الترميز الدولي / ISSN (P) :2710-2653
ISSN (E) :2960-253X /
رقم الايداع الوطني / 2375 /2019

تاريخ استلام البحث : ٢٠٢٥/١٢/١٧
تاريخ قبول البحث : ٢٠٢٦/٢/٨
تاريخ النشر : ٢٠٢٦/٣/٣٠

الجيوبولتيك الرقمي في العراق: صعود فاعل ناشئ في بيئة سيبرانية مضطربة

The Digital Geopolitics of Iraq: The Rise of an Emerging Actor in a Turbulent Cyber Environment

م.م. نورا رياض الدباغ
Assit. Lecture. Noura Riyadh Aldabagh
جامعة بغداد / مركز الدراسات الإستراتيجية والدولية /
University of Baghdad/ Center for Strategic and International Studies
noura.r@cis.uobaghdad.edu.iq
ORCID:https://orcid.org/0009-0009-6722-7326

IRAQI
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

الجيوبولتيك الرقمي في العراق: صعود فاعل ناشئ في بيئة سيبرانية مضطربة

م.م. نورا رياض الدباغ

الملخص:

يتناول هذا البحث موقع العراق ضمن معادلة الجيوبولتيك الرقمي في الشرق الأوسط، من خلال تحليل مزدوج يربط بين اختراقات الفاعلين الإقليميين للحدود السيبرانية العراقية، ومحاولات العراق تأكيد نفوذه الرقمي في البيئة المحيطة. يسلط البحث الضوء على الهجمات السيبرانية الإيرانية والتركية وأشكال التهديدات غير المباشرة من أطراف أخرى، مقابل الإجراءات العراقية في تعزيز قدراته السيبرانية، قانونياً ومؤسسياً وبشرياً. كما يستعرض البحث دور العراق في شبكات التعاون الدولي، ومحاولاته تجاوز موقع الضحية إلى موقع الفاعل السيبراني الإقليمي، رغم التحديات البنيوية والسياسية. اعتمد البحث منهج تحليل السياسات، مستنداً إلى تقارير ميدانية ومصادر مفتوحة ووثائق رسمية، لتقديم رؤية نقدية تدمج بين البعد الأمني والبعد الاستراتيجي للفضاء الرقمي في العراق.

الكلمات المفتاحية: السيادة الرقمية، التهديدات السيبرانية الإقليمية، الأمن السيبراني العراقي، النفوذ الرقمي الجيوسياسي.

Abstract :

This study examines Iraq’s position within the regional digital geopolitics of the Middle East, through a dual-track analysis that explores both cross-border cyber intrusions by regional actors and Iraq’s efforts to assert its digital influence in the surrounding environment. The research highlights Iranian and Turkish cyber operations, along with indirect threats from other actors, and contrasts these with Iraq’s institutional, legal, and human capacity-building initiatives in the cybersecurity domain. It further assesses Iraq’s engagement in international cyber cooperation networks and its strategic attempt to shift from a reactive target to a proactive regional cyber actor, despite persistent structural and political challenges. The study adopts a policy analysis approach, drawing on open-source intelligence, official documents, and field-based reporting to present a critical perspective that links Iraq’s national security with its digital sovereignty ambitions.

Keywords: Digital sovereignty, regional cyber threats, Iraqi cybersecurity, geopolitical digital influence.

المقدمة:

يشهد العالم في العقدين الأخيرين تحولاً جذرياً في مفهوم السيادة، لم تعد الجغرافيا وحدها تحدد نفوذ الدول، بل بات الفضاء السيبراني ميداناً استراتيجياً للصراع والتنافس. في هذا السياق، برز مفهوم (الجيوبولتيك الرقمي) بوصفه إطاراً تفسيرياً جديداً لفهم امتدادات القوة والنفوذ عبر أدوات غير مرئية: البيانات، الشبكات، الخوارزميات.

يشكل العراق نموذجاً معقداً ضمن هذه المعادلة. فمن جهة، يتعرض لإختراقات سيبرانية متكررة من قبل فاعلين إقليميين يمتلكون بنى رقمية متقدمة، ومن جهة أخرى يسعى، بخطى مترددة، إلى تثبيت حضوره

بوصفه فاعلاً سيبرانياً له قواعده ومصالحه. هذه المفارقة تثير تساؤلاً مركزياً: هل يمكن للعراق أن يتحول من ساحة اختراق إلى طرف مؤثر في البيئة الرقمية الإقليمية؟

يتناول هذا البحث هذه الإشكالية من خلال مقاربة تحليل السياسات، معتمداً على مصادر مفتوحة، وثائق رسمية، وتقارير فنية. ويركز على محورين رئيسيين: أنماط اختراق الحدود السيبرانية العراقية، ومحاولات تشكيل نفوذ رقمي إقليمي فاعل. كما يسعى إلى تفكيك التحديات البنيوية والتشريعية التي تعيق العراق، واقتراح خارطة طريق لتعزيز موقعه السيبراني ضمن النظام الإقليمي والدولي.

أهمية البحث:

- يقدم قراءة تحليلية جديدة لمفهوم الجيوبولتيك الرقمي بوصفه امتداداً للتحولات في طبيعة القوة والنفوذ.
- يسلط الضوء على التحديات البنيوية والقانونية التي تواجه العراق في تحقيق سيادته الرقمية.
- يضع مؤشرات كمية ونوعية لفهم التهديدات السيبرانية وآليات النفوذ الرقمي الإقليمي.
- يعزز فهم دور العراق داخل شبكات التعاون السيبراني الدولي.

إشكالية البحث:

كيف يمكن للعراق أن يتحول من ساحة مستهدفة في الجيوبولتيك الرقمي إلى فاعل سيبراني إقليمي، في ظل اختراقات مستمرة لحدوده السيبرانية، وهشاشة بنيته الرقمية، وضعف تشريعاته السيبرانية؟

فرضية البحث:

رغم تصاعد الاختراقات السيبرانية الإقليمية، فإن العراق يمتلك فرصاً واقعية للتحول إلى فاعل رقمي، إذا ما استثمر في بناء تشريعات سيادية، وقدرات بشرية وطنية، وبنية رقمية مرنة، مع تكثيف انخراطه في التحالفات السيبرانية الدولية.

منهجية البحث:

إعتمد البحث منهج تحليل السياسات، قائماً على:

١. مراجعة تقارير دولية ووثائق رسمية مفتوحة المصدر.
٢. دراسة مقارنة بين نماذج تهديد ونفوذ رقمية في البيئة الإقليمية.
٣. تصنيف التحديات العراقية ضمن أربعة محاور: بنيوية، تشريعية، أمنية، ودبلوماسية.
٤. بناء جداول تحليلية لفهم طبيعة التهديدات وتحديد الثغرات المؤسساتية.

المبحث الأول

تحولات الجيوبولتيك من الجغرافيا الصلبة إلى الهيمنة الرقمية

يشهد العالم تحولاً عميقاً في طبيعة القوة والنفوذ مع صعود الفضاء السيبراني بوصفه ساحة جديدة للصراع الجيوسياسي. لم تعد الجغرافيا التقليدية وحدها تحدد معادلات الهيمنة، بل أصبحت البيانات، الشبكات، والمعايير الرقمية عناصر حاسمة في تشكيل توازنات القوة. في هذا السياق، باتت الدول مطالبة بإعادة تعريف مفاهيم السيادة والأمن ضمن بيئة رقمية معقدة تتجاوز الحدود المادية. يستعرض هذا المبحث الجذور النظرية للجيوبولتيك الرقمي، ومسارات تحوله من نموذج تقليدي إلى فضاء افتراضي، مع تحليل لطبيعة التحديات التي تفرضها الحدود السيبرانية على الدول.

المطلب الأول: إعادة تعريف الجيوبولتيك في العصر السيبراني:

لم يعد نفوذ الدولة يتحدد فقط بما تملكه من مساحة جغرافية أو موارد طبيعية، بل بات يتشكل كذلك عبر سيطرتها على تدفقات البيانات، والبنى التحتية الرقمية، والمعايير التقنية، وقواعد الحوكمة العابرة للحدود. هكذا انتقل مفهوم الجيوبولتيك من إدارة (الأقاليم) إلى هندسة (الأكوان الشبكية)، حيث تُعاد صياغة السيادة من خلال أدوات تنظيمية وتقنية وأمنية تضبط من يدخل ويخرج من الفضاءات الرقمية وكيفية تبادل المعلومات عبرها. يمكن تلمس هذا التحول في سياسات كبرى مثل: استراتيجية الأمن السيبراني للبيت الأبيض للعام (٢٠٢٣) التي تعيد توزيع أعباء الأمن السيبراني من المستخدمين إلى الشركات الأكثر قدرة (The White House 2023, 30)، وإطلاق الناتو عام (٢٠٢٣) لقدرات دعم افتراضية للحوادث السيبرانية (NATO 2024)، و إقرارّ الاتحاد الأوروبي في عام ٢٠٢٤ لائحة الصمود السيبراني التي تلزم بفرض متطلبات أمنية موحّدة على جميع المنتجات الرقمية، بغض النظر عن مجال استخدامها. يتزامن هذا مع تنامي ظاهرة (تفتت الإنترنت) التي تعبّر عن تشظي البنية العالمية للشبكة نتيجة السياسات الوطنية المتباينة بشأن تدفق البيانات والمعايير التقنية (European Union 2024). هذه المؤشرات تكشف عن تحول جذري في بنية الجيوبولتيك المعاصر، حيث تتداخل القوة الصلبة المتمثلة في كابلات الإتصالات البحرية والبنية التحتية الفيزيائية، مع القوة الناعمة للبيانات والمعايير والبرمجيات وثقة الأسواق الرقمية (European Union 2024) .

من الناحية اللغوية مصطلح الجيوبولتيك (Geopolitics) مشتق من مقطعين إغريقيتين: (Geo) بمعنى الأرض، (politics) بمعنى السياسة (العلاق ٢٠٢٥). وبذلك فإن المعنى اللغوي للمصطلح هو: سياسة الأرض، أو السياسة المرتبطة بالمكان، في إشارة إلى الترابط بين الجغرافيا وشؤون الحكم (العلاق ٢٠٢٥).

يُعرف الجيوبولتيك التقليدي بأنه صراع سيطرة على المواقع الجغرافية ذات الأهمية مثل: النقاط الملاحية والمواقع العسكرية والموارد الطبيعية مثل: النفط والمعادن، إذ أن التنافس على هذه الموارد والأراضي

يؤدي إلى صراعات دولية ومن ثَمَّ تُعتبر المساحة الجغرافية والحدود ثابتة ومهمة، وتُستخدم كنقطة انطلاق لتخطيط السياسة الخارجية وبناء التحالفات (بوغرسة ٢٠٢٥، ٢٨–٢٩).

أما لغوياً مفردة رقمي (Digital)، هي صفة تعود إلى منتصف القرن الخامس عشر، وتعني: الأعداد الأقل من عشرة، وهي مشتقة من الكلمة اللاتينية (Digitus) التي تعني: الإصبع، حيث يعزى المعنى العددي إلى أن الأعداد الأقل من ١٠ كانت تُعد على الأصابع **(Huskaj 2023,152)**. لاحقاً في عام ١٩٣٨ أصبح مصطلح (رقمي) يُعنى بإستخدام الأرقام عموماً، و في عام ١٩٤٥ أخذ معنى الحواسيب التي تعمل على بيانات على شكل أرقام (Huskaj 2023,152)، ثم أخذ المصطلح معنى إشارة إلى التسجيل أو البث في عام ١٩٦٠ (Huskaj 2023,152). بذلك يشير مفهوم الجيوبولتيك الرقمي: إلى دراسة تأثير الأنظمة المعلوماتية والشبكات الرقمية (الفضاء السيبراني) بجانب العوامل الجغرافية التقليدية على القوة والعلاقات الدولية في مختلف المجالات. بعبارة أخرى، لم يعد التنافس الجيوسياسي مقتصراً على السيطرة الإقليمية والموارد الطبيعية فحسب، بل اتسع ليشمل السيطرة على البيانات والبنية التحتية السيبرانية وتدفق المعلومات عبر الحدود (قادري ٢٠٢٥).

شهد مفهوم الجيوبولتيك تطوراً جذرياً، حيث انتقل من تركيزه التقليدي على الخصائص المادية للأراضي والسعي للسيطرة على المساحات الجغرافية في أوائل القرن العشرين، إلى مجال أكثر تجريداً يتأثر بشكل كبير بالأدوات الرقمية في العصر الحديث هذا الانتقال يعكس حقيقة أن التكنولوجيا أصبحت أساس القوة المعاصرة، حيث توفر تقنيات مثل: الذكاء الاصطناعي، والبيانات الضخمة، والبنية التحتية الرقمية، والجيل الخامس، أدوات جديدة وهائلة للقوى الكبرى لفرض نفوذها وتجميع المزيد من القوة (Zirojević 2024,80). بذلك، القوة اليوم لم تعُد مرتبطة فقط بامتلاك الأرض والموارد، بل بالذكاء الرقمي والقدرة على اختراق المعلوماتية. لقد أدى الترابط العالمي الذي أوجدته التقنيات الرقمية إلى طمس الحدود الفاصلة بين الشؤون الداخلية والخارجية للدول، مما أعاد تشكيل كيفية فهم القوة الجيوبولتيكية وممارستها وبالتالي، لم تعد القوة محصورة في السيطرة الإقليمية (القوة الصلبة)، بل امتدت لتشمل الهيمنة الرقمية، حيث تحولت التحالفات السياسية التقليدية إلى شراكات تكنولوجية استراتيجية، وأصبحت المنافسة على وضع المعايير الدولية جزءاً لا يتجزأ من هذه الديناميكية الجديدة فمثلاً، يناقش البعض أنّ الدول الكبرى لم تعد تعتمد على الإجهاز العسكري وحده، بل تستخدم البيانات الكبيرة والذكاء الاصطناعي بوصفها معيار جديد للهيمنة (حدادة وقعلول ٢٠٢٢).

في هذا السياق، أصبحت (الجغرافيا الناعمة) التي تتكون من البيانات والشبكات، هي الساحة الجديدة للصراع والتعاون. البيانات أصبحت سلعة ثمينة توفر مزايا اقتصادية وعسكرية وجيوستراتيجية هائلة لمن يسيطر عليها. حيث الفضاء السيبراني بوصفه بيئة تمكينية يسمح بنقل المعلومات بتكلفة منخفضة، وبشكل شبه فوري عبر الحدود، مع إمكانية إخفاء الهوية، مما يجعله أداة قوية للتأثير والنفوذ. تجدر الإشارة إلى أنّ

التحوّل من الجغرافيا الصلبة إلى الناعمة لم ينبذ الجغرافيا التقليدية بالكامل، بل مزج بين الأبعاد؛ إذ ظلت مفاهيم الدولة والمصالح الإستراتيجية قائمة، مع تنامي البُعد الرقمي. وتبقى الصراعات القادمة تُحلل عبر مزيج من العوامل المكانية والإلكترونية (Abdelkarim 2024,369). **(أنظر الجدول رقم:١)** .

الخاصية	الجيوبولتيك التقليدي (الجغرافيا الصلبة)	الجيوبولتيك الرقمي (الجغرافيا الناعمة)
محور القوة	السيطرة على الأرض، الموارد الطبيعية، والممرات الاستراتيجية.	السيطرة على البيانات، الشبكات، البنية التحتية الرقمية، وتدفق المعلومات.
الحدود	مادية، واضحة، ومرسومة (حدود إقليمية).	افتراضية، غير واضحة، وديناميكية (حدود سيبرانية).
أدوات النفوذ	القوة العسكرية، التحالفات السياسية، السيطرة الاقتصادية التقليدية.	الحرب السيبرانية، التجسس الرقمي، المعلومات المضللة، وضع المعايير التقنية، هيمنة الشركات التكنولوجية، والحصار الرقمي.
الفاعلون الرئيسيون	الدول القومية بشكل أساسي.	الدول، الشركات التكنولوجية الكبرى، مجموعات القرصنة (Hacktivism)، المنظمات الإرهابية، والمنظمات غير الحكومية.

جدول رقم : ١

الجدول من عمل الباحثة.

هذا المزج بين البعدين المادي والرقمي لا يعني إلغاء الجغرافيا التقليدية تماماً، بل إعادة تشكيلها. فلا تزال مفاهيم الدولة والمصلحة القومية قائمة، لكن أُضيف لها بُعد رقمي حاسم (Zirojević 2024,85). وتشير الأدبيات الحديثة إلى أن صراعات المستقبل يجب تحليلها في إطار مزيج من العوامل المكانية الجيوسياسية والإلكترونية. إذ أدى الترابط العالمي الذي أوجدته التقنيات الرقمية إلى محو الخط الفاصل بين الداخل والخارج، مما أعاد تشكيل أسس القوة الجيوبولتيكية **(Zirojević** 2024,86**)**. وبالتالي، يتعين على الدول أن تتكيف مع هذه الحقيقة الجديدة حيث لم تعد السيطرة الإقليمية وحدها كافية لضمان النفوذ، بل أصبح النفوذ الرقمي عنصراً مكملاً لكفة القوة الشاملة للدولة (Zirojević 2024,86).

المطلب الثاني: وسائل الصراع السيبراني بوصفها أداة للنفوذ الجيوبولتيكي الرقمي:

لقد خلق الفضاء السيبراني جغرافيا جديدة تتعايش فيها الحدود المادية التقليدية مع الفضاء الافتراضي، مما يطرح تحديات أمنية جديدة ويعيد تعريف مفهوم السيادة الوطنية اصبحت فيها الحدود السيبرانية محورياً في النقاشات حول السيادة الرقمية، حيث تسعى الدول إلى بسط سلطتها على بنيتها التحتية الرقمية وبيانات مواطنيها، لذلك يصعب تطبيق هياكل الحوكمة التقليدية المرتبطة بالإقليم المادي على الفضاء السيبراني؛ بسبب طبيعته التي تعيد ترميز الحدود ومع ذلك، تحاول الدول بلورة سيادتها السيبرانية من خلال فرض تدابير تقنية للحد من تدفق البيانات، ومراقبة الأنشطة المشبوهة، واستغلال غموض الفضاء السيبراني ضد خصومها (Tan et al. 2023, 2–3)**.** فالسيادة الرقمية هي: قدرة الدولة على تشكيل تحولها الرقمي

بطريقة مستقلة، مع اتخاذ قرارات سيادية بشأن المجالات التي تسعى فيها للاستقلال التكنولوجي. لقد أصبحت الاختراقات والهجمات الرقمية أشكالاً جديدة وفعالة من التوسع والنفوذ الجيوبولتيكي. فالحرب السيبرانية، والتجسس الرقمي، وحملات التضليل عبر وسائل التواصل الاجتماعي، كلها أدوات تتحدى المفاهيم التقليدية للأمن القومي والسيادة (Tan et al. 2023, 3).

إن الصراع الروسي–الأوكراني قدم مثالاً حياً على ذلك، حيث تم استخدام الهجمات السيبرانية لاستهداف البنية التحتية الحيوية، ونشر المعلومات المضللة، وتعطيل الخدمات الحكومية. كما أظهر الصراع كيف يمكن لشركات التكنولوجيا العالمية أن تتصرف بوصفها دول رقمية، حيث فرضت حصاراً رقمياً على روسيا وقدمت الدعم لأوكرانيا، مما أعاد تشكيل نماذج المرونة والسيادة الرقمية (Aviv and Ferri 2023). حيث لم تعد الهجمات الإلكترونية والاختراقات الرقمية مجرد أنشطة إجرامية فردية، بل تحولت في العقد الأخير إلى أدوات تستخدمها الدول، ومن خلفها الجهات الفاعلة لتحقيق أهداف سياسية وأمنية واقتصادية. مثلما استُخدمت الجيوش تقليدياً للتوسع والنفوذ، باتت البرمجيات الخبيثة وهجمات القرصنة اليوم وسيلة فعّالة لتوسيع النفوذ دون إطلاق رصاصة واحدة. وقد شهدنا أمثلة عديدة تؤكد هذا التحول، حيث أصبحت الهجمات السيبرانية امتداداً للصراع الجيوسياسي بين الدول (العتيبي ٢٠٢٥).

على الصعيد السياسي، يمكن للهجمات الإلكترونية أن تؤثر في استقرار الحكومات وعملية صنع القرار في الدول المستهدفة. مثل: هجمات سيبرانية روسية على أنظمة الانتخابات في رومانيا عام ٢٠٢٤ التي شملت ٨٥ الف هجوم سيبراني وتسريب بيانات قبيل الانتخابات (CSIS 2025,3).

من الناحية الأمنية والعسكرية، باتت الهجمات الرقمية شكلاً جديدًا من أشكال الاشتباك والاعتداء. حيث يمكن لدولة ما أن تشن هجوماً سيبرانياً يشلُّ مرافق حيوية في دولة أخرى مثل: شبكات الكهرباء أو الاتصالات أو أنظمة النقل دون الحاجة لاجتياز حدودها العسكرية. مثل: هجوم Stuxnet الشهير عام ٢٠١٠ إستهدف برنامج تخصيب اليورانيوم الإيراني، ما أدى إلى تعطيل مئات أجهزة الطرد المركزي. يُعتقد على نطاق واسع أن تلك العملية نفذتها جهات مدعومة من الولايات المتحدة وإسرائيل (محمود ٢٠٢٥).

إقتصادياً، أصبحت القرصنة وسيلة لإضعاف الاقتصادات المنافسة أو سرقة أسرارها. فقد انخرطت مجموعات تجسس إلكتروني تابعة لدول كبرى في حملة مستمرة لاختراق شركات كبرى ومؤسسات مالية للحصول على أسرار تجارية وتقنية تمنح بلدانها أفضلية تنافسية. على سبيل المثال، اتُهمت مجموعات قرصنة صينية مراراً بإختراق شركات غربية وسرقة ملكيات فكرية في مجالات التقانة المتقدمة لتعزيز اقتصاد الصين وتقليل الفجوة التقنية (محمود ٢٠٢٥).

يُعد العراق مثلاً مهماً لفهم تحديات الجيوبولتيك الرقمي في منطقة الشرق الأوسط، حيث يتقاطع ضعف البنية التحتية السيبرانية مع التنافس الإقليمي على النفوذ. فمنذ تغير النظام عام ٢٠٠٣ وانفتاح العراق

على العالم الرقمي، أصبح البلد معرضاً لتهديدات سيبرانية متكررة استهدفت مؤسساته الحيوية وأنظمته الحكومية (الجبوري ٢٠٢٥، ١٢). **(أنظر الجدول رقم:٢)** .

التحدي	الوصف التفصيلي	التأثير على السيادة الوطنية العراقية
البنية التحتية القديمة والمحدودة	يعاني العراق من بنية تحتية رقمية قديمة، بما في ذلك شبكات الاتصالات ومراكز البيانات.	يؤدي هذا الضعف إلى إعاقة التحول الرقمي في الخدمات الحكومية والاقتصاد، ويزيد من الاعتماد على البنية التحتية والموارد الخارجية، مما يقوض الاستقلالية الوطنية.
ضعف الأمن السيبراني	توجد نقاط ضعف كبيرة في الأمن السيبراني للبنية التحتية الحيوية والمؤسسات الحكومية والخاصة في العراق.	يجعل هذا الضعف أمن المعلومات الوطنية عرضة للخطر، ويُسهل على الجهات الخارجية دول أو جماعات تنفيذ عمليات تجسس أو تخريب رقمي، مما يهدد الأمن القومي.
الفجوات التنظيمية والقانونية	هناك غياب لأطر قانونية وتشريعية حديثة ومتكاملة تنظم الفضاء الرقمي، بما في ذلك جرائم المعلومات، حماية البيانات، والمنافسة في الأسواق الرقمية.	تصعّب هذه الفجوات من قدرة الدولة على فرض سيادتها على الفضاء الرقمي، ومكافحة الجرائم الإلكترونية، وحماية بيانات المواطنين والشركات، ومنع الاحتكارات الرقمية.
القيود الاقتصادية والاعتماد على النفط	الاعتماد الكبير على إيرادات النفط يحد من الاستثمار في قطاعات أخرى مثل: التكنولوجيا الرقمية. كما أن الظروف الاقتصادية الصعبة تقيد الموارد المتاحة لتطوير البنية التحتية.	يبطئ هذا من وتيرة التطور التكنولوجي في العراق ويقلل من قدرته على المنافسة في الاقتصاد الرقمي العالمي، مما يجعله تابعاً تكنولوجياً للدول والشركات الكبرى.
الاعتماد على التكنولوجية والخدمات الأجنبية	يعتمد العراق بشكل كبير على الشركات الأجنبية لتوفير التكنولوجيا والبرمجيات والخدمات الرقمية الأساسية.	هذا الاعتماد يقوض الاستقلالية التكنولوجية للعراق ويعرضه لمخاطر الاستعمار الرقمي والضغوط الجيوبولتيكية، حيث يمكن لهذه الشركات أو دولها الأصلية أن تستغل هذا الإعتماد لتحقيق مصالحها.
جدول رقم : ٢		

الجدول من عمل الباحثة بالعودة إلى المصدر: (Al Barazanchi et al. 2024, 90–94)

المبحث الثاني

العراق بوصفه فاعل ناشئ في ساحة الجيوبولتيك الرقمي

يشهد العراق تحولات متسارعة في موقعه ضمن النظام السيبراني الإقليمي، حيث لم يعد مجرد ساحة مستهدفة بالهجمات والاختراقات، بل بدأ يتجه نحو بناء تموضع رقمي يتيح له التفاعل مع بيئة الجيوبولتيك الرقمي بصفته طرفاً فاعلاً. هذا المبحث يناقش طبيعة التهديدات السيبرانية التي يتعرض لها العراق من قوى إقليمية، ويرصد في الوقت ذاته خطوات الاستجابة المؤسسية والسياسية لتثبيت الحضور الرقمي وتعزيز السيادة الوطنية في الفضاء السيبراني.

المطلب الأول: خريطة التهديدات السيبرانية الموجهة للعراق:

١. **التمركز الإيراني:** يشكل العراق هدفاً استراتيجياً دائماً للاستخبارات السيبرانية الإيرانية، عبر مجموعات مرتبطة بها أو محسوبة عليها، مثل مجموعة (BladedFeline). أشارت تقارير شركة (ESET) للأمن السيبراني، الصادرة منتصف عام ٢٠٢٥، إلى أن هذه المجموعة المرتبطة أيضاً بالمجموعة التجسسية APT34 (وتُعرف أيضاً بإسم OilRig) نفذت حملة تجسس سيبراني مطوّلة استهدفت مسؤولين في الحكومة المركزية وحكومة إقليم كردستان. بدأت هجماتها منذ عام ٢٠١٧ بإختراق أنظمة حكومية في الإقليم، ثم توسعت لاحقاً لتشمل مؤسسات في بغداد. استخدمت المجموعة برمجيات خبيثة للسيطرة على أجهزة الضحايا وسرقة بياناتهم، مما مكّنها من التغلغل في مفاصل القرار. يعكس هذا النشاط نمطاً متصاعداً من الحروب السيبرانية الخفية التي يشهدها العراق، تقودها أطراف دولية أو جهات فاعلة بالوكالة، ضمن صراع نفوذ رقمي طويل الأمد (Antoniuk 2025).

٢. **التموضع التركي:** تُظهر الهجمات السيبرانية الأخيرة تركيزاً واضحاً على إقليم كردستان داخل العراق، من خلال تقنيات متقدمة مثل: ثغرات (صفر يوم) وعمليات إختطاف نظام أسماء النطاقات (DNS hijack). هذه الهجمات استهدفت قطاعات الإتصالات والخدمات التقنية الحكومية، ما جعل البنية المعلوماتية السيادية في كردستان والعراق عرضة للاستهداف المتكرر. وفي أيار عام ٢٠٢٥، كشفت شركة مايكروسوفت عن هجوم سيبراني معقد نُسب إلى جهة على صلة بالإستخبارات التركية، استغل ثغرة من نوع (صفر يوم) في تطبيق المراسلة المحلي (Output Messenger) للتجسس على قوات البشمركة الكردية (Turkish Minute 2025).

٣. **الغياب الإثباتي لإسناد مباشر لإسرائيل داخل العراق:** لا تتوفر أدلة رقمية منشورة تُثبت بشكل مباشر تورط جهات إسرائيلية في عمليات تجسس أو تعطيل سيبراني داخل العراق في المرحلة الأخيرة، رغم تصاعد الحروب السيبرانية في الإقليم. هذا الغياب الإثباتي يمثل فجوة معرفية لا يجوز ملؤها بالافتراض، بل يتطلب مواصلة الرصد عبر مصادر مفتوحة وتحليل شفاف للأنماط والسياسات (Freedom House 2024).

٤. **الخليج والتهديد السيبراني غير المباشر للعراق:** رغم تصاعد نشاط مجموعات الفدية والقرصنة في الخليج خلال عامي ٢٠٢٤–٢٠٢٥، لا يظهر العراق ضمن الدول الأكثر استهدافاً بهجمات حجب الخدمة (DDoS) وفق البيانات المعلنة. كما لا توجد إسنادات علنية تربط الهجمات الداخلية بجهات رسمية خليجية. لذلك تبقى طبيعة التهديد في هذا السياق عامة ومفتوحة، ما يفرض على العراق اعتماد دفاعات سيبرانية مرنة تستجيب لموجات هجمات سريعة ومتقلبة، يصعب التنبؤ بمصدرها أو نمطها (Macakanja 2025).

٥. **هشاشة البنية الرقمية في القطاعات الحيوية العراقية:** رغم عدم تسجيل هجمات سيبرانية معلنة على قطاعات مثل: المياه والطاقة خلال عام ٢٠٢٥، إلا أن التقييمات الإستخباراتية تؤكد ضعف الحماية الرقمية في هذه المجالات. وتشير دراسة أمنية عراقية إلى تصاعد التهديدات التي قد تُسبب خسائر اقتصادية جسيمة إذا استمرت ثغرات حماية البيانات دون معالجة فعّالة (شنشول وحمد ٢٠٢٥، ٨).

٦. **الإستجابة السياسية وتعزيز الجاهزية السيبرانية:** سياسياً أكد رئيس الوزراء محمد شياع السوداني أن الحكومة العراقية تولي أولوية لبناء القدرات البشرية والتقنية في مجال الأمن السيبراني، عبر تدريب كوادر متخصصة وإعداد خطط لمواجهة الهجمات المحتملة (السوداني ٢٠٢٥). كما أشار إلى أهمية التعاون مع القطاع الخاص لترصين قواعد البيانات الحكومية ومنع اختراقها. في السياق ذاته، تواصل الأجهزة الأمنية تنفيذ تمارين دورية تحاكي سيناريوهات هجومية مختلفة، وتُجري عمليات تحديث للأنظمة وتثبيت تصحيحات الأمان بشكل منتظم، في إطار استراتيجية استباقية لتعزيز الجاهزية السيبرانية (السوداني ٢٠٢٥). و رداً على تصاعد التهديدات السيبرانية، اتخذت الحكومة العراقية خطوات لتقوية دفاعها الرقمي. ففي كانون الثاني ٢٠٢٥، افتتح رئيس الوزراء المركز الوطني للأمن السيبراني بإشراف وزارة الداخلية، واطّلع على تجهيزاته ومهامه في حماية أنظمة البيانات الحكومية. كما وقّعت بغداد مذكرة تفاهم مع شركة (Resecurity) الأميركية لتعزيز البنية الدفاعية السيبرانية، وأجرت مشاورات تقنية مع شركة (BAE Systems) البريطانية لتطوير قدرات الأمن الإلكتروني ومعدات الاتصالات الدفاعية (Lee 2025).

٧. **أنماط التهديدات السيبرانية ضمن البيئة العراقية:** تُظهر الحالات التي تم تحليلها في هذا المطلب أن العراق يواجه طيفاً واسعاً من التهديدات السيبرانية، تختلف من حيث طبيعة الجهات الفاعلة، والأهداف المستهدفة، وآثارها المحتملة. ويمكن تصنيف هذه التهديدات ضمن أربعة نماذج أساسية تُلخص في **(الجدول رقم: ٣)** أدناه، الذي يساعد على فهم طبيعة المخاطر السيبرانية التي تتقاطع مع الأمن الوطني العراقي (Roumani and Alraee 2025).

نوع التهديد السيبراني	الجهات الفاعلة	الهدف الرئيسي	التأثير
هجمات الفدية	عصابات الجريمة المنظمة.	الإبتزاز المالي.	تشفير البيانات، تعطيل الخدمات.
هجمات الدول القومية	وكالات حكومية أو عسكرية.	التجسس، التخريب، التأثير الجيوسياسي.	سرقة بيانات حساسة، تعطيل طويل الأمد للبنية التحتية الحيوية.
هجمات على أنظمة التحكم الصناعي (ICS/SCADA)	دول قومية، إرهابيون سيبرانيون.	إحداث أضرار مادية في البنية التحتية (طاقة، مياه)	تدمير المعدات، انقطاع الخدمات الحيوية.

هجمات على سلاسل التوريد	جهات فاعلة متقدمة (APTs).	اختراق الأنظمة عبر برامج أو أجهزة موثوقة.	وصول واسع النطاق إلى شبكات متعددة.

جدول رقم : ٣

الجدول من عمل الباحثة بالعودة إلى المصدر: (Roumani and Alraee 2025).

المطلب الثاني: هندسة الدور الرقمي للعراق في البيئة الإقليمية:

منذ عام ٢٠٠٣، يشهد العراق فراغاً استراتيجياً تستثمره قوى إقليمية ودولية لفرض نفوذها عبر أدوات متعددة، أبرزها الفضاء الرقمي الذي تحوّل إلى ساحة صراع غير تقليدي. يُعزى تحول العراق إلى ساحة للصراع الرقمي إلى أهميته الاستراتيجية التي تنبع من عدة عوامل متكاملة تتضمن موقعه الجغرافي بوصفه حلقة وصل بين قارات آسيا وأوروبا وأفريقيا، وامتلاكه لثروات طبيعية هائلة، خاصة النفط، يجعله محط أطماع وتنافس القوى الكبرى (Shebani and Irheim 2019,558). فلم يعد التأثير محصوراً في العمل العسكري أو السياسي، بل شمل الحملات المعلوماتية، إدارة التصورات، والحروب الافتراضية (Al-Hassani 2021). حيث إستغلت جهات داخلية وخارجية هذا الفضاء لتأجيج الانقسامات، وظهرت بعد هزيمة (داعش) شبكات منظمة من المتصيدين الإلكترونيين تستهدف إسكات المعارضين وتفريغ النقاش العام من مضمونه (Al-Hassani 2021).

أظهرت أحدث البيانات الرسمية ارتفاع نسبة مستخدمي الإنترنت في العراق لتصل إلى ٨٢.٩% من السكان بحلول نهاية عام ٢٠٢٤ **(Lee 2025).** وقد أعلنت وزارة الاتصالات العراقية هذه النسبة استنادًا إلى بيانات الاتحاد الدولي للإتصالات (ITU)، مما يمثل زيادة ملحوظة عن نسبة ٨١.٧% المسجلة في عام ٢٠٢٣ وفق بيانات البنك الدولي (World Bank 2025). تعكس هذه الأرقام قفزة كبيرة بالمقارنة مع حوالي ٤٤.٣% في عام ٢٠١٩، مما يشير إلى نمو متسارع في تبني الإنترنت خلال السنوات الأخيرة (Lee 2025). رافق ذلك تصاعد أدوات وأساليب النفوذ الرقمي المستخدمة من قبل أطراف مختلفة، من أبرزها:

- **حملات التجسس السيبراني والاختراقات المتقدمة:** قيام جهات معادية بشن هجمات تجسس إلكتروني وعمليات اختراق متطورة للبنية التحتية الرقمية بهدف جمع المعلومات أو تخريب الأنظمة **(Saad 2024,56).**
- **حملات التضليل المعلوماتي والهندسة الاجتماعية:** استخدام المعلومات المضللة وتقنيات التأثير الرقمي أو ما يُعرف بالهندسة الاجتماعية لنشر الشائعات وتوجيه النقاش العام بما يخدم أجندات معينة **(Saad 2024,55).**
- **حجب المنصات وقطع الإنترنت المتكرر:** لجوء بعض الجهات إلى حظر مواقع التواصل الاجتماعي والمنصات الرقمية أو فرض انقطاعات متكررة لخدمة الإنترنت بوصفها وسيلة للتحكم في تدفق المعلومات أو لأسباب أمنية وإدارية **(Saad 2024,57).**

بات العراق، في ظل ارتفاع الاتصال الرقمي، ساحة مفتوحة لصراعات النفوذ الرقمي، حيث تتداخل التكنولوجيا مع السياسة. ومع تزايد التحديات السيبرانية، أصبحت التجربة الرقمية العراقية نموذجاً لفهم العلاقة بين التطور التقني والتحولات الجيوسياسية في المنطقة (Saad 2024,58). **(أنظر الجدول رقم : ٤).**

نوع التحدي	الوصف
البنية التحتية الرقمية	بنية تحتية محدودة تعتمد على تقنيات قديمة، ضعف في الاتصال بالإنترنت، واعتماد كبير على الأسواق الخارجية لتوفير موارد تكنولوجيا المعلومات والاتصالات.
الأطر القانونية والتنظيمية	فجوات تنظيمية واسعة، وقوانين حالية غير كافية لمواجهة الجرائم السيبرانية المعقدة، وضعف في سياسات حماية البيانات والمنافسة العادلة.
القدرات البشرية	نقص حاد في الكفاءات والكوادر البشرية المؤهلة والمدربة في مجالات التكنولوجيا الرقمية والأمن السيبراني، وضعف الوعي الرقمي العام.
التحديات السياسية والأمنية	عدم الاستقرار السياسي والأمني، الفساد المستشري الذي يعيق تنفيذ المشاريع الرقمية، ومقاومة النخب السياسية للإصلاح والتغيير.
جدول رقم : ٤	

الجدول من عمل الباحثة.

يعكس الجدول أعلاه مشهداً معقّداً من التحديات المتداخلة التي تُقيد قدرة العراق على التفاعل السيادي مع الفضاء الرقمي. هذا الواقع لا يمكن فصله عن الموقع الجيوبولتيكي للعراق بوصفه ساحة تقاطع لمشاريع النفوذ الرقمي الإقليمي والدولي، حيث تؤدي هشاشة البنية القانونية، وضعف القدرات البشرية، وتباين سياسات الحوكمة إلى تعزيز الاختراقات وتقويض فرص التمركز السيادي الرقمي. غير أن هذه التحديات لا تمثل نهاية المعادلة، بل تؤسس لنقطة انطلاق لإعادة هندسة الدور العراقي في الفضاء السيبراني. فالانتقال من موقع الساحة المتلقية للنفوذ إلى طرف فاعل يتطلب حزمة من المسارات الإصلاحية والسياسات السيبرانية المؤسِسة، التي تشكل في مجموعها أدوات لتثبيت النفوذ الرقمي العراقي في البيئة الإقليمية (Al-Dabbagh et al. 2025, 65-61). وفيما يلي أبرز هذه المسارات:

١. **الحوكمة والتشريع:** يستدعي الأمر إقرار استراتيجية وطنية شاملة تُعرِّف الأدوار والمسؤوليات بين المجلس الوطني للأمن السيبراني ووزارات الاختصاص والهيئات التنظيمية وIQ-CERT، مع تحديث الأطر القانونية بطريقة تُراعي المعايير الدولية للضرورة والتناسب والشرعية. وعلى صعيد الخصوصية، تُفيد التقارير القانونية بأن قانون حماية البيانات الشخصية رقم ٢٤ لسنة ٢٠٢٣ الذي نُشِر في الجريدة الرسمية في ١٧ ايلول ٢٠٢٣ ودخل حيز النفاذ في ١٧ آذار ٢٠٢٤، يتيح نافذة لتفعيل حقوق أصحاب البيانات، وبناء سلطة إشراف مستقلة وإنفاذ إلزامي على المعالجين، شريطة الإسراع بإصدار اللوائح التطبيقية وبناء القدرات الرقابية (Proelium Law 2025).

٢. **حماية البنية التحتية الحيوية والمرونة التشغيلية:** و هي ليست قضية تقنية فقط، بل مسألة سيادية من الطراز الأول، تعكس قدرة الدولة على فرض تنظيمها السيبراني وضبط الفضاء الرقمي وفق أولوياتها الوطنية. ولهذا، فإن تبنّي أطر إدارة المخاطر الدولية يمثّل خياراً سياسياً واعياً نحو بناء منظومة دفاع رقمية مؤسسية، تُخضع الجهات الحكومية وغير الحكومية لمعايير موحّدة تتجاوز الارتجال وتُرسّخ ثقافة الحوكمة والمساءلة (NetBlocks 2023) في هذا السياق، يُعد تأسيس مراكز عمليات أمنية قطاعية وشبكات متخصصة بإشراف IQ-CERT، مع فرض الإبلاغ الإلزامي عن الحوادث، جزءاً من إعادة هندسة العلاقة بين الدولة وفاعليها الرقميين. ويُعد تطبيق سياسات الأمن عبر دورة التوريد في عقود الشراء العام، خاصة في قطاعات حيوية مثل: الطاقة والاتصالات، خطوة حاسمة نحو كسر الاعتماد غير الآمن على برمجيات ومصادر خارجية (NetBlocks 2023). هذه السياسات، حين تُدمج باختبارات اختراق دورية، ومختبرات محاكاة (Cyber Range)، ونظم تبادل تهديدات آنية مع القطاع الخاص، فإنها لا تحمي فقط بنية الدولة، بل تُعيد تعريف دورها بوصفها فاعل رقمي منضبط وذو سيادة في بيئة دولية تعيد تشكيل موازين القوة عبر الفضاء السيبراني (NetBlocks 2023).

٣. **توسيع البنية الرقمية في العراق:** التي تُشكل أداة سيادية لتحفيز الاقتصاد الرقمي الآمن. توصي الدراسات الدولية بضرورة تبنّي نماذج أعمال مرنة لتسريع الانتشار الواسع للإنترنت عالي السرعة، بما يضمن تقليص فجوة الوصول، وتوفير بيئة تنافسية جاذبة، وتحفيز الاستثمار المحلي والأجنبي (FBI and DOJ 2024). لكن هذا التوسّع يجب أن يُصمّم منذ لحظته الأولى وفق متطلبات أمنية وخصوصية افتراضية مضمّنة في البنية، لحماية الأفراد والمؤسسات، لا سيما المنشآت الصغيرة والمتوسطة التي تُشكّل عصب الاقتصاد المحلي (FBI and DOJ 2024). كما يشكّل تطوير بيئة سحابية وطنية مؤمّنة، ووضع سياسة شفافة لتنظيم حركة البيانات عبر الحدود، وإنشاء مراكز بيانات بمعايير دولية، ركائز سياسية ضرورية لبناء منظومة رقمية سيادية، وتحفيز الابتكار وريادة الأعمال، واستقطاب الشركات الناشئة والاستثمارات عالية القيمة. هذه المقومات ليست فقط مكونات تقنية، بل هي عناصر استراتيجية في هندسة الاقتصاد الرقمي العراقي ضمن الإقليم والتحولات العالمية (FBI and DOJ 2024).

٤. **تعزيز القدرات البشرية في المجال السيبراني:** الذي يمثل ركيزة سياسية استراتيجية لأي تحول رقمي سيادي. ولا يمكن بناء أمن وطني رقمي دون تأسيس منظومة مستدامة لإعداد الكفاءات و رفد مؤسسات الدولة بخبرات قادرة على الاستجابة لتهديدات متقدمة من نمط (APT34) و(MuddyWater). يتطلب ذلك إطلاق برنامج وطني للمهارات السيبرانية يُصاغ بوصفه جزء من السياسة العامة للدولة، ويربط بين الجامعات، ومؤسسات القطاع العام، والقطاع الخاص ضمن مسارات مهنية واضحة، وشهادات احترافية معتمدة، وآليات لتأهيل

الكوادر (Global Cyber Security Capacity Centre 2022). يشمل: البرنامج أيضاً حوافز لجذب المواهب العراقية من الخارج، وتنظيم مسابقات تقنية مثل: Capture the Flag، وتفعيل برامج الإبلاغ عن الثغرات (VDP/Bug Bounty) تحت إشراف IQ-CERT، بما يضمن توطين الخبرة داخل مؤسسات الدولة، ويُنتج شبكة استجابة وطنية مؤهلة، تمتلك المعرفة، وتعمل ضمن قنوات مؤسسية منضبطة في حالات الطوارئ الرقمية. هذه الرؤية لا تهدف فقط لسد النقص الفني، بل لتثبيت السيادة الرقمية بوصفها خيار استراتيجي قائم على العنصر البشري (Global Cyber Security Capacity Centre 2022).

٥. **الدبلوماسية السيبرانية وبناء التحالفات الأمنية:** يمثل الانخراط العراقي النشط في مبادرات الاتحاد الدولي للاتصالات، وشبكات بناء القدرات، وتحالفات تبادل المعلومات، مساراً سياسياً حاسماً لتعزيز الأمن الرقمي الوطني (Al-Dabbagh et al. 2025, 6562). وتوسيع التعاون مع شركاء إنفاذ القانون الدوليين، ممن نفذوا عمليات نوعية ضد البنى الدعائية الإرهابية، لا يساهم فقط في تحييد التهديدات العابرة للحدود، بل يُراكم خبرات عملية قابلة للتدوير داخل المؤسسات العراقية (Al-Dabbagh et al. 2025, 6562). هذا النوع من التعاون يُعيد تعريف مكانة العراق بوصفه طرفاً فاعلاً و ليس مجرد ساحة، ويمنحه أدوات سيادية للتفاعل مع البيئة الدولية وفق منطق شراكة واستباق لا رد فعل (Al-Dabbagh et al. 2025, 65-62).

الخاتمة:

أن التحول الجيوبولتيكي لم يعد يقتصر على صراع المواقع والنفوذ الجغرافي، بل توسع ليشمل ساحات رقمية جديدة تُدار عبر أدوات سيبرانية معقّدة. العراق، بما يملكه من موقع استراتيجي وثقل اقتصادي – أمني في المنطقة، بات في قلب هذا التحول؛ ليس فقط بوصفه دولة متأثرة، بل بكونه ساحة مستهدفة ضمن صراعات النفوذ الرقمي المتصاعدة بين الفاعلين الإقليميين والدوليين. هذا التحول يضع العراق أمام مفترق حاسم: إما أن يظل بيئة رخوة للاختراقات والتجاذب السيبراني، أو أن يتحول إلى فاعل رقمي سيادي قادر على إدارة مصالحه وتشكيل معادلات النفوذ الرقمي في الإقليم.

لقد أظهر البحث أن الساحة الرقمية العراقية ما تزال هشّة وغير مؤمّنة، إلا أن بوادر التحول نحو الجيوبولتيك الرقمي الفاعل بدأت تتشكل عبر خطوات تشريعية ومؤسساتية أولية. السيادة الرقمية لم تعد ترفاً تقنياً أو مشروعاً إدارياً، بل أصبحت امتداداً مباشراً للسيادة الوطنية. وبذلك، فإن موقع العراق في الجيوبولتيك الرقمي لا يتحدد فقط بقدراته التقنية، بل أيضاً بإرادته السياسية وقدرته على بناء تحالفات رقمية استراتيجية، وتطوير سياسات سيبرانية تؤطر علاقته بالبيئة الرقمية الإقليمية والدولية.

الإستنتاجات:

١. لم يعد العراق محكوماً بالجغرافيا التقليدية فقط، بل أضحى جزءاً من نظام جيوبولتيكي رقمي جديد يُعاد فيه تعريف النفوذ والسيادة من خلال التحكم في البيانات والشبكات والبنى التحتية الرقمية.
٢. التهديدات السيبرانية التي تستهدف العراق تعبّر عن صراع جيوبولتيكي بأدوات جديدة، حيث تُوظّف الهجمات السيبرانية والتجسس الرقمي كوسائل لتعديل موازين القوة دون تكلفة عسكرية مباشرة.
٣. تعدد الفاعلين الرقميين داخل الساحة العراقية، من دول قومية إلى جماعات قرصنة وشركات تكنولوجيا، يعكس تشابكاً عميقاً بين الجيوبولتيك التقليدي والرقمي، ويُضعف قدرة الدولة على إدارة أمنها السيبراني بشكل مستقل.
٤. العراق لا يزال يعاني من غياب الرؤية الجيوبولتيكية الرقمية الشاملة، إذ تفتقر سياساته الرقمية إلى التنسيق الإستراتيجي مع الأمن الوطني والسياسة الخارجية.
٥. على الرغم من التقدم القانوني الأخير المتمثل بقانون حماية البيانات، فإن ترجمة هذه الخطوات إلى سيادة رقمية فعالة تتطلب إصلاحاً هيكلياً شاملاً في بنية الدولة، ومأسسة الأمن السيبراني بوصفه جزءاً من القرار السياسي.

التوصيات:

- صياغة عقيدة جيوبولتيكية رقمية عراقية تُدرج الأمن السيبراني ضمن السياسات العليا للدولة، وتنسّق بين وزارات الدفاع والاتصالات والخارجية والمخابرات.
- بناء نموذج وطني للسيادة الرقمية يتضمن حماية تدفقات البيانات، وتحقيق الاستقلالية التكنولوجية، ومراقبة نفوذ الشركات الرقمية العابرة للحدود.
- تعزيز التفاعل مع التحالفات الإقليمية والدولية في إطار الدبلوماسية السيبرانية لضمان الاعتراف بمصالح العراق في البيئة الرقمية الإقليمية.
- إطلاق برامج وطنية لصناعة الأمن السيبراني المحلي، بما يقلص الاعتماد على الحلول الأجنبية ويعزز مفهوم التمركز الرقمي.
- اعتماد السياسات الجيوبولتيكية في التعامل مع الفضاء السيبراني بوصفه امتداداً للأمن الوطني، وليس ملفاً تقنياً معزولاً عن عمق الدولة الاستراتيجي.

المصادر باللغة العربية:

١. أحمد شاكر العلاق، ٢٠٢٥، «الجيوبولتيك والذكاء الاصطناعي، تداخل الأبعاد وتأثيرها على العلاقات الدولية»، مجلة الدراسات الاستراتيجية للكوارث وإدارة الفرص، المركز الديمقراطي العربي: ألمانيا، ١٨ تموز، تاريخ الوصول ٢٠ كانون الأول ٢٠٢٥،
https://democraticac.de/?p=105635

٢. خالد وليد محمود، ٢٠٢٥، «الحدود السيبرانية إذ تعيد تعريف السيادة والجغرافيا»، شبكة الجزيرة الإعلامية – مدونات: الدوحة، ٢٣ كانون الثاني، https://www.aljazeera.net/blogs/2025/1/23/الحدود-السيبرانية-إذ-تعيد-تعريف-السيادة-والجغرافيا
٣. دبير نوف العتيبي، ٢٠٢٥، «هجمات إلكترونية متطوّرة تضرب البنية الحيوية بالشرق الأوسط»، الزمان – طبعة العراق: بغداد، ٢٣ حزيران، https://www.azzaman-iraq.com/content.php?id=106925
٤. رباب حدادة وبدرة قعلول، ٢٠٢٢، «جيوبوليتيك: الذكاء الاصطناعي السياسي»، المركز العربي لأبحاث الفضاء الإلكتروني، ٢٢ شباط، https://accronline.com/article_detail.aspx?id=31702
٥. رئيس مجلس الوزراء محمد شياع السوداني، ٢٠٢٥، «السوداني يؤكد على مواجهة الهجمات السيبرانية المتوقعة»، بغداد اليوم: بغداد، ١٩ نيسان، https://baghdadtoday.news/272470-.html
٦. عادل محمد علي بوغرسة، ٢٠٢٥، «مقاربة مفاهيمية تاريخية تحليلية للتنظير الجيوبوليتيكي التقليدي»، ضمن كتاب التنظير الجيوبولتيكي للقوة في العلاقات الدولية، المركز الديمقراطي العربي: ألمانيا.
٧. علاء عبيس راضي الجبوري، ٢٠٢٥، الهجمات السيبرانية والأمن الوطني العراقي: بين المواجهة والإدارة، ورقة بحثية، مركز البيان للدراسات والتخطيط: بغداد، https://www.bayancenter.org/wp-content/uploads/2025/02/ghjklo0ie18.pdf
٨. نسرين رياض شنشول وأنور حامد حمد، ٢٠٢٥، «الأمن السيبراني وحماية الاقتصاد العراقي: التهديدات السيبرانية واستراتيجيات المواجهة»، مركز البيان للدراسات والتخطيط: بغداد، ٢٣ نيسان، https://www.bayancenter.org/wp-content/uploads/2025/04/Cyber-%E2%80%8B%E2%80%8Bsecurity2342025.pdf
٩. نور سهيلة قادري، ٢٠٢٥، «السيادة الرقمية.. عندما يرتهن مصير دول بكبسة زر»، الجزيرة نت: الدوحة، ١٣ آب، تاريخ الوصول ٢٠ كانون الأول ٢٠٢٥، https://www.aljazeera.net/politics/2025/8/13/السيادة-الرقمية-عندما-يرتهن-مصير-دول-بكبسة-زر

المصادر باللغة الانكليزية:

1. Abdelkarim, Yassin Abdalla. 2024. “A Literature Review of the Evolution of Sovereignty and Borders Concepts in Cyberspace.” *International Cybersecurity Law Review* 5, no. 2. https://doi.org/10.1365/s43439-024-00118-0
2. Al Barazanchi, Israa Ibraheem, and Dima Haider Rasheed. 2024. “The Role of the Iraqi National Data Center in Advancing Digital Transformation and Data Sovereignty.” *SHIFRA 2024* (June). https://doi.org/10.70470/shifra/2024/010
3. Al-Dabbagh, Zeyad Samir, Arshed Adil Rashed, and Ghufran Younus Hussein. 2025. “Challenges of Iraqi National Security in Confronting Cyber Terrorism and Ways to Strengthen It.” *Dirasat: Human and Social Sciences* 52, no. 5. https://doi.org/10.35516/hum.v52i5.6562

4. Al-Hassani, Ruba A. 2021. "Hate Speech, Social Media and Political Violence in Iraq: Virtual Civil Society and Upheaval." *Tahrir Institute for Middle East Policy*, February 11, 2021. https://timep.org/2021/02/11/hate-speech-social-media-and-political-violence-in-iraq-virtual-civil-society-and-upheaval
5. Antoniuk, Daryna. 2025. "Iran-linked Hackers Target Kurdish and Iraqi Officials in Long-running Cyber-espionage Campaign." *The Record from Recorded Future News*, June 5, 2025. https://therecord.media/iran-linked-hackers-target-kurdish-iraq-cyber-espionage
6. Aviv, Itzhak, and Uri Ferri. 2023. "Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem." *International Journal of Critical Infrastructure Protection* 43 (December). https://www.sciencedirect.com/science/article/abs/pii/S1874548223000501
7. Center for Strategic and International Studies (CSIS). 2025. *Significant Cyber Incidents*. Washington, D.C.: CSIS, June 10, 2025. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-06/250610_Significant_Cyber_Incidents.pdf
8. European Union. 2024. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cyber Security Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).* Official Journal of the European Union (OJ L 2847), 20 November 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
9. FBI Miami Field Office and U.S. Department of Justice. 2024. "FBI Miami Field Office and DOJ Join European Partners in Major Takedown of Critical Online Infrastructure to Disrupt ISIS Propaganda." *Federal Bureau of Investigation*, June 17, 2024. https://www.fbi.gov/contact-us/field-offices/miami/news/fbi-miami-field-office-and-doj-join-european-partners-in-major-takedown-of-critical-online-infrastructure-to-disrupt-isis-propaganda
10. Freedom House. 2024. "Iraq: Freedom on the Net 2024 Country Report." *Freedom on the Net 2024*. Freedom House. Accessed August 19, 2025. https://freedomhouse.org/country/iraq/freedom-net/2024
11. Global Cyber Security Capacity Centre (GCSCC). 2022. "Iraq CMM Review in Progress." *GCSCC News*, June 21, 2022. https://gcscc.ox.ac.uk/article/iraq-cmm-review-progress
12. Huskaj, Gazmend. 2023. "Digital Geopolitics: A Review of the Current State." In *Proceedings of the 18th International Conference on Cyber Warfare and Security*, 152–160. Geneva: Geneva Centre for Security Policy.
13. Lee, John. 2025. "Iraq Launches National Cybersecurity Centre." *Iraq Business News*, January 13, 2025. https://www.iraq-businessnews.com/2025/01/13/iraq-launches-national-cybersecurity-centre
14. Lee, John. 2025. "Iraq Sees Surge in Internet Penetration." *Iraq Business News*, July 15, 2025. Accessed December 20, 2025. https://www.iraq-businessnews.com/2025/07/15/iraq-sees-surge-in-internet-penetration

15. Macakanja, Jovana. 2025. "2024 Year in Review: Ransomware Groups, Hacktivists, and IABs Targeting the Middle East." *Cyjax*, January 29, 2025. https://www.cyjax.com/resources/blog/2024-year-in-review-ransomware-groups-hacktivists-and-iabs-targeting-the-middle-east
16. Mohammed Shebani, and Raedi Irheim. 2019. "The Strategic Importance of Iraq in the International System." *Tikrit Journal for Political Science* (September): 558–580. https://doi.org/10.25130/poltic.v0i0.179
17. NATO. 2024. "Cyber Defence." Accessed July 30, 2024. https://www.nato.int/cps/en/natohq/topics_78170.htm
18. NetBlocks. 2023. "Telegram Restricted in Iraq over Personal Data Leaks." *NetBlocks Reports*, posted August 6, 2023, updated August 7, 2023. https://netblocks.org/reports/telegram-restricted-in-iraq-over-personal-data-leaks-9AkJ4o8D
19. Proelium Law. 2025. "Data Protection Regulation Tracker." Accessed August 21, 2025. https://proeliumlaw.com/data-protection-regulation-tracker
20. Roumani, Yaman, and Mais Alraee. 2025. "Examining the Factors That Impact the Severity of Cyberattacks on Critical Infrastructures." *Computers & Security* 148 (January). https://doi.org/10.1016/j.cose.2024.104074
21. Saad, Fatimah Faraj. 2024. "The Role of Digital Transformation in Promoting Economic Growth in Iraq 2010–2022." *Anggaran: Jurnal Publikasi Ekonomi dan Akuntansi* 3, no. 1. https://doi.org/10.61132/anggaran.v3i1.1117
22. Tan, Kheng Leong, Chi-Hung Chi, and Kwok-Yan Lam. 2023. "Survey on Digital Sovereignty and Identity: From Digitization to Digitalization." *ACM Computing Surveys* 56, no. 3. https://doi.org/10.1145/3616400
23. The White House. 2023. *National Cybersecurity Strategy*. Washington, D.C.: The White House.
24. Turkish Minute. 2025. "Turkey-backed Hackers Used Software Flaw to Spy on Kurdish Security Forces in Iraq: Microsoft." *Turkish Minute*, May 13, 2025. https://www.turkishminute.com/2025/05/13/turkey-backed-hackers-used-software-flaw-to-spy-on-kurdish-security-forces-in-iraq-microsoft
25. World Bank. 2025. "Individuals Using the Internet (% of Population) – Iraq." *TheGlobalEconomy.com*. Accessed December 20, 2025. https://www.theglobaleconomy.com/iraq/internet_users
26. Zirojević, Ivana Z. 2024. "Digital Transformation of Geopolitics: New Tools, Actors, and Power Dynamics." *Kultura Polisa* 21, no. 3. https://doi.org/10.51738/kpolisa2024.21.3r.77z