراهنة.

3. استقراء الدلالات الاستراتيجية والسيناريوهات المستقبلية لمعادلة الردع السيبراني المتبادل بين دول الخليج وإيران لعام 2026.

1.4 فرضيات الدراسة

- الفرضية الأولى: تؤدي عسكرة الفضاء الافتراضي والعمليات المعلوماتية الإيرانية لعام 2026 إلى صياغة نمط جديد من التهديدات الجيوسياسية غير المتماثلة التي تؤثر مباشرة في استقرار وتصدير قطاع الطاقة الخليجي وعوائده الاقتصادية.
- الفرضية الثانية: يرتبط نجاح حوكمة السياسات الدفاعية الخليجية المستجدة طردياً بمدى الانتقال من الأطر الوطنية المنفردة إلى بناء نموذج ردع جماعي ملزم قادر على تحجيم الانكشاف الرقمي المشترك.

1.5 الإطار النظري والمفاهيمي

تستند الدراسة إلى مدخلين نظريين متكاملين في حقل العلاقات الدولية والدراسات الأمنية:

1. مفهوم عسكرة الفضاء الافتراضي (Cyber Militarization): ويُعني به نقل الشبكات الرقمية من فضاءات التداول المدني والتنموي إلى بيئة عملياتية قتالية هجومية ودفاعية تُدار عبر مؤسسات رسمية أو مجموعات قرصنة برعاية دول (State-Sponsored\ Actors) لتحقيق مآرب جيوسياسية (International Affairs Journal, 2025).
2. نظرية الردع غير المتماثل (Asymmetric Deterrence) في العصر الرقمي: وتفسر كيف يمكن للفاعل الإقليمي الأقل تفوقاً مادياً (إيران) أن يعوض عجز القوة الصلبة عبر أدوات سيبرانية هجومية منخفضة التكلفة وعالية الأثر لإجبار خصومه الأكثر تفوقاً على إعادة تسعير مخاطر مواجهته (RAND Corporation, 2025).
3. نظرية الأمن الإقليمي الصاعد (Regional Security Complex): لباري بوزان، وتُستخدم لتأصيل الترابط البنيوي لعقيدة الأمن والتهديد بين دول ضفتي الخليج العربي (Buzan & Wæver, 2003).

1.6 الدراسات السابقة

بمراجعة نقدية للأدبيات المعاصرة، يمكن تصنيفها إلى مسارين تبرز من خلالهما الفجوة البحثية:

- ✓ المسار الأول: أدبيات تقنية محضة (مثل تقارير وكالة ENISA الأوروبية وتقارير ميكروسوفت للدفاع الرقمي)، وهي دقيقة برمجياً لكنها منبتة الصلة تماماً بالدوافع الجيوسياسية وبوصلة صنع القرار السياسي في الشرق الأوسط (Microsoft, 2026).
- ✓ المسار الثاني: أدبيات جيوسياسية كلاسيكية (مثل دراسات مركز الإمارات للسياسات ومركز الحبتور للأبحاث لعام 2026)، والتي ركزت على أمن الممرات المائية والمضايق والأبعاد الجغرافية التقليدية للصراع، مع إغفال واضح لـ "معركة المضيق الرقمية" وهندسة حروب الجيل الخامس. وتأتي هذه الدراسة لتسد هذه الفجوة الهيكلية عبر المزاوجة النقدية بين عسكرة الافتراضي الإيراني لعام 2026 وانعكاساته على حوكمة الطاقة الخليجية.

2. منهجية الدراسة

تتطلب دراسة هذه الظاهرة المركبة لعام 2026 مقاربة منهجية تجمع بين اقترابين متكاملين ينتميان لحقل العلوم السياسية لإظهار "النفس البحثي" النقدي القادر على ربط السلوك التقني بالدلالة الجيوسياسية وحوكمة النظم الإقليمية:

2.1 اقتراب تحليل النظم (Systems Approach)

يُعد اقتراب تحليل النظم، المستوحى من أدبيات ديفيد إيستون، الأداة المثالية لتفكيك البيئة الأمنية لقطاع الطاقة الخليجي وفهم ديناميكيات التفاعل المستمر بين ضفتي الخليج العربي (Easton, 1965). ويتم إسقاط هذا الاقتراب إجرائياً وفق التمفصلات التالية:

- ✓ المدخلات (Inputs): التهديدات السيبرانية الهجومية والعمليات المعلوماتية الإيرانية المستجدة لعام 2026 المستهدفة لشبكات التحكم الصناعي النفطية، والتحولات الدولية المصاحبة (Cyber Defense Review, 2026).
- ✓ عمليات المعالجة والتحويل (Conversion Processes): السياسات الدفاعية الوقائية، والأطر الأمنية الوطنية المشتركة لدول مجلس التعاون الخليجي، وحوكمة السيادة التكنولوجية وآليات التنسيق والاتفاقيات الأمنية المستجدة لامتصاص الصدمات الرقمية.
- ✓ المخرجات (Outputs): النتيجة النهائية وتتمثل إما في صيانة وحصانة أمن الطاقة واستقرار الإمدادات، أو في تداعي منظومة الردع والانزلاق نحو اختلالات هيكلية في سلاسل التوريد والقرار الاقتصادي والنفطي.
- ✓ التغذية العكسية (Feedback): رصد كيف تؤثر المخرجات الأمنية في إعادة صياغة الوعي الاستراتيجي لدول الخليج، ودفعها نحو تعديل مدخلات وميكانيزمات النظام الأمني الإقليمي لتلافي نقاط الضعف المستقبلية وضمان استقراره.

2.2 أداة التحليل الجيوسياسي (Geopolitical Analysis)

تُستخدم لتأصيل البعد الجغرافي والمجالات الحيوية للبنية التحتية للطاقة في الخليج، ورصد كيف تتدخل التقنية الافتراضية العابرة للحدود في إعادة صياغة معالم الجغرافيا السياسية لعام 2026؛ حيث ينجح الفضاء السيبراني المعسكر في تحويل المعالم الجغرافية الصلبة والثابتة (الحقول، الأنابيب، الموانئ) إلى جغرافيا افتراضية قابلة للاستهداف الفوري والردع الصامت، والالتفاف على نقاط الاختناق الجغرافي التقليدي لخلق مفهوم "معركة المضيق الرقمية" (حجاب، 2026).

3. الإطار النظري والتحليلي للبحث

3.1 المبحث الأول: استراتيجية العسكرة الافتراضية: طبيعة التهديدات السيبرانية الإيرانية لعام 2026.

3.1.1 المطلب الأول : تطور العقيدة الهجومية الإيرانية (من حروب الوكلاء الصلبة إلى الفضاء الرقمي والتهديدات الهجينة)

شهدت العقيدة الأمنية الإيرانية تحولاً دراماتيكياً وصولاً إلى عام 2026؛ فبالتوازي مع الاعتماد التاريخي الكلاسيكي على الوكلاء المحليين في الإقليم (القوة الصلبة غير المتماثلة)، أدركت طهران – تحت وطأة الضغوط الهيكلية والعقوبات – حدود الفاعلية الجيوسياسية للأدوات التقليدية وسهولة كشفها وتتبعها. من رحم هذا الإدراك، برزت استراتيجية "عسكرة الفضاء الافتراضي" كركيزة عقائدية موازية. وتتشابك الهجمات السيبرانية المنظمة التي تشنها مجموعات قرصنة متقدمة برعاية الدولة (APTs) مع الضغط الميداني لإنتاج نمط "الحروب الهجينة" (Cyber Defense Review, 2026). تكمن العبقرية الجيوسياسية لهذه العقيدة المستجدة في صياغة مفهوم "الإنكار المعقول" (Plausible\ Deniability)، مما يمنح طهران القدرة على شن ضربات موجعة للبنى التحتية الخليجية مع الاحتفاظ بالقدرة على التنصل السياسي والقانوني، وهو جوهر نظرية الردع غير المتماثل في العصر الرقمي.

3.1.2 هندسة "معركة المضيق الرقمية": أدوات الاختراق والعمليات المعلوماتية الموجهة لشبكات التحكم الصناعي الخليجية (ICS/SCADA)

الايمثل عام 2026 ذروة التموضع الإيراني فيما يمكن تسميته بـ"معركة المضيق الرقمية"؛ حيث انتقلت الهجمات نحو "العمليات المعلوماتية السيبرانية التدميرية" المستهدفة لشبكات التحكم الصناعي ونظم تحصيل البيانات (ICS/SCADA) الحاكمة والمشغلة لحقول النفط، ومصافي التكرير، ومحطات إسالة الغاز في دول مجلس التعاون الخليجي (ENISA, 2026). وتعتمد الهندسة التقنية لهذه العمليات على تطوير برمجيات خبيثة فائقة التعقيد مصممة خصيصاً لاختراق البيئات الصناعية المعزولة تكنولوجياً (Air-Gapped\ Systems) كبرمجيات المسح الشامل للبيانات (Wipers)، أو عمليات التسلل الصامت بهدف التلاعب بالقيم الفيزيائية للمعدات والضغط والحرارة داخل المنشآت الحيوية. إن هذا النمط التقني يحول الاختراق الرقمي من حدث برمجي إلى "سلاح فيزيائي تدميري" قادر على إخراج منشآت كاملة عن الخدمة دون إطلاق رصاصة واحدة (ربيع، 2026).

3.1.3 المطلب الثالث: أبعاد الارتباط بين التصعيد الإقليمي الميداني وضغوط الطاقة الافتراضية لفرض شروط توازنات التفاوض الدولي لعام 2026

يكشف التحليل النقدي للسلوك الرقمي الإيراني لعام 2026 أنه أداة منضبطة ومحسوبة بدقة تقع في خدمة السياسة الخارجية ومسارات التفاوض؛ إذ ثمة ارتباط شرطي وعضوي بين وتيرة التصعيد الميداني في ساحات الإقليم (كالبحر الأحمر وجنوب شبه الجزيرة العربية) وبين موجات الهجمات السيبرانية الموجهة ضد قطاع الطاقة الخليجي (شبكة النبأ، 2026). فعندما تتصاعد الضغوط الدولية على طهران، تعمد إلى تفعيل "ضغوط

الطاقة الافتراضية" عبر الفضاء السيبراني كبديل استراتيجي خفي لإرسال رسائل مشفرة مفادها أن كلفة أي تصعيد صلب ضدها ستُدفع رقمياً من عوائد النفط والغاز واستقرار البورصات العالمية، وبذلك تحول أمن الطاقة الخليجي إلى رهينة جيوسياسية رقمية لتعديل موازين القوى على طاولات التفاوض (مركز الحبتور، 2026).

3.2 المبحث الثاني: استراتيجيات الاستجابة والدفاع الخليجي: حوكمة الأمن السيبراني وحماية البنية التحتية للطاقة

3.2.1 المطلب الأول تقييم البنية التحتية الرقمية ومستويات السيادة التكنولوجية الحالية في منشآت النفط والغاز لدول مجلس التعاون

يمثل عام 2026 محطة تقييمية حاسمة تكشف معضلة بنيوية مزدوجة في قطاع الطاقة الخليجي؛ فمن جهة، تمتلك دول مجلس التعاون أحدث نظم التحكم البرمجي والذكاء الاصطناعي لإدارة مكامن النفط وأتمتة المصافي، مما جعلها الأكثر كفاءة عالمياً. ولكن من جهة أخرى، يبرز مأزق "السيادة التكنولوجية" (Technological\| Sovereignty)؛ حيث تعتمد هذه البنى التحتية الحساسة بالكامل تقريباً على برمجيات، وتقنيات تشفير، ومعدات صلبة مستوردة من شركات تكنولوجية غربية عملاقة (CSIS, 2026). إن هذه الاعتمادية العميقة تخلق مساحات انكشاف غير مرئية جراء احتمال احتواء الأنظمة المستوردة لشبكات التحكم (ICS/SCADA) على ثغرات برمجية غير مكتشفة (Zero-day) قد تُستغل من قبل طهران قبل ترقيعها، مما يوضح أن كثافة الرقمنة من دون "استقلال برميجي" أصبحت تشكل خاصرة رخوة تضعف القدرة على الاستقلالية المطلقة في إدارة الأزمات الرقمية المستجدة.

3.2.2 المطلب الثاني: السياسات الوقائية والدفاعية الخليجية: دراسة مقارنة لآليات التنسيق المشترك وهياكل الدفاع السيبراني الوطنية

عند إخضاع السياسات الدفاعية الخليجية لـ "المنهج المقارن"، يتضح وجود تباين هيكلي في البنى المؤسسية والتشريعية المعنية بالأمن الرقمي بين دول مجلس التعاون؛ فقد نجحت دول كالمملكة العربية السعودية ودولة الإمارات العربية المتحدة في بناء هياكل وطنية دفاعية بالغة التطور (مثل الهيئة الوطنية للأمن السيبراني في السعودية، ومجلس الأمن السيبراني في الإمارات) تمكنت من صياغة استراتيجيات استباقية متقدمة لحماية قطاع الطاقة (مجلة السياسة الدولية، 2026). في المقابل، ما زالت بعض الحلقات الإقليمية الأخرى تعتمد على أطر دفاعية وقائية تقليدية ومجزأة. أما على صعيد "آليات التنسيق المشترك"، فإن الرؤية النقدية تستقرئ تفضيل دول الخليج حتى عام 2026 للأطر الثنائية أو التنسيق الأمني الوطني المنفرد، على حساب تفعيل مركز موحد فاعل للدفاع السيبراني الخليجي المشترك، مما يخلق ثغرة في آلية "تحليل النظم"؛ إذ إن نجاح الهجمات في اختراق المنظومة النفطية للدولة الأقل تحصيناً تكنولوجياً قد يُستغل كـ "حصان طروادة" للوصول إلى شبكات الدول الأكثر تحصيناً عبر شبكات الربط والخطوط المشتركة (مجلة آراء الخليج، 2026).

3.2.3 المطلب الثالث: الشراكات الأمنية الدولية والردع التكنولوجي المتكامل: حدود وجدوى الاعتماد على الحلفاء الدوليين في الفضاء الافتراضي

أمام هذا الانكشاف الاستراتيجي، اتجهت بعض دول الخليج في أوائل عام 2026 إلى تفعيل وتوسيع بنود اتفاقيات الشراكة الدفاعية والأمنية الشاملة مع القوى الكبرى (مثل تفعيل البحرين لبنود اتفاقية التكامل الأمني والازدهار الشامل C-SIPA مع الولايات المتحدة)، مستهدفةً بناء شبكة "ردع تكنولوجي متكامل" والاعتماد على مظلة "الردع الممتد" (Extended\ Deterrence) في الفضاء السيبراني (مركز الإمارات للسياسات، 2026). وتكمن القراءة النقدية في تفكيك "حدود وجدوى" هذا الاعتماد؛ فالفضاء السيبراني يختلف جذرياً عن جغرافية الأرض، إذ لا يمكن للحلفاء الدوليين تطبيق بنود الدفاع المشترك التقليدية بشكل فوري لمواجهة هجوم برمجي مجهول المصدر أو يقع تحت مظلة "الإنكار المعقول" الإيرانية. فضلاً عن ذلك، فإن القوى الدولية غالباً ما تعمد إلى إخفاء قدراتها السيبرانية الهجومية الأكثر تقدماً لحماية أمنها القومي الخاص، وبالتالي، يخلص هذا المطلب إلى أن الاعتماد على المظلات الدولية يحمل جدوى مشروطة، ولا يمكن أن يشكل بديلاً عن بناء قدرات ردع ذاتية عميقة وحوكمة سيادية خليجية خالصة.

3.3 المبحث الثالث: الدلالات الجيوسياسية والسيناريوهات المستقبلية لأمن الطاقة الإقليمي

3.3.1 المطلب الأول: استقراء تأثير الصراع الافتراضي الصامت على توازنات القوى وصناعة القرار الاقتصادي والنفطي الإقليمي لعام 2026

يكشف الاستقراء الجيوسياسي لعام 2026 أن عسكرة الفضاء الافتراضي أحدثت تآكلاً ملموساً في المفاعيل التقليدية "لميزان القوى" الصلب في منطقة الخليج العربي؛ فالتفوق المادي والمنظومات الدفاعية الكلاسيكية لم تعد كافية لحسم معادلة الأمن القومي، نظراً لطبيعة الهجمات السيبرانية الهجينة العابرة للحدود والمنفلتة من قيود الردع التقليدي. هذا الاختلال البنيوي انعكس مباشرة على "بيئة صناعة القرار الاقتصادي والنفطي" الخليجي؛ إذ لم يعد القرار الإستراتيجي المتعلق بمعدلات الإنتاج أو مسارات التصدير خاضعاً فقط لمعادلات العرض والطلب وحسابات "أوبك+" الكلاسيكية، بل أصبحت "مخاطر الانكشاف الرقمي للبنى التحتية" متغيراً ثابتاً ومؤثراً. إن مجرد نجاح هجوم سيبراني إيراني في إحداث شلل مؤقت في مصفاة تكرير خليجية، يُترجم فوراً في الأسواق الدولية على شكل صدمة جيوسياسية ترفع من كلفة التأمين على ناقلات النفط وتعيد تسعير البرميل دولياً بشكل قسري، مما يعني أن طهران باتت تمتلك من خلال أدوات العسكرة الافتراضية القدرة على "الفيتو الرقمي الصامت" المؤثر في عمق التخطيط الاقتصادي الخليجي والدولي بالتبعية.

3.3.2 المطلب الثاني: سيناريو "الردع الرقمي المتبادل": صياغة قواعد اشتباك سيبرانية غير مكتوبة وأطر أمنية هجينة بين ضفتي الخليج

ينطلق السيناريو الأول من فرضية نجاح آلية "التغذية العكسية" داخل النظام الأمني الخليجي؛ حيث تدفع صدمات عام 2026 دول مجلس التعاون نحو تسريع وتيرة التكامل الدفاعي الرقمي وتطوير قدرات سيبرانية هجومية ذاتية رادعة، بالتوازي مع حوكمة حقيقية لسيادتها التكنولوجية. في ظل هذا المسار، يدرك الطرفان (الخليجي والإيراني) أن كلفة الانزلاق نحو حرب سيبرانية شاملة ومفتوحة ستؤدي إلى تدمير متبادل للبنى التحتية والاقتصادية للطرفين معاً دون تمييز (Mutually\ Assured\ Destruction). هذا الإدراك المشترك يدفع نحو نشوء حالة من "الردع الرقمي المتبادل"، تفضي بدورها إلى تبلور "قواعد اشتباك غير مكتوبة وصامتة" في الفضاء الافتراضي؛ بحيث يلتزم كل طرف

بسقوف محددة للهجمات لا تتخطى إرسال الرسائل السياسية، وتتجنب إحداث شلل كامل أو تدمير فيزيائي كارثي لمنشآت النفط والغاز، مما يؤدي إلى نمط استقرار هجين وهش يحكم العلاقات الإقليمية.

3.3.3 المطلب الثالث: سيناريو "الانفتاح الهجين والتصعيد": احتمالات تصاعد الهجمات الافتراضية المؤدية لشلل هيكلي في سلاسل إمداد الطاقة الدولية

أما السيناريو الثاني، فيفترض حدوث انهيار في كوابح الردع وحسابات العقلانية السياسية جراء تصاعد حدة التوترات الميدانية في الساحات الإقليمية الرديفة لعام 2026. في هذا المسار، تعمد طهران – تحت وطأة ضغوط هيكلية خانقة أو شعور بتهديد وجودي لنظامها – إلى تفعيل "الخيار السيبراني الأقصى" والخروج التام عن قواعد الاشتباك التقليدية. بموجب هذا السيناريو، يتم شن هجمات سيبرانية شاملة ومنسقة تستهدف تدمير نظم التحكم الصناعي (ICS/SCADA) ومحطات إسالة الغاز وتوزيع النفط في عمق دول الخليج بشكل متزامن، مما يتسبب في خروج ملايين البراميل من النفط والغاز عن الخدمة لأسابيع طويلة. إن مآلات هذا السيناريو تتجاوز الصراع الإقليمي لتحدث "شللاً هيكلياً وصدمة وجودية في سلاسل إمداد الطاقة الدولية"، تنهار على إثرها البورصات العالمية وتدخل المنظومة الاقتصادية الدولية في ركود تضخمي غير مسبوق، مما يفرض انخراطاً عسكرياً وتكنولوجياً دولياً مباشراً لإدارة الأزمة وحماية الممرات السيبرانية والجغرافية للمنطقة، وهو مسار يحمل كلفاً جيوسياسية كارثية على استقرار الإقليم ككل.

3.4 النتائج العامة للدراسة

خلصت هذه الدراسة من خلال مقاربتها التحليلية النقدية القائمة على تقاطع "جيوبوليتيكا جغرافيا الطاقة" و"جيوبوليتيكا الفضاء السيبراني" لعام 2026، إلى أن منطقة الخليج العربي باتت تعيش في ظل معادلة أمنية شديدة السيولة والتعقيد. فقد أثبت التفكيك المنهجي للظاهرة أن التفوق المادي والنفطي الكلاسيكي لم يعد كافياً لصيانة الأمن القومي في العصر الرقمي، طالما أن هذا التفوق يتحرك داخل بنية رقمية مستوردة تفتقر للسيادة التكنولوجية الكاملة. إن التفاعل البنيوي بين الاستراتيجية الهجومية الإيرانية (المدخلات) والسياسات الدفاعية الخليجية (العمليات) يكشف أن الفضاء الافتراضي تحول إلى "أداة لكسر احتكار القوة المادية"، حيث نجحت طهران في توظيف "معركة المضيق الرقمية" لفرض كلف اقتصادية وسياسية باهظة دون الانزلاق إلى مواجهة عسكرية صلبة ومكشوفة دولياً. وبناءً على ذلك، فإن مخرجات النظام الأمني الخليجي ستبقى رهن القدرة على الانتقال الجاد والمنسق من استراتيجيات الحماية الوطنية المنفردة إلى بناء نموذج رادع وشبكي متكامل يعيد صياغة قواعد الاشتباك الإقليمية لعام 2026.

4. الخاتمة

تأتي هذه الدراسة لتقدم معالجة تفكيكية رصينة لواحدة من أكثر المعضلات الأمنية إلحاحاً في العلاقات الدولية المعاصرة؛ وهي أثر عسكرة الفضاء الافتراضي على أمن وحصانة قطاع الطاقة الخليجي لعام 2026. إن استقراء الدلالات الجيوسياسية الواردة في متن البحث يؤكد بشكل قاطع أن مفهوم السيادة الوطنية لم يعد مرتبطاً فقط بحدود الأرض والممرات المائية الجغرافية الصلبة (كمضيق هرمز وباب المندب)، بل بات متلازماً عُضوياً وسياقياً مع حصانة السيادة الرقمية والممرات البرمجية الحاكمة لتدفقات الطاقة. وفي ظل بيئة إقليمية تموج بالحروب الهجينة والعمليات المعلوماتية المعقدة، تبرز الحاجة الملحة لتبني استراتيجيات دفاعية خليجية موحدة ومتجاوزة للأطر التقليدية الجافة، بما يضمن الحفاظ على عصب الاقتصاد العالمي واستقرار النظام الأمني الإقليمي الصاعد.

4.1 المساهمة العلمية

تساهم هذه الدراسة في الأدبيات العلمية من خلال تقديم دليل جيوسياسي وتأطير نظري متقدم يربط بشكل مباشر وبشري نقدي بين "جيوبوليتيكا جغرافيا الطاقة التقليدية" وصلابتها، وبين "جيوبوليتيكا الفضاء الرقمي وافتراضيته" في سياق العلاقات الخليجية-الإيرانية لعام 2026، مما يفتح آفاقاً بحثية جديدة لدراسة التهديدات غير النمطية كمتغيرات هيكلية في حقل العلوم السياسية.

4.2 التوصيات

- ✓ تأسيس "مظلة دفاع سيبراني خليجية موحدة لقطاع الطاقة": تشمل إنشاء مركز عمليات أمنية مشترك (Joint\ SOC) للتبادل اللحظي والاستخباراتي للبيانات والتهديدات المتقدمة (APTs) بين شركات النفط والغاز في مجلس التعاون.
- ✓ حوكمة وتعميق "السيادة التكنولوجية والبرمجية": عبر صياغة خطط وطنية لتعريب وتوطين بناء الخوارزميات والأنظمة المغلقة المشغلة للمنشآت النفطية الحيوية، وتقليل الاعتماد المطلق على الشركات الوسيطة العابرة للقارات.
- ✓ تبني عقيدة "الردع السيبراني النشط": من خلال إفهام الأطراف الإقليمية أن أي اختراق برمجي لمنشآت الطاقة الخليجية سيقابل برد رقمي مضاد ومتماثل يرفع كلفة الهجوم ويجبر طهران على احترام قواعد اشتباك رقمية صارمة.
- ✓ توصيات للبحوث المستقبلية: دراسة أثر حوكمة تطبيقات الحوسبة الكمومية (Quantum\ Computing) والجيل الجديد من خوارزميات التشفير على حصانة شبكات الطاقة الخليجية ضد الاختراقات المستقبلية.

المراجع

1. حجاب، محمد (2026). مستقبل العلاقات الخليجية الإيرانية وهندسة مسارات الطاقة وتوازنات الردع. *صحيفة السياسة*. المسترجع من: https://alseyassah.com/article/466648
2. ربيع، دينا رجب (2026). تقرير الحالة الإيرانية: معركة المضيق الرقمية والعمليات المعلوماتية وأثرها على أمن الطاقة. *شبكة الخليج للاستشارات الاستراتيجية*. المسترجع من: https://alkhalej.net/news/report-iran-cyber-energy
3. الرشيدي، أحمد (2018). *مناهج البحث في العلوم السياسية*. القاهرة: كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.
4. شبكة النبأ المعلوماتية (2026). مستقبل العلاقات الإيرانية-الخليجية: قراءة في مسارات الردع وضغوط الطاقة ما بعد المواجهات المستجدة. المسترجع من: https://amp.annabaa.org/arabic/reports/45718
5. مركز الإمارات للسياسات (2026). الاختبار بالنار: أزمة البحر الأحمر ومستقبل حوكمة الأمن البحري في المنطقة. *EPC*. المسترجع من: https://epc.ae/ar/details/featured/azmat-albahr-alahmar
6. مركز الحبتور للأبحاث (2026). صدمة هرمز: مستقبل الإمدادات النفطية في ظل التصعيد الجيوسياسي. *قسم الدراسات الاستراتيجية*. المسترجع من: https://www.habtoorresearch.com/ar/programmes/hormuz-energy-shocks
7. التقرير الاستراتيجي الخليجي (2026). *التحولات الهيكلية في البيئة الأمنية الإقليمية والدولية ومستقبل توازنات القوى*. جدة: مركز الخليج للأبحاث.
8. فهمي، عبد القادر محمد (2014). *النظرية في العلاقات الدولية*. عمان: دار المسيرة للنشر والتوزيع.
9. مجلة آراء الخليج (2026). أمن الخليج ومتطلباته الاعتمادية: أطر التنسيق الردعية والوقائية لبناء صيغ التعاون والتنسيق. *مركز الخليج للأبحاث*. المسترجع من: id=8334&https://araa.sa/index.php?option=com_content
10. مجلة السياسة الدولية (2026). تأثيرات البيئة الأمنية المعقدة في الشرق الأوسط ومستقبل التهديدات غير النمطية السيبرانية. *مؤسسة الأهرام*. المسترجع من: https://www.siyassa.org.eg/News/22350.aspx
11. Buzan, B., & Wæver, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.
12. Center for Strategic and International Studies - CSIS. (2026). *The Cyber-Energy Nexus: Redefining Deterrence and Vulnerabilities in the GCC Region*. CSIS Middle East Program. Washington, D.C.
13. Cyber Defense Review. (2026). *State-Sponsored Cyber Operations: An Analytical Approach to Iranian Hybrid Threats Against Critical Infrastructure*. West Point: Academic Press.
14. Easton, D. (1965). *A Systems Analysis of Political Life*. New York: John Wiley & Sons.
15. European Union Agency for Cybersecurity - ENISA. (2026). *Threat Landscape for Energy and Water Sectors: Industrial Control Systems (ICS/SCADA) Vulnerabilities*. Athens: ENISA Publications.
16. Gray, C. S. (2012). *Geopolitics and National Security*. London: Oxford University Press.
17. International Affairs Journal. (2025). *Asymmetric Warfare in the Persian Gulf: The Digital Militarization of Energy Infrastructure*. Oxford: Oxford University Press.
18. Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.
19. Microsoft. (2026). *The Digital Defense Report 2025/2026: Analyzing Advanced Persistent Threats (APTs) in Eastern Mediterranean and Gulf Energy Sectors*. Redmond: Microsoft Security Operations.

20. RAND Corporation. (2025). *Deterrence in the Digital Age: Geopolitical Implications of Cyber Attacks on Maritime and Energy Hubs*. Santa Monica: RAND Research Report.