Journal of Al-Farabi for Humanity Sciences

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://iasj.rdd.edu.iq/journals/journal/view/95
مجلة الفارابي للعلوم الإنسانية تصدرها جامعة الفارابي

التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي وتأثيره في الأمن السيبراني العراقي

أ.د. ماجد صدام سالم

جامعة بغداد/ المركز الوطني للدراسات السكانية والديموغرافية

majid.s@ncpds.uobaghdad.edu.iq

Geopolitical competition over artificial intelligence technologies and its impact on Iraqi cybersecurity

Prof. Majid Saddam Salim
University of Baghdad / National Centre for Population and Demographic Studies
majid.s@ncpds.uobaghdad.edu.iq

الملخص:

يهدف البحث الى تحليل التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي وتأثيره على الامن السيبراني في العراق، يستخدم البحث المنهج الوصفي التحليلي، ويعتمد على البيانات من التقارير الدولية والدراسات السابقة مع التحليل الجيوسياسي للقوى العالم الكبرى (الولايات المتحدة، الصين، روسيا، الاتحاد الاوربي). أظهرت النتائج أن العراق يقع ضمن منطقة حساسة جيوسياسياً. وأن ضعف البنية التحتية الرقمية وغياب استراتيجية وطنية واضحة للأمن السيبراني، يجعلان العراق عرضه للتهديدات والهجمات السيبرانية الاقليمية والدولية. كما ان التنافس الدولي على تقنيات الذكاء الاصطناعي يزيد من هذه المخاطر، ولكنه في الوقت نفسه يمثل فرصة لتعزيز القدرات الرقمية الوطنية، اذا ما تم تبني استراتيجية وطنية شاملة تربط بين الذكاء الاصطناعي والأمن السيبراني. يقترح البحث مجموعة من التوصيات لتعزيز الامن السيبراني، تشمل تطوير البنية التحتية الرقمية، تحسين التشريعات والسياسات الوطنية، بناء قدرات بشرية متخصصة، وتعزيز التعاون الدولي، وتطبيق الذكاء الاصطناعي في منظومات المراقبة والكشف عن التهديدات، ويوفر اطاراً استراتيجيا للتعامل مع التحديات المستقبلية.

الكلمات المفتاحية: الجيوبوليتيك الرقمي، الأمن الوطني، التكنولوجيا، القوة الناعمة الرقمية، أمن المعلومات.

Abstract:

The research aims to analyse geopolitical competition over artificial intelligence technologies and its impact on cybersecurity in Iraq. The research uses a descriptive analytical approach and relied on data from international reports and previous studies, along with a geopolitical analysis of the major world powers (United States, China, Russia and the European Union). The results of the research show that Iraq is located in a geopolitically sensitive region .The weakness of its digital infrastructure and the absence of a clear national cybersecurity strategy make Iraq vulnerable to regional and international cyber threats and attacks. International competition over artificial intelligence technologies increases these risks, but at the same time represents an opportunity to strengthen national digital capabilities, if a comprehensive national strategy linking artificial intelligence and cybersecurity is adopted. The research proposes a set of recommendations to enhance cybersecurity, including developing digital infrastructure, improving national legislation and policies, building specialised human capacity, strengthening international cooperation, and applying artificial intelligence in threat monitoring and detection

systems. It also provides a strategic framework for dealing with future challenges .**Keywords:** Digital geopolitics, National security, Technology, Digital soft power, Information security.

المقدمة

شهد العالم خلال السنوات الماضية تحولاً جذرياً في طبيعة القوة الدولية، اذ برز الذكاء الاصطناعي بوصفه أحد أهم محركات التنافس الجيوسياسي، وإدارة لإعادة تشكيل موازين النفوذ والسيطرة في النظام الدولي المعاصر. ولم يعد مجرد تقنية متقدمة بقدر ما أصبح عنصراً استراتيجياً في صياغة السياسات الدفاعية والهجومية، والتحكم بالبنى الرقمية، وتوجيه الاقتصاد العالمي وادارة الحروب المستقبلية، وتعزيز القدرات الاستخباراتية والامنية للدول. وكذلك الفضاء السيبراني اصبح يمثل ساحة للصراع بين القوى الاقليمية والدولية المختلفة، وهو لم يكن فقط منصة للابتكار والتطوير بل يمثل تحدياً كبيراً يتعلق بأمن المعلومات وخصوصية الافراد مع التوسع الكبير في استخدام الانترنيت وتكامل الانظمة الرقمية (محمود، ٢٠٢٥، صفحة ٣١٥).وقد دفع هذا التحول القوى الكبرى مثل (الولايات المتحدة الامريكية والصين وروسيا والاتحاد الاوربي) الى الاستثمار المكثف في تقنيات الذكاء الاصطناعي، باعتبارها رصيداً جيوسياسياً يعزز النفوذ العالمي ويخلق بيئة ردع رقمي جديدة تتجاوز الحدود التقليدية للصراع، كما اصبحت السيطرة على البيانات والخوارزميات والبنى التحتية الرقمية عنصراً محورياً في تعزيز الأمن الوطني والقدرة على المواجهة في بيئة دولية تتسم بتصاعد المنافسة التقنية. أصبح الذكاء الاصطناعي عاملاً محورياً في الأمن السيبراني، أذ يستخدم لتعزيز أنظمة الدفاع الالكترونية والتنبؤ بالهجمات وتحليل البيانات المهمة والمعقدة واكتشاف التهديدات قبل وقوعها .(Thompson, 2024, p. 28) يمثل العراق واحدة من الدول التي تواجه تحديات متزايدة في ظل التنافس الدولي، نظراً لموقعه الجيوسياسي الحيوي في منطقة الشرق الاوسط (Shires, 2021, p. 236). ووجوده ضمن فضاء اقليمي تتداخل فيه مصالح القوى الكبرى، فضلاً عن هشاشة البنية الرقمية والامنية نسبياً. وقد تعرضت المؤسسات العراقية خلال السنوات الاخيرة لهجمات سيبرانية متعددة استهدفت البنى الحكومية وقطاعات الطاقة والاتصالات والمصارف، في مؤشر على تحول العراق الى ساحة تنافس سيبراني تتداخل فيه أطراف اقليمية ودولية وجهات غير حكومية مستفيدة من الثغرات الامنية في البنى الرقمية وغياب استراتيجية متكاملة للذكاء الاصطناعي والامن السيبراني. من هنا تنبع اهمية البحث في محاولة تحليل التنافس الجيوسياسي العالمي على تقنيات الذكاء الاصطناعي وأستكشاف انعكاساته المباشرة وغير المباشرة على الامن السيبراني العراقي، وتقديم رؤية عملية لبناء استراتيجية وطنية قادرة على حماية المجال الرقمي العراقي وتعزيز السيادة التكنولوجية للدولة.

أولاً: مشكلة البحث:

يشهد النظام الدولي تحولات استراتيجية نتيجة التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي، ما أدى إلى بروز البيئة السيبرانية كساحة رئيسة للصراع والتأثير، خاصة في الدول ذات الأهمية الجيوسياسية مثل العراق. ويمكن صياغة مشكلة البحث: **إلى أي مدى يؤثر التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي بين القوى الدولية في الأمن السيبراني العراقي؟**

ثانياً: فرضية البحث:

ينطلق البحث من الفرضية الآتية **يؤثر التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي بشكل مباشر في الأمن السيبراني العراقي،** بحيث يؤدي ضعف التكامل التقني والاستراتيجي إلى زيادة التهديدات الرقمية وتقييد قدرات الدولة على حماية فضائها السيبراني.

ثالثاً: أهداف البحث: تحليل تأثير التنافس الجيوسياسي على تقنيات الذكاء الاصطناعي في الأمن السيبراني العراقي، واستكشاف السبل الاستراتيجية لتعزيز القدرات السيبرانية الوطنية ومن أهم أهداف البحث:

١. توضيح الإطار المفاهيمي للعلاقة بين الذكاء الاصطناعي والجغرافيا السياسية والأمن السيبراني. وتحليل أشكال التنافس الدولي على تقنيات الذكاء الاصطناعي وتأثيرها على البيئة الأمنية الإقليمية.

٢. دراسة واقع الأمن السيبراني في العراق وتحديد نقاط القوة والضعف. ومعرفة مدى تأثير التنافس الجيوبوليتكي الرقمي مع ابراز المخاطر والتهديدات الناتجة من هذا التنافس.
٣. تحليل التهديدات السيبرانية التي تواجه العراق في ظل التنافس الدولي. يمكن توظيف تقنيات الذكاء الاصطناعي لتعزيز قدرة العراق الرقمية الدفاعية.
٤. تقديم رؤية استراتيجية لتطوير منظومة الأمن السيبراني العراقي باستخدام تقنيات الذكاء الاصطناعي.

رابعاً: مراجعة الأدبيات والدراسات السابقة:

تشكل مراجعة الأدبيات أطاراً علمياً لفهم الاشكالية البحثية وتوضيح الجهود الاكاديمية التي سبقت هذا البحث، مع ابراز الفجوات المعرفية التي يسعى اليها البحث لمعالجتها والتي يمكن تقسيم تلك الدراسات الى اربع محاور رئيسة:

١. **الأمن السيبراني:** تطرقت العديد من الدراسات على مفهوم الامن السيبراني بوصفه الأداة الاستراتيجية لحماية البيانات والشبكات من التهديدات الرقمية وأشار (صليبي، ٢٠٢٤، صفحة ٥١٠) الى ان الأمن السيبراني هو الجهود المبذولة لضمان حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، أما كل من (أوسوبا و ويليام، ٢٠١٧، صفحة ٥) فقد ركزا على البعد الدولي للأمن السيبراني وأنه يشكل ميدان جديد للتعاون والصراع بين الدول.
٢. **الذكاء الاصطناعي والأمن السيبراني:** تناولت الدراسات الحديثة الدور الكبير للذكاء في تحسين قدرة الامن السيبراني للكشف المبكر للهجمات والتنبؤ بالتهديدات والاستجابة التلقائية وبسرعة فقد بين (الحجرف، ٢٠٢٤، صفحة ٧٨)، الى ان دمجهما يعزز القدرة على مواجهة التهديدات العابرة للحدود. كما أشار (الراشدي، ٢٠٢٥، صفحة ١٤١). الى ان الذكاء الاصطناعي أصبح أداة مزدوجة الاستخدام يمكن ان يعمل للدفاع او الهجوم مما يرفع من أهميته الجيوبوليتكية.
٣. **الأمن السيبراني في السياق الجيوبوليتكي:** تناولت عدة دراسات العلاقة بين الأمن السيبراني والتنافس الدولي، فقد أكدا (أوسوبا و ويليام، ٢٠١٧، صفحة ١٦). الى ان الفضاء السيبراني أصبح ميدان رئيس للصراع الجيوبوليتكي لتستخدمه القوى الكبرى في تعزيز نفوذها الدولي، كما أوضح (فضلالله، ٢٠٢٥، صفحة ١٣٥٨) الى أن الأمن السيبراني يشكل امتداد للأمن القومي وأن الهجمات السيبرانية كانت سلاح غير تقليدي في التوازنات الاقليمية والدولية.
٤. **الدراسات العراقية:** تشير التقارير ومنها تقرير مركز البيان للدراسات والتخطيط الى أن العراق يعاني من ضعف في البنية التحتية الرقمية وغياب الاستراتيجية الوطنية المتكاملة (شنشول و حمد، ٢٠٢٥، صفحة ٧). ولا تزال الدراسات الأكاديمية العراقية حول الذكاء الاصطناعي كأداة لتعزيز الأمن السيبراني محدودة للغاية، ما يبرز الفجوة البحثية التي يسعى هذا البحث إلى سدها.

المبحث الاول: الاطار النظري للبحث

أولاً: مفهوم الأمن السيبراني:

يشير المفهوم الى مجموعة الاجراءات والسياسات والتقنيات المصممة لحماية الانظمة الرقمية والبيانات والشبكات من جميع التهديدات والاختراقات الالكترونية من سرقة المعلومات والتخريب والبرمجيات الخبيثة. وقد عرف الاتحاد الدولي للاتصالات (مجموعة الادوات والسياسات والمفاهيم والضمانات والمنهجيات ادارة المخاطر وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وظروف المستخدمين) (Al-Bayati, 2023, p. 63). ويمكن تصنيف الأمن السيبراني إلى ثلاثة مستويات رئيسية:

١. **الأمن السيبراني الوطني:** أصبح وثيق الصلة بالأمن الوطني والقومي لأية دولة وتزداد الخطورة كلما زاد الاعتماد على تقنيات المعلومات وارتباطها بالفضاء السيبراني، كونٌ الهجمات السيبرانية يمكن ان تقوضّ الأمن الوطني

(الشمري، ٢٠٢١، صفحة ١٧٠)، وهذا المستوى يتطلب وضع سياسات واستراتيجيات واضحة وتطوير الانظمة للمراقبة وتأهيل الكوادر المتخصصة والقادرة على التعامل مع التهديدات المتزايدة.

٢. **الأمن السيبراني الإقليمي:** يتضمن التعاون مع الدول المجاورة والمنظمات الاقليمية لمواجهة الهجمات العابرة للحدود، بالإضافة الى مشاركة المعلومات حول التهديدات المشتركة، وهذا المستوى يساهم في بناء منظومة أمن جماعية تقلل المخاطر وتحدد من أنتشار الهجمات.

٣. **الأمن السيبراني الدولي:** يرتبط بالتعاون مع المنظمات الدولية والدول المختلفة لوضع المعايير والقواعد المشتركة للأمن الرقمي، بما في ذلك وضع البروتوكولات الدولية للوقاية من الهجمات وبالإضافة الى تبادل الخبرات وتطوير القدرات الدفاعية المشتركة. ولا يقتصر تأثير الفضاء السيبراني على الأمن على داخل الدول، بل يؤثر على البيئة الدولية بطريقة واسعة لتغيير هيكل ومحتوى الأمن الدولي وإنشاء نماذج جديدة لطبيعة العلاقات الدولية وأمن الدول (المنصوري، ٢٠٢٥، صفحة ٥٦٨).

يمثل الأمن السيبراني أداة حيوية لتحقيق الاستقرار السياسي، الاقتصادي، والعسكري للدول، خاصة في بيئات تتسم بالتوترات الجيوبوليتيكية والصراعات الرقمية المتزايدة.

ثانياً: مفهوم الذكاء الاصطناعي ودوره الجيوسياسي:

الذكاء الاصطناعي هو تقنية تمكنّ الحواسيب والآلات من محاكاة الذكاء البشري وقدرات حل المشكلات، سوآء بمفرده أو مع تقنيات أخرى مثل (أجهزة الاستشعار وتحديد المواقع الجغرافية والروبورتات) (Rios-Campos, 2024, p. 6). وأصبح الذكاء الاصطناعي إحدى أهم أدوات القوة الجيوسياسية في النظام الدولي الحديث، إذ باتت الدول الكبرى تتنافس على امتلاك التقنيات المتقدمة وتطبيقاتها، لما تمنحه من تفوّق عسكري وأمني واقتصادي. ومن العناصر الأساسية في تطوير الأمن السيبراني، نظراً لقدراته في معالجة كميات كبيرة وضخمة من البيانات بسرعة وكفاءة، واكتشاف الانماط غير العادية التي قد تشير الى وجود تهديدات سيبرانية محتملة. ويقدم كذلك تهديدات خطيرة مثل تطوير البرامج الخبيثة (Thompson, 2024, p. 33) ويستخدم الذكاء الاصطناعي في الأمن السيبراني على مستويين رئيسيين:

١. **الدفاع السيبراني:** يعتمد الذكاء الاصطناعي على خوارزميات التعلم الآلي والتعلم العميق لتحليل البيانات الضخمة، والتنبؤ بالهجمات المحتملة قبل وقوعها، والكشف المبكر علن الانشطة المشبوهة، كما يتيح تطوير الانظمة الدفاعية الذكية والقادرة على الاستجابة التلقائية للهجمات ومن خلال تقليل الضرر على البنية التحتية الحيوية بما في ذلك شبكات الاتصالات والكهرباء والمصارف (أحلام، ٢٠٢٤، صفحة ١٠٣٥)، هذا الاستخدام يقلل الاعتماد على العنصر البشري ويزيد من سرعة وكفاءة الاستجابة، ويعزز القدرة الدفاعية للدولة بشكل استراتيجي.

٢. **الهجوم السيبراني:** على الجانب الآخر يمكن استغلال الذكاء الاصطناعي في تنفيذ هجمات سيبرانية معقدة ومؤتمتة، أذ تستطيع الأنظمة الذكية من استهداف نقاط الضعف للشبكات والبرمجيات وبدقة عالية، وتنفيذ اختراقات متزامنة وعلى نطاق واسع، هذا يضاعف من تعقيد المشهد الأمني ويجعل المنافسة بين الدول في المجال الرقمي أكثر حدة (علي، ٢٠٢٥، صفحة ٢٩).

يمكن القول إن الذكاء الاصطناعي أصبح محور الصراعات بين القوى الكبرى وسلاحاً استراتيجياً لا يقل عن الأسلحة التقليدية. وأداة لتعزيز النفوذ السياسي والعسكري والاقتصادي. ووسيلة لإعادة تشكيل الأمن الدولي وخاصة الأمن السيبراني. وعامل ضغط وتبعية تقنية للدول الضعيفة رقمياً مثل العراق. وعليه، فإن فهم الذكاء الاصطناعي لم يعد مقتصراً على الجانب التقني فحسب، بل أصبح ضرورة لفهم العلاقات الدولية المعاصرة وتحولات القوة العالمية.

ثالثاً: الجيوبوليتك الرقمي:

أن الفضاء السيبراني أصبح ساحة جديدة للتنافس الجيوبوليتكي بين الدول، أذ لم تعد القوة العسكرية التقليدية وحدها تحدد النفوذ والسيطرة، بل أضيف اليها البعد الرقمي، والذي يشمل القدرة على جمع المعلومات ومراقبة الخصوم والتحكم في البنية

التحتية الرقمية الحيوية، وهو يعكس العلاقة بين القوة التكنولوجية والأمن الوطني وتسعى الدول المختلفة الى تعزيز نفوذها الرقمي عبر:

١. تطوير القدرات الهجومية والدفاعية السيبرانية المتقدمة باستخدام تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة.
٢. التحكم في الفضاء الرقمي الدولي عن طريق المعايير والبروتوكولات المشتركة للأمن السيبراني بما يتيح ممارسة النفوذ على الدول الاخرى.
٣. توظيف الأمن كأداة للضغط السياسي والاقتصادي عبر الهجمات الرقمية.

يأتي العراق في قلب هذه التحولات بوصفه دولة تمتلك موقعاً استراتيجياً حيوياً، يربط بين الخليج العربي وشرق المتوسط، وحلقة وصل بين القوى الإقليمية الكبرى(إيران وتركيا والسعودية). إلا أنّ هذا الموقع الجغرافي التقليدي تزايدت أهميته اليوم بارتباطه بموقع العراق في الجيوبوليتك الرقمي، إذ يشكّل ممراً لشبكات الألياف الضوئية الدولية، ومجالاً تتنافس فيه القوى العالمية لتعزيز نفوذها عبر مشاريع البنية التحتية الرقمية، والأمن السيبراني، وتطوير أنظمة الحوكمة التكنولوجية. ورغم تقدّم العراق في بعض جوانب التحول الرقمي، مثل تطوير استراتيجيات الأمن السيبراني وتعزيز البنى الاتصالية، إلا أنّه ما يزال يواجه تحديات بنيوية تشمل تهديدات الهجمات السيبرانية.يمكن النظر إلى العراق على أنه دولة متأثرة بالجيوبوليتيك الرقمي، حيث تتداخل فيها المخاطر والهجمات العابرة للحدود، ويتطلب ذلك تبني استراتيجية وطنية شاملة للأمن السيبراني تعتمد على الذكاء الاصطناعي لتعزيز الدفاعات، ومواجهة التهديدات المحتملة، والهدف من هذه الاستراتيجية هو توفير خارطة متماسكة ومبادرات وآليات لتنفيذ ولتحقيق الرؤية الوطنية بشأن الأمن السيبراني (الوطني، ٢٠٢٤، صفحة ٢).

المبحث الثاني: العراق بين الجيوبوليتك الرقمي والذكاء الاصطناعي

يعيش العالم اليوم تحوّلاً جذرياً تقوده الثورة الرقمية وتقنيات الذكاء الاصطناعي، حيث أصبحت البيانات والمعلومات والقدرة على توظيف الخوارزميات أدوات رئيسية لإعادة تشكيل موازين القوى الجيوسياسية. وفي هذا السياق برز مفهوم الجيوبوليتك الرقمي (Digital Geopolitics) بوصفه الإطار التحليلي الذي يربط بين التكنولوجيا والبنية السياسية والأمنية للدول، ويُعيد تحديد قدراتها وموقعها الإقليمي والدولي. فالدول لم تعد تتنافس فقط على الممرات البحرية والموارد الطبيعية، بل باتت تتصارع على البنى التحتية الرقمية، ومراكز البيانات، والتفوّق في الذكاء الاصطناعي، والتحكم بحركة المعلومات عبر الفضاء السيبراني.

اولاً: موقع العراق الجيوبوليتكي:

أن موقع العراق الحساس في منطقة الشرق الاوسط، والتي تتقاطع فيها مصالح العديد من الدول مما يجعله في منطقة حرجة للتنافس على الفضاء السيبراني، والتي تسعى فيها الدول لتأمين مصالحها الاستراتيجية في المنطقة. يُمكّن الموقع الجغرافي للعراق من أن يكون مركزاً رئيسياً لحركة الاتصالات والبيانات. ويعود موقعه القريب من دول الخليج وبلاد الشام وقربه من أوروبا بفوائد جمة على العراق، ومنها تعزيز التعاون الدولي (Iraq, 2025, p. 38). ويمكن تناول ذلك من خلال ثلاثة محاور مترابطة:

١. **الجيوبوليتك والفضاء السيبراني:** الجيوبوليتك التقليدي ارتبط تاريخياً بالصراع على المكان الجغرافي والموارد الطبيعية، الا أن القرن الحادي والعشرين، شهد بروز الفضاء السيبراني كمجال استراتيجي جديد للصراع، ويرى منظرو العلاقات الدولية أن السيطرة على الفضاء السيبراني باتت توازي السيطرة على المجال البري أو البحري أو الجوي، نظراً لتأثيرها المباشر على الأمن القومي والسيادة الرقمية (قرطاس، ٢٠٢٣، صفحة ٢٥). ومن هذا المنطلق، أصبح الفضاء السيبراني جزءاً من معادلات القوة الجيوبوليتيكية، تستخدمه الدول الكبرى لتعزيز نفوذها أو لإضعاف خصومها عبر الهجمات الرقمية والتجسس الإلكتروني وحروب المعلومات.

٢. **الأمن السيبراني كأداة للردع والحماية:** الأمن السيبراني لا يُعد مجرد حماية تقنية للأنظمة، بل هو عنصر مركزي في استراتيجيات الأمن القومي، وتشير نظرية الأمن المركّب **(Complex Security)** إلى أن التهديدات لم تعد حكراً على الجيوش التقليدية، بل تشمل التهديدات غير المادية مثل الهجمات الرقمية (سالم، ٢٠٢٢، صفحة ٧٢).

٣. **الذكاء الاصطناعي كعامل مساعد للأمن السيبراني:** يعد الذكاء الاصطناعي بمثابة ثورة تقنية تعزز إمكانيات الأمن السيبراني، إذ يوفر قدرات متقدمة للكشف المبكر عن التهديدات والتنبؤ بها والتعامل معها بشكل شبه ذاتي، والتي يعد فيها دعم البنية التحتية أمراً بالغ الاهمية ومن خلال دمج التقنيات المتقدمة والوظائف الحكومية لتوسيع نطاقها في القطاع العام (UNESCO, 2024, p. 42).وأصبح الأمن السيبراني مفهوماً متنامياً في قطاع التكنولوجيا، وقد أدرجت العديد من الشركات تكنولوجيا المعلومات في أعمالها (Sudan, 2025, p. 1883) وقد دفع هذا العامل الشركات والمؤسسات إلى المطالبة بمزيد من التدابير الأمنية، وقد أدت جهود حماية البيانات والمعلومات المتاحة إلى نمو الأمن السيبراني، وقد أدى إلى تحفيز التعلم الآلي بشكل كبير في التقنيات الحديثة الداعمة للأمن السيبراني (Rios-Campos, 2024, p. 8).

ثانياً: مؤشر جاهزية الدول للذكاء الاصطناعي لعام ٢٠٢٤:

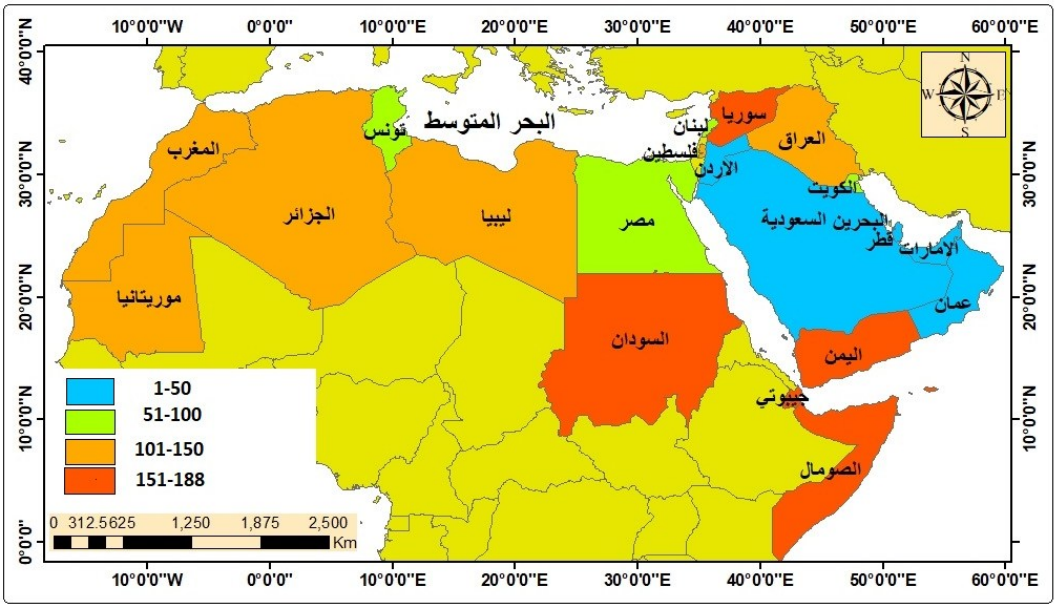
يصنف مؤشر جاهزية الذكاء الاصطناعي (Government Al Readiness IndeX 2024) الذي أصدرته (Oxford Insights) (١٨٨ دولة) حسب مدى استعداد حكوماتها لاستخدام الذكاء الاصطناعي في الخدمات العامة. ينشر المؤشر سنويا ويصنف الدول بناءً على (٣٩) مؤشر عبر ثلاث ركائز الحكومة (Government) والتكنولوجيا (Technology) والبنية التحتية (Data and Infrastructure). يعكس مؤشر جاهزية الذكاء الاصطناعي لعام ٢٠٢٤ تفاوتاً واضحاً في مستويات القدرة المؤسسية والتكنولوجية والبشرية بين الدول العربية، بما يؤثر مباشرة في إمكاناتها لتبني حلول الذكاء الاصطناعي وتطبيقاتها ضمن القطاعات الاقتصادية والأمنية والخدمية. وتظهر البيانات أن دول الخليج العربي تتصدر المشهد الإقليمي نظراً لاستثماراتها الكبيرة في البنى التحتية الرقمية، ووضوح استراتيجياتها الوطنية للتحول الرقمي. وكما موضح بجدول (١). تأتي الإمارات العربية المتحدة في المرتبة الأولى عربياً (١٣ عالمياً) بدرجة (٧٥,٦٦)، وهو ما يعكس نضجاً مؤسسياً كبيراً، وتوفر بيئة تشريعية محفزة، ومشاريع واسعة في الذكاء الاصطناعي على المستوى الحكومي والخاص. وتليها السعودية في المرتبة الثانية عربياً (٢٢ عالمياً) بدرجة (٧٢,٣٦)، مدفوعة باستراتيجية (رؤية ٢٠٣٠) التي تعطي أولوية لتنمية القدرات الحاسوبية والابتكار التقني. أما قطر، عُمان، والأردن فقد جاءت في المراتب (٣-٥) عربياً مع مستويات مرتفعة نسبياً من الجاهزية، نتيجة لاستثماراتها في المؤسسات العلمية وشبكات الاتصالات المتقدمة.

جدول (١) ترتيب العراق والدول العربية حسب مؤشر جاهزية الذكاء الاصطناعي ٢٠٢٤

الدولة العربية	ترتيب عربيا	ترتيب دوليا	جاهزية الذكاء الاصطناعي	الدول العربية	ترتيب عربيا	ترتيب دوليا	جاهزية الذكاء الاصطناعي
الإمارات	1	13	75.66	موريتانيا	12	105	41.40
السعودية	2	22	72.36	العراق	13	107	40.91
قطر	3	32	68.22	الجزائر	14	115	39.06
عُمان	4	45	62.91	فلسطين	15	125	37.53
الأردن	5	49	61.57	جيبوتي	16	138	35.19
مصر	6	65	55.63	ليبيا	17	149	33.25
البحرين	7	68	54.33	جرز القمر	18	170	26.65
الكويت	8	77	51.26	الصومال	19	174	25.32
لبنان	9	82	46.67	السودان	20	176	24.63
تونس	10	92	43.68	سوريا	21	186	16.95
المغرب	11	101	41.78	اليمن	22	188	14.62

المصدر : https://oxfordinsights.com/ai-readiness- ai-readiness-index

من جهة أخرى، تظهر معظم الدول العربية ذات الدخل المتوسط والمنخفض مستويات ضعيفة أو متدنية من الجاهزية. كما موضح في جدول (١). إذ حلّت موريتانيا، الجزائر، فلسطين، جيبوتي، ليبيا، جزر القمر، الصومال، السودان، سوريا، واليمن في مراتب متأخرة عربياً وعالمياً، نتيجة محدودية البنى التحتية الرقمية، وتراجع مؤشرات الاستقرار السياسي، وغياب الاستراتيجيات الفعالة في مجال الذكاء الاصطناعي. أما العراق فقد جاء في المرتبة (١٣ عربياً و١٠٧ عالمياً) بدرجة (٤٠,٩١)، وهو ما يعكس فجوة تقنية واضحة مقارنة بدول الخليج، والخريطة (١) توضح هذا التباين، وتشير هذه المرتبة إلى عدد من التحديات أبرزها ضعف البنية التحتية الرقمية، محدودية الاستثمار في البحث والتطوير، وتأخر صياغة سياسات حكومية متخصصة بالذكاء الاصطناعي، رغم وجود قدرات بشرية مؤهلة يمكن أن تدعم هذا القطاع في حال توفرت بيئة مناسبة.



خريطة(١) تصنيف الدول العربية وفق مؤشر جاهزية الذكاء الاصطناعي لعام ٢٠٢٤

وبشكل عام، تُظهر النتائج وجود انقسام عربي واضح بين مجموعة دول رائدة تمتلك استراتيجيات واضحة (الإمارات، السعودية، قطر) وأخرى تواجه قيوداً تنموية وأمنية تحول دون تحقيق تقدم ملموس. وهو ما يشير إلى ضرورة تعزيز التعاون الإقليمي وبناء شراكات تكنولوجية، فضلاً عن وضع سياسات وطنية فاعلة لرفع مستوى الجاهزية التقنية في الدول الأقل تقدماً. بالنسبة للعراق، فإن تطوير منظومة الذكاء الاصطناعي بات ضرورة استراتيجية لدعم الأمن السيبراني، وتحسين الخدمات الحكومية، وتعزيز القدرة على مواجهة التهديدات الرقمية المتصاعدة . يُشكّل سباق التسلح بالذكاء الاصطناعي نوعاً جديداً من المنافسة الجيوسياسية، حيث لا تقل أهمية التفوق التكنولوجي عن القوة العسكرية التقليدية.

المبحث الثالث: التحليل الجيوبوليتكي للأمن السيبراني العراقي

شهدت البيئة الأمنية في العراق خلال العقدين الأخيرين تحولات عميقة ارتبطت بتطورات النظام الدولي، وانتشار التقنيات الرقمية، وتنامي دور الفواعل غير التقليدية في الصراع. ومع توسّع الاعتماد على الأنظمة الشبكية في المؤسسات الحكومية والاقتصادية والعسكرية، أصبح الفضاء السيبراني أحد أكثر المجالات حساسية وتأثيراً على الأمن الوطني. ولم يعد الأمن السيبراني مسألة تقنية فحسب، بل تحوّل إلى قضية جيوبوليتكية بامتياز، تُعيد صياغة توازنات القوة داخل الدولة ومع محيطها الإقليمي والدولي.

اولاً: مؤشر الأمن السيبراني العالمي(Global Cybersecurity Index):

تم أنشاء هذا المؤشر من خلال الاتحاد الدولي للاتصالات أحدى وكالات الامم المتحدة المتخصصة والمسؤولة عن الامور المتعلقة بتكنولوجيا الاتصالات والمعلومات (قرطاس، ٢٠٢٣، صفحة ١٤) وهو مؤشر مركب وذو فاعلية لقياس لقياس مدى التزام الدول بالأمن السيبراني هادفاً لحماية المعلومات والممتلكات من السرقة، ويجمع (٢٥) معياراً في مقياس واحد لرصد التزام (١٩٣ دولة) عضواً في الاتحاد الدولي للاتصالات ومن خلال خمس ركائز:

١. **الركائز القانونية:** تشمل الاطر القانونية ووضع تشريعات تحدد ما يشكل الانشطة غير المشروعة في الفضاء السيبراني بالإضافة الى تعريف الادوات الاجرائية اللازمة لتحقيق والمقاضاة وانفاذ التشريعات وانشاء خطوط اساسية للأمن السيبراني ووضع اجراءات لضمان الاتساق مع الالتزامات الدولية (للاتصالات، ٢٠٢١، صفحة ٢).
٢. **التدابير التقنية:** من الضروري على الصعيد الوطني وضع أليات وهياكل مؤسسية فعالة للتعامل مع التهديدات والحوادث السيبرانية على نحو موثوق، وتشجيع اتخاذ اجراءات سريعة ومنهجية وتمكين الدول من التعلم من الخبرات وبناء القدرة على الصمود في مجال الامن السيبراني (للاتصالات، ٢٠٢١، صفحة ٥).
٣. **التدابير التنظيمية:** تدرس التدابير التنظيمية آليات الادارة والتنسيق داخل الدول المعنية بالأمن السيبراني، وتشمل ضمان الاستدامة على اعلى مستوى من السلطة التنفيذية واسناد الادوار والمسؤوليات ذات الصلة لمختلف الكيانات الوطنية وجعلها مسؤولة عن وضع الامن السيبراني الوطني.
٤. **تدابير تنمية القدرات:** أن مزايا التكنولوجيا الرقمية تجلب فوائد اقتصادية واجتماعية كبيرة ويمكن للمخاطر السيبرانية ان تعادل فوائد الرقمنة، وان تأمين المجال السيبراني من خلال أنشطة تنمية القدرات أمر أساسي اذ يساهم في الحد من قضايا مثل الفجوة الرقمية والمخاطر السيبرانية. ومن المتوقع أن تتزايد هذه المخاوف مع تنامي الوعي العملي بأن استخدام التقنيات الحديثة لا ينطوي فقط على تهديدات ومخاطر خطيرة (مثل التضليل، وانتهاك الخصوصية الشخصية، والهجمات الإلكترونية، وما إلى ذلك) والتي يجب تجنبها (García-Saúco, 2021, p. 78).
٥. **التدابير التعاونية:** يظل التعاون أدارة أساسية لمواجهة تحديات الامن السيبراني، لايزال الامن السيبراني قضية عابرة للحدود الوطنية، وتشمل الاهداف النموذجية للتعاون في مجال الامن السيبراني تنسيق تدابير الحد الادنى من الامن وتبادل المعلومات والممارسات الجيدة وتدوين قواعد السلوك (للاتصالات، ٢٠٢١، صفحة ١٨).

يؤثر اعتماد تقنيات الذكاء الاصطناعي في ممارسات الأمن السيبراني على الديناميكيات الجيوسياسية والتنافسات والتحالفات بين الدول (Vance, 2023, p. 98). يمكن لدول للشرق الأوسط تعزيز جهودها الدبلوماسية لمواجهة التهديدات السيبرانية من خلال تعزيز منتدى حوكمة الإنترنت (IGF). وقد استند إنشاء هذا المنتدى إلى الفقرة (٧٢) من أجندة تونس، وهي الوثيقة الختامية للمرحلة الثانية من القمة العالمية لمجتمع المعلومات التي عُقدت في الفترة من ١٦_١٨ تشرين الثاني ٢٠٠٥ (Aboul-Enein, 2017, p. 28).يستخدم المؤشر البيانات التي يتم جمعها من الدول ووضع الاسئلة لتقييم الالتزام ومن خلال التشاور مع الخبراء المتخصصين يتم ترجيح الاسئلة من أجل الحصول على مجموع نقاط المؤشر لأي دولة، وبالنسبة للدول التي تسعى الى تحقيق اتصال سيبراني آمن وهادف يقدم المؤشر صورة واضحة عن وضعها وخارطة طريق للأنشطة اللازمة لتحقيق التقدم ومع ذلك يجب على الدول أن تكون مستعدة للانخراط في العمليات الجارية لتعزيز الأمن السيبراني والعمل على تحسين جودة أنشطتها (ITU, 2024, p. 13). وبالنسبة للعراق فانه يقع ضمن:وفق تقرير Global Cybersecurity Index 2024 (ITU)، أن العراق في مرتبة منخفضة عالمياً بسبب غياب استراتيجية وطنية شاملة للأمن السيبراني وضعف وهشاشة في البنية التحتية الرقمية ونقص الكوادر المدربة والمتخصصة، فالعراق يصنف ضمن الدول في المستوى الرابع ذو مستوى الاستعداد المحدود (Limited Commitment)على مؤشر الامن السيبراني العالمي ومقارنة مع دول اخرى التي وصلت الى المستوى الاول ومنها الامارات العربية والسعودية. ويلاحظ في جدول (٢) ان العراق حصل المرتبة ١٣ عربياً في المؤشر عام ٢٠٢٤. اذ تقدم العراق عن موريتانيا والصومال وجزر القمر وجيبوتي واليمن. وسبب التراجع أن العراق لم يقدم (اجابات عن الاستبيان الذي جمعه فريق المؤشر والذي تضمن بعض المعلومات والبيانات، وهو الامر الذي يطرح عدة اسئلة حول سبب هذا التجاهل للجهات المسؤولة عن هذا ملف الامن السيبراني في العراق) وتشير

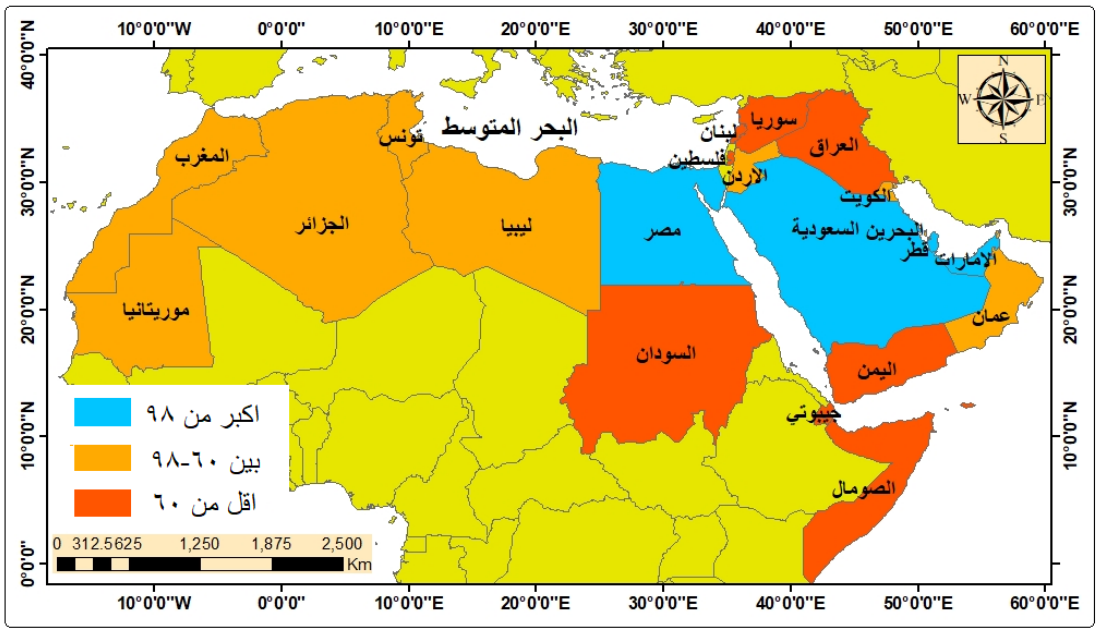
بعض الدراسات ان هذا التراجع في الملف الامني السيبراني انما يعود الى عدم وجود مؤسسة متخصصة بالأمن السيبراني في العراق (وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها).

جدول (٢) ترتيب العراق والدول العربية بمؤشر الامن السيبراني العالمي ٢٠٢٤

الدولة العربية	ترتيب عربيا	مؤشر الامن السيبراني	الدول العربية	ترتيب عربيا	مؤشر الامن السيبراني
الإمارات	1	100	الكويت	12	60,58
السعودية	2	100	العراق	13	53,07
قطر	3	100	سوريا	14	51,39
مصر	4	100	السودان	15	48,17
الأردن	5	98,6	موريتانيا	16	39,33
البحرين	6	97,94	جرز القمر	17	39,15
المغرب	7	97,5	فلسطين	18	37,72
عُمان	8	97,01	الصومال	19	37,38
تونس	9	82	لبنان	20	32,37
ليبيا	10	68,09	جيبوتي	21	31,49
الجزائر	11	65,87	اليمن	22	7,19
https://de.wikipedia.org/wiki/Global_Cybersecurity_Index_2024					

يمثل جدول(٢) ترتيب الدول العربية في مؤشر الأمن السيبراني العالمي لعام ٢٠٢٤ انعكاساً لمستويات النضج الرقمي والقدرة على حماية الفضاء السيبراني في المنطقة العربية. ويكشف تحليل البيانات وجود تفاوتات واضحة بين الدول، تعود في معظمها إلى اختلاف الإمكانات الاقتصادية والبنى التحتية الرقمية والتشريعات السيبرانية ومدى تبني استراتيجيات الأمن المعلوماتي. وكما موضح بخريطة (٢) تضم القائمة (٢٢) دولة عربية، يمكن تصنيفها ضمن ثلاث مجموعات رئيسية من حيث أداء الأمن السيبراني:

١. **مجموعة الأداء المرتفع جداً (درجات تقارب ١٠٠ نقطة):** تشمل الإمارات والسعودية وقطر ومصر، وقد حصلت هذه الدول على مراتب متقدمة عربياً ودرجات كاملة أو شبه كاملة. ويعكس هذا التفوق توفر بنية رقمية متطورة، واستراتيجيات وطنية واضحة للأمن السيبراني، واستثمارات مستمرة في تطوير القدرات البشرية والتقنية.
٢. **مجموعة الأداء المتوسط (بين ٦٠–٩٨ نقطة):** وتشمل الأردن، البحرين، المغرب، عُمان، تونس، ليبيا، الجزائر والكويت. وتظهر هذه الدول مستوى جيداً من الجاهزية، إلا أنها لا تزال تواجه بعض التحديات المتعلقة بتفعيل الأطر التشريعية، وتطوير مراكز الاستجابة للحوادث، وتعزيز الوعي المجتمعي بالأمن السيبراني.
٣. **مجموعة الأداء المنخفض (أقل من ٦٠ نقطة):** تضم العراق ومعظم الدول ذات البنية الرقمية الهشة مثل سوريا، السودان، فلسطين، الصومال، جيبوتي، ولبنان واليمن. وتُظهر نتائج هذه المجموعة ضعفاً واضحاً في القدرة على حماية الأصول الرقمية والاستجابة للهجمات الإلكترونية، غالباً بسبب محدودية الموارد الاقتصادية، أو عدم الاستقرار السياسي، أو غياب استراتيجيات سيبرانية متكاملة.



خريطة (٢) تصنيف الدول العربية وفق مؤشر الأمن السيبراني العالمي لعام ٢٠٢٤

احتل العراق المرتبة (١٣) عربياً بدرجة (53.07)، وهي درجة تضعه ضمن مجموعة الأداء المنخفض في المنطقة العربية ويعكس هذا الموقع:

١. وجود فجوة كبيرة بين العراق والدول المتقدمة في المؤشر إذ يصل الفارق بين العراق ودول الخليج المتصدرة (مثل الإمارات والسعودية وقطر) إلى أكثر من (٤٥) نقطة، مما يشير إلى ضعف واضح في مستويات الحماية الرقمية وغياب بنى تحتية سيبرانية ناضجة.

٢. تقارب العراق مع دول تعاني ظروفاً سياسية أو اقتصادية صعبة (مثل سوريا والسودان والصومال)، وهو ما يسلّط الضوء على تحديات مؤسسية وإدارية تتعلق بضعف التشريعات السيبرانية، ونقص الكوادر المتخصصة، وبطء تنفيذ الاستراتيجيات الوطنية في مجال الأمن السيبراني.

٣. أن ترتيب العراق في الثلث الأخير من القائمة يشير إلى أن الجهود الوطنية في مجال الأمن السيبراني لا تزال دون المستوى المطلوب مقارنة بمعايير المنطقة.

يتضح من تحليل الجدول لمؤشر الأمن السيبراني العربي لعام (٢٠٢٤) أن المنطقة العربية تشهد تفاوتاً كبيراً في مستوى الأمان الرقمي، وأن العراق يقع في النصف الأدنى من الترتيب، مما يعكس الحاجة إلى جهود أكبر لتعزيز قدراته السيبرانية. ويشير التحليل إلى ضرورة تبني سياسات وطنية أكثر فاعلية في مجال الأمن السيبراني، وإطلاق برامج تدريبية متخصصة، وتطوير بنى تحتية رقمية حديثة، فضلاً عن تعزيز التعاون الإقليمي لمواجهة التحديات المشتركة (خريسان، ٢٠٢٥، صفحة ٨).

ثانياً: موقع العراق الجيوبوليتكي في الفضاء السيبراني:

لم تعد الحدود السياسية وحدها من تحدد القوة الجيوبوليتكية للدول بل برزت الفضاءات غير المادية مثل الفضاء السيبراني كأداة نفوذ وصراع بين القوى الإقليمية والعالمية، فالأمن السيبراني أصبح عنصراً أساسياً من عناصر الأمن القومي لأنه يطال كل مفاصل الدول، رغم موقع العراق الجغرافي الحيوي بين ايران وتركيا والسعودية، الا أنه يحتل مرتبة متأخرة جداً وهذا يعكس أن الفراغ الرقمي العراقي أصبح جزءاً من الفراغ الجيوبوليتكي الأوسع، الذي يجعله ساحة تأثير رقمية للقوى الاقليمية والدولية.إن ضعف العراق في مؤشر الأمن السيبراني العالمي لا يمثل مجرد تأخر تقني، بل هو خلل جيوبوليتكي في بيئة إقليمية متنافسة تستخدم الفضاء الرقمي كأداة نفوذ واستقطاب. ولذا، فإن تعزيز الأمن السيبراني في العراق ليس خياراً تقنياً فحسب، بل ضرورة استراتيجية لحماية السيادة الوطنية واستعادة التوازن الإقليمي (الانمائي، ٢٠٢٣، صفحة ١٥). يواجه

العراق تحديات كبيرة في مجال الأمن السيبراني تتعلق بالقدرات التقنية والبشرية والسياساتية، مما يجعله عرضه للتهديدات الرقمية المتزايدة على المستويات الوطنية والاقليمية والدولية ومن أبرز التحديات:

١. **ضعف البنية التحتية الرقمية:** تعتمد القطاعات الحيوية في العراق مثل الاتصالات والكهرباء والطاقة على أنظمة قديمة أو غير مجهزة بما يكفي لمواجهة الهجمات الالكترونية الحديثة، هذا الضعف يجعل من هذه القطاعات أهدافاً سهلة للهجمات التخريبية، ويؤثر سلباً على استقرار الخدمات الحيوية، ورغم الانفتاح على مجال تكنولوجيا المعلومات والاتصالات بعد عام ٢٠٠٣ أصبح العراق ساحة مفتوحة يسهل اختراقها (صليبي، ٢٠٢٤، صفحة ٥١٦)، وكذلك سهولة التجسس على المعلومات الحساسة في المؤسسات المختلفة وهذا يعود الى عدم وجود بنية تحتية آمنة لجميع أنظمة المعلومات المختلفة ومنها الشخصية والمصرفية، وهذا ترك المجال لبعض التنظيمات الارهابية والتخريبية والاجرامية التي انتشرت بعد سقوط النظام السابق عام ٢٠٠٣ (Al-Bayati, 2023, p. 78).

٢. **نقص الكوادر المدربة:** تعاني المؤسسات العراقية المختلفة من محدودية الكوادر المؤهلة والمتخصصة في مجال الأمن السيبراني والذكاء الاصطناعي، وعدم القدرة على تطوير نظم الحماية المتقدمة بالإضافة الى محدودية مواجهة الهجمات والاستجابة السريعة والفعالة لها (علوان، ٢٠٢٥، صفحة ٤١).

٣. **غياب السياسات الوطنية المتكاملة:** يفتقر العراق الى استراتيجية وطنية شاملة للأمن السيبراني تربط بين القطاعات الحكومية المختلفة والخاصة، وهذا الغياب يعيق التنسيق بين الجهات المختلفة ويجعل الجهود المبذولة غير متكاملة، مما يزيد من هشاشة البنية الرقمية للدولة أمام التهديدات السيبرانية العابرة للحدود.

٤. **تعرض للهجمات الرقمية:** شهد العراق خلال السنوات الماضية الى العديد من محاولات الاختراق والاستهداف للأنظمة الحكومية والمصرفية، هذه الهجمات تكشف عن نقاط ضعف كبيرة في الأمن الرقمي وتعكس الحاجة الماسة الى تعزيز القدرات الدفاعية باستخدام التقنيات الحديثة مثل الذكاء الاصطناعي لتقليل المخاطر وحماية البنية التحتية الرقمية الحيوية، ومن ابرز الامثلة على هذه الهجمات، الهجوم السيبراني الكبير الذي استهدف النظام المصرفي في عام (٢٠٢٠) والذي أثر على الآلاف المستخدمين وأدى الى تسرب بيانات حساسة (شنشول و حمد، ٢٠٢٥، صفحة ٧). أن هذه التحديات تجعل العراق أرضاً خصبة للهجمات السيبرانية، خصوصاً في ظل التنافس الاقليمي والدولي في مجال الفضاء الرقمي .

المبحث الرابع: المنافسة الجيوبوليتكية الرقمية على العراق

إنّ المنافسة الجيوبوليتكية الرقمية على العراق ليست مجرد تنافس اقتصادي أو تقني، بل هي صراع على النفوذ السياسي والأمني، ومحاولة للسيطرة على مسارات البيانات، وبناء مراكز ثقل رقمية قادرة على التأثير في القرار العراقي. فالعراق يمثل جسراً بين الشرق والغرب، ويرتبط بشبكات لوجستية واتصالية مهمة، ويملك بنى تحتية للطاقة والنقل تعد هدفاً محورياً في استراتيجيات القوى الكبرى. لذلك سعت هذه القوى (الولايات المتحدة، الصين، روسيا، إيران) إلى توسيع حضورها الرقمي داخل العراق عبر عقود الاتصالات، ومشاريع التحول الرقمي، وتقديم تقنيات المراقبة، وتدريب الكوادر السيبرانية، وبناء شراكات مع المؤسسات الحكومية.

أولاً: التنافس الدولي والاقليمي: تبرز عدة أبعاد للدول المختلفة ومنها:

١. **الولايات المتحدة الامريكية:** تسعى لتعزيز نفوذها الرقمي في العراق عبر برامج دعم للأمن السيبراني وتدريب الكوادر الوطنية وتقديم الاستشارات التقنية لتطوير البنية الرقمية، ومع ذلك يمثل النفوذ الامريكي عامل تهديد اذ يمكن أن يؤثر هذا الدعم على القيود الرقمية للأمن الوطني العراقي. ووضعت الولايات المتحدة استراتيجية الخاصة بمجال الفضاء الالكتروني والسياسية الرقمية لتعزيز الدبلوماسية الرقمية والتضامن الرقمي والحفاظ على التفوق التقني وقيادة العالم في مجال التكنولوجيا (الدباغ، ٢٠٢٥، صفحة ٢٠٨).

٢. **روسيا والصين:** تعمل كلتا الدولتين على تعزيز علاقاتهما التكنلوجية مع العراق، بما في ذلك توفير تقنيات الذكاء الاصطناعي وأنظمة الأمن الرقمي، بهدف زيادة حضورهما في المنطقة وتأثيرهما على منظومة الفضاء الرقمي الاقليمي

وقد يتخذ التعاون المشترك صيغة اقامة مشروعات مشتركة (محسن، ٢٠٢٤، صفحة ٢٧٠)، هذا التعاون التقني يمكن ان يوفر فرصاً لتعزيز القدرات التقنية العراقية .

٣. **الاتحاد الاوربي:** لقد تبنت العديد من الدول وخصوصاً الغربية منها الرؤية الامريكية للأمن السيبراني القائمة على الفضاء الالكتروني المفتوح والمشترك من اجل المنفعة العامة والمتبادلة للجميع، وهي في الوقت نفسه تتهم منافسيها على رأسهم روسيا والصين وحلفائهما بالاستفادة من الانترنيت من جهة والقيام بتقييد ومراقبة وصول شعوبهم من جهة اخرى (محسن، ٢٠٢٤، صفحة ٢٨٢).

٤. **إيران:** تعد لاعب اقليمي فاعل في الفضاء السيبراني وتستخدم عادة الهجمات الرقمية كأداة للضغط السياسي أو العسكري على الدول الاقليمية والدولية المختلفة، وقد شهدت السنوات الأخيرة استهداف بعض القطاعات العراقية بهجمات إلكترونية مرتبطة بإيران، ما يعكس التداخل بين الصراع الإقليمي والأمن السيبراني العراقي (Al-Kaabi & Hassan, 2022). أن الادوات السيبرانية هي أحدى الادوات المهمة لإيران لجمع المعلومات أن برنامج الدفاع السيبراني الايراني له هدفين الاول يتمثل بمنع الهجمات التي تستهدف البنى التحتية لا سيما النووية والثاني مراقبة تدفق المعلومات التي تمثل خطر على النظام (الناصري و مرعي، ٢٠٢٢، صفحة ٣٦٧).

٥. **إسرائيل:** تشكل لاعب رئيسي وكبير في الفضاء السيبراني الاقليمي، وتمتلك خبرات متقدمة في الهجمات الرقمية والتجسس السيبراني، وتستخدم هذه القدرات أحيانا في تأثير المباشر والغير مباشر على العراق. ومن الضروري أن تمتلك الدولة أدوات القوة السيبرانية، بل أن تستخدمها كأدوات داعمة للقوة الناعمة والصلبة (Al-Bayati, 2023, p. 71).

ثانياً: دور الذكاء الاصطناعي في تعزيز الامن السيبراني العراقي:

يشكل الذكاء الاصطناعي أداة استراتيجية لتعزيز القدرات، أذ يمكن أن يعالج نقاط الضعف الموجودة في البنية التحتية الرقمية ويعوض محدودية الكوادر البشرية المتخصصة (UNESCO, 2024, p. 48) ويبرز دوره في عدة محاور رئيسية:

١. **الكشف المبكر عن الهجمات:** تستخدم الأنظمة الذكية تقنيات التعلم الآلي وتحليل البيانات الضخمة لرصد الأنشطة المشبوهة على الشبكات الحكومية والخاصة الحيوية، مما يتيح التنبؤ بالهجمات قبل وقوعها وهذا يقلل من فرص الاختراقات ويعزز قدرة الدولة ومؤسساتها على التصدي للتهديدات الرقمية المتقدمة (Ahmed, 2024, p. 56).

٢. **الاستجابة التلقائية للهجمات:** يمكن تطوير أنظمة دفاعية قادرة على الرد الفوري، مثل منع الوصول غير المصرح به، حجب البرامج الخبيثة، عزل أجزاء الشبكة المتضررة دون تدخل بشري مباشر، وتعد الحكومة الرقمية العالمية ضرورية لتحقيق التوازن بين تعظيم الفوائد المتحققة وتقليل المخاطر والتهديدات المحتملة (Garofali, 2024, p. 109).

٣. **حماية ومراقبة البنية التحتية:** يتيح الذكاء الاصطناعي مراقبة الأنظمة الحيوية في قطاعات النفط، الكهرباء، والاتصالات بشكل مستمر، وتحليل أي تغييرات غير طبيعية في الأداء أو النشاط الرقمي. ومع تزايد الاعتماد على التجارة الالكترونية في العراق أصبحت الشركات الصغيرة والمتوسطة عرضه للهجمات السيبرانية تستهدف نتصات الدفع الرقمي.

٤. **تحسين كفاءة الموارد البشرية:** يساهم في تعويض نقص الخبرات المحلية، حيث يمكن للأنظمة الذكية القيام بعمليات تحليلية معقدة واتخاذ قرارات سريعة في مواجهة التهديدات، ما يسمح للكوادر الوطنية بالتركيز على الاستراتيجيات والتخطيط الأمني بعيد المدى.

٥. **التنبؤ بالتهديدات المستقبلية:** عبر تحليل الأنماط السابقة للهجمات السيبرانية على العراق والمنطقة، يمكن للذكاء الاصطناعي تطوير نماذج للتنبؤ بالتهديدات المستقبلية، ما يعزز من قدرة الدولة على التخطيط المسبق ووضع سياسات وقائية فعالة، ان ما يميز الهجمات السيبرانية عن غيرها من أشكال الصراعات التقليدية هو عنصر المفاجأة الذي يصاحبها (محمود، ٢٠٢٥، صفحة ٣١٦).

تلعب الاستراتيجيات والسياسات الوطنية دوراً حاسماً في تحديد كيفية استفادة الدول من الذكاء الاصطناعي في مجال الأمن السيبراني (Vance, 2023, p. 100) وقد اعتمدت الدول حول العالم مناهج متنوعة في صياغة استراتيجياتها لتسخير

إمكانات تقنيات الذكاء الاصطناعي في سياق الأمن السيبراني. وهنا يبرز الذكاء الاصطناعي كفرصة جديدة بفضل قدرته المتنامية على تحليل كم هائل من البيانات ما يفتح الباب امام سياسة ردع سيبراني قائمة على ما يعرف ب التوائم الرقمية (نوبرغر، ٢٠٢٥، صفحة ٥) .

النتائج والمناقشة:

١. **هشاشة الأمن السيبراني العراقي:** أظهرت نتائج المؤشرات العالمية الى أن العراق يعاني من ضعف كبير في البنية التحتية الرقمية ونقص الكوادر المتخصصة والمدربة في الأمن السيبراني والذكاء الاصطناعي على حد سواء، هذه العوامل تجعل العراق هدف سهل أمام الهجمات الرقمية سواء من قبل مجموعات (هاكرز) غير منظمة أو من قوى اقليمية ودولية مختلفة.

٢. **التنافس الجيوبوليتكي الرقمي:** يشهد العراق تأثيراً مباشراً للتنافس الجيوبوليتكي في الفضاء السيبراني، إذ أصبح هذا المجال ساحة جديدة للصراع بين القوى الإقليمية والدولية. ويُعد موقع العراق الجغرافي والرقمي عنصراً محورياً في هذا الصراع، حيث تتقاطع فيه مصالح قوى متعددة تمتلك قدرات سيبرانية متقدمة. هذا التداخل في النفوذ يفاقم من تعقيد البيئة الأمنية العراقية، ويجعلها عرضة لتجاذبات رقمية تؤثر في سيادتها المعلوماتية واستقرارها الداخلي.

٣. **الذكاء الاصطناعي فرصة لتعزيز الأمن الوطني:** يمثل تقنية وأداة حيوية لتعزيز قدرة العراق الدفاعية، أذ يمكن من استخدامه في الكشف المبكر عن الهجمات والاستجابة التلقائية ومراقبة البنية التحتية الرقمية، كما يساهم في تحسين كفاءة الكوادر الوطنية وتعويض نقص الخبرات، بشكل عام يظهر الذكاء الاصطناعي قدرات ثابتة على استيعاب بيانات كبيرة وضخمة وكشف الانماط الدقيقة وتحديد السلوكيات الطبيعية والغير طبيعية (Ahmed, 2024, p. 62).

٤. **غياب استراتيجية وطنية متكاملة:** على الرغم من الإمكانيات التقنية المتاحة، إلا أن غياب إطار وطني شامل للأمن السيبراني يمثل عقبة أساسية أمام تطوير منظومة متكاملة.

من المتوقع أن يُحدث الذكاء الاصطناعي نقلة نوعية في تحويل ممارسات الأمن السيبراني التقليدية، والأقل فعالية، إلى أنظمة ذكية وديناميكية واستباقية، قادرة على اكتشاف التهديدات الجديدة، والتكيف الفوري، بل وحتى البدء في التفكير مثل الخصم (Ahmed, 2024, p. 42). العلاقة بينهما أصبحت تكاملية، إذ يُستخدم الذكاء الاصطناعي لتعزيز الدفاعات السيبرانية، في حين يشكّل أيضاً مصدراً جديداً للتهديدات إذا أُسيء استخدامه.

الاستنتاجات:

١. **هشاشة الأمن السيبراني في العراق:** أن ضعف البنية التحتية الرقمية ونقص الكوادر المدربة يجعل العراق هدفاً سهلاً للهجمات السيبرانية، مما يهدد استقرار ويضعف القدرة الدفاعية الوطنية.

٢. **البعد الجيوبوليتيكي الرقمي:** يتضح أن العراق يتأثر بشكل مباشر بتنافس القوى الكبرى والإقليمية في الفضاء السيبراني، وهو ما يزيد من تعقيد المشهد الأمني ويجعل الحاجة إلى وعي استراتيجي عالي المستوى أمراً ضرورياً.

٣. **دور الذكاء الاصطناعي في تعزيز الأمن الوطني:** من خلال الكشف المبكر عن الهجمات، الاستجابة التلقائية، وتحليل الأنشطة المشبوهة، ما يقلل المخاطر على البنية التحتية الحيوية ويعزز القدرة الدفاعية للعراق.

٤. **أهمية وجود استراتيجية وطنية متكاملة:** بدون وجود سياسة شاملة تربط بين القطاع الحكومي والخاص، وتحدد آليات التعاون والتنسيق، ستظل جهود حماية العراق محدودة وذات أثر جزئي، وهو ما يضع الدولة في موقف ضعيف .

التوصيات:

١. **تطوير استراتيجية وطنية شاملة للأمن السيبراني:** صياغة سياسات واضحة تربط بين القطاعات الحكومية، والخاصة. وتحديد أولويات لحماية البنية التحتية الحيوية وتوفير الموارد اللازمة لتنفيذها.

٢. **استثمار الذكاء الاصطناعي في الأمن السيبراني:** دمج أنظمة الذكاء الاصطناعي في شبكات الدفاع الرقمي للكشف المبكر والاستجابة التلقائية للهجمات.

٣. **تطوير الكوادر البشرية المتخصصة:** إنشاء برامج تدريبية متقدمة لتأهيل خبراء الأمن السيبراني والذكاء الاصطناعي، وتعزيز التعاون مع الجامعات ومراكز البحث. إطلاق حملات توعية عامة حول أهمية الأمن السيبراني على مستوى المؤسسات والمواطنين.

٤. **تعزيز التعاون الإقليمي والدولي:** عقد شراكات مع الدول والمنظمات الدولية للاستفادة من الخبرات والتقنيات الحديثة.

الخاتمة:

الأمن السيبراني في العراق يمر الآن بمرحلة صعبة، حيث تعاني البنية التحتية الرقمية من هشاشة واضحة، ونقص في الكوادر المدربة يجعل الوضع أكثر تعقيداً، هذا الواقع يعرضه لخطر تهديدات رقمية متعددة على الصعيدين الاقليمي والدولي. في نفس الوقت، التنافس بين القوى العالمية في الفضاء الرقمي يزيد من تعقيد المشهد، ويضع العراق أمام تحديات كبيرة تتطلب فهماً واستراتيجية واضحة وفعالة.

على الجانب الآخر، الذكاء الاصطناعي يظهر كفرصة كبيرة لتعزيز الأمن السيبراني في العراق. قدرته على التعرف المبكر على الهجمات، والاستجابة السريعة، وحماية الأنظمة الحيوية تجعل منه أداة لا يمكن الاستغناء عنها. البحث يؤكد أن دمج الذكاء الاصطناعي في السياسات الوطنية للأمن السيبراني ليس مجرد خيار تقني، بل ضرورة استراتيجية تحمي العراق وتعزز سيادته الرقمية، وتطور من قدرته على مواجهة التهديدات العابرة للحدود. وهذا الدمج يمكن أن يكون نموذجاً يحتذى به في المنطقة، ليعزز الاستقرار الأمني الرقمي في ظل بيئة تنافسية معقدة على المستوى الجيوبوليتيكي.

المصادر العربية

١. الاتحاد الدولي للاتصالات. (٢٠٢١). *الرقم القياسي العالمي للامن السيبراني لعام ٢٠٢٠* . ٥: منشورات ITU.

٢. آن نوبرغر. (٢٠٢٥). *الصين تتفوق في حرب الفضاء السيبراني والولايات المتحدة مطالبة باستراتيجية ردع جديدة*. بابل: مركز حمورابي للبحوث والدراسات الاستراتيجية.

٣. أوسوندي أ. أوسوبا، و ويلسر ، ويليام. (٢٠١٧). *مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل*. موسسة رند.

٤. باسم علي خريسان. (٢٠٢٥). *موقع العراق في مؤشرات الامن السيبراني الدولية الواقع وآفاق المستقبل*. بغداد: مركز المنبر للدراسات والتنمية المستدامة.

٥. برنامج الامم المتحدة الانمائي. (٢٠٢٣). *تقييم المشهد الرقمي في العراق*. نيويورك: الامم المتحدة.

٦. حسن نايف مبارك الحجرف. (٢٠٢٤). دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية. *مجلة الدراسات الجامعية للبحوث الشاملة*، الصفحات ٧١-٩٠.

٧. رعد خضير صليبي. (٢٠٢٤). تعزيز الامن السيبراني في العراق التحديات والفرص. *مجلة دراسات دولية العدد ٩٩* ، الصفحات ٥٠٥-٥٢٨.

٨. سيناء علي محمود. (٢٠٢٥). التحديات الامنية للدول في الفضاء السيبراني. *مجلة قضايا سياسية العدد ٨٠*، الصفحات 311-334 https://creativecommons.org/licenses/by/4.0.

٩. عباس فاضل علوان. (٢٠٢٥). سياسات الامن الوطني العراقي في ظل التحديات العالمية للامن السيبراني. *المجلة العلمية لمكافحة الارهاب العدد ٩ المجلد ٥* ، الصفحات ٢٨-٤٨.

١٠. فيصل مبارك الراشدي. (٢٠٢٥). الامن السيبراني وتحديات الذكاء الالكتروني. *مجلة المعرفة العدد ٣٠* ، الصفحات ١٣٦-١٤٢.

١١. ماجد صدام سالم. (٢٠٢٢). الامن السيبراني واثره في قوة الدولة. *مجلة العلوم التربوية والانسانية العدد ١٨* ، الصفحات ٦٩- ٨٥ https://doi.org/10.33193/JEAHS.18.2022.302.

١٢. محمد كاظم هادي عنجور المنصوري. (٢٠٢٥). الواقع التشريعي للأمن السيبراني في العراق: التحديات والطموحات. *مجلة العلوم الإنسانية والطبيعية المجلد ٦ العدد ٨*، الصفحات ٥٦١-٥٧٦.

١٣. مستشارية الامن الوطني. (٢٠٢٤). *استراتيجية الامن السيبراني العراقي*. National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf: امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.

١٤. مصطفى ابراهيم سلمان الشمري. (٢٠٢١). الامن السيبراني واثره في الامن الوطني العراقي. *مجلة العلوم القانونية والسياسية المجلد ١٠ العدد ١* ، الصفحات ١٤٩-١٩٠.

١٥. مصطفى كامل قرطاس. (٢٠٢٣). *الأمن السيبراني وحقوق الإنسان الرقمية*. بغداد: المفوضية العليا لحقوق الانسان.

١٦. مفيد عوض حسن علي. (٢٠٢٥). *الامن السيبراني واساسياته*. مسقط: مكتبة الدراسات العربية.

١٧. منصور أحلام. (٢٠٢٤). الأمن السيبراني في ظل الذكاء الاصطناعي. *مجلة الحكمة للدراسات والابحاث*، الصفحات ١٠٢٦-١٠٤٣.
١٨. نسرين رياض شنشول، و انور حامد حمد. (٢٠٢٥). *الامن السيبراني وحماية الاقتصاد العراقي التهديدات السيبرانية واستراتجيه المواجهة*. بغداد: مركز البيان للدراسات والتخطيط.
١٩. نورا رياض الدباغ. (٢٠٢٥). تطور الاستراتيجية الامن السيبراني الامريكية الدور الحاسم لادراة جوزيف بايدن. *مجلة حمورابي للدراسات العدد ٥٥*، الصفحات ١٨٨- ٢١٦.
٢٠. هاشم عبد المطلب محسن. (٢٠٢٤). التعاون الدولي في مجال الامن السيبراني من المنظور القيمي روسيا انموذجا. *مجلة حمورابي للدراسات العدد ٥١*، الصفحات ٢٦٧- ٢٨٧.
٢١. هبة الناصري، و مثنى مرعي. (٢٠٢٢). مؤسسات الفضاء السيبراني في منطقة الشرق الاوسط ايران وإسرائيل انموذجا. *مجلة تكريت للعوم السياسية العدد ٣٠ مجلد ٤*، الصفحات ٣٦٠-٣٨١.
٢٢. هيثم رزق فضلالله. (٢٠٢٥). دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني دراسة تحليلية للتحديات والحلول المستقبلية. *المجلة المصرية للدراسات المتخصصة المجلد ١٣ العدد ٤٦*، الصفحات ١٣٤٣-١٣٦٢.

المصادر العربية باللغة الانكليزية

1. International Telecommunication Union. (2021). Global Cybersecurity Index 2020. 5: ITU Publications.
2. Anne Noburger. (2025). China Leads the Way in Cyberspace Warfare and the US Needs a New Deterrence Strategy. Babylon: Hammurabi Centre for Research and Strategic Studies.
3. Osundi A. Osuba, and Wilser, William. (2017). The Risks of Artificial Intelligence to Security and the Future of Work. Rand Corporation.
4. Basim Ali Khreisaan. (2025). Iraq's Position in International Cybersecurity Indicators: Reality and Future Prospects. Baghdad: Al-Manbar Centre for Studies and Sustainable Development.
5. United Nations Development Programme. (2023). Assessment of the Digital Landscape in Iraq. New York: United Nations.
6. Hassan Nayef Mubarak Al-Hajraf. (2024). The Role of Artificial Intelligence in Enhancing Cybersecurity: Theoretical Perspectives. Journal of University Studies for Comprehensive Research, pp. 71–90.
7. Ra'ad Khudair Salibi. (2024). Enhancing Cybersecurity in Iraq: Challenges and Opportunities. Journal of International Studies, Issue 99, pp. 505–528.
8. Sina Ali Mahmoud. (2025). Security Challenges for States in Cyberspace. Journal of Political Issues, Issue 80, pp. https://creativecommons.org/licenses/by/4.0 311–334.
9. Abbas Fadel Alwan. (2025). Iraqi National Security Policies in the Face of Global Cybersecurity Challenges. Scientific Journal of Counter-Terrorism, Issue 9, Volume 5, pp. 28–48.
10. Faisal Mubarak Al-Rashidi. (2025). Cybersecurity and the Challenges of Cyber Intelligence. Al-Ma'rifa Journal, Issue 30, pp. 136–142.
11. Majid Saddam Salim. (2022). Cybersecurity and its impact on state power. Journal of Educational and Human Sciences, Issue 18, pp. 69–85 https://doi.org/10.33193/JEAHS.18.2022.302.
12. Mohammed Kazim Hadi Anjur Al-Mansouri. (2025). The Legislative Reality of Cybersecurity in Iraq: Challenges and Aspirations. Journal of Humanities and Natural Sciences, Vol. 6, No. 8, pp. 561–576.
13. National Security Advisory Board. (2024). Iraqi Cybersecurity Strategy. National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf: Secretariat of the Higher Technical Committee for Communications and Information Security.
14. Mustafa Ibrahim Salman Al-Shammari. (2021). Cyber Security and its Impact on Iraqi National Security. Journal of Legal and Political Sciences, Vol. 10, No. 1, pp. 149–190.
15. Mustafa Kamel Qartas. (2023). Cyber Security and Digital Human Rights. Baghdad: High Commission for Human Rights.
16. Mufid Awad Hassan Ali. (2025). Cyber Security and its Fundamentals. Muscat: Library of Arab Studies.
17. Mansour Ahlam. (2024). Cyber Security in the Age of Artificial Intelligence. Al-Hikma Journal of Studies and Research, pp. 1026–1043.

18. Nisreen Riad Shanshoul and Anwar Hamid Hamad. (2025). Cyber Security and the Protection of the Iraqi Economy: Cyber Threats and Counter-Strategies. Baghdad: Al-Bayan Centre for Studies and Planning.
19. Nora Riad Al-Dabbagh. (2025). The Evolution of US Cybersecurity Strategy: The Crucial Role of the Joseph Biden Administration. Hammurabi Journal of Studies, Issue 55, pp. 188–216.
20. Hashim Abdul-Muttalib Mohsen. (2024). International Cooperation in Cybersecurity from a Values-Based Perspective: Russia as a Case Study. Hammurabi Journal of Studies, Issue 51, pp. 267–287.
21. Heba Al-Nasiri and Muthanna Marai. (2022). Cyberspace Institutions in the Middle East: Iran and Israel as Case Studies. Tikrit Journal of Political Science, Issue 30, Volume 4, pp. 360–381.
22. Haitham Rizk Fadlallah. (2025). The role of artificial intelligence in enhancing the effectiveness of cybersecurity: An analytical study of future challenges and solutions. The Egyptian Journal of Specialised Studies, Vol. 13, No. 46, pp. 1343–1362.

المصادر الاجنبية:

1. Aboul-Enein, S. (2017). *Cybersecurity Challenges in the Middle East.* GENEVA PAPERS: Geneva Centre for Security Policy,.
2. Ahmed, S. A. (2024). The Impact of Artificial Intelligence on Cybersecurity. *International Journal of Computers and Informatics, London Vol (3), No (2),* , pp. https://doi.org/10.59992/IJCI.2024.v3n2p3 -39-70.
3. Al-Bayati, K. A. (2023). *Cyber Security and its impact on national security.* THE SCIENTIFIC JOURNAL OF IRAQI COUNTER TERRORISM SERVICE Volume (3), Issue
4. García-Saúco, A. N. (2021). *DIPLOMACY IN THE DIGITAL ERA AND THE NEED FOR REGULATION.* European Institute of International Studies.
5. Garofali, A. (2024). *OPPORTUNITIES FOR EXTERNAL SERVICES IN THE AGE OF ARTIFICIAL INTELLIGENCE.* SELA, September 2024. URL: www.sela.org.
6. Iraq, C. a. (2025). *Iraq National ICT Industry Development Whitepaper.*
7. ITU. (2024). *Global Cybersecurity Index 2024 5th Edition.* International Telecommunication Union.
8. Rios-Campos, C. (2024). Cybersecurity and artificial intelligence (AI). *South Florida Journal of Development, Miami, v.5, n.8. , ISSN 2675-5459*, pp. . 01-17.
9. Shires, J. (2021). *THE POLITICS OF CYBERSECURITY IN THE MIDDLE EAST.* LONDON: HURST & COMPANY.
10. Sudan, K. S. (2025). Artificial Intelligence and its impact on Geopolitics. *The Academic Volume 3 | Issue 7 |*, pp. 1880-1890.
11. Thompson, S.-N. (2024). The Impact of Artificial Intelligence on Cybersecurity: Opportunities and Threats. *Global Journal on Innovation, Opportunities and Challenges in AAI and Machine Learning - Vol. 8 Issue 1*, pp. 25-55.
12. UNESCO, O. (2024). *G7 TOOLKIT FOR AI IN THE PUBLIC SECTOR.* Italy.
13. Vance, T. R. (2023). Artificial, Geopolitical Implications of Intelligence in Cybersecurity: A Comprehensive Analysis. *International Journal of Computer Science and Information Technology Research Vol. 11, Issue 3,*, pp. 91-105.