



Original article

The impact of technology and cyberspace on geopolitics

Kawthar Hassan Ali 

University of Baghdad- Center for Urban and Regional Planning_Iraq

ABSTRACT

This study examines the impact of technology and cyberspace on geopolitics, focusing on Iraq and its regional environment. It analyzes how digital transformation has reshaped power, sovereignty, and national security.

The study uses a descriptive-analytical and comparative approach, and develops a Geo-Cyber Exposure Index based on five dimensions: digital dependency, cybersecurity readiness, geopolitical fragility, informational exposure, and institutional response capacity. The findings show that Iraq has a high level of digital dependency, scoring 89.6, while its cybersecurity readiness reached only 53.07 in the 2024 Global Cybersecurity Index. Iraq also recorded a geo-cyber exposure score of 72.1, the highest among the selected countries.

The study concludes that cyberspace has become a geopolitical domain that affects state power and security. Strengthening Iraq's geopolitical position requires improving cybersecurity readiness, protecting digital infrastructure, and developing a national strategy for digital sovereignty.

*Correspondence author:

kawthar.h@iurp.uobaghdad.edu.iq

Received: 06 May 2026

Accepted: 26 May 2026

Published: 01 August 2026

DOI:

<https://doi.org/10.31185/wjfh.Vol22.Iss3/Pt1.1950>



1812-0512 /© 2026 The Author(s). Published by Wasit Journal for Humanities Sciences, Wasit University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Cite:

Ali, K. H. (2026). The impact of technology and cyberspace on geopolitics. Wasit Journal for Human Sciences, 22(3/Pt1).

<https://doi.org/10.31185/wjfh.Vol22.Iss3/Pt1.1950>

Keywords: Technology, Cyberspace, Geopolitics, Cybersecurity, Digital Sovereignty, Iraq

تأثير التكنولوجيا والفضاء السيبراني على الجغرافيا السياسية

م.م. كوثر حسن علي

جامعة بغداد / مركز التخطيط الحضري والإقليمي للدراسات العليا / العراق

المستخلص

يهدف هذا البحث إلى دراسة أثر التكنولوجيا والفضاء السيبراني على الجغرافيا السياسية، من خلال تحليل التحولات التي طرأت على مفاهيم القوة والسيادة والأمن القومي في العصر الرقمي، مع التركيز على العراق ومحيطه الإقليمي. انطلق البحث من فرضية أساسية مفادها أن الفضاء السيبراني لم يعد مجالاً تقنياً محايداً، بل أصبح مجالاً جيوسياسياً مؤثراً يعيد تشكيل علاقة الدولة بالموقع والحدود والموارد والمجتمع والبنية التحتية.

اعتمد البحث على المنهج الوصفي التحليلي في دراسة المفاهيم النظرية، وعلى المنهج المقارن في تحليل موقع العراق مقارنة بدول مختارة هي: تركيا، إيران، السعودية، الأردن، والإمارات. كما بنى البحث نموذجاً تطبيقياً بعنوان مؤشر التعرض الجيوسبيرواني، يقوم على خمسة أبعاد رئيسية: الاعتماد الرقمي، الجاهزية السيبرانية، الهشاشة الجيوسياسية، التعرض المعلوماتي، والقدرة المؤسسية على الاستجابة.

أظهرت النتائج أن العراق يمتلك اعتماداً رقمياً مرتفعاً بلغ 89.6 في المؤشر المركب، إلا أن جاهزيته السيبرانية بلغت 53.07 فقط في مؤشر الأمن السيبراني العالمي لعام 2024، الأمر الذي خلق فجوة واضحة بين الاستخدام الرقمي والقدرة على الحماية. كما سجل العراق درجة تعرض جيوسبيرواني بلغت 72.1، وهي الأعلى بين الدول المختارة، نتيجة تداخل الاعتماد الرقمي المرتفع مع الهشاشة الجيوسياسية وضعف القدرة المؤسسية على الاستجابة.

خلص البحث إلى أن التكنولوجيا لم تلغ الجغرافيا، لكنها أضافت إليها بعداً رقمياً جديداً، وأن تعزيز موقع العراق الجيوسياسي يتطلب بناء استراتيجية وطنية للسيادة الرقمية والأمن السيبراني، وربط التحول الرقمي بالأمن القومي والتنمية والاستقرار السياسي..

الكلمات المفتاحية: التكنولوجيا، الفضاء السيبراني، الجغرافيا السياسية، الأمن السيبراني، السيادة الرقمية، العراق

المقدمة:

شهدت الجغرافيا السياسية خلال العقود الأخيرة تحولاً جوهرياً في طبيعة القوة ومجالات التنافس بين الدول، فلم تعد السيطرة الجغرافية مرتبطة فقط بالموقع الأرضي، والممرات البحرية، والموارد الطبيعية، والحدود السياسية، بل أصبحت التكنولوجيا والفضاء السيبراني من العناصر المؤثرة في إعادة تشكيل النفوذ الدولي والإقليمي.

ولم يعد الفضاء السيبراني مجرد مجال تقني محايد، بل أصبح ساحة جيوسياسية تتنافس فيها الدول والشركات الكبرى والجماعات المسلحة والفاعلون غير الحكوميين. فالهجمات السيبرانية، وحملة التضليل الرقمي، والسيطرة على البيانات، وامتلاك البنية التحتية للاتصال، باتت أدوات جديدة للتأثير السياسي والاقتصادي والأمني. ومن ثم أصبح الفضاء السيبراني عاملاً بنوياً يعيد

تشكيل العلاقات الدولية والجغرافيا السياسية، لا من خلال إلغاء الجغرافيا التقليدية، وإنما من خلال توسيع حدودها وإضافة مجال رقمي جديد إلى مجالات القوة والنفوذ .

ومن هنا جاءت هذه الدراسة لتبحث في أثر التكنولوجيا والفضاء السيبراني على الجغرافيا السياسية، والتي اعتمدت على بناء مؤشر تطبيقي للتعرض الجيوسيراني، بهدف قياس موقع العراق مقارنة بعدد من الدول الإقليمية، وتحليل مستوى التداخل بين الاعتماد الرقمي، والجاهزية السيبرانية، والهشاشة الجيوسياسية.

مشكلة البحث

1. كيف غير الفضاء السيبراني مفهوم الجغرافيا السياسية التقليدية؟
2. ما علاقة التكنولوجيا الرقمية بمفاهيم القوة والسيادة والأمن القومي؟
3. كيف تستخدم الدول والفاعلون غير الحكوميين الفضاء السيبراني كأداة للتأثير الجيوسياسي؟
4. ما مستوى تعرض العراق للتأثيرات الجيوسيرانية مقارنة بمحيطه الإقليمي؟
5. ما المؤشرات التي اعتمدها البحث لقياس العلاقة بين الاعتماد الرقمي والمخاطر الجيوسياسية؟

فرضيات البحث

1. كلما زاد الاعتماد الرقمي للدولة، زادت أهمية الأمن السيبراني في تحديد قوتها الجيوسياسية .
2. الفضاء السيبراني لا يلغي الجغرافيا التقليدية، بل يعيد تشكيلها من خلال إضافة مجال جديد للصراع والنفوذ .
3. الدول ذات البنية الرقمية الضعيفة تكون أكثر عرضة للتأثيرات السيبرانية الخارجية، حتى وإن كانت تمتلك موقعاً جغرافياً مهماً .
4. يمتلك العراق موقعاً جيوسياسياً حساساً، إلا أن ضعف البنية السيبرانية قد يحول هذا الموقع من عنصر قوة إلى مصدر هشاشة استراتيجية .
5. التنافس الإقليمي في الشرق الأوسط لم يعد محصوراً في المجال العسكري والسياسي، بل امتد إلى المجال الرقمي والإعلامي والسيبراني .

أهمية البحث

أولاً: الأهمية العلمية

تتبع الأهمية العلمية للبحث من كونه يعالج موضوعاً حديثاً يقع عند تقاطع الجغرافيا السياسية، والعلاقات الدولية، والدراسات الأمنية، والتكنولوجيا الرقمية. كما يسهم البحث في فهم أوسع لمفهوم القوة الجيوسياسية من خلال الانتقال من التركيز على المكان المادي وحده إلى دراسة العلاقة بين المجال الجغرافي التقليدي والمجال الرقمي.

ثانياً: الأهمية التطبيقية

تتمثل الأهمية التطبيقية للبحث في أنه اعتمد نموذجاً تحليلياً لقياس التعرض الجيوسيراني للدول، من خلال مجموعة من المؤشرات، منها: انتشار الإنترنت، جاهزية الأمن السيبراني، الهشاشة المؤسسية، الاعتماد على البنية التحتية الرقمية، وحجم التعرض لحملات التضليل والهجمات السيبرانية.

أهداف البحث

1. توضيح التحولات التي أحدثتها التكنولوجيا في الجغرافيا السياسية .
2. تحليل مفهوم الفضاء السيبراني بوصفه مجالاً جديداً للصراع والنفوذ .
3. بيان أثر الأمن السيبراني في السيادة الوطنية والأمن القومي.
4. دراسة موقع العراق في البيئة الجيوسياسية الإقليمية.

منهجية البحث

اعتمد البحث على المنهج الوصفي التحليلي في دراسة المفاهيم النظرية المرتبطة بالتكنولوجيا والفضاء السيبراني والجغرافيا السياسية، وذلك من خلال تحليل التحولات التي طرأت على مفاهيم القوة، والسيادة، والأمن، والحدود في البيئة الرقمية. كما اعتمد البحث على المنهج المقارن في دراسة موقع العراق مقارنة بالدول الإقليمية المختارة، وهي: إيران، وتركيا، والسعودية، والأردن، والإمارات.

وفي الجانب التطبيقي، بنى البحث مؤشراً مركباً بعنوان **مؤشر التعرض الجيوسبراني**، وذلك بهدف قياس مستوى تعرض العراق ومحيطه الإقليمي للمخاطر الجيوسبرانية. واعتمد البحث في بناء هذا المؤشر على بيانات ومؤشرات صادرة عن الاتحاد الدولي للاتصالات، والبنك الدولي، وتقارير DataReportal، وتقارير Freedom House، إضافة إلى تقارير الأمن السيبراني. كما دعم البحث تحليله باستبانة خبراء موجهة إلى مختصين في الجغرافيا السياسية، والأمن السيبراني، والإعلام الرقمي، والعلاقات الدولية، بهدف تعزيز الجانب التطبيقي وربط المؤشرات الرقمية بالتحليل الجيوسياسي.

حدود البحث

أولاً: الحدود الموضوعية

اقتصر البحث على دراسة أثر التكنولوجيا والفضاء السيبراني في الجغرافيا السياسية، مع التركيز على مفاهيم القوة، والسيادة، والأمن، والتنافس الإقليمي. كما ركز على العلاقة بين الاعتماد الرقمي والجاهزية السيبرانية والهشاشة الجيوسياسية.

ثانياً: الحدود المكانية

تمثلت الحدود المكانية للبحث في العراق ومحيطه الإقليمي، مع اختيار خمس دول للمقارنة، وهي: إيران، وتركيا، والسعودية، والأردن، والإمارات. وقد جاء اختيار هذه الدول بسبب قربها الجغرافي أو تأثيرها الإقليمي أو حضورها في بيئة التنافس الجيوسياسي والسيبراني المحيطة بالعراق.

ثالثاً: الحدود الزمانية

غطى البحث الفترة الممتدة من عام 2020 إلى عام 2026، وهي فترة شهدت تسارعاً واضحاً في التحول الرقمي، وتضاعفاً في توظيف الفضاء السيبراني ضمن الصراعات الدولية والإقليمية، فضلاً عن ازدياد الاعتماد على الإنترنت والمنصات الرقمية في المجالات السياسية والاقتصادية والاجتماعية والأمنية.

الدراسات السابقة

1. دراسة Foulon and Meibauer ، 2024

تناولت دراسة فولون ومايباور أثر الفضاء السيبراني في العلاقات الدولية، وقدمت تصورًا نظريًا مهمًا يرى أن الفضاء السيبراني يعمل بوصفه "معدّلًا بنيويًا" للعلاقات الدولية، أي أنه لا يستبدل النظام الدولي التقليدي، ولا يلغي منطق القوة والجغرافيا، ولكنه يغير طريقة اشتغالها وحدود تأثيرها. وقد اعتمد البحث الحالي على هذه الدراسة في بناء الإطار النظري المتعلق بعلاقة الفضاء السيبراني بالجغرافيا السياسية (Foulon & Meibauer, 2024)

2. تقرير الاتحاد الدولي للاتصالات: مؤشر الأمن السيبراني العالمي 2024

يُعد تقرير مؤشر الأمن السيبراني العالمي 2024 الصادر عن الاتحاد الدولي للاتصالات من أهم المصادر التطبيقية التي اعتمد عليها البحث في قياس جاهزية الدول في مجال الأمن السيبراني. وقد اعتمد البحث الحالي على هذا التقرير في بناء البعد الخاص بالجاهزية السيبرانية ضمن مؤشر التعرض الجيوسياسي (International Telecommunication Union, 2024)

3. مؤشر القوة السيبرانية الوطنية، مركز بلفر، جامعة هارفارد، 2022

قدم مؤشر القوة السيبرانية الوطنية 2022 الصادر عن مركز بلفر في جامعة هارفارد إطارًا تحليليًا لقياس القوة السيبرانية للدول من خلال الجمع بين القدرات السيبرانية والأهداف الوطنية. وقد اعتمد البحث الحالي على هذا المؤشر في فهم العلاقة بين القوة السيبرانية والقوة الجيوسياسية، وفي دعم التحليل الخاص بكيفية انتقال القوة من المجال العسكري والمادي التقليدي إلى المجال الرقمي والسيبراني (Voo et al., 2022)

4. تقرير IISS Cyber Power Matrix ، 2024

يعرض تقرير IISS Cyber Power Matrix: Context and Methodology الصادر عن المعهد الدولي للدراسات الاستراتيجية تصورًا حديثًا لكيفية استخدام الدول للقدرات السيبرانية وقد اعتمد البحث على هذا التقرير في تحليل العلاقة بين البنية التحتية الرقمية، والعمليات السيبرانية، وموقع الدولة ضمن بيئة التنافس الدولي والإقليمي (International Institute for Strategic Studies, 2024)

المبحث الأول

الإطار المفاهيمي للتكنولوجيا والفضاء السيبراني في الجغرافيا السياسية

أحدثت التكنولوجيا الرقمية تحولًا عميقًا في بنية الجغرافيا السياسية المعاصرة، إذ لم تعد القوة تُقاس فقط بعناصرها التقليدية المتمثلة في الموقع، والمساحة، والموارد، والسكان، والقدرة العسكرية، بل أصبحت تُقاس أيضًا بقدرة الدولة على امتلاك التكنولوجيا، وإدارة البيانات، والتحكم بتدفقات المعلومات، وحماية بنيتها الرقمية. ومن ثم فإن دراسة الجغرافيا السياسية في العصر الراهن لم تعد تكتمل من دون إدخال البعد السيبراني بوصفه مجالًا جديدًا لإنتاج القوة والتأثير والصراع (محمود، 2025، ص. 250-260)

والدولة التي تمتلك القدرة على إنتاج المعرفة الرقمية، وحماية شبكاتها، وتطوير تقنياتها، والتأثير في الفضاء المعلوماتي، تصبح أكثر قدرة على تحويل التكنولوجيا إلى نفوذ سياسي وأمني واقتصادي. وبذلك انتقلت التكنولوجيا من كونها وسيلة تقنية إلى كونها عنصرًا جيوسياسيًا مؤثرًا في ترتيب الدول ومكانتها داخل النظام الدولي (عياد، 2023، ص. 113-147)

المطلب الأول

مفهوم التكنولوجيا والفضاء السيبراني

يقصد بالتكنولوجيا مجموع الأدوات والأنظمة والمعارف الرقمية التي تستخدم في إنتاج المعلومات، ومعالجتها، وتخزينها، ونقلها، وتوظيفها في مجالات القوة المختلفة. وبهذا المعنى لا تنحصر التكنولوجيا في الأجهزة أو البرمجيات، بل تشمل البنية الرقمية الكاملة التي تضم شبكات الاتصال، والخوادم، وقواعد البيانات، وأنظمة الذكاء الاصطناعي، والمنصات الرقمية، وأنظمة الحماية والهجوم السيبراني. وبذلك تصبح التكنولوجيا أداة لإدارة المجال وإعادة توزيع القوة بين الدول (دسوقي وقطب، 2025، ص. 471-561).

أما الفضاء السيبراني فيقصد به المجال الرقمي الناتج عن ترابط الشبكات الحاسوبية وأنظمة الاتصال وقواعد البيانات والمنصات الرقمية، وهو مجال لا يقوم على الأرض بمعناها التقليدي، لكنه لا ينفصل عنها تمامًا. فالفضاء السيبراني يقوم على طبقات متعددة، منها طبقة مادية تتمثل في الكابلات البحرية، والأقمار الصناعية، ومراكز البيانات، ومحطات الاتصالات، وشبكات الطاقة، وطبقة منطقية تتمثل في البروتوكولات والبرمجيات وأنظمة التشغيل، وطبقة اجتماعية/معلوماتية تتعلق بالمستخدمين والمحتوى والبيانات والتفاعل الرقمي. (صابر، 2022، ص. 31-45).

ويختلف الفضاء السيبراني عن الفضاء الجغرافي التقليدي من حيث طبيعة الحدود والسرعة والقدرة على الاختراق. ففي الجغرافيا التقليدية تكون الحدود السياسية واضحة نسبيًا، وترتبط السيادة بالأرض والبحر والجو، أما في الفضاء السيبراني فإن الاختراق قد يتم عبر الحدود دون انتقال مادي، وقد تنطلق الهجمات أو حملات التأثير من خوادم موزعة في أكثر من دولة. لذلك فإن مفهوم الحدود في العصر الرقمي لم يعد كافيًا لفهم الأمن القومي، لأن الدولة قد تتعرض لتهديدات داخل مجالها الحيوي من دون أن يحدث عبور عسكري أو احتلال جغرافي مباشر (مسكة، 2022، ص. 447-462) ولا يعني ذلك أن الفضاء السيبراني يلغي الجغرافيا، بل إنه يعيد تشكيلها. فالكابلات البحرية التي تنقل معظم حركة الإنترنت العالمية تمر عبر ممرات بحرية ونقاط اختناق استراتيجية، ومراكز البيانات تحتاج إلى طاقة وموقع آمن واستقرار سياسي، والأقمار الصناعية ترتبط بمدارات ومراكز تحكم أرضية، وشبكات الاتصالات ترتبط بسلطة الدولة وقوانينها. وبذلك فإن الفضاء السيبراني يبدو عابرًا للحدود، لكنه في جوهره مشروط بمواقع مادية وبنى تحتية قائمة داخل الجغرافيا السياسية للدول (الدروزي، 2024، ص. 851-880).

ومن الناحية السياسية، أصبح الفضاء السيبراني مجالًا لإنتاج التأثير، لأن البيانات والمنصات الرقمية لم تعد أدوات تواصل فقط، بل تحولت إلى أدوات لتشكيل الرأي العام، وبناء الصورة الذهنية، والتأثير في السلوك الانتخابي والاجتماعي، وإدارة الأزمات، ونشر التضليل أو مقاومته. (فوزي، 2019، ص. 99-139) كما أصبح الفضاء السيبراني ساحة لصراع القوى

الدولية والإقليمية، حيث تستخدم الدول المتقدمة قدراتها الرقمية لتعزيز نفوذها، وجمع المعلومات، وإدارة العمليات الاستخباراتية، والتأثير في الخصوم دون اللجوء إلى حرب عسكرية مباشرة. (ذاري، 2023، ص. 338-367).

وتتضح أهمية هذا التحول عند النظر إلى حجم الاعتماد الرقمي في العراق، إذ أظهرت بيانات DataReportal لعام 2024 أن عدد مستخدمي الإنترنت في العراق بلغ 36.22 مليون مستخدم في بداية عام 2024، بنسبة انتشار بلغت 78.7% من السكان، كما بلغ عدد مستخدمي وسائل التواصل الاجتماعي 31.95 مليون مستخدم، أي ما يعادل 69.4% من السكان. وتعني هذه الأرقام أن المجتمع العراقي أصبح جزءاً واسعاً من الفضاء الرقمي، الأمر الذي يجعل الأمن السيبراني والتأثير المعلوماتي عنصرين مباشرين في الجغرافيا السياسية الداخلية والخارجية للدولة (DataReportal, 2024).

وتزداد أهمية الفضاء السيبراني عندما يُقارن مستوى الاعتماد الرقمي بمستوى الجاهزية السيبرانية، لأن ارتفاع الاستخدام لا يعني بالضرورة ارتفاع القدرة على الحماية. فقد أظهر مؤشر الأمن السيبراني العالمي لعام 2024 أن تقييم الدول يتم وفق خمسة محاور هي: الإجراءات القانونية، والإجراءات التقنية، والإجراءات التنظيمية، وبناء القدرات، والتعاون. ووفق بيانات المؤشر، جاء العراق ضمن مستوى التأسيس/التطور المحدود بدرجة 53.07، في حين جاءت الأردن بدرجة 98.6، وإيران بدرجة 65.52، وهو ما يكشف أن الفجوة بين الاستخدام الرقمي والجاهزية السيبرانية تمثل عامل هشاشة جيوسياسية مهماً. (الزبيدي والتميمي، 2022، ص. 39-60).

ومن هذا المنطلق، اعتمد البحث مفهوم الفضاء السيبراني باعتباره مجالاً جيوسياسياً مركباً، فالفضاء السيبراني لا يلغي القوة العسكرية أو الموقع الجغرافي لكنه يضيف إليها بعداً جديداً من التنافس، ويجعل الدول والفاعلين غير الحكوميين قادرين على التأثير بوسائل منخفضة الكلفة وسريعة الانتشار وصعبة الإسناد أحياناً. وبذلك يصبح الفضاء السيبراني "معدلاً بنيوياً" في العلاقات الدولية والجغرافيا السياسية.

المطلب الثاني

تطور الجغرافيا السياسية في ظل الثورة الرقمية

عرفت الجغرافيا السياسية التقليدية اهتماماً أساسياً بعناصر الأرض والموقع والحدود والممرات والموارد والسكان، إلا أن الثورة الرقمية أضافت إلى هذه العناصر مجالاً جديداً هو المجال السيبراني. فلم يعد الموقع الجغرافي وحده كافياً لتفسير قوة الدولة، بل أصبحت قدرة الدولة على إدارة المجال الرقمي، وحماية بياناتها، والسيطرة والتأثير في الفضاء المعلوماتي، جزءاً من تحليل موقعها الجيوسياسي. ولذلك انتقلت الجغرافيا السياسية من تحليل المجال المادي وحده إلى تحليل التفاعل بين المجال المادي والمجال الرقمي (جمال الدين، 2023، ص. 189-230) وقد أدى تطور الذكاء الاصطناعي والمنصات الرقمية إلى إعادة تعريف القوة في العلاقات الدولية، بل أصبحت تشمل امتلاك الخوارزميات، والقدرة على تحليل البيانات، والتحكم في سلاسل التكنولوجيا، وحماية البنية التحتية الرقمية. كما أن السيطرة على المنصات وشبكات الاتصال قد تمنح الدولة أو الشركة قدرة على التأثير تتجاوز أحياناً حدودها الجغرافية. (خليل، 2023، ص. 266-302).

وفي ظل هذه التحولات، أصبحت الحروب غير التقليدية تعتمد بصورة متزايدة على الفضاء السيبراني، سواء من خلال الهجمات الإلكترونية، أو تعطيل الخدمات، أو اختراق المؤسسات، أو نشر الدعاية والتضليل، أو توظيف جماعات وفاعلين غير حكوميين في تنفيذ عمليات يصعب ربطها مباشرة بالدول. (عبد الحميد، 2021، ص. 167-190).

وتظهر التجربة الروسية في توظيف القوة السيبرانية مثالاً فقد استخدمت روسيا القوة السيبرانية ضمن أدواتها الاستراتيجية في إدارة علاقاتها وصراعاتها الخارجية، إذ أن الدول الكبرى باتت تتعامل مع الفضاء السيبراني بوصفه امتداداً لسياستها الخارجية. (محمود، 2025، ص. 311-334) وأما بالنسبة للدول ذات البنية المؤسسية الضعيفة، فإن الثورة الرقمية تخلق فرصاً وتحديات في الوقت نفسه. فمن جهة، تمنح التكنولوجيا إمكانات لتطوير الإدارة والخدمات والتعليم والاقتصاد، ومن جهة أخرى تفتح المجال أمام مخاطر الاختراق والتبعية التقنية وفقدان السيطرة على البيانات. لذلك فإن امتلاك التكنولوجيا دون امتلاك القدرة لإدارتها قد يحول التحول الرقمي من فرصة تنموية إلى مصدر هشاشة استراتيجية (Kello, 2017).

وفي هذا السياق، أصبحت السيادة الرقمية امتداداً للسيادة التقليدية، لأن الدولة لم تعد مطالبة بحماية حدودها البرية والبحرية والجوية فقط، بل أصبحت مطالبة بحماية بياناتها، وشبكاتها، وبنيتها التحتية الحيوية، ومنصاتها الإعلامية، وفضائها المعلوماتي. ومن ثم فإن الأمن السيبراني أصبح جزءاً من الأمن القومي، (Fischerkeller et al., 2022).

المبحث الثاني

أثر الفضاء السيبراني في قوة السيادة للأمن القومي

أدى صعود الفضاء السيبراني إلى إعادة تشكيل العلاقة بين القوة والسيادة والأمن القومي، إذ لم تعد الدولة تواجه تهديداتها من المجال العسكري أو السياسي أو الاقتصادي فقط، بل أصبحت تواجه نمطاً جديداً من التهديدات العابرة للحدود، التي تستهدف البيانات والشبكات والبنى التحتية والرأي العام والمؤسسات الحيوية. ومن ثم فإن الأمن القومي في البيئة الرقمية لم يعد مقتصرًا على حماية الأرض والحدود، بل امتد إلى حماية المجال السيبراني للدولة بوصفه مجالاً جديداً تتفاعل فيه عناصر القوة والضعف (طه، 2023، ص. 178-229).

وتتبع أهمية هذا المبحث من أن الفضاء السيبراني لم يعد مجرد امتداد تقني للاتصالات، بل أصبح أداة لإنتاج القوة وممارسة التأثير. فالدولة التي تمتلك القدرة على جمع البيانات وتحليلها، وحماية شبكاتنا، وتطوير قدراتها الهجومية والدفاعية، وإدارة تدفقات المعلومات، تستطيع أن تعزز موقعها الجيوسياسي حتى لو لم تستخدم القوة العسكرية المباشرة. (عزيز ومحمد، 2023، ص. 228-256).

المطلب الأول

الفضاء السيبراني وإعادة تشكيل مفهوم القوة

أصبحت القوة في العصر الرقمي تشمل السيطرة على البيانات، وامتلاك البنية التحتية الرقمية، والقدرة على حماية الشبكات، وتنفيذ العمليات السيبرانية، وإدارة الرأي العام عبر المنصات الرقمية. وبذلك أصبح الفضاء السيبراني ميداناً جديداً للقوة، لأنه يسمح للدول بتحقيق أهداف سياسية وأمنية واقتصادية بكلفة أقل وبسرعة أكبر من الأدوات التقليدية (محسن، 2025).

وتحتاج القوة السيبرانية إلى بنية تحتية رقمية، ومراكز بيانات، وشبكات اتصال، وكوادر تقنية، وتشريعات، ومؤسسات أمنية، وقدرات استخبارية، فضلاً عن قدرة على التأثير الإعلامي والنفسي.

لذلك فإن القوة السيبرانية هي قدرة استراتيجية مركبة، تتداخل فيها التكنولوجيا مع السياسة والأمن والاقتصاد والقانون (شويرب ومراد، 2023، ص. 157-178).

وتظهر خطورة القوة السيبرانية في أنها تمنح الفاعلين قدرة على تعطيل البنى التحتية الحيوية من دون الدخول في مواجهة عسكرية مباشرة. فقد أصبحت شبكات الكهرباء والمياه والطاقة والمصارف والمطارات والمستشفيات والاتصالات أهدافاً محتملة للهجمات السيبرانية، لأن هذه القطاعات تعتمد على أنظمة رقمية مترابطة تحول التهديد السيبراني إلى تهديد وطني شامل (بوطالعة ووكورو، 2022، ص. 322-355). وأصبح مفهوم الردع القدرة على منع الهجمات السيبرانية، وكشف مصادرها، والرد عليها، ورفع كلفة الاعتداء على الخصم. غير أن الردع السيبراني يواجه صعوبة أساسية تتمثل في مشكلة الإسناد، أي صعوبة تحديد الجهة التي نفذت الهجوم بدقة، خصوصاً عندما تستخدم الخوادم الوسيطة أو الجماعات الوكيلية أو الهويات الرقمية المزيفة (العيسى وعناب، 2019، ص. 81-95)، مكن الفضاء السيبراني الفاعلين غير الحكوميين من امتلاك أدوات تأثير لم تكن متاحة سابقاً إلا للدول. وهذا التحول أضعف احتكار الدولة التقليدي لأدوات القوة، وجعل المجال الشباني أكثر تعقيداً من المجال الجغرافي التقليدي (الديب، 2025، ص. 1203-1238).

وتبرز الانتخابات والرأي العام بوصفهما مجالين أساسيين لتأثير القوة السيبرانية، إذ يمكن استخدام القرصنة الإلكترونية، وتسريب البيانات، والحسابات الوهمية، والإعلانات السياسية الموجهة، والتضليل الرقمي، للتأثير في مواقف الناخبين أو تشويه صورة الخصوم أو زعزعة الثقة بالمؤسسات. وفي هذه الحالة لا يكون الخطر السيبراني مجرد اختراق ل خادم أو موقع إلكتروني، بل يصبح اختراقاً للمجال العام، وإعادة توجيه للنقاش السياسي والاجتماعي، وإضعافاً للثقة بين المواطن والدولة (باسماعيل، 2022، ص. 141-160).

وقد أظهرت المؤشرات الدولية الحديثة أن البيئة السيبرانية العالمية تتجه نحو مزيد من التعقيد؛ إذ أشار تقرير المنتدى الاقتصادي العالمي لعام 2025 إلى أن 72% من المشاركين في الاستطلاع أكدوا ارتفاع المخاطر السيبرانية خلال السنة السابقة، كما أشار إلى أن 54% من المؤسسات الكبرى تعد مخاطر سلاسل التوريد من أبرز عوائق المرونة السيبرانية. وهذا يعني أن الخطر السيبراني لم يعد خطراً منفصلاً داخل مؤسسة واحدة، بل أصبح مرتبطاً بشبكات الموردين والشركات والمنصات والبنى الرقمية العابرة للحدود (شحيوط وقريب، 2022، ص. 58)، اعتمد البحث مفهوم القوة السيبرانية بوصفها امتداداً للقوة الجيوسياسية. فالدولة القوية في العصر الرقمي ليست فقط الدولة التي تملك جيشاً واقتصاداً وموقعاً استراتيجياً، بل هي الدولة التي تملك كذلك قدرة سيبرانية متقدمة، ومؤسسات رقمية مرنة، ونظاماً قانونياً وتنظيمياً قادراً على حماية المجال الرقمي.

المطلب الثاني

السيادة الرقمية والأمن القومي في البيئة السيبرانية

تعني السيادة الرقمية قدرة الدولة على ممارسة سلطتها داخل المجال الرقمي، من خلال حماية بياناتها الوطنية، وتنظيم منصاتها، وتأمين بنيتها التحتية، وضبط انتقال المعلومات، وصياغة التشريعات والسياسات التي تمنع تحول الفضاء السيبراني إلى مجال

مفتوح للاختراق أو التبعية. (عبد العظيم، 2023، ص. 67) ويُعد توطين البيانات أحد مظاهر السيادة الرقمية، لأنه يرتبط بسؤال جوهري: أين تُخزن بيانات المواطنين والمؤسسات؟ ومن يملك حق الوصول إليها؟ وما القوانين التي تخضع لها؟ فالدولة التي تعتمد كلياً على بنى تحتية رقمية خارجية أو منصات أجنبية في حفظ بياناتها الحساسة قد تواجه تهديداً مباشراً لسيادتها، خصوصاً عند حدوث أزمات سياسية أو عقوبات أو صراعات إقليمية. ولذلك اتجهت بعض الدول إلى سياسات توطين البيانات من أجل تقليل التبعية الرقمية وتعزيز التحكم الوطني بالمعلومات (لطي، 2022، ص. 151-178) ولا تتفصل السيادة الرقمية عن الأمن القومي، لأن اختراق البيانات الحكومية أو المصرفية أو الأمنية يمكن أن يؤدي إلى آثار سياسية واقتصادية واجتماعية خطيرة. فالهجوم السيبراني على مؤسسة مالية قد يؤدي إلى تعطيل المعاملات، وفقدان الثقة بالنظام المصرفي، وتسريب معلومات العملاء، بينما قد يؤدي الهجوم على شبكة كهرباء أو اتصالات إلى شلل في الخدمات الأساسية، وهو ما يجعل الأمن السيبراني جزءاً مباشراً من الأمن الوطني الشامل (International Monetary Fund, 2024).

وفي هذا السياق، أشار صندوق النقد الدولي في تقرير الاستقرار المالي العالمي لعام 2024 إلى أن عدد الهجمات السيبرانية تضاعف تقريباً مقارنة بما قبل جائحة كوفيد-19، وأن القطاع المالي يتعرض بدرجة عالية للمخاطر السيبرانية، إذ إن ما يقارب خمس الحوادث السيبرانية يؤثر في المؤسسات المالية، كما ارتفع خطر الخسائر الشديدة إلى ما لا يقل عن 2.5 مليار دولار في بعض الحالات. وتؤكد هذه المؤشرات أن المصارف والخدمات المالية أصبحت من أكثر القطاعات حساسية في الأمن القومي السيبراني (علام، 2025، ص. 373-394) كما يشكل قطاع الطاقة أحد أكثر القطاعات تعرضاً للخطر، لأن منظومات الكهرباء والنفط والغاز تعتمد على أنظمة تحكم صناعي وشبكات اتصال ومراكز مراقبة رقمية. وأي اختراق لهذه المنظومات قد يؤدي إلى تعطيل الإنتاج أو النقل أو التوزيع، وقد يتحول إلى أزمة اقتصادية وسياسية. لذلك فإن حماية البنية التحتية للطاقة لم تعد مسألة هندسية فقط، بل أصبحت جزءاً من استراتيجية الأمن القومي والسيادة الرقمية (بيرم، 2020). أما قطاع الاتصالات فيمثل العمود الفقري للسيادة الرقمية، لأنه يربط الأفراد والمؤسسات والأسواق والحكومة. فإذا فقدت الدولة السيطرة على شبكات الاتصال أو تعرضت هذه الشبكات للاختراق أو التعطيل، فإن قدرتها على إدارة الأزمات وتقديم الخدمات وحماية البيانات تصبح مهددة. ومن هنا تظهر أهمية بناء شبكات اتصال آمنة، وتطوير مراكز استجابة وطنية، وتعزيز التشريعات التي تنظم حماية البيانات والبنى التحتية الرقمية. إذ يؤدي التحول نحو الحكومة الإلكترونية إلى زيادة اعتماد المواطنين والمؤسسات على المنصات الحكومية.

الدراسة التطبيقية

قياس الأثر الجيوسياسي للتكنولوجيا على موقع العراق الجغرافي الإقليمي

ينتقل هذا المبحث من الإطار النظري إلى التحليل التطبيقي، من خلال بناء نموذج قياسي مركب لقراءة أثر التكنولوجيا والفضاء السيبراني في موقع العراق الجيوسياسي مقارنة بعدد من الدول الإقليمية المختارة، وهي: تركيا، إيران، السعودية، الأردن، والإمارات. وقد اعتمد البحث على مؤشرات كمية مأخوذة من مصادر دولية حديثة، منها تقارير DataReportal الخاصة بالتحول الرقمي، ومؤشر الأمن السيبراني العالمي الصادر عن الاتحاد الدولي للاتصالات، ومؤشر حرية الإنترنت الصادر عن Freedom House، ومؤشر الدول الهشة الصادر عن Fund for Peace. ويهدف هذا الدمج إلى تجاوز الوصف

العام نحو بناء قراءة مركبة تربط بين الاعتماد الرقمي، والجاهزية السيبرانية، والهشاشة الجيوسياسية، والتعرض المعلوماتي، والقدرة المؤسسية على الاستجابة .

المطلب الأول

تصميم النموذج التطبيقي ومؤشرات القياس

اعتمد البحث نموذجًا تطبيقيًا بعنوان **مؤشر التعرض الجيوسيراني للعراق ومحيطه الإقليمي**، وهو مؤشر مركب يقيس درجة تعرض الدولة للمخاطر الناتجة عن تداخل الاعتماد الرقمي مع ضعف الجاهزية السيبرانية والهشاشة الجيوسياسية والتعرض المعلوماتي. وقد تم اختيار هذا النموذج لأن الخطر الجيوسيراني لا ينتج عن عامل واحد، بل عن علاقة مركبة بين كثافة استخدام الإنترنت والمنصات الرقمية، وقدرة الدولة على الحماية والاستجابة، وطبيعة موقعها السياسي والأمني داخل الإقليم. وقد اعتمد البحث خمسة أبعاد هي: الاعتماد الرقمي، والجاهزية السيبرانية، والهشاشة الجيوسياسية، والتعرض المعلوماتي، والقدرة على الاستجابة. وتم تحويل القيم إلى مقياس موحد من 0 إلى 100 لتسهيل المقارنة بين الدول، مع مراعاة أن ارتفاع الدرجة لا يحمل المعنى نفسه في جميع الأبعاد؛ فارتفاع الاعتماد الرقمي يعني اتساع المجال الرقمي وارتفاع الجاهزية السيبرانية يعني قدرة أعلى على الحماية، بينما ارتفاع الهشاشة أو التعرض المعلوماتي يعني مستوى خطر أكبر.

الجدول (1): أبعاد مؤشر التعرض الجيوسيراني ومؤشرات القياس

البعد	المؤشرات الفرعية المعتمدة	مصدر البيانات	طريقة القياس
الاعتماد الرقمي	انتشار الإنترنت، كثافة وسائل التواصل، اتصالات الهاتف المحمول	DataReportal / GSMA / ITU	متوسط معياري من 0 إلى 100
الجاهزية السيبرانية	الإطار القانوني، التقني، التنظيمي، بناء القدرات، التعاون الدولي	ITU Global Cybersecurity Index 2024	درجة من 0 إلى 100
الهشاشة الجيوسياسية	هشاشة الدولة، الاستقرار المؤسسي، الضغط الأمني والسياسي	Fragile States Index 2024	تحويل درجة المؤشر من 100 إلى 120
التعرض المعلوماتي	كثافة وسائل التواصل + انخفاض حرية الإنترنت	Freedom House / DataReportal	معادلة مركبة من 0 إلى 100
القدرة على الاستجابة	الجاهزية السيبرانية + انخفاض الهشاشة الجيوسياسية	ITU GCI / FSI	معادلة مركبة من 0 إلى 100

مصدر الجدول: من إعداد الباحث بالاعتماد على منهجية مؤشر الأمن السيبراني العالمي الذي يقيس الالتزام السيبراني عبر خمسة محاور رئيسية، وعلى بيانات DataReportal و Freedom House و Fragile States Index. واحتسب البحث درجة الاعتماد الرقمي من خلال متوسط ثلاثة مؤشرات: نسبة انتشار الإنترنت، وكثافة مستخدمي وسائل التواصل الاجتماعي، ونسبة اتصالات الهاتف المحمول إلى السكان. وعند تجاوز بعض القيم نسبة 100%، كما في حالات الإمارات والسعودية والعراق في اتصالات الهاتف أو وسائل التواصل، تم تثبيت الحد الأعلى عند 100% حتى لا تؤدي الحسابات إلى تضخيم المؤشر، لأن بعض الأفراد يمتلكون أكثر من اتصال أو أكثر من هوية رقمية. وقد أشار DataReportal نفسه إلى أن أرقام وسائل التواصل قد تتجاوز عدد السكان لأسباب تتعلق بتعدد الحسابات أو منهجية قياس "هويات المستخدمين" لا الأفراد الفريدين .

أما درجة الجاهزية السيبرانية فقد اعتمدت على مؤشر الأمن السيبراني العالمي لعام 2024، إذ حصل العراق على 53.07، مقابل 100 لكل من تركيا والسعودية والإمارات، و 98.60 للأردن، و 65.52 لإيران. وتكشف هذه القيم أن العراق لا يعاني من ضعف في الاستخدام الرقمي، بل من فجوة بين اتساع الاعتماد الرقمي ومستوى الجاهزية المؤسسية والسيبرانية . واعتمد البحث في قياس الهشاشة الجيوسياسية على مؤشر الدول الهشة لعام 2024، حيث سجل العراق 88.6 من أصل 120، وهي درجة مرتفعة مقارنة بالإمارات التي سجلت 34.7، والسعودية 63.2، والأردن 74.3، وإيران 82.9، وتركيا 84.0. وقد تم تحويل هذه القيم إلى مقياس 100 لتوحيدها مع بقية أبعاد المؤشر .

المطلب الثاني

عرض النتائج التطبيقية وتحليلها

أظهرت النتائج أن العراق يقع في منطقة خطر جيوسيراني مرتفعة نسبيًا، ليس لأنه الأعلى رقميًا بين الدول المختارة، بل لأن اعتماده الرقمي يتزايد بالتزامن مع جاهزية سيبرانية أقل وهشاشة جيوسياسية أعلى. فقد بلغ عدد مستخدمي الإنترنت في العراق وفق تقرير Digital 2026 نحو 39.6 مليون مستخدم، بنسبة انتشار 83.8%، كما بلغ عدد هويات مستخدمي وسائل التواصل 40.1 مليون، أي ما يعادل 84.9% من السكان، مع وجود 50.8 مليون اتصال خلوي بما يعادل 108% من السكان .

الجدول (2): مقارنة الاعتماد الرقمي بين العراق ودول مختارة

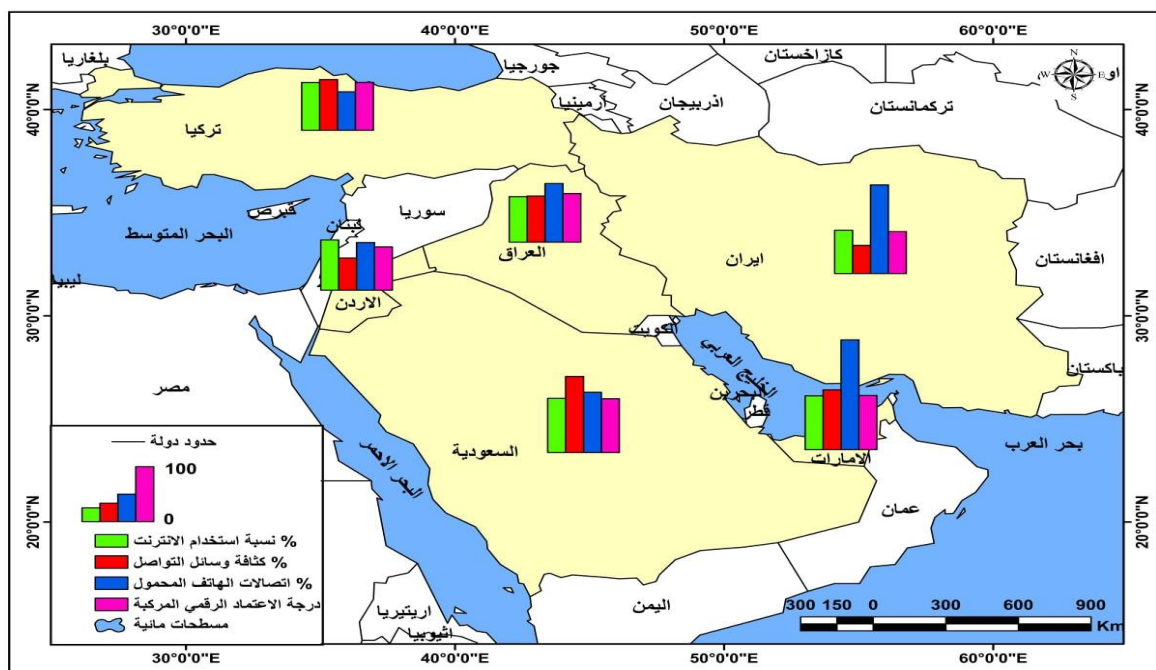
الدولة	نسبة استخدام الإنترنت %	كثافة وسائل التواصل %	اتصالات الهاتف المحمول %	درجة الاعتماد الرقمي المركبة	مستوى الاعتماد الرقمي
العراق	83.8	84.9	108	89.6	مرتفع جدًا
تركيا	88.3	70.9	93.4	84.2	مرتفع
إيران	79.6	51.8	163.1	77.1	مرتفع

السعودية	99	111	140	99.7	مرتفع جدًا
الأردن	92.5	59.2	87.7	79.8	مرتفع
الإمارات	99	110	202	99.7	مرتفع جدًا

مصدر الجدول :من إعداد الباحث اعتمادًا على تقارير DataReportal Digital 2026 للعراق وتركيا وإيران والسعودية والأردن والإمارات .

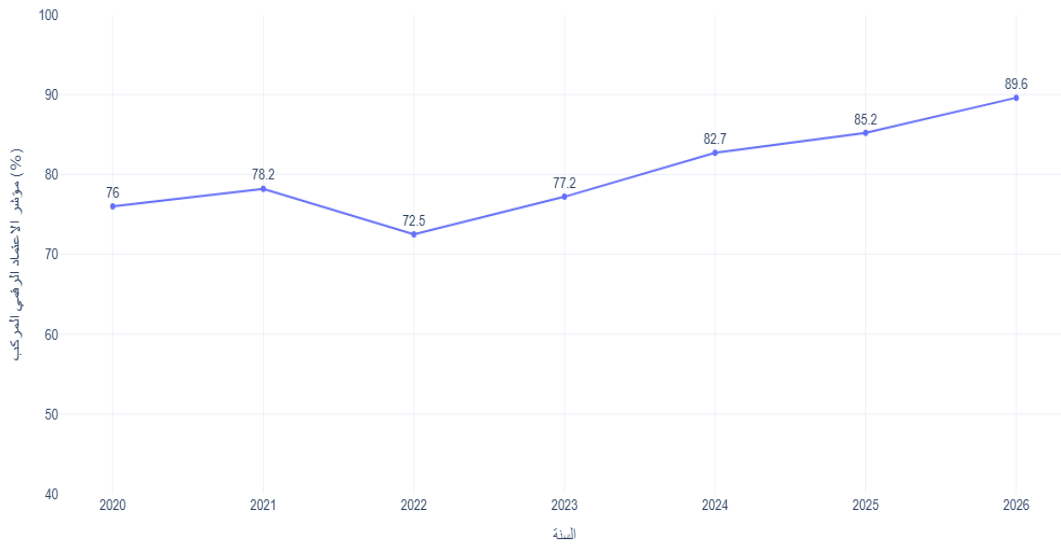
يبين الجدول أن السعودية والإمارات تمثلان أعلى مستوى في الاعتماد الرقمي بسبب شبه اكتمال انتشار الإنترنت وارتفاع كثافة الاتصالات والمنصات الرقمية. إلا أن العراق يبرز بوصفه حالة خاصة، إذ إن درجة الاعتماد الرقمي المركبة بلغت 89.6، وهي قريبة من مستويات الدول الأعلى رقميًا، لكنها لا تقابلها درجة جاهزية سيبرانية مماثلة، الأمر الذي يخلق فجوة بين الاستخدام والحماية. وهذه الفجوة هي جوهر الخطر الجيوسياسي في الحالة العراقية.

خريطة (1) التوزيع الجغرافي للاعتماد الرقمي بين العراق ودول مختارة



مصدر الخريطة : من اعداد الباحث بالاعتماد على بيانات جدول (2)

الشكل (1): تطور مؤشر الاعتماد الرقمي المركب في العراق 2020-2026



%المتوسط = متوسط انتشار الإنترنت + كفاءة وسائل التواصل + اتصالات الهاتف المحمول بعد ضبط القيم في تجزئة 100

الشكل (1): منحى تطور الاعتماد الرقمي المركب في العراق 2026-2020

يظهر الشكل أن مؤشر الاعتماد الرقمي المركب في العراق ارتفع من 76.0 عام 2020 إلى 89.6 عام 2026، مع تنذب واضح في عام 2022 بسبب اختلاف منهجيات القياس وتعديل بيانات مستخدمي الإنترنت في تقارير DataReportal. وعلى الرغم من هذا التذبذب، فإن الاتجاه العام يؤكد انتقال العراق إلى مجتمع أكثر ارتباطاً بالفضاء الرقمي، وهو ما يعني أن أي اختراق أو تعطيل أو حملة تضليل واسعة يمكن أن تترك أثراً مباشراً في المجالين السياسي والاجتماعي.

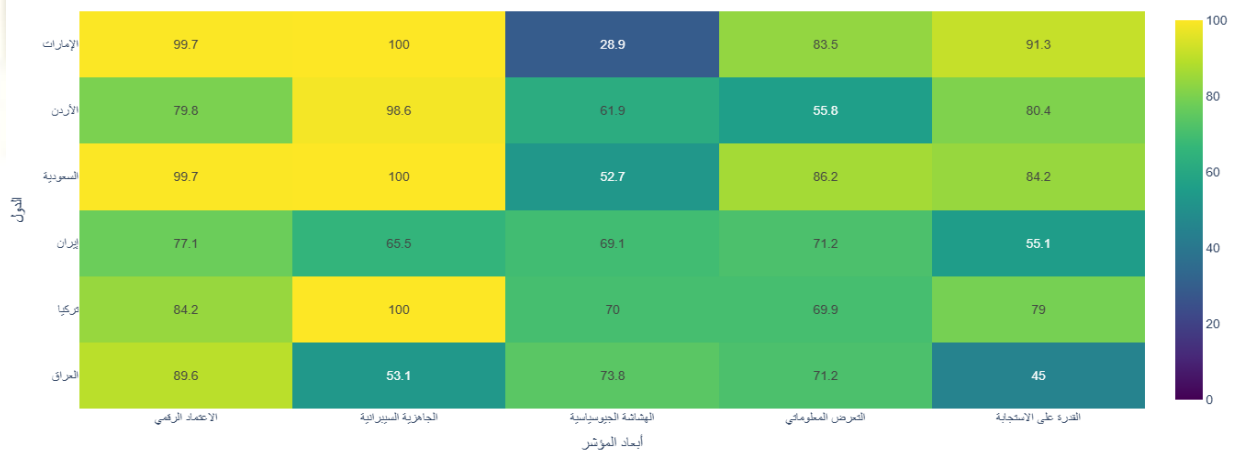
الجدول (3): مقارنة الجاهزية السيبرانية والهشاشة الجيوسياسية والتعرض الجيوسيراني

الدولة	الجاهزية السيبرانية GCI 2024	مؤشر الدول الهشة 2024	حرية الإنترنت 2024	التعرض المعلوماتي	مؤشر التعرض الجيوسيراني	التقييم العام
العراق	53.07	88.6	40	71.2	72.1	حساس/مرتفع الخطورة
تركيا	100	84	31	69.9	57.4	متوازن مع قيود معلوماتية
إيران	65.52	82.9	13	71.2	63.7	تصادمي / عالي التحكم

السعودية	100	63.2	25	86.3	62.7	متقدم سيبرانيًا مع تعرض معلوماتي
الأردن	98.6	74.3	47	55.8	51.8	مستقر نسبيًا
الإمارات	100	34.7	30	83.5	57.4	متقدم جدًا مع كثافة رقمية عالية

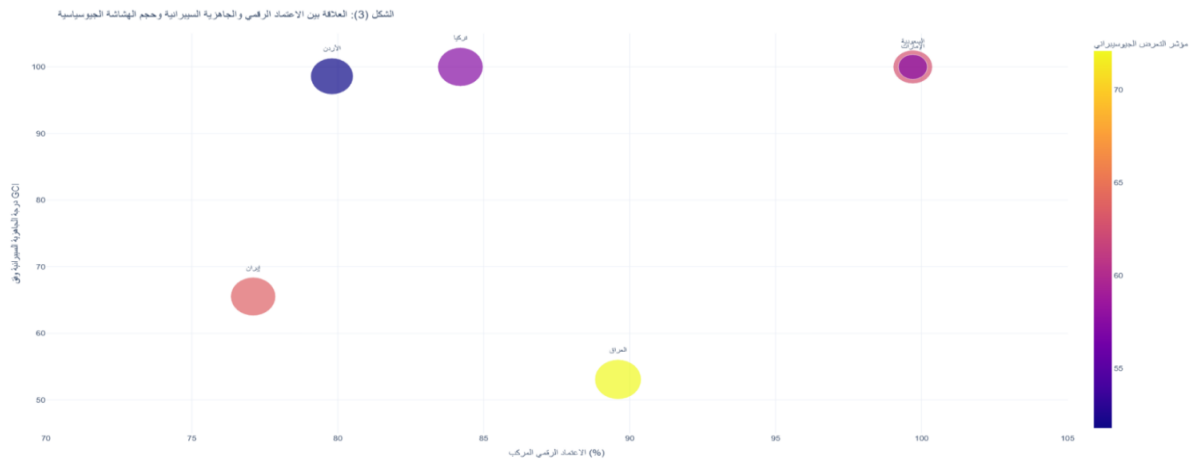
مصدر الجدول: من إعداد الباحث اعتمادًا على مؤشر الأمن السيبراني العالمي 2024، مؤشر Freedom on the Net 2024، ومؤشر الدول الهشة 2024. تكشف نتائج الجدول أن العراق حصل على أعلى قيمة في مؤشر التعرض الجيوسبراني بين الدول المختارة، إذ بلغت الدرجة 72.1. ويرجع ذلك إلى اجتماع ثلاثة عوامل: اعتماد رقمي مرتفع، وجاهزية سيبرانية متوسطة/منخفضة مقارنة بالدول الأخرى، وهشاشة جيوسياسية مرتفعة. أما تركيا والإمارات فقد سجلتا درجة تعرض متقاربة 57.4، لكن لأسباب مختلفة؛ ففي تركيا يرتبط التعرض بالهشاشة والقيود المعلوماتية، بينما يرتبط في الإمارات بكثافة رقمية عالية جدًا رغم قوة الجاهزية السيبرانية. وتظهر إيران في مستوى خطر مرتفع 63.7 بسبب انخفاض حرية الإنترنت، وارتفاع الهشاشة، ومتوسط الجاهزية السيبرانية.

الشكل (2): خريطة حرارية لأبعاد التعرض الجيوسبراني في دول مختارة



الشكل (2): خريطة حرارية لأبعاد التعرض الجيوسبراني في دول مختارة

توضح الخريطة الحرارية أن العراق يتميز بدرجات مرتفعة في الاعتماد الرقمي والهشاشة الجيوسياسية والتعرض المعلوماتي، مقابل درجة أقل في الجاهزية السيبرانية والقدرة على الاستجابة. وهذه القراءة البصرية تكشف ما لا يظهره الجدول مباشرة؛ فالمشكلة ليست في الاعتماد الرقمي بحد ذاته، بل في عدم التوازن. هذا الاعتماد مع الجاهزية المؤسسية والسيبرانية.



الشكل (3): العلاقة بين الاعتماد الرقمي والجاهزية السيبرانية وحجم الهشاشة الجيوسياسية

يبين الشكل المبستر أن العراق يقع في منطقة حرجة؛ فهو يمتلك اعتمادًا رقميًا مرتفعًا، لكنه لا يمتلك جاهزية سيبرانية تضاهي هذا الاعتماد. ويظهر حجم الدائرة الخاص بالعراق كبيرًا نسبيًا، لأن الهشاشة الجيوسياسية المحولة إلى مقياس 100 ما تزال مرتفعة. وهذا يعني أن العراق لا يواجه خطرًا تقنيًا فقط، بل يواجه خطرًا مركبًا ينتج عن تداخل التقنية مع الجغرافيا والسياسة والأمن.

الجدول (4): مصفوفة أثر الفضاء السيبراني في عناصر الجغرافيا السياسية للعراق

عنصر الجغرافيا السياسية	التأثير السيبراني	مستوى التأثير	الانعكاس الجيوسياسي
الموقع الجغرافي	تحول العراق إلى نقطة تفاعل رقمية وإعلامية داخل بيئة إقليمية متوترة	مرتفع	زيادة الحساسية الإقليمية للمجال الرقمي العراقي
الحدود	صعوبة ضبط الاختراقات الرقمية العابرة للحدود مقارنة بالحدود المادية	مرتفع	تراجع كفاية أدوات الحماية التقليدية
الموارد	قابلية قطاعات الطاقة والمصارف والخدمات للاستهداف السيبراني	مرتفع جدًا	تهديد الأمن الاقتصادي والخدمات الحيوية
السكان	ارتفاع كثافة استخدام وسائل التواصل وزيادة قابلية التأثر بالتضليل	مرتفع	ضغط اجتماعي وسياسي عبر المجال الرقمي
السيادة	تحديات التحكم بالبيانات والمنصات والبنية الرقمية	مرتفع	الحاجة إلى بناء سيادة رقمية وطنية

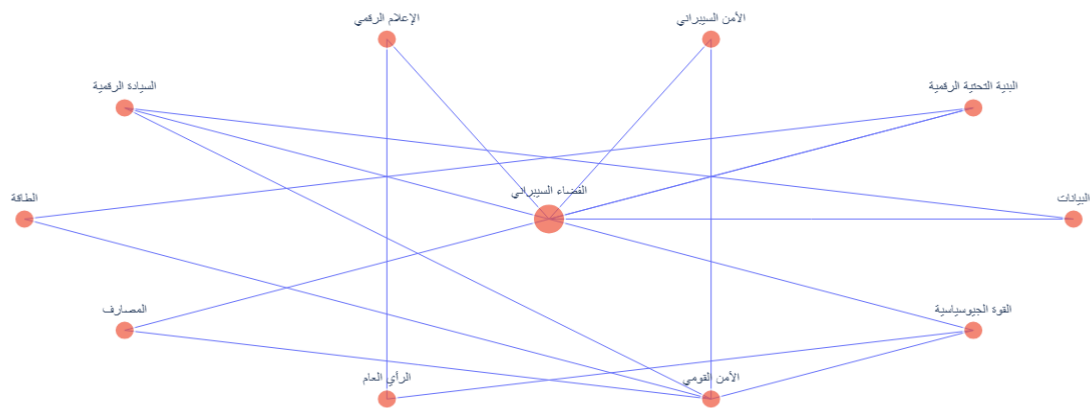
الأمن القومي	انتقال الخطر من الحدود العسكرية إلى الشبكات والبنى الحيوية	مرتفع جداً	ضرورة دمج الأمن السيبراني في استراتيجية الأمن الوطني
--------------	--	------------	--

مصدر الجدول: من إعداد الباحث بالاستناد إلى نتائج التحليل التطبيقي وبيانات العراق الرقمية والجاهزية السيبرانية ومؤشرات حرية الإنترنت .

يوضح الجدول أن الفضاء السيبراني لا يؤثر في عنصر واحد من عناصر الجغرافيا السياسية، بل يعيد تركيب العلاقة بين الموقع والحدود والموارد والسكان والسيادة والأمن القومي. فالعراق لم يعد يتأثر فقط بحساسية موقعه البري وحدوده مع دول إقليمية مؤثرة، بل بات يتأثر أيضاً بحركة البيانات، وتدفقات المعلومات، وحملات التضليل، وتهديد البنية التحتية الرقمية، واستهداف القطاعات الحيوية.

الشكل (4): شبكة تأثير الفضاء السيبراني في عناصر القوة الجيوسياسية

الشكل (4): شبكة تأثير الفضاء السيبراني في عناصر القوة الجيوسياسية



الشبكة عسكيرية لا رقمية؛ تظهر أن التأثير السيبراني يهزله عبر بيانات وبنية تحتية وإعلام وأمن وسيادة قبل أن يتحول إلى أثر جيوسياسي.

يبين الشكل الشبكي أن الفضاء السيبراني يؤثر في القوة الجيوسياسية عبر شبكة مترابطة، تبدأ من البيانات والبنية التحتية الرقمية والإعلام الرقمي، ثم تنتقل إلى السيادة والأمن القومي والقطاعات الحيوية، وصولاً إلى القوة الجيوسياسية. وهذه النتيجة تؤكد أن الخطر السيبراني لا يمكن التعامل معه بوصفه خطراً تقنياً معزولاً، بل يجب النظر إليه باعتباره مجالاً جيوسائياً مؤثراً في بنية الدولة وموقعها الإقليمي.

الاستنتاجات

1. أثبت البحث أن الفضاء السيبراني أصبح مجالاً جيوسائياً مؤثراً، ولم يعد مجرد بيئة تقنية أو اتصالية، بل تحول إلى ساحة للصراع والنفوذ والتأثير بين الدول والفاعلين غير الحكوميين .

2. توصل البحث إلى أن التكنولوجيا لم تلغ الجغرافيا التقليدية، لكنها أضافت إليها بعدًا جديدًا يتمثل في البيانات، والشبكات، والمنصات، والبنية التحتية الرقمية، والنكاء الاصطناعي، والأمن السيبراني .
3. بين البحث أن مفهوم القوة في العصر الرقمي لم يعد محصورًا في القوة العسكرية والاقتصادية، بل أصبح يشمل القدرة على جمع البيانات، وحماية الشبكات، وتعطيل البنى التحتية، والتأثير في الرأي العام، وإدارة المجال المعلوماتي .
4. أظهر البحث أن السيادة الرقمية أصبحت امتدادًا للسيادة الوطنية، لأن الدولة التي لا تتحكم ببياناتها ومنصاتها وبنيتها الرقمية تكون أقل قدرة على حماية قرارها السياسي والاقتصادي والأمني .
5. كشف الجانب التطبيقي أن العراق يمتلك اعتمادًا رقميًا مرتفعًا، حيث بلغ مؤشر الاعتماد الرقمي المركب 89.6، وهي درجة تعكس اتساع حضور الإنترنت ووسائل التواصل والاتصالات الخلوية في المجتمع العراقي .
6. أظهرت النتائج أن العراق سجل 53.07 في مؤشر الأمن السيبراني العالمي لعام 2024، وهي درجة تكشف وجود فجوة بين مستوى الاستخدام الرقمي ومستوى الجاهزية السيبرانية والمؤسسية.

المصادر والمراجع

أولاً: الكتب العربية

محمود، خالد وليد. (2025). *الفضاء السيبراني وتحولات القوة في العلاقات الدولية*. المركز العربي للأبحاث ودراسة السياسات .

ثانياً: المقالات والدراسات العربية في المجالات العلمية

- عياد، إيهاب محمد أبو المجد محمود. (2023). الجيوسياسية العالمية والتحولات في أبعاد وخصائص القوة: آليات التوظيف في الاستراتيجية الروسية والصينية. *مجلة البحوث المالية والتجارية*، 24(1)، ج 3 .
- دسوقي، عيسى السيد عيسى، وقطب، حسن قطب حسن. (2025). الجيوبوليتيكا في زمن الفضاء السيبراني: بين الكلاسيكية والنقدية، رؤية معاصرة في الجغرافية السياسية. *مجلة كلية الآداب بقنا*، 34(67).
- صابر، سالم. (2022). انعكاسات البعد العسكري للفضاء السيبراني على الجغرافيا السياسية للدولة. *مجلة ستراتيجيا*، 9(17).
- مسيكة، محمد الصغير. (2022). الفضاء السيبراني وتحديات الأمن القومي للدول. *مجلة العلوم القانونية والاجتماعية*، 7(4).
- الدروزي، الشيماء فؤاد. (2024، يوليو). الفضاء السيبراني ما بين تحول القوة والصراع والأمن القومي للدول. *مجلة الحقوق للبحوث القانونية والاقتصادية*، 2(1)، 851. <https://doi.org/10.21608/lalexu.2024.390542>
- فوزي، إسلام. (2019، مايو). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي. *المجلة الاجتماعية القومية*، 56(2). <https://doi.org/10.21608/jns.2019.205220>
- ذاري، هديل حربي. (2023). قوة الفضاء السيبراني: ساحة صراع جديدة بين القوى الدولية والإقليمية في القرن الحادي والعشرين. *مقضايا سياسية*، 72، <https://doi.org/10.58298/2023339>

- جمال الدين، هبة. (2023، يناير). الأمن السيبراني والتحول في النظام الدولي. *مجلة كلية الاقتصاد والعلوم السياسية*، 24 <https://doi.org/10.21608/jpsa.2023.279877> (1)
- خليل، حازم محمد. (2023، يناير). استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني. *المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية*، 8(15).
- عبد الحميد، أماني عصام محمد. (2021). استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية. *مجلة كلية الاقتصاد والعلوم السياسية*، 22 (4).
- محمود، سيناء علي. (2025). التحديات الأمنية للدول في الفضاء السيبراني قضايا سياسية، 80.
- طه، جاسم محمد. (2023). التهديدات السيبرانية وانعكاسها على الأمن القومي الأمريكي. *مجلة تكريت للعلوم السياسية*، 2 <https://doi.org/10.25130/tjfps.v2i32> (32)
- عزيز، فراس كوركيس، ومحمد، فاضل جاسم. (2023). القوة السيبرانية والقرصنة الإلكترونية وتأثيرها في الانتخابات الأمريكية 2020. *مجلة دراسات دولية*، 94.
- محسن، محمد معن. (2025). مستقبل مكانة القوة السيبرانية في استراتيجيات القوى الإقليمية: إيران نموذجًا قضايا سياسية . شويرب، جيلالي، ومراد، فائزة. (2023). مفهوم الحروب السيبرانية والأمن السيبراني. *مجلة الحقوق والحريات*، 11(1).
- بوطالعة، وداد، ووكرور، منال. (2022). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. *مجلة حقوق الإنسان والحريات العامة*، 7(2).
- العيسى، طلال ياسين، وعناب، عدي محمد. (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. *مجلة الزرقاء للبحوث والدراسات الإنسانية*، 19(1) <https://doi.org/10.34028/1069>
- الديب، نانسي عبد الله حامد. (2025). السيادة الرقمية للدول في مواجهة التهديدات السيبرانية غير الحكومية نحو بناء إطار قانوني دولي من ومتكامل. *المجلة القانونية*، 25(1)، <https://doi.org/10.21608/jlaw.2025.410172.1296>
- بإسماعيل، عبد الكريم. (2022). تأثير الفضاء الافتراضي على الأمن القومي. *مجلة البحوث والدراسات*، 19(1).
- شحيرط، أحمد، وقريبز، مراد. (2022). تحديات الإنترنت لسيادة الدول: السيادة الرقمية. *مجلة البحوث القانونية والاقتصادية*، 5(1).
- عبد العظيم، فتحي جمعة. (2023، يوليو). اتجاه الدول نحو تبني سياسات توطين البيانات: دراسة في السيادة الرقمية. *مجلة كلية السياسة والاقتصاد*.
- لطفي، وفاء. (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجًا. *مجلة كلية الاقتصاد والعلوم السياسية*، 23(1).
- علام، مها. (2025). السيادة السيبرانية بين الرؤيتين الغربية والصينية. *مجلة كلية الاقتصاد والعلوم السياسية*، 26 (3).

بيرم، فاطمة. (2020). السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمي: الصين نموذجاً. *المجلة الجزائرية للأمن الإنساني*، 5. (1).

الزبيدي، زهير خضير عباس، والتميمي، ظفر عبد مطر. (2022). العراق والأمن السيبراني: الفرص والتحديات. *مجلة واسط للعلوم الإنسانية*، 18 (51)، 249. <https://doi.org/10.31185/Vol18.Iss51.249>

ثالثاً: الكتب الأجنبية

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). *Cyber persistence theory: Redefining national security in cyberspace*. Oxford University Press.

رابعاً: المقالات الأجنبية في المجالات العلمية

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, 45(3) <https://doi.org/10.1080/13523260.2024.2365062>

خامساً: التقارير والمؤشرات الدولية

International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). ITU.

Voo, J., Hemani, I., & Cassidy, D. (2022, September). *National cyber power index 2022*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

International Institute for Strategic Studies. (2024, September). *The IISS cyber power matrix: Context and methodology*. IISS.

DataReportal. (2024). *Digital 2024: Iraq*. DataReportal.

International Monetary Fund. (2024, April). *Global financial stability report: Cyber risk—A growing concern for macrofinancial stability* (Chapter 3). IMF.