مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

مكانة العراق في المؤشرات الدولية للأمن السيبراتي بعد عام ٢٠٢٠

دراسة تحليلية مقارنة

تاريخ استلام البحث ٢٠٢٦/٦/١
تاريخ قبول البحوث ٢٠٢٦/٦/١٠

م.د.علاء عبد الرزاق عبد القادر(*)

الملخص

تتناول الدراسة مكانة العراق في المؤشرات الدولية للأمن السيبراني بعد عام ٢٠٢٠ بوصفها مؤشراً على مستوى جاهزية الدولة في حماية الفضاء الرقمي والبنى التحتية الحيوية في ظل تسارع التحول الرقمي. وتعتمد الدراسة منهجاً تحليلياً مقارناً يربط بين الإطار المفاهيمي للأمن السيبراني ومعايير المؤشرات الدولية، ولا سيما مؤشر الأمن السيبراني العالمي (GCI)، مع تحليل واقع القدرات العراقية من حيث الأطر التشريعية والبنية المؤسسية والجاهزية التقنية والموارد البشرية، وذلك بهدف فهم طبيعة التحديات البنيوية التي تواجه الدولة في بناء منظومة أمن سيبراني متكاملة.

الكلمات المفتاحية: الامن السيبراني، المؤشرات الدولية ، العراق.

المقدمة

تتناول هذه الدراسة موقع العراق في المؤشرات الدولية للأمن السيبراني بوصفه أحد المجالات التي أصبحت تمثل مقياساً لمدى جاهزية الدول في مواجهة التهديدات الرقمية وحماية البنى التحتية الحيوية، وتبرز أهمية الموضوع في ظل التحول المتسارع نحو الخدمات الإلكترونية واعتماد المؤسسات الحكومية على الأنظمة الرقمية مما يجعل تقييم الوضع السيبراني ضرورة لفهم قدرة الدولة على حماية فضائها الرقمي، يتصل موضوع البحث بمجموعة من المؤشرات الدولية التي تقيس قدرات الدول في مستويات التشريع والتنظيم والتقنية وبناء القدرات، ويؤثر ترتيب العراق فيها على قدرته على الانخراط في الاقتصاد الرقمي العالمي واستقطاب الاستثمار، ويقدم تحليل المؤشرات إطاراً يساعد في فهم التحديات البنيوية التي تواجه الدولة وإبراز الفجوات التي تعيق بناء منظومة حماية فعالة.

(*) وزارة التربية alaa1970top@gmail.com

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

اولا:أهمية البحث

تنبع أهمية البحث من أنه يحدد موقع العراق في مؤشرات الأمن السيبراني الدولية بعد ٢٠٢٠ بوصفه مؤشراً على جاهزيته لحماية الفضاء الرقمي والبنى التحتية الحيوية، كما يساهم في كشف الفجوات التشريعية والمؤسسية والتقنية التي تعيق التحول الرقمي وجذب الاستثمار والاندماج في الاقتصاد الرقمي العالمي.

ثانياً:هدف البحث

يهدف البحث إلى تقييم مكانة العراق في المؤشرات الدولية للأمن السيبراني بعد عام ٢٠٢٠ تقييماً تحليلياً مقارناً من خلال الاتي

١.بيان الأطر المفاهيمية للمؤشرات ومعاييرها.

٢.تشخيص واقع القدرات العراقية تشريعياً ومؤسسياً وتقنياً.

٣.تفسير أسباب بقاء العراق في مراتب متأخرة مقارنةً بدول إقليمية مختارة.

٤.تقديم آفاق ومتطلبات عملية يمكن أن تسهم في تحسين ترتيب العراق بعد عام ٢٠٢٥ بصورة مستدامة.

ثالثاً:إشكالية البحث

تتمثل إشكالية البحث في السؤال الرئيس الآتي:

لماذا بقي العراق بعد عام ٢٠٢٠ في موقع متوسط إلى متأخر ضمن المؤشرات الدولية للأمن السيبراني، وما العوامل البنيوية (التشريعية–المؤسسية–التقنية–البشرية) التي تفسّر هذا الموقع مقارنةً بدول إقليمية حققت تقدماً ملحوظاً، وما المسار الأكثر فاعلية لتحسين ترتيب العراق بعد ٢٠٢٥؟

ويتفرع عن ذلك أسئلة فرعية حول أثر غياب التشريع الشامل، وتشتت الصلاحيات، وضعف البنى التحتية ومراكز الاستجابة، ونقص الكوادر، على نتائج العراق في المؤشرات.

رابعاً:فرضية البحث

تفترض الدراسة أن تأخر ترتيب العراق في المؤشرات الدولية للأمن السيبراني بعد عام ٢٠٢٠ يعود إلى ضعف الإطار التشريعي وتشتت البنية المؤسسية وقصور القدرات التقنية والبشرية، كما تفترض أن تحسين موقع العراق مرهون بإصلاحات متكاملة تشمل تشريعاً وطنياً موحداً، وهيئة عليا للأمن السيبراني، وتحديث البنى الرقمية وبناء القدرات.

الحدود الزمانية والمكانية للبحث

١.الحدود الزمانية :تمتد الدراسة من عام ٢٠٢٠ بوصفه نقطة تحوّل في تسارع التحول الرقمي وتنامي التهديدات، وصولاً إلى ٢٠٢٥ في التحليل والتقييم، مع استشراف آفاق التحسين بعد ٢٠٢٥ ضمن سيناريوهات ومقترحات الدراسة.

٢.الحدود المكانية: تتركز الدراسة على جمهورية العراق (المؤسسات الحكومية والبنى

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

الرقميــة الوطنيــة)، مــع اعتماد مقارنــة إقليمية بدول مختارة في الشــرق الأوسط هي: السعودية، الإمارات، تركيا، مصر، الأردن بوصفها حالات مرجعية لقياس الفجوة واســتخلاص الدروس القابلة للتطبيق.

خامساً: هيكلية البحث

تقوم هيكلية البحــث على تنظيمه في أربعة محــاور رئيســية مترابطــة تنسجــم مــع طبيعتــه التحليلية المقارنة، يتناولـــ المحــور الأول الإطار المفاهيمي والنظري للأمــن الســيبراني، ويعالج المحــور الثاني واقع القدرات الســيبرانية العراقية بعد عام ٢٠٢٠ من خلال تحليل البنية التشريعية والمؤسســية ومستوى الجاهزية التقنية والبنى التحتيــة الرقمية، مع تشخيص مكامــن القوة والضعف، ويركز المحور الثالــث على دراسة مقارنة لمكانة العراق في المؤشــرات الدولية عبر مقارنتــه بدول إقليمية مختــارة، أما المحور الرابع فيتناول آفاق تعزيز مكانة العراق في المؤشرات الدوليــة بعد عام ٢٠٢٥، من خلالـــ تحديد متطلبات الإصلاح وصياغــة رؤية اســتراتيجية وسيناريوهات مستقبلية لتحقيق صعود مستدام في الجاهزية السيبرانية.

اولاً: الإطــار المفاهيمي والنظري للأمن السيبر اني والمؤشرات الدولية

يهــدف هذا الموضوع إلى وضــع إطار مفاهيمي ونظري يوضح موقع الأمن الســيبراني ضمن منظومة الأمن الوطني، ويفسر الأســس التي تعتمدها المؤشــرات الدولية في قيــاس جاهزية الدول رقمياً.

١.مفهوم الأمن الســيبر اني وتطور مكانته في الأمن الوطني

يشكل الأمن السيبراني أحد المفاهيم الحديثة التي اكتسبت أهمية متصاعدة في بنية الأمن الوطني فقد أدى التحول الرقمي الواســع إلى خلق فضاء جديــد تتفاعل فيه الــدول والفاعلون غير الحكوميين عبر شــبكات معقدة تعتمد على تدفق المعلومات ومع هذا التحول ظهر الأمن الســيبراني بوصفه ضــرورة لبناء منظومــة حماية قادرة على مواجهة التهديدات الرقمية التي تستهدف الأنظمة الحيوية للدول ويشــير الأمن السيبراني في جوهره إلى قدرة الدولة على حمايــة بنيتهــا الرقمية من المخاطــر التي تطال البيانــات أو الأنظمة أو البنى التحتية الرقمية ويتضمن ذلك وضع سياسات وإجراءات وتقنيات تحافظ على ســرية المعلومات وسلامتها واستمرار انسيابها دون تعطيل[1].

وقــد تعددت التعريفات التي تناولت مفهوم الأمن الســيبراني في الأدبيات السياسية والاستراتيجية فبعضها ركز على الجانب التقني وربط الأمن الســيبراني بإدارة المخاطر الرقمية بينما رأت دراسات أخرى أن الأمن السيبراني مفهوم أشمل يتداخل مع الأمن القومي والأمن الاقتصادي والأمن المجتمعي وعلى الرغم من اختلاف التعريفات إلا أنها تلتقي عنــد فكرة أساســية وهي أن الأمن الســيبراني يمثل مجموعة من القدرات المؤسسية التي تمكن الدولة من منع الاختراقــات الرقمية والتعامل معهــا عند وقوعها ويعد تعريف الاتحاد الدولي للاتصالات من أكثر التعريفات تداولاً حيث يــرى الاتحــاد أن الأمن الســيبراني هو منظومة تهدف إلى حفظ ســرية

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

البيانات وضمان سلامتها والحفاظ على توافرها للمستخدمين ويبدو هذا التعريف منسجماً مع الطبيعة العملية للأمن السيبراني بوصفه أداة لحماية الدول في عالم يتزايد اعتماده على التكنولوجيا[٢].

وتتأسس البنية المفاهيمية للأمن السيبراني على ثلاثة أركان ،**الركن الأول** هو السرية التي تمنع أي وصول غير مشروع إلى المعلومات و**الركن الثاني** هو السلامة التي تضمن عدم تغيير البيانات أو إتلافها أما **الركن الثالث** فهو التوافر الذي يعكس قدرة الدولة على استمرار عمل الأنظمة الرقمية دون توقف ويشكل أي خلل في أحد هذه الأركان تهديداً قد ينعكس على مؤسسات الدولة الحيوية كالمصارف والمطارات وشبكات الطاقة والخدمات الطبية[٣].

وقد أصبح الأمن السيبراني عنصراً محورياً في إدارة الدولة الحديثة فلم يعد مجرد وظيفة تقنية تتولاها المؤسسات التكنولوجية بل تحول إلى جزء من إدارة الحكم وصنع القرار الأمني وتدرك الدول اليوم أن أي تهديد رقمي يمكن أن يحمل أثراً مباشراً على الاستقرار السياسي وعلى الثقة العامة بالدولة وعلى قدرتها في إدارة مواردها لذلك اتجهت أغلب الدول إلى بناء استراتيجيات وطنية للأمن السيبراني تتضمن الأدوار المؤسسية والقانونية والوقائية وتشمل هذه الاستراتيجيات إطاراً تشريعياً يغطي الجرائم الإلكترونية وإجراءات الدفاع الرقمي ومراكز الاستجابة للحوادث السيبرانية[٤].

كما ارتبط مفهوم الأمن السيبراني منذ بداية العقد الأخير بتحولات بنية القوة الدولية إذ لم تعد القوة تقاس فقط بالعنصر العسكري التقليدي أو القدرات الاقتصادية بل دخلت القدرات الرقمية في صلب معادلة القوة وفرضت البيئة الرقمية تحديات جديدة جعلت الدول تتنافس على تطوير أدواتها الهجومية والدفاعية في الفضاء السيبراني وقد أدت هذه التحولات إلى بروز مفهوم ما يسمى بـ القوة الرقمية التي تمثل مزيجاً من القدرات التقنية ورأس المال البشري والبنى التحتية الرقمية وأصبح الأمن السيبراني جزءاً من هذه القوة حيث تعتمد عليه الدول في حماية أنظمتها ومؤسساتها ومصالحها الاقتصادية والسياسية[٥].

وتشير التجارب الدولية إلى أن الدول التي تمتلك قدرات سيبرانية متقدمة تتمتع بقدرة أكبر على مواجهة التهديدات الداخلية والخارجية فهي قادرة على حماية شبكاتها الحيوية وإدارة أزمات الاختراق والتعافي منها بسرعة كما تستطيع هذه الدول فرض ردع سيبراني يحد من محاولات الهجوم عليها في المقابل تواجه الدول ذات القدرات الضعيفة مخاطر كبيرة فالهجمات الرقمية يمكن أن تعطل بنى الطاقة والمياه والمصارف والنقل وقد تشكل أداة ضغط سياسية أو اقتصادية ويبرز هنا الدور الجوهري للأمن السيبراني بوصفه أحد المكونات التي تحفظ سيادة الدولة في عالم متداخل رقمياً[٦].

ويرتبط المفهوم أيضاً بتعزيز الثقة في المؤسسات الحكومية فالدولة التي تمتلك منظومة سيبرانية قوية تستطيع حماية بيانات المواطنين وضمان سرية معاملاتهم وهذا يسهم في رفع مستوى الثقة بالخدمات الحكومية

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

الرقميــة ويشجع علــى الانتقالـــ نحــو الإدارة الإلكترونية كما يوفر الأمن السيبراني إطاراً داعماً للاقتصاد االرقمي الذي يعتمد في بنيته على التدفقات المستمرة للمعلومات والمعاملات المالية الإلكترونية

ويتضح من تحليل الأدبيات أن الأمن السيبراني أصبــح أحــد مفاتيــح إدارة الدولــة الحديثة ولم يعد خياراً تقنياً لكن أصبح ضرورة استراتيجية فالدول التي تســتثمر في قدراتها الرقمية تستطيع بنــاء منظومــة أمنية متكاملة تحمي مصالحها وتدعم استقرارها بينما تغدو الدولـــ التي تهمل هذا الجانب أكثر عرضة للتهديدات التي تتجاوز الحدود الجغرافية وتعملـــ في فضاء غير مرئي لكنه شديد التأثير ومن هنا تتضح أهمية الأمن السيبراني كمفهوم يعكس قدرة الدولة على حماية نفسها في بيئة رقمية تتطور بسرعة كبيرة[٧].

٢.المؤشرات الدولية للأمن السيبر اني (GCI – NCSI – ITU)

١.المؤشرات الدولية للأمن السيبر اني

تُعدّ المؤشرات الدولية للأمن السيبراني أدوات مرجعية أساســية لقياس مستوى جاهزية الدول في حمايــة فضائها الرقمي، إذ تقوم على منهجيات شاملة لا تقتصر على البعد التقني لكن تشمل الأطر التشــريعية والتنظيمية والمؤسســية، وبناء القدرات البشــرية، والتعاون الدولي،ش وتبرز أهمية هذه المؤشرات مثل مؤشر الأمن السيبراني العالمي (GCI) ومؤشر الأمن السيبراني الوطني (NCSI) وتقييمــات الاتحاد الدولي للاتصالات، في كونها توفر تقييماً مقارناً يكشف مواطن القوة والقصور ويساعد الحكومات على تشخيص أوضاعها الرقمية ضمن ســياق دولي متغير يتسم بتصاعــد التهديدات الســيبرانية وتعقّدها[٨]، ولا تقتصر وظيفة هذه المؤشــرات على القياس والتصنيف لكنها تؤدي دوراً تحفيزياً في تحسين الأداء وصياغة السياسات العامة، إذ تدفع الدول إلى تطوير تشــريعاتها، وتعزيز هياكلها التنظيمية، وبناء كوادر متخصصة قــادرة على إدارة المخاطر الرقمية، كما تســهم في تعزيــز الثقــة الدولية وجاذبية بيئة الاستثمار بما يجعلـــ التقدم فيها مؤشراً على الاســتقرار الرقمي والاقتصادي معاً، ويؤكد أن الأمن السيبراني باتـــ عنصراً بنيوياً في قوة الدولــة وقدرتها على مواكبــة التحول الرقمي والاستعداد لتحدياته المستقبلية[٩].

تُعدّ المقارنات الدولية أداة تحليلية محورية في تقييم جاهزية الدولـــ السيبرانية، إذ توفر رؤية شاملة لموقع الدولة ضمن البيئة الرقمية العالمية، وتكشف الفجوات البنيوية التي تعيق بناء منظومة أمن ســيبراني متكاملة، وتمكّن هذه المقارنات صناع القرار من تشخيص مواطن القوة والضعف عبر أبعاد متعددة تشــملـــ القدرات التقنيــة، والتشــريعية، والمؤسســية، والمــوارد البشرية، بما يساعد على صياغة سياسات واقعية تستند إلى نماذج ناجحة وتجارب دولية رائدة. كما تكتسب أهميتها من طبيعة التهديدات السيبرانية العابرة للحدود، الأمر الذي يجعــل التعلم من خبرات الدول المتقدمة ضرورة استراتيجية وليس خياراً ثانوياً[١٠].

ولا تقتصــر وظيفــة المقارنات الدولية على التشخيــص لكنها تؤدي دوراً فاعلاً في تحســين الأداء وتعزيز التنافس الإيجابي بين الدول،

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

إذ تسعى الحكومات إلى تحسين مواقعها في المؤشرات العالمية بوصفها أحد عناصر القوة الناعمة ومؤشراً على الاستقرار الرقمي وجاذبية بيئة الاستثمار، كما تسهم هذه المقارنات في دعم التخطيط طويل الأمد، وتقييم فعالية السياسات العامة، وتوفير إنذارات مبكرة بشأن المخاطر المحتملة، فضلاً عن تعزيز التعاون الدولي وبناء القدرات التعليمية والتدريبية[١١].

٢.واقع القدرات السيبرانية العراقية بعد عام ٢٠٢٠

يتناول هذا الموضوع تقييم واقع القدرات السيبرانية العراقية بعد عام ٢٠٢٠ من خلال تحليل مستوى الجاهزية التشريعية والمؤسسية والتقنية، وبيان مدى قدرة الدولة على مواجهة التهديدات الرقمية في ضوء المعايير والمؤشرات الدولية، وسوف يتم تناولها كالاتي:

-البنية المؤسسية والتشريعية للأمن السيبراني في العراق

شهد العراق خلال السنوات التي تلت عام ٢٠٢٠ اهتماماً متزايداً ببناء إطار تشريعي وتنظيمي يعالج قضايا الأمن السيبراني بعد أن أصبحت التهديدات الرقمية تمثل خطراً مباشراً على المؤسسات الحكومية والبنى التحتية ويعود هذا الاهتمام إلى تطور الهجمات الإلكترونية التي استهدفت مواقع حكومية ومؤسسات مالية مما دفع الدولة إلى التفكير في تأسيس منظومة قانونية تؤمن الاحتياجات الأساسية للحماية الرقمية ورغم هذا التطور ما يزال الإطار التشريعي في العراق يعاني من فجوات واضحة تحتاج إلى معالجة.[١٢]

يمتلك العراق اليوم عدداً من القوانين ذات العلاقة بالأمن السيبراني إلا أن معظمها لا يمثل تشريعاً سيبرانياً متكاملاً فقانون الاتصالات والمعلوماتية الذي طرح منذ سنوات ما يزال ضمن إطار النقاش ولم يقر بشكل كامل رغم أهميته في تنظيم القطاع الرقمي كما يستند العراق في جزء كبير من سياساته إلى قوانين العقوبات التقليدية التي لا تغطي الجرائم الإلكترونية الحديثة تغطية كاملة وهذا يؤدي إلى صعوبة التعامل مع الهجمات الرقمية المعقدة التي تحتاج إلى تعريفات قانونية واضحة وإجراءات قضائية متخصصة، وتسعى الدولة منذ عام ٢٠٢٠ إلى إعداد استراتيجية وطنية للأمن السيبراني تتضمن مبادئ للحماية الرقمية والاستجابة للحوادث الإلكترونية وقد شاركت مؤسسات عديدة في صياغة مسودات هذه الاستراتيجية مثل وزارة الداخلية وجهاز الأمن الوطني وهيئة الاتصالات والإعلام إلا أن الاستراتيجية لم تتحول حتى الآن إلى إطار ملزم يوجه عمل المؤسسات الحكومية ويعود ذلك إلى طبيعة البيئة التشريعية المعقدة التي تتطلب توافقاً سياسياً ومؤسسياً واسعاً قبل إقرار مثل هذه الاستراتيجيات.

أما الأطر التنظيمية المتعلقة بحماية البيانات فقد شهدت تطوراً جزئياً عبر بعض التعليمات التي أصدرتها مؤسسات حكومية مثل البنك المركزي العراقي وهيئة الإعلام والاتصالات فقد تبنت هذه المؤسسات أنظمة لحماية البيانات المالية وأنظمة تتعلق بإدارة المواقع الإلكترونية والبوابات الرقمية إلا أن هذه الجهود ما تزال محدودة لأنها تصدر بصورة منفصلة ودون إطار وطني موحد ينسق بين المؤسسات وهذا يؤدي إلى

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

ازدواجية في العمل وضعفاً في القدرة على مواجهة التهديدات السيبرانية على المستوى الوطني[١٣].

كما يعاني العراق من غياب قانون شامل لحماية البيانات الشخصية وهذا يشكل تحدياً كبيراً لأنه يؤثر في مستوى الثقة بين المواطن والمؤسسات الحكومية فالدول التي تمتلك قوانين لحماية البيانات توفر بيئة آمنة تتيح تطوير الحكومة الإلكترونية والتحول الرقمي وفي غياب مثل هذه التشريعات تكون البيانات مكشوفة أمام مخاطر التسريب أو الاختراق ويؤدي ذلك إلى ضعف قدرة العراق على الانخراط في الاقتصاد الرقمي العالمي[١٤]، وعلى الرغم من هذه الفجوات فإن العراق يمتلك فرصة مهمة لتطوير منظومته التشريعية فالتحول الرقمي الذي تبنته الحكومة في السنوات الأخيرة يحتاج إلى إطار قانوني يدعم الاستجابة الأمنية كما أن التعاون مع المنظمات الدولية يوفر فرصة للاستفادة من التجارب المقارنة وقد بدأت بعض المؤسسات الحكومية بتنفيذ برامج تدريبية لتعزيز الوعي بالقوانين والتشريعات الخاصة بالأمن السيبراني إلا أن هذه البرامج ما تزال في مرحلة أولية وتحتاج إلى توسيع.

يمثل الأمن السيبراني في العراق مجالاً متعدد المؤسسات نظراً لطبيعته المتداخلة التي تشمل الجوانب الأمنية والقانونية والتقنية وقد سعت الدولة منذ عام ٢٠٢٠ إلى توزيع الأدوار بين الوزارات والهيئات الوطنية بهدف إنشاء منظومة قادرة على مواجهة التهديدات الرقمية إلا أن هذا التوزيع ما يزال يعاني من فجوات واضحة في التنسيق وغياب الأطر الإلزامية مما يجعل أداء هذه المؤسسات دون المستوى المطلوب مقارنة بالتحديات المتزايدة ويعد فهم دور هذه المؤسسات خطوة أساسية لتحديد نقاط القوة والضعف في البنية السيبرانية للدولة[١٥].

تبدأ المنظومة المؤسسية بوزارة الداخلية التي تتحمل مسؤولية كبيرة في إدارة الجرائم الرقمية وتمتلك الوزارة وحدات للتحقيق الجنائي الرقمي وأقساماً مختصة بتتبع الأنشطة الإلكترونية التي تهدد الأمن الداخلي إلا أن هذه القدرات ما تزال محدودة لعدم توفر كوادر كافية أو تقنيات متطورة تستطيع تحليل الهجمات المعقدة كما أن وزارة الداخلية ما تزال تعتمد على تشريعات قديمة لا تغطي الجرائم الإلكترونية الحديثة وهذا يجعل عملية ضبط الجرائم الرقمية أكثر صعوبة ويؤثر في فاعلية الوزارة عند مواجهة هجمات ذات طابع متطور[١٦]، أما جهاز الأمن الوطني فقد أصبح منذ ٢٠٢٠ أحد أهم المؤسسات الفاعلة في الأمن السيبراني إذ يقوم برصد الهجمات التي تستهدف البنى التحتية ومراقبة الأنشطة الإلكترونية التي قد تحمل تهديدات تمس الأمن القومي ويعمل الجهاز على تطوير قدرات تحليل التهديدات ورفع مستوى التنسيق مع المؤسسات الأمنية الأخرى إلا أن الجهاز يعاني هو الآخر من تحديات تتعلق بتداخل الصلاحيات مع جهات أخرى إضافة إلى محدودية الإطار القانوني الذي ينظم عمله في المجال السيبراني وهذا يحدث أحياناً فجوة في إدارة المعلومات الأمنية أو يسبب بطئاً في اتخاذ القرار[١٧].

ومن المؤسسات المركزية في هذا القطاع هيئة الإعلام والاتصالات التي تتولى تنظيم قطاع الاتصالات والإنترنت وتمتلك الهيئة دوراً مباشراً

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

في مراقبة شبكات الاتصالات ووضع ضوابط فنية تمنع استغلالها في الهجمات الرقمية كما تتولى إصدار التعليمات المتعلقة بتأمين البنى التحتية التابعة لشركات الاتصالات إلا أن هذا الدور يظل غير مكتمل لعدم وجود تشريع وطني موحد يربط الهيئة ببقية المؤسسات الأمنية وبالتالي تبقى إجراءاتها تنظيمية أكثر من كونها تشريعية أو تنفيذية مما يحد من قدرتها على فرض قواعد إلزامية شاملة تغطي جميع المؤسسات الحكومية والقطاع الخاص[١٨].

وتبرز كذلك أهمية وزارة الدفاع التي دخلت خلال السنوات الأخيرة في مجال الأمن السيبراني من خلال وحدات متخصصة تتولى حماية الأنظمة الدفاعية ومراكز القيادة والسيطرة وتعمل الوزارة ضمن إطار حماية الأمن الوطني من التهديدات التي تستهدف البنى العسكرية إلا أن دورها محصور في الجانب العسكري ولا يمتد إلى المستوى الوطني العام وهذا يعكس الحاجة إلى إنشاء مركز سيبراني وطني موحد يجمع القدرات العسكرية والمدنية في إطار تكاملي بدلاً من بقاء هذه القدرات موزعة دون تنسيق فعال[١٩].

ويعد البنك المركزي العراقي مثالاً آخر على المؤسسات التي تمتلك دوراً في الأمن السيبراني من خلال فرض معايير حماية على المصارف والأنظمة المالية وقد طور البنك المركزي تعاميم تتعلق بأمن البيانات المالية وإدارة المخاطر التقنية إلا أن هذا الدور يقتصر على القطاع المالي دون شمول بقية القطاعات الاقتصادية كما أن التزام بعض المصارف بهذه المعايير يبقى متفاوتاً مما يخلق فجوة في الأمن الرقمي للقطاع كله وهذا يشير إلى حاجة الدولة إلى تشريع موحد يجعل هذه المعايير إلزامية على جميع المؤسسات المالية[٢٠]، وبالإضافة إلى ذلك تعمل وزارة التعليم العالي ووزارة الاتصالات على تطوير البنى التحتية الرقمية بما في ذلك مراكز البيانات الرسمية وشبكات الجامعات وأنظمة الحكومة الإلكترونية إلا أن هذه الجهود تبقى منفصلة ولا ترتبط باستراتيجية وطنية واحدة وهذا يشكل تحدياً لأنها تجعل الجهود مبعثرة وغير متسقة مع متطلبات الأمن السيبراني الوطني[٢١].

ويتضح من تحليل هذه المؤسسات أن المشكلة الرئيسية لا تكمن فقط في نقص القدرات التقنية أو التشريعية بل في تعدد الجهات التي تعمل دون وجود مركز وطني سيبراني يملك صلاحيات واضحة فعند مقارنة العراق بدول المنطقة يتبين أن دولاً مثل السعودية والإمارات أنشأت هيئات وطنية عليا مسؤولة عن الأمن السيبراني وتملك سلطة إلزامية على جميع القطاعات أما في العراق فالصلاحيات موزعة بين مؤسسات كثيرة مما يسبب فجوات تنظيمية ويصعب عملية اتخاذ القرار في حالة وقوع هجوم سيبراني واسع[٢٢].

ومن أبرز الفجوات التي تعاني منها المنظومة السيبرانية العراقية غياب قانون حكومي شامل ينظم الأمن السيبراني إذ تعتمد المؤسسات على تعليمات داخلية أو مسودات غير مقرة كما لا توجد إجراءات إلزامية لحماية البيانات الحكومية أو لفرض معايير الأمن السيبراني على المؤسسات الخاصة وقد أدى هذا الغياب إلى تفاوت في مستوى الحماية بين المؤسسات فبعض الوزارات تمتلك أنظمة حماية متقدمة بينما

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

تعاني وزارات أخرى من ضعف واضح يجعلها هدفاً سهلاً للهجمات[٢٣]، وتتمثل فجوة أخرى في غياب التنسيق المؤسساتي فلا يوجد حتى الآن نظام موحد لتبادل المعلومات حول التهديدات الرقمية بين وزارة الداخلية والأمن الوطني وهيئة الاتصالات والوزارات الأخرى ويؤدي هذا إلى تأخر الاستجابة أو ضعفها كما أن غياب التدريب المتخصص يشكل عقبة كبيرة لأن الأمن السيبراني يحتاج إلى كوادر تمتلك مهارات تقنية عالية تساعد في مواجهة الهجمات المتقدمة[٢٤].

كما يعاني العراق من غياب سياسة وطنية لحماية البيانات وهذا يؤثر بشكل مباشر على الثقة بالخدمات الحكومية الإلكترونية ويجعل الدولة غير قادرة على الانخراط الكامل في مشاريع الحوكمة الرقمية والتجارة الإلكترونية إذ تعتمد معظم الدول المتقدمة على قوانين صارمة لحماية بيانات المواطنين بينما تفتقر البيئة العراقية إلى هذه القوانين، وبالرغم من هذه التحديات إلا أن العراق يمتلك فرصة لتطوير منظومته السيبرانية إذا تمكن من إصدار تشريع موحد للأمن السيبراني وإنشاء مجلس وطني يضم جميع المؤسسات تحت مظلة واحدة كما يمكن للعراق الاستفادة من التعاون مع المنظمات الدولية لتطوير مهارات الكوادر الأمنية وتعزيز بنية الاستجابة للحوادث[٢٥]، يتضح من هذا التحليل أن البنية المؤسسية للأمن السيبراني في العراق تحتاج إلى تحديث منظم يقوم على دمج الصلاحيات وتوحيد الجهود وتشريع قوانين شاملة إذ لا يمكن بناء منظومة سيبرانية وطنية دون بنية تشريعية واضحة وتنسيق مؤسسي فعال يضمن حماية البنى التحتية الحيوية للدولة.

-البنى التحتية الرقمية والجاهزية التقنية لمواجهة التهديدات

تعد البنى التحتية الرقمية أحد أهم الأسس التي تعتمد عليها الدول في تعزيز قدرتها على مواجهة التهديدات السيبرانية وفي العراق شهد هذا القطاع تطوراً متفاوتاً بعد عام ٢٠٢٠ نتيجة تنفيذ مشروعات للتحول الرقمي في المؤسسات الحكومية إلا أن هذه الجهود لم تصل إلى مستوى بناء منظومة متكاملة للأمن السيبراني إذ ما يزال الواقع التشغيلي للأنظمة الرقمية يعاني من ضعف على مستوى الحماية والاستجابة للحوادث الإلكترونية[٢٦]، وتعتمد أغلب المؤسسات الحكومية العراقية على أنظمة معلوماتية تقليدية تفتقر إلى التحديث المستمر وعلى الرغم من وجود بعض المبادرات لتحسين أنظمة الحماية مثل استخدام الجدران النارية وبرمجيات مكافحة الاختراق إلا أن هذه الأدوات لا تمثل منظومة دفاعية متكاملة فمعظم المؤسسات لا تمتلك مراكز عمليات أمنية قادرة على مراقبة الشبكات بشكل لحظي أو تحليل الأنشطة المشبوهة كما أن الأنظمة التي توفرها الشركات الخاصة غالباً ما تكون معزولة عن بقية المؤسسات الحكومية مما يعرضها للاختراق[٢٧].

أما الاستجابة للحوادث السيبرانية فهي من أكثر الجوانب التي تعاني ضعفاً واضحاً فالعراق لا يمتلك حتى الآن مركزاً وطنياً للاستجابة للحوادث السيبرانية يعمل على مدار الساعة كما لا توجد خطوط اتصال واضحة بين الوزارات والمؤسسات عند وقوع هجوم رقمي وهذا يؤدي إلى بطء كبير في

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

اكتشـاف الهجمات أو التعامل معها وقد شهدت السنوات الأخيرة حوادث اختراق استهدفت مواقع حكومية ولم يتم التعامل معها بسـرعة بسبب غياب فريق متخصص للاسـتجابة والتحليل[٢٨]، وفيما يتعلق بالمنصات الرقمية الحكومية فقد اتجه العراق إلى توسـيع استخدام البوابات الإلكترونية والخدمات الرقمية في المؤسسـات العامة إلا أن هذه المنصات لا تخضع دائماً لمعايير أمنية موحدة فبعض الوزارات تستخدم بروتوكولات قديمة أو تعتمد على خوادم داخلية ضعيفة وهذا يرفع احتمال تعرض البيانات الحكومية للسرقة أو التلاعب كما أن كثيراً من المنصات لا تمتلك أنظمة تحقق متعددة الطبقات مما يجعلها عرضة للاختراق في حال تمكن المهاجم من تجاوز طبقة الحماية الأولى[٢٩].

ويعاني قطاع الحكومة الإلكترونية من تحديات في التكامل بين الأنظمة فغياب قاعدة بيانات وطنية موحدة يؤدي إلى تكرار المعلومات وتبادلها بطرق غير مؤمنة وهذا يزيد من احتمال تسـريب البيانات أو العبث بها كما أن المؤسسات الحكومية تعتمد في أغلب الأحيان على تخزين البيانات داخل مراكز بيانات صغيرة وغير مجهزة تقنياً وهذه المراكز لا توفر أنظمة تبريد مناسبة أو مصادر كهرباء احتياطية ما يجعلها عرضة للتعطل عند حدوث أي خلل تقني أو هجمات حجب الخدمة[٣٠]، وعلى الرغم من بعض التقدم المتقطع مثل إنشاء منصات للدفع الإلكتروني وإطلاق بوابات خدمات موحدة فإن هذه الجهود تبقى محدودة لأنها لا ترتبط باستراتيجية وطنية موحدة للأمن السيبراني كما أن ضعف الرقابة التقنية وعدم وجود معايير إلزامية يجعل مسـتوى الحماية يختلف من وزارة إلى أخرى وهذا التفاوت يشـكل ثغرة يمكن للمهاجمين استغلالها بسهولة[٣١].

يتضح من خلال تحليل الواقع التشـغيلي أن البنى التحتية الرقمية في العراق تحتاج إلى تحديث شامل ويشمل ذلك بناء مراكز بيانات وطنية متطورة وربط المنصات الحكومية بمنظومة أمن موحدة وتأسيس مركز استجابة وطني كما يحتاج العراق إلى اعتماد بروتوكولات دولية لحماية البيانات وتعزيز مراقبة الشبكات الحكومية فبدون هذه الإصلاحات سيظل العراق معرضاً لهجمات متكررة وغير قادر على حماية منظومته الرقمية[٣٢].

ثانياً: تحديات صعود العراق في المؤشرات الدولية

يعكس مستوى التطور التكنولوجي في العراق طبيعة البيئة الرقمية التي تعتمد عليها الدولة في مواجهة التهديدات السيبرانية ورغم الجهود المبذولة خلال السنوات الأخيرة لتحسين البنى التقنية إلا أن العراق ما يزال يعاني فجوة كبيرة مقارنة بالدول الإقليمية التي استطاعت بناء منظومات سيبرانية متقدمة ويعود هذا التراجع إلى محدودية الاستثمار في التكنولوجيا وضعف الكوادر المتخصصة وانعدام منظومات الإنذار المبكر[٣٣]، ويعد نقص الكوادر التقنية أحد أبرز التحديات التي تواجه الأمن السيبراني في العراق فالمؤسسات الحكومية لا تمتلك عدداً كافياً من الخبراء في مجالات تحليل الهجمات والتشفير وإدارة الشبكات كما أن التدريب المهني في هذا المجال ما يزال محدوداً ويعتمد على برامج قصيرة

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

لا توفر معرفة كافية لإدارة هجمات متقدمة فضلا عن ذلك عزوف الكفاءات العراقية عن العمل في المؤسسات الحكومية بسبب ضعف الرواتب وعدم توفر بيئة عمل مناسبة مما يؤدي إلى فقدان الدولة لخبرات تحتاجها بشكل عاجل[٣٤].

أما التكنولوجيا المستخدمة في المؤسسات الحكومية فهي في معظم الأحيان قديمة ولا تتوافق مع متطلبات الأمن السيبراني الحديث فالكثير من الأنظمة تعتمد على برمجيات غير محدثة أو أنظمة تشغيل لم تعد مدعومة وهذا يجعلها عرضة للثغرات الأمنية التي يمكن استغلالها بسهولة كما أن بعض المؤسسات ما تزال تعتمد على شبكات محلية مفتوحة لا توفر طبقات كافية من التشفير والحماية وهذا يتعارض مع المعايير الدولية التي تتطلب بنى شبكية مغلقة ومحمية[٣٥]، ويظهر ضعف منظومة الإنذار المبكر بشكل كبير في المؤسسات العراقية فالدول المتقدمة تمتلك أنظمة مراقبة رقمية تعمل على مدار الساعة وتكشف أي نشاط مشبوه خلال ثوان أما في العراق فتتم مراقبة الشبكات عادة من خلال فرق بشرية صغيرة تستخدم أدوات بدائية وهذا يؤدي إلى تأخر اكتشاف الهجمات وقد تعرضت مؤسسات عراقية لهجمات استمرت ساعات أو أيام قبل أن يتم كشفها مما يدل على غياب نظام إنذار متطور يستطيع رصد الهجمات في بدايتها[٣٦].

وتؤثر هذه التحديات في قدرة العراق على تحسين موقعه في المؤشرات الدولية للأمن السيبراني فمؤشر GCI و NCSI يعتمدان على تقييم قدرات الدول في مجالات التكنولوجيا والكوادر والبنى التحتية وكلما كانت هذه القدرات ضعيفة انخفض ترتيب الدولة ولهذا احتل العراق مواقع متأخرة في أغلب المؤشرات خلال السنوات الأخيرة وهذا يشير إلى حاجة ملحة لتطوير البنية الرقمية بما يتوافق مع المعايير التي تعتمدها المؤشرات العالمية[٣٧].

ومن التحديات التقنية كذلك ضعف مراكز البيانات الوطنية فالعراق لا يمتلك حتى الآن مركز بيانات وطني موحد قادر على إدارة المعلومات الحكومية بشكل آمن وتعتمد المؤسسات على خوادم محلية صغيرة وهذه الخوادم غير قادرة على تحمل الهجمات ولا توفر تقنيات النسخ الاحتياطي الفوري كما أن غياب السحابة الحكومية يجعل تحويل البيانات إلى بيئات محمية مسألة صعبة[٣٨]، وتبرز أيضاً مشكلة ضعف التنسيق التقني بين المؤسسات فالمؤسسات لا تشارك المعلومات بشأن الهجمات السيبرانية أو الثغرات المكتشفة وهذا يجعل كل مؤسسة تعمل بمعزل عن الأخرى أما الدول المتقدمة فقد استطاعت بناء شبكات ربط آمنة تسمح بتبادل المعلومات بشكل فوري وهذا يساهم في منع انتشار الهجمات وحماية البنى الحيوية[٣٩].

كما يعاني العراق من تحديات تتعلق بسرعة الإنترنت وجودته فالبنى التحتية للاتصالات لا توفر دائماً سرعة عالية أو استقراراً فنياً وهذا يؤثر في قدرة المؤسسات على استخدام أنظمة مراقبة متقدمة تعتمد على تحليل البيانات الضخمة أو الذكاء الاصطناعي وبمن ثم تبقى

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

منظومة الحماية محدودة في قدرتها التقنية

فضلا عن ذلك أن قطاع الاتصالات الخاص لا يخضع دائماً لمعايير أمنية إلزامية فالشركات تعتمد على معاييرها الداخلية ولا يوجد تشريع يلزمها باتباع بروتوكولات موحدة للحماية وهذا يشكل خطرًا كبيرًا لأنه يجعل الشبكات التجارية عرضة للهجمات وقد يؤدي ذلك إلى استهداف المستخدمين والمؤسسات في الوقت نفسه[٤٠].

ثالثاً: مكانة العراق في المؤشرات الدولية للأمن السيبر اني (دراسة مقارنة)

يُظهر مؤشر الأمن السيبراني العالمي[٤١] GCI ٢٠٢٤ الصادر عن الاتحاد الدولي للاتصالات تبايناً واضحاً في مستويات أداء دول الشرق الأوسط، إذ جاء العراق ضمن المستوى الرابع(Tier 4 – Evolving)، وهو مستوى يعكس جاهزية سيبرانية محدودة مقارنة بدول إقليمية استطاعت ترسيخ منظومات متقدمة خلال العقد الأخير، ويعود هذا الموقع المتأخر للعراق إلى فجوات بنيوية في الإطار التشريعي والتنظيمي، وضعف الاستثمار في البنى التحتية الرقمية وبناء القدرات، في مقابل تبني دول أخرى سياسات سيبرانية شاملة انعكست إيجاباً على ترتيبها الدولي والإقليمي[٤٢].

وتتصدر المملكة العربية السعودية دول المنطقة في مؤشر GCI حيث صُنفت ضمن المستوى الأول (Tier 1 – Role Model)، نتيجة امتلاكها هيئة وطنية عليا للأمن السيبراني، واعتمادها استراتيجية وطنية شاملة تغطي القطاعات الحيوية كافة، إضافة إلى فرض معايير إلزامية على المؤسسات الحكومية والخاصة مما أسهم في بناء منظومة دفاع رقمي متقدمة وضعتها في مصاف الدول النموذجية عالمياً، كما جاءت الإمارات العربية المتحدة ضمن المستوى الأول (Tier 1) أيضاً مستندة إلى بنى تحتية رقمية حديثة، وأطر مؤسسية متخصصة، وبرامج ابتكار سيبراني متقدمة، فضلاً عن شراكات فعالة بين القطاعين العام والخاص عززت قدرتها على تحليل التهديدات والاستجابة لها[٤٣].

وفي السياق نفسه، حققت جمهورية مصر العربية موقعاً متقدماً ضمن المستوى الأول (Tier 1)بعد تبنيها استراتيجية وطنية للأمن السيبراني، وتأسيس مجلس أعلى مختص، وتطوير منظومة الاستجابة للحوادث، وإطلاق برامج تدريب واسعة لبناء الكوادر البشرية الأمر الذي مكّنها من تحسين ترتيبها الدولي رغم استمرار بعض التحديات القطاعية، كما جاء الأردن ضمن المستوى الأول (Tier 1)مستفيداً من تطور قطاع الاتصالات ووضوح الإطار الاستراتيجي للأمن السيبراني، إضافة إلى توفر خبرات بشرية متخصصة، وإن كانت محدودية الموارد المالية تشكل قيداً نسبياً على تنفيذ مشاريع وطنية كبرى[٤٤].

في المقابل بقي العراق في المستوى الرابع (Tier 4) وفق GCI ٢٠٢٤ وهو ما يعكس غياب قانون وطني شامل للأمن السيبراني، وتأخر إنشاء هيئة وطنية موحدة ذات صلاحيات إلزامية، إلى جانب ضعف التنسيق المؤسسي ونقص الكوادر المتخصصة والاستثمار التقني، ويكشف هذا التفاوت أن الفجوة بين العراق والدول المتقدمة سيبرانياً ليست تقنية فحسب لكن هي بالأساس فجوة حوكمة ورؤية استراتيجية، الأمر الذي

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

يستدعي إصلاحات تشريعية ومؤسسية وتنفيذية متكاملة إذا ما أراد العراق تحقيق قفزة نوعية وتحسين موقعه في المؤشرات الدولية مستقبلاً[٤٥].

تعود الفجوة بين العراق والدول المتقدمة في الأمن السيبراني إلى ثلاثة محاور رئيسية: التشريعات، القدرات التقنية، والموارد البشرية وتمثل هذه المحاور ركائز أساسية في المنظومة التي تعتمد عليها المؤشرات الدولية لتقييم جاهزية الدول وكل خلل في أحد هذه المحاور ينعكس بشكل مباشر على ترتيب الدولة ويضعها في مستويات متأخرة، ويمكن تفصيل هذه الفجوات من خلال الاتي[٤٦]:

١.تبدأ **الفجوة الأولى** من الجانب التشريعي إذ لا يمتلك العراق حتى الآن قانوناً وطنياً متكاملاً للأمن السيبراني وتعتمد الدولة على قوانين جزئية أو تعليمات تنظيمية غير ملزمة وهذا يؤدي إلى غياب إطار قانوني واضح يحدد مسؤوليات المؤسسات ويفرض معايير إلزامية للحماية بينما تعتمد دول المنطقة على قوانين متقدمة توفر حماية شاملة للبيانات وتحدد العقوبات المتعلقة بالجرائم الرقمية وتوضح طرق الاستجابة للهجمات وبسبب هذه الفجوة يفشل العراق في تلبية أحد أهم المعايير التي تعتمدها المؤشرات الدولية.

٢.أما **الفجوة التقنية** فتظهر في ضعف البنى التحتية الرقمية فالعراق يفتقر إلى مراكز بيانات وطنية متطورة، ولا يمتلك منظومة إنذار مبكر قادرة على رصد الهجمات كما أن كثيراً من المؤسسات الحكومية تعتمد على أنظمة تشغيل وبرمجيات قديمة وهذا يجعلها عرضة للاختراق ويؤدي إلى انخفاض قدرتها على حماية البيانات في المقابل تمتلك السعودية والإمارات وتركيا بنى تحتية حديثة تعتمد على تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة وهذا يمنحها قدرة عالية على مواجهة الهجمات ويرفع ترتيبها في المؤشرات الدولية[٤٧].

٣.وتتمثل **الفجوة الثالثة** في نقص الكوادر البشرية فالأمن السيبراني مجال تقني يحتاج إلى مهارات متقدمة في تحليل البرمجيات الخبيثة وإدارة الشبكات وتطوير الحلول الأمنية إلا أن العراق يعاني نقصاً حاداً في الخبراء المتخصصين كما تفتقر المؤسسات الحكومية إلى برامج تدريب مستمرة بينما تمتلك دول مثل الإمارات والسعودية مراكز تدريب وطنية وبرامج أكاديمية متخصصة وهذا يجعلها قادرة على تأمين كوادر عالية الكفاءة ويعد هذا العامل أحد أسباب ارتفاع ترتيب هذه الدول.

ويؤدي مجموع هذه الفجوات إلى تأثير مباشر على ترتيب العراق في المؤشرات الدولية فغياب التشريع ينعكس في ضعف النقاط التي يحصل عليها العراق في محور الحوكمة الوطنية وضعف البنى التحتية يؤدي إلى تراجع نقاط محور الجاهزية التقنية ونقص الكوادر يقلل من نقاط محور القدرات البشرية وعندما تتراكم هذه العوامل يظهر العراق في مستوى متأخر مقارنة بجيرانه[٤٨]، كما تؤثر هذه الفجوات في قدرة العراق على التعاون الدولي فالدول ذات الترتيب المتقدم تشارك عادة في مبادرات أمن سيبراني إقليمية وعالمية مما يمنحها دعماً فنياً ويساعدها في تحسين قدراتها أما العراق فيفتقر إلى المبادرات

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

الوطنية التي تشجع على التعاون الدولي وهذا يؤدي بدوره إلى ضعف منظومته وإلى تأخره في المؤشرات[٤٩].

ويتضح من التحليل أن العراق يحتاج إلى إصلاحات واسعة إذا أراد تقليص الفجوة مع الدول المتقدمة وتشمل هذه الإصلاحات إصدار قانون وطني موحد، وإنشاء هيئة عليا للأمن السيبراني، وتطوير منظومة تقنية حديثة، وإعداد برامج تدريبية متخصصة لبناء جيل جديد من الخبراء فهذه الخطوات الأساسية قادرة على رفع ترتيب العراق وتحسين موقعه في المؤشرات الدولية خلال فترة زمنية قصيرة.

رابعاً: آفاق تعزيز مكانة العراق في المؤشرات الدولية بعد ٢٠٢٥

يركّز هذا الموضوع على دراسة الإمكانات المتاحة لتطوير موقع العراق في المؤشرات الدولية للأمن السيبراني، من خلال تحديد أولويات الإصلاح واستكشاف المسارات التي يمكن أن تسهم في تعزيز الجاهزية السيبرانية على المدى المتوسط والبعيد، وسيتم تقسيم هذا الموضوع الى الاتي:

١.المتطلبات الأساسية لتحسين موقع العراق في المؤشرات الدولية

يمتلك العراق فرصة واسعة لتحسين موقعه في المؤشرات الدولية للأمن السيبراني بعد عام ٢٠٢٥، شرط تنفيذ مجموعة من الإصلاحات الجوهرية التي تعالج نقاط الضعف في البنى المؤسسية والتقنية والتشريعية وتعد هذه المتطلبات أساساً لا يمكن تجاوزه إذا أرادت الدولة تحقيق قفزة نوعية تضعها ضمن الدول المتقدمة في مجال الحماية الرقمية ويأتي في مقدمة هذه المتطلبات إصدار قانون وطني شامل للأمن السيبراني يتضمن تعريفات واضحة للجرائم الإلكترونية وآليات الاستجابة للحوادث الرقمية كما يجب أن ينص هذا القانون على تشكيل هيئة عليا تمتلك صلاحيات تنفيذية وإلزامية على مستوى الدولة، مما يسهم في توحيد الجهود وتجاوز حالة التشتت المؤسسي التي يعاني منها العراق منذ سنوات[٥٠].

ومن المتطلبات الأساسية تطوير منظومة الاستجابة للحوادث السيبرانية عبر إنشاء مركز وطني يعمل على مدار الساعة ويضم خبراء متخصصين في تحليل الهجمات ويمثل هذا المركز قاعدة لربط الوزارات والمؤسسات الحكومية بمنظومة موحدة تشرف على مراقبة الشبكات وتقديم الإنذار المبكر كما يجب أن يمتلك هذا المركز القدرة على تحليل البرمجيات الخبيثة وتقديم تقارير فورية عن الثغرات المكتشفة وهذا يمثل خطوة مهمة لرفع جاهزية العراق وفق معايير مؤشر (GCI) ومؤشر (NCSI) اللذين يمنحان نقاطاً كبيرة للدول التي تمتلك قدرات فعالة في الاستجابة للحوادث[٥١].

ويعد الاستثمار في البنى التحتية الرقمية أحد أهم المتطلبات فالعراق بحاجة إلى بناء مراكز بيانات وطنية حديثة تعتمد على تقنيات السحابة الحكومية وتوفر بيئات تخزين آمنة للبيانات الحكومية كما يتطلب تطوير شبكات اتصال ذات سرعة عالية لضمان عمل أنظمة الإنذار والتحليل بشكل مستقر ويمكن للعراق

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

أن يستفيد من مبادرات القطاع الخاص في هذا المجال عبر إنشاء شراكات استراتيجية تسهم في تسريع عملية التحديث[٥٢]، كما يحتاج العراق إلى رفع مستوى الكوادر الوطنية العاملة في القطاع السيبراني ويتحقق ذلك من خلال إنشاء برامج تدريبية طويلة الأمد بالتعاون مع الجامعات المحلية والدولية ويمكن تطوير مناهج أكاديمية تعالج موضوعات الأمن الرقمي وتحليل الهجمات والتشفير والإدارة التقنية كما يجب إنشاء مراكز تدريب وطنية توفر بيئة تقنية عالية تساعد المتدربين على اكتساب المهارات المتخصصة وتظهر التجارب الدولية أن الدول التي استثمرت في الكوادر استطاعت تحقيق قفزات ملحوظة في المؤشرات السيبرانية[٥٣].

أما من حيث السيناريوهات المحتملة لصعود العراق في المؤشرات الدولية بعد ٢٠٢٥ فيمكن تقديم ثلاثة سيناريوهات رئيسية يستند السيناريو الأول إلى الإصلاحات المتدرجة والمتوسطة، وفي هذا السيناريو يستطيع العراق تحسين موقعه تدريجياً ليصل إلى مستوى متوسط إقليمياً خلال عدة سنوات يتحقق ذلك بإقرار القوانين الأساسية وتطوير جزء من البنى التحتية وتحسين مستوى التنسيق بين المؤسسات بينما يبقى التقدم محدوداً في حال لم يتم الاستثمار بشكل واسع.

أما السيناريو الثاني فهو سيناريو الصعود السريع، ويقوم على تنفيذ إصلاحات شاملة خلال فترة قصيرة ويتضمن هذا السيناريو تأسيس هيئة وطنية للأمن السيبراني، وإنشاء مركز وطني للاستجابة للحوادث، وتحديث شامل للبنى الرقمية، وإطلاق برامج تدريبية واسعة وفي هذا السيناريو يمكن للعراق أن يحقق قفزة كبيرة في المؤشرات وأن يصل إلى مواقع قريبة من مصر وتركيا وربما يدخل ضمن المراتب المتقدمة إقليمياً خلال أقل من خمس سنوات[٥٤]

أما السيناريو الثالث فيمثل سيناريو الجمود أو التراجع، وهو السيناريو الممكن في حال لم تعالج نقاط الضعف المؤسسية والتشريعية وفي هذه الحالة يبقى العراق في نهاية سلم المؤشرات الإقليمية ويكون أكثر عرضة للهجمات السيبرانية وضعف الجاهزية التقنية ويؤثر هذا السيناريو في الاستقرار الاقتصادي والسياسي للدولة كما يحد من قدرة العراق على الاندماج في الاقتصاد الرقمي العالمي[٥٥].

ويعتمد ترجيح أحد هذه السيناريوهات على الإرادة السياسية وعلى حجم الاستثمار في القطاع السيبراني فالدول التي حققت تقدماً اعتمدت خططاً وطنية شاملة نفذتها مؤسسات مركزية قوية بينما تبقى الدول التي تعتمد على حلول جزئية غير قادرة على تحسين موقعها في المؤشرات.

٢.رؤية استراتيجية لتعزيز القدرة المؤسساتية والتكنولوجية للعراق

تتطلب الرؤية الاستراتيجية لرفع مكانة العراق في المؤشرات الدولية للأمن السيبراني بعد ٢٠٢٥ اعتماد منهج شامل ومتكامل يجمع بين الإصلاح المؤسسي والتمكين التقني وتطوير رأس المال البشري وتقوم هذه الرؤية على عدة محاور مترابطة تؤدي في مجموعها إلى بناء منظومة سيبرانية قوية تواكب التحولات العالمية وتحمي

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

مصالح الدولة، تتمثل هذه المحاور في الاتي[٥٦]:

١.المحور الأول يتمثل في توحيد الأطر المؤسسية عبر إنشاء "الهيئة الوطنية العليا للأمن السيبراني" التي تمتلك صلاحية وضع السياسات والإشراف على تنفيذها وتكون هذه الهيئة مسؤولة عن تنسيق الجهود بين وزارة الداخلية والأمن الوطني وهيئة الاتصالات ووزارة الدفاع وغيرها من المؤسسات ويمثل وجود قيادة موحدة خطوة أساسية لتجاوز حالة التشتت التي تعاني منها المنظومة الحالية كما يجب أن تكون الهيئة مسؤولة عن جمع المعلومات وتحليل التهديدات وتقديم التوصيات للحكومة، مما يجعلها مركز قيادة سيبرانية متكاملة.

٢.ويتمثل المحور الثاني في تطوير البنى التحتية الرقمية ويتضمن هذا بناء مراكز بيانات وطنية تعتمد على تقنيات الحوسبة السحابية الحكومية كما يتطلب تعزيز شبكات الاتصالات وتحديث الأنظمة التشغيلية المستخدمة في المؤسسات الحكومية ويمكن للعراق الاستفادة من تجارب دول مثل الإمارات وتركيا التي بنت مراكز رقمية متقدمة ساعدتها في تعزيز مكانتها في المؤشرات الدولية ويجب أن تلتزم المؤسسات الحكومية بمعايير موحدة لحماية البيانات لضمان الاتساق بين جميع القطاعات[٥٧].

٣.أما المحور الثالث فيتمثل في إطلاق برنامج وطني شامل لبناء القدرات البشرية ويشمل هذا إنشاء أكاديمية وطنية للأمن السيبراني تقدم برامج تدريب متخصصة في مجالات تحليل الهجمات والتشفير وإدارة الشبكات الرقمية كما يجب دمج موضوعات الأمن السيبراني في المناهج الجامعية وتوفير منح دراسية للطلاب المتفوقين في هذا المجال وتعتمد الدول المتقدمة على رأس المال البشري كعامل رئيسي في بناء منظومة سيبرانية قوية ولذلك يجب على العراق الاستثمار في الشباب والخبراء لتقليل الاعتماد على الشركات الأجنبية

٤.ويتمثل المحور الرابع في تعزيز التعاون الدولي فالأمن السيبراني مجال عالمي لا يمكن عزله عن البيئة الدولية ويجب على العراق الانخراط في المبادرات الإقليمية والدولية مثل برامج الاتحاد الدولي للاتصالات ومبادرات الأمن السيبراني العربية كما يجب تطوير شراكات مع الدول المتقدمة لنقل الخبرات والتكنولوجيا وبناء مراكز تدريب مشتركة ويؤدي هذا التعاون إلى رفع جاهزية العراق ويسهم في تحسين ترتيبه في المؤشرات العالمية[٥٨].

٥.ويركز المحور الخامس على تعزيز دور القطاع الخاص فالقطاع الخاص يمتلك خبرات تقنية واسعة يمكن للدولة أن تستفيد منها ويمكن للحكومة إنشاء شراكات مع شركات التكنولوجيا لتعزيز البنى التحتية وبناء منصات رقمية آمنة كما يجب فرض معايير إلزامية للأمن السيبراني على الشركات لتعزيز حماية البيانات الخاصة والعامة ومن خلال هذه الشراكات يمكن للعراق تحقيق تقدم كبير في مؤشرات الحماية الرقمية.

٦.أما المحور السادس فهو تعزيز الابتكار الوطني في المجال السيبراني عبر دعم الشركات الناشئة ومراكز الأبحاث المتخصصة في تطوير حلول أمنية ويمكن للحكومة توفير حواضن أعمال ومختبرات تقنية تساعد الشباب على

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

تطوير تطبيقات وأنظمة حماية محلية ويؤدي هذا إلى خلق اقتصاد رقمي متقدم يرفع من مكانة العراق في مؤشرات الجاهزية التقنية.

٧.**وتتطلب هذه الرؤية** اعتماد آليات متابعة دقيقة لضمان تنفيذها ويشمل ذلك إنشاء نظام قياس دوري للأداء يحدد مدى تقدم المؤسسات في تطوير قدراتها كما يجب إعداد تقارير سنوية ترفع إلى الحكومة تتضمن تقييمات مستقلة للجاهزية السيبرانية وهذا يعزز الشفافية ويساعد في اتخاذ القرارات المناسبة.

٨.**توفر هذه الرؤية الاستراتيجية** مساراً واضحاً للعراق ليصبح ضمن الدول الصاعدة في المؤشرات الدولية للأمن السيبراني وإذا تمكن العراق من تنفيذ هذه الخطوات بشكل منظم ومتدرج فإنه قادر على تحقيق صعود حقيقي ومستدام خلال السنوات القادمة[٥٩].

الخاتمة

تبين من خلال هذه الدراسة أن الأمن السيبراني أصبح عنصراً محورياً في بنية الأمن الوطني ومعادلات القوة المعاصرة، وأن المؤشرات الدولية مثل GCI وNCSI تمثل أدوات أساسية لقياس جاهزية الدول في حماية فضائها الرقمي، حيث أظهرت التجارب المقارنة أن التقدم في هذه المؤشرات يرتبط بتكامل التشريع والبنية المؤسسية والتقنية وبناء القدرات البشرية ضمن رؤية استراتيجية واضحة، وفي ضوء ذلك يتبين أن تأخر ترتيب العراق يعود إلى فجوات تشريعية ومؤسسية وتقنية وتشتت الجهود أكثر من كونه نقصاً في الإمكانات، الأمر الذي يتيح للعراق فرصة واقعية لتحسين موقعه بعد عام ٢٠٢٥ عبر تبني إصلاحات شاملة تضع الأمن السيبراني في صلب مشروع الدولة لحماية السيادة وتعزيز التنمية والاندماج في الاقتصاد الرقمي العالمي.

الاستنتاجات

أظهرت الدراسة أن الأمن السيبراني لم يعد مجالاً تقنياً محدوداً بل أصبح عنصراً أساسياً في حماية الاستقرار السياسي وحفظ السيادة الرقمية وضمان استمرار عمل القطاعات الحيوية في الدولة.

١.بيّنت نتائج البحث أن مؤشرات مثل GCI و NCSI لا تقيس الجوانب التقنية فقط بل تشمل الأطر القانونية والمؤسسية والقدرات البشرية، وأن موقع الدول في هذه المؤشرات بات يؤثر في صورتها الدولية وجاذبيتها الاستثمارية.

٢.أظهرت المقارنة مع السعودية والإمارات ومصر والأردن أن العراق ما يزال في مرتبة متأخرة في المؤشرات الدولية، بينما حققت هذه الدول قفزات واضحة نتيجة سياسات سيبرانية متماسكة واستثمارات واسعة في هذا المجال.

٣.تبيّن أن العراق يفتقر إلى قانون وطني شامل للأمن السيبراني وإلى تشريعات متكاملة لحماية البيانات الشخصية، وأن الاعتماد على قوانين العقوبات التقليدية والتعليمات الجزئية لا ينسجم مع طبيعة التهديدات الرقمية المعاصرة.

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

٤.أظهر تحليل البنية المؤسسية أن أدوار وزارة الداخلية والأمن الوطني وهيئة الإعلام والاتصالات ووزارات أخرى ما تزال متداخلة وغير منسقة، وأن غياب هيئة وطنية عليا يساهم في تشتت الجهود وضعف الاستجابة للهجمات.

٥.بيّنت الدراسة أن اعتماد المؤسسات على أنظمة قديمة، وغياب مركز وطني للاستجابة للحوادث، وضعف مراكز البيانات والإنذار المبكر، كلها عوامل تُبقي العراق في موقع متأخر في المؤشرات الدولية للأمن السيبراني.

٦.إن موقع العراق قابل للتحسن في حال تنفيذ إصلاحات تشريعية ومؤسسية وتقنية وبشرية، وأن الانتقال من سيناريو الجمود إلى سيناريو الصعود يتوقف على الإرادة السياسية وحجم الاستثمار في القطاع السيبراني.

التوصيات

توصي الدراسة بالإسراع في تشريع قانون متكامل للأمن السيبراني يتضمن تعريف الجرائم الرقمية وآليات التحقيق والعقاب، ويشمل فصلاً خاصاً بحماية البيانات الشخصية بما ينسجم مع المعايير الدولية.

١.توصي بإنشاء هيئة مستقلة ذات صلاحيات تنفيذية وإلزامية تشرف على وضع السياسات الوطنية وتنسيق أدوار وزارة الداخلية والأمن الوطني والدفاع وهيئة الاتصالات وبقية المؤسسات ذات العلاقة.

٢.توصي بإنشاء مركز وطني يعمل على مدار الساعة لمراقبة الشبكات الحكومية وتحليل التهديدات وتقديم إنذار مبكر، وربطه بجميع الوزارات والهيئات الحيوية ضمن منظومة موحدة.

٣.توصي بتحديث الأنظمة التشغيلية واعتماد مراكز بيانات وطنية تعتمد على الحوسبة السحابية الحكومية، وبناء شبكة اتصالات آمنة تدعم أنظمة المراقبة والتحليل والنسخ الاحتياطي الفوري.

٤.توصي بتبني برامج تدريب طويلة الأمد بالتعاون مع الجامعات المحلية والدولية، وإدماج تخصصات الأمن السيبراني في المناهج الجامعية، وتقديم حوافز لاستبقاء الكفاءات في المؤسسات الحكومية.

٥.توصي بوضع أطر معيارية وطنية لأمن المعلومات تلزم بها الوزارات والشركات، خاصة في قطاعات الاتصالات والمال والطاقة والصحة، مع آليات رقابة وتقييم دوري.

٦.توصي بانخراط العراق في مبادرات الاتحاد الدولي للاتصالات والمنصات العربية والإقليمية للأمن السيبراني، وتوقيع مذكرات تفاهم مع الدول المتقدمة لنقل الخبرة وبناء برامج تدريب مشتركة.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

الهوامش

(١) خالد عبد الرحمن العزي، الأمن السيبراني وأبعاده الاستراتيجية، ط١، دار الرشاد للنشر، عمّان، ٢٠١٩، ص٥٥.

(٢) حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العاق في الفضاء السيبراني: مقاربة بين المعضلة الأمنية والمكنة الادائية، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الوادي، الجزائر، العدده، ٢٠٢٠، ص٥٥١.

(٣) عبد الرحمن شحاتة، الأمن الرقمي في عصر المعلومات، ط١، مركز دراسات المستقبل، القاهرة، ٢٠٢٠، ص١١٢.

(٤) ماجد جاسم السعدي، الحروب السيبرانية وتحولات القوة، ط١، دار غيداء للنشر، عمّان، ٢٠٢١، ص٨٧.

(٥) سليم دحماني، اثر التهديدات السيبرانية على الامن القومي الولايات المتحدة الامريكية انموذجا ٢٠٢١-٢٠١٧، رسالة ماجستير (غير منشورة)، جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٤١-٤٢.

(٦) أسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، مجلة العلوم القانونية والسياسية ، ، العدد (١) ، جامعة محمد بوضياف المسلة، الجزائر، ٢٠١٩، ص١٠-٢٢.

(٧) سالم محمد الزبيدي، الأمن السيبراني وإدارة المخاطر الرقمية، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٨، ص٢٠٣.

(٨) خالد نجيب المصري، الحرب الرقمية وتوازنات القوة، ط١، دار العبيكان للنشر، الرياض، ٢٠٢١، ص٧٢.

(٩) فريد عبد النبي حسن، التحول الرقمي والأمن السيبراني في دول الشرق الأوسط، ط١، المركز العربي للأبحاث، بيروت، ٢٠٢١، ص١٤٤.

(١٠) فاطمة محمد القيسي، الأمن الرقمي وتحديات ما بعد الجائحة، ط١، دار الفكر الجامعي، القاهرة، ٢٠٢٢، ص٧٧.

(١١) وليد عبد الجبار الربيعي، الذكاء الاصطناعي والأمن الوطني، ط١، دار الأكاديميون للنشر، عمّان، ٢٠٢١، ص١٢١.

(١٢) عمار محمد المشهداني، التهديدات غير المتناظرة وحرب الفضاء السيبراني، ط١، مركز الدراسات الاستراتيجية – الجامعة الأردنية، عمّان، ٢٠٢١، ص١٥٩.

(١٣) علي حسين مشتت، الثورة الصناعية الرابعة والأمن الوطني، ط١، بيت الحكمة، بغداد، ٢٠٢١، ص١٠١.

(١٤) ريم عبد الله المحيسن، المخاطر السيبرانية في المؤسسات الحكومية، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٢٠، ص٨٨.

(١٥) ناصر عبد الخالق، إدارة الأزمات الرقمية وأمن الفضاء الإلكتروني، ط١، دار أسامة للنشر، عمّان، ٢٠٢٢، ص١٣٥.

(١٦) مصطفى سلمان منسي، تأثير الحكومة الالكترونية في اداء المنظمات « دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة / مديرية تسجيل المركبات واجازات السياقة «، جامعة كربلاء – كلية الادارة والاقتصاد، رسالة دبلوم،٢٠٢٢، ص٤٠.

(١٧) الاتحاد الدولي للاتصالات، تقرير مؤشر الأمن السيبراني العالمي GCI، ط١، ITU Publications، جنيف، ٢٠٢١، ص٢١٠.

(١٨) مروان سالم العلي، رؤية استراتيجية تحليلية لواقع الحوكمة الرقمية في العراق (التحديات والفرص)، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص٨٦.

(١٩) إيمان أحمد علي، الحماية التشريعية للحق في الخصوصية في العصر الرقمي؛ مجلة كلية الشريعة والقانون بطنطا، ٢٠٢٢، العدد ٣٦، ص٧٤.

(٢٠) هيئة الأمن السيبراني الإستونية، دليل مؤشر NCSI للجاهزية الوطنية، ط١، وزارة الاقتصاد الرقمي، تالين، ٢٠٢٠، ص٥٥.

(٢١) أماندا كلوفر، تقييم القدرات الوطنية للأمن السيبراني، ط١، مركز الدراسات الأوروبية، بروكسل، ٢٠١٩، ص٧٣.

(٢٢) يونس مؤيد يونس مصطفى، العراق بين ضرورات التحول الرقمي وتحديات المحافظة على امنه الوطني، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص١٢٣-١٢٤.

(٢٣) قاسم عبد الرضا شغيت، الأمن السيبراني اوكسجين التحول الرقمي العراقي، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص٥٣.

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

(٢٤) مروان سالم العلي (واخرون)، الحوكمة الرشيدة وإدارة المؤسسات الدستورية في الدولة العراقية: التحديات والمعالجات، ط١، شركة الأكاديميون للنشر، عمان،٢٠٢٢، ص٢٦٦-٢٧٨.

(٢٥)محمد عبد الرازق، الفجوة الرقمية والسياسات السيبرانية العربية، ط١، مركز رؤية للدراسات، القاهرة، ٢٠٢١، ص١٠٠.

(٢٦) خالد العتيبي، تحليل مؤشر الجاهزية السيبرانية في الدول الخليجية، ط١، دار جامعة الملك سعود للنشر، الرياض، ٢٠٢٠، ص٦٤.

(٢٧) سعيد بن علي بن حسن المعمري ورضوان أحمد الحاف، مبدأ الامن القانوني ومقومات الجودة التشريعية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٧٩، ٢٠٢٢، ص ص٥٣.

(٢٨) حيدر حسن صافي الجبوري، دراسة تحليلية وحلول منطقية لتطبيق مشروع الحكومة الالكترونية في العراق « رؤية شاملة»، الجامعة المستنصرية – كلية التربية الاساسية، العدد ٧٦، ٢٠١٢، ص ١١.

(٢٩) طلال ناظم الزُهيري ، مُبادرات الحوكمة الالكترونية في العِراق وعوامل نجاحها، مجلة الحوكمة: المسؤولية الاجتماعية والتنمية المستدامة، المجلد٥، العدد١، كُلية العلوم الاقتصادية التجارية، الجزائر، اذار/مارس٢٠٢٣، ص٢٥-٢٨.

(٣٠) سارة محمد جواد، المؤشرات الدولية في الأمن المعلوماتي، ط١، دار اليازوري للنشر، عمّان، ٢٠٢١، ص١٣٢.

(٣١) مصطفى سلمان منسي، تأثير الحكومة الالكترونية في أداء المنظمات دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة / مديرية تسجيل المركبات وإجازات السياقة، رسالة ماجستير، غير منشورة، جامعة كربلاء، كلية الإدارة والاقتصاد، كلية إدارة الاعمال، ٢٠٢٢، ص٤٠.

(٣٢)جهاد البستاني، الأمن السيبراني ومؤشرات التنمية الرقمية، ط١، دار الرافدين، بيروت، ٢٠٢٢، ص٥٩.

(٣٣) محمد مصطفى القصيمي، ايمان مرعي حسن، متطلبات تطبيق الحكومة الالكترونية في المنظمات العراقية «دراسة استطلاعية لإراء القيادات الادارية في مديرية بلدية الموصل «، العراق – الموصل، مجلة تنمية الرافدين، ملحق العدد ١١٣، المجلد ٣٥، ٢٠١٣، ص١٧.

(٣٤) طلال ناظم الزُهيري، مُبادرات الحوكمة الالكترونية في العِراق وعوامل نجاحها، مصدر سبق ذكره، ص٣٣.

(٣٥) هشام خليل، مؤشرات التنافسية الرقمية في الشرق الأوسط، ط١، مركز دراسات الخليج، الدوحة، ٢٠٢١، ص٨٢.

(٣٦)ضياء كريم صالح، التحديات الأمنية غير التقليدية وانعكاساتها على الامن الوطني العراقي (التحديات السيبرانية انموذجاً)، رسالة ماجستير، غير منشورة، معهد العلمين للدراسات العليا، النجف الاشرف، ٢٠٢٤، ص٥٠.

(٣٧) المجلس الأوروبي للأمن السيبراني، مراجعة السياسات الرقمية الأوروبية، ط١، بروكسل، ٢٠٢٢، ص١٤٤.

(٣٨) هشام خليل، مؤشرات التنافسية الرقمية في الشرق الأوسط، مصدر سبق ذكره، ص٨٣.

(٣٩) ضياء كريم صالح، التحديات الأمنية غير التقليدية وانعكاساتها على الامن الوطني العراقي (التحديات السيبرانية انموذجاً)، مصدر سبق ذكره، ص٥٤.

(٤٠) يونس مؤيد يونس مصطفى، العراق بين ضرورات التحول الرقمي وتحديات المحافظة على امنه الوطني، مصدر سبق ذكره، ص١٢٩.

(٤١) مؤشر الأمن السيبراني العالمي (GCI ٢٠٢٤) هو مؤشر دولي يصدر عن الاتحاد الدولي للاتصالات (ITU) لقياس مستوى التزام الدول وجاهزيتها في مجال الأمن السيبراني. ويعتمد على تقييم الأطر القانونية والمؤسسية والتقنية وبناء القدرات والتعاون الدولي، ويصنّف الدول ضمن مستويات أداء تعكس درجة نضج منظوماتها السيبرانية، للمزيد ينظر: International Telecommunication Union (ITU), Global Cybersecurity Index 2024: 5th Edition, ITU Publications, Geneva, 2024, p. 27 (Tier Performance: Arab States).

الرابط:

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

(٤٢) صبـاح مهدي الياسـري، الإطار القانوني للأمن السـيبراني العربي، ط١، بيت الحكمة، بغداد، ٢٠٢٠، ص٦١.

(٤٣) مـنى عبد الله السـمحان، متطلبات تحقيق الامن السـيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (١١١)، (مصر: ٢٠٢٢)، ص٩.

(٤٤)منى الاشـقر جبور، الامن السيبراني: التحديات ومستلزمات المواجهة، جامعة الـدول العربية، المركز العربي للبحوث القانونية والقضائية، ٢٠١٢، ص٧-٨.

(٤٥) زهير خضير عباس وظفر عبد مطر، العراق والامن السـيبراني الفرص والتحديات، مجلة واسـط للعلوم الانسانية والاجتماعية، جامعة واسـط، المجلد (١٨)، العـدد (٥١)، العراق، ٢٠٢٢، ص١٣.

(٤٦) حسن علي السامرائي، التهديدات السيبرانية وتأثيرها في الأمن الوطني، ط١، دار أمجد للنشر، عمّان، ٢٠٢٢، ص٤٤.

(٤٧) علي فاضل الساعدي، نظم الإنذار المبكر السيبراني، ط١، دار المعرفة الجامعية، القاهرة، ٢٠٢١، ص٦٦.

(٤٨) المجلس الأعلى للأمن السيبراني المصري، دليل الجاهزية الوطنية، ط١، القاهرة، ٢٠٢١، ص٥٨.

(٤٩) هاني يوسـف الكبيسي، الأمن الوطني في البيئة الرقمية، ط١، مركز البيان للدراسات والتخطيط، بغداد، ٢٠٢١، ص٩٣.

(٥٠) عبدالرحمن محمد عيسى، الحوكمة الرقمية والحد من الفساد في العراق بعد عام ٢٠٠٣، أطروحة دكتوراه (غير منشـورة)، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٥، ص١٢٨.

(٥١)يوسـف أحمد الخطاب، القوة السيبرانية في العلاقات الدولية، ط١، دار صفحات للدراسـات والنشـر، دمشـق، ٢٠٢٠، ص٦٣.

(٥٢) برنامج الأمم المتحدة الإنمائي، التحول الرقمي والتنمية، ط١، نيويورك، ٢٠٢١، ص٧٨.

(٥٣)عبد الله بن صالح المالكي، الأمن السـيبراني في رؤية ٢٠٣٠، ط١، مركز البحوث الأمنية، الرياض، ٢٠٢٠، ص٩٨.

(٥٤)محمد هيثم العتوم، الجرائم الإلكترونية والأمن المعلوماتي، ط١، دار المسيرة للنشر، عمّان، ٢٠٢٠، ص١٣٠.

(٥٥) البنـك الـدولي، الجاهزيـة الرقمية في الدول الهشـة، ط١، واشنطن، ٢٠٢٢، ص١٢٢.

(٥٦)فهد الحربي، بناء القدرات الوطنية في الأمن السـيبراني، ط١، مركز الأبحاث الأمنية، الرياض، ٢٠٢٠، ص٩١.

(٥٧) عبدالرحمن محمد عيسى، الحوكمة الرقمية والحد من الفساد في العراق بعد عام ٢٠٠٣، مصدر سبق ذكره، ص١٣١.

(٥٨) زينة الربيعي، مسـتقبل الأمن السيبراني في العراق، ط١، بيت الحكمة، بغداد، ٢٠٢٢، ص٦٨.

(٥٩) محمد فوزي، اسـتراتيجيات الصعود الرقمي للدول، ط١، دار العين، القاهرة، ٢٠٢١، ص١٣٤.

قائمة المصادر والمراجع

١.الاتحاد الدولي للاتصالات، تقرير مؤشر الأمن السيبراني العالمي GCI، ط١، ITU Publications، جنيف، ٢٠٢١، ص٢١٠.

٢.أسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، مجلة العلوم القانونية والسياسية ، العدد (١) ، جامعة محمد بوضياف المسلة، الجزائر، ٢٠١٩، ص١٠-٢٢.

٣.أماندا كلوفر، تقييم القدرات الوطنية للأمن السيبراني، ط١، مركز الدراسات الأوروبية، بروكسل، ٢٠١٩، ص٧٣.

٤.إيمان أحمد علي، الحماية التشريعية للحق في الخصوصية في العصر الرقمي؛ مجلة كلية الشريعة والقانون بطنطا، ٢٠٢٢، العدد ٣٦، ص٧٤.

٥.برنامج الأمم المتحدة الإنمائي، التحول الرقمي والتنمية، ط١، نيويورك، ٢٠٢١، ص٧٨.

٦.البنك الدولي، الجاهزية الرقمية في الدول

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

الهشة، ط١، واشنطن، ٢٠٢٢، ص١٢٢.

٧.جهاد البستاني، الأمن السيبراني ومؤشرات التنمية الرقمية، ط١، دار الرافدين، بيروت، ٢٠٢٢، ص٥٩.

٨.حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العاق في الفضاء السيبراني: مقاربة بين المعضلة الأمنية والمكنة الادائية، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الوادي، الجزائر، العدد٥، ٢٠٢٠، ص٥٥١.

٩.حسن علي السامرائي، التهديدات السيبرانية وتأثيرها في الأمن الوطني، ط١، دار أمجد للنشر، عمّان، ٢٠٢٢، ص٤٤.

١٠.حيدر حسن صافي الجبوري، دراسة تحليلية وحلول منطقية لتطبيق مشروع الحكومة الالكترونية في العراق «رؤية شاملة»، الجامعة المستنصرية – كلية التربية الاساسية، العدد ٧٦، ٢٠١٢، ص ١١.

١١.خالد العتيبي، تحليل مؤشر الجاهزية السيبرانية في الدول الخليجية، ط١، دار جامعة الملك سعود للنشر، الرياض، ٢٠٢٠، ص٦٤.

١٢.خالد عبد الرحمن العزي، الأمن السيبراني وأبعاده الاستراتيجية، ط١، دار الرشاد للنشر، عمّان، ٢٠١٩، ص٥٥.

١٣.خالد نجيب المصري، الحرب الرقمية وتوازنات القوة، ط١، دار العبيكان للنشر، الرياض، ٢٠٢١، ص٧٢.

١٤.الرابط:

١٥.ريم عبد الله المحيسن، المخاطر السيبرانية في المؤسسات الحكومية، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٢٠، ص٨٨.

١٦.زهير خضير عباس وظفر عبد مطر، العراق والامن السيبراني الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط، المجلد (١٨)، العدد (٥١)، العراق، ٢٠٢٢، ص١٣.

١٧.زينة الربيعي، مستقبل الأمن السيبراني في العراق، ط١، بيت الحكمة، بغداد، ٢٠٢٢، ص٦٨.

١٨.سارة محمد جواد، المؤشرات الدولية في الأمن المعلوماتي، ط١، دار اليازوري للنشر، عمّان، ٢٠٢١، ص١٣٢.

١٩.سالم محمد الزبيدي، الأمن السيبراني وإدارة المخاطر الرقمية، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٨، ص٢٠٣.

٢٠.سعيد بن علي بن حسن المعمري ورضوان أحمد الحاف، مبدأ الامن القانوني ومقومات الجودة التشريعية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٧٩، ٢٠٢٢، ص ص٥٣.

٢١.سليم دحماني، اثر التهديدات السيبرانية على الامن القومي الولايات المتحدة الامريكية انموذجا ٢٠٢١-٢٠١٧، رسالة ماجستير (غير منشورة)، جامعة محمد بوضياف – المسيلة،

مجلَّة نصف سنوية محكَّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٤١-٤٢.

٢٢.صباح مهدي الياسري، الإطار القانوني للأمن السيبراني العربي، ط١، بيت الحكمة، بغداد، ٢٠٢٠، ص٦١.

٢٣.ضياء كريم صالح، التحديات الأمنية غير التقليدية وانعكاساتها على الامن الوطني العراقي (التحديات السيبرانية انموذجاً)، رسالة ماجستير، غير منشورة، معهد العلمين للدراسات العليا، النجف الاشرف، ٢٠٢٤، ص٥٠.

٢٤.ضياء كريم صالح، التحديات الأمنية غير التقليدية وانعكاساتها على الامن الوطني العراقي (التحديات السيبرانية انموذجاً)، مصدر سبق ذكره، ص٥٤.

٢٥.طلال ناظم الزُهيري ، مُبادرات الحوكمة الالكترونية في العِراق وعوامل نجاحها، مجلة الحوكمة: المسؤولية الاجتماعية والتنمية المُستدامة، المُجلد٥، العدد١، كُلية العلوم الاقتصادية التجارية، الجزائر، اذار/ مارس٢٠٢٣، ص٢٥-٢٨.

٢٦.طلال ناظم الزُهيري، مُبادرات الحوكمة الالكترونية في العِراق وعوامل نجاحها، مصدر سبق ذكره، ص٣٣.

٢٧.عبد الرحمن شحاتة، الأمن الرقمي في عصر المعلومات، ط١، مركز دراسات المستقبل، القاهرة، ٢٠٢٠، ص١١٢.

٢٨.عبد الله بن صالح المالكي، الأمن السيبراني في رؤية ٢٠٣٠، ط١، مركز البحوث الأمنية، الرياض، ٢٠٢٠، ص٩٨.

٢٩.عبدالرحمن محمد عيسى، الحوكمة الرقمية والحد من الفساد في العراق بعد عام ٢٠٠٣، أطروحة دكتوراه (غير منشورة)، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٥، ص١٢٨.

٣٠.عبدالرحمن محمد عيسى، الحوكمة الرقمية والحد من الفساد في العراق بعد عام ٢٠٠٣، مصدر سبق ذكره، ص١٣١.

٣١.علي حسين مشتت، الثورة الصناعية الرابعة والأمن الوطني، ط١، بيت الحكمة، بغداد، ٢٠٢١، ص١٠١.

٣٢.علي فاضل الساعدي، نظم الإنذار المبكر السيبراني، ط١، دار المعرفة الجامعية، القاهرة، ٢٠٢١، ص٦٦.

٣٣.عمار محمد المشهداني، التهديدات غير المتناظرة وحرب الفضاء السيبراني، ط١، مركز الدراسات الاستراتيجية – الجامعة الأردنية، عمّان، ٢٠٢١، ص١٥٩.

٣٤.فاطمة محمد القيسي، الأمن الرقمي وتحديات ما بعد الجائحة، ط١، دار الفكر الجامعي، القاهرة، ٢٠٢٢، ص٧٧.

٣٥.فريد عبد النبي حسن، التحول الرقمي والأمن السيبراني في دول الشرق الأوسط، ط١، المركز العربي للأبحاث، بيروت، ٢٠٢١، ص١٤٤.

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

٣٦.فهد الحربي، بناء القدرات الوطنية في الأمن السيبراني، ط١، مركز الأبحاث الأمنية، الرياض، ٢٠٢٠، ص٩١.

٣٧.قاسم عبد الرضا شغيت، الأمن السيبراني اوكسجين التحول الرقمي العراقي، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص٥٣.

٣٨.ماجد جاسم السعدي، الحروب السيبرانية وتحولات القوة، ط١، دار غيداء للنشر، عمّان، ٢٠٢١، ص٨٧.

٣٩.المجلس الأعلى للأمن السيبراني المصري، دليل الجاهزية الوطنية، ط١، القاهرة، ٢٠٢١، ص٥٨.

٤٠.المجلس الأوروبي للأمن السيبراني، مراجعة السياسات الرقمية الأوروبية، ط١، بروكسل، ٢٠٢٢، ص١٤٤.

٤١.محمد عبد الرازق، الفجوة الرقمية والسياسات السيبرانية العربية، ط١، مركز رؤية للدراسات، القاهرة، ٢٠٢١، ص١٠٠.

٤٢.محمد فوزي، استراتيجيات الصعود الرقمي للدول، ط١، دار العين، القاهرة، ٢٠٢١، ص١٣٤.

٤٣.محمد مصطفى القصيمي، ايمان مرعي حسن، متطلبات تطبيق الحكومة الالكترونية في المنظمات العراقية «دراسة استطلاعية لإراء القيادات الادارية في مديرية بلدية الموصل «، العراق – الموصل، مجلة تنمية الرافدين، ملحق العدد ١١٣، المجلد ٣٥، ٢٠١٣، ص١٧.

٤٤.محمد هيثم العتوم، الجرائم الإلكترونية والأمن المعلوماتي، ط١، دار المسيرة للنشر، عمّان، ٢٠٢٠، ص١٣٠.

٤٥.مروان سالم العلي (واخرون)، الحوكمة الرشيدة وإدارة المؤسسات الدستورية في الدولة العراقية: التحديات والمعالجات، ط١، شركة الأكاديميون للنشر، عمان،٢٠٢٢، ص٢٦٦-٢٧٨.

٤٦.مروان سالم العلي، رؤية استراتيجية تحليلية لواقع الحوكمة الرقمية في العراق (التحديات والفرص)، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص٨٦.

٤٧.مصطفى سلمان منسي، تأثير الحكومة الالكترونية في اداء المنظمات « دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة / مديرية تسجيل المركبات واجازات السياقة «، جامعة كربلاء – كلية الادارة والاقتصاد، رسالة دبلوم،٢٠٢٢، ص٤٠.

٤٨.مصطفى سلمان منسي، تأثير الحكومة الالكترونية في أداء المنظمات دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة / مديرية تسجيل المركبات وإجازات السياقة، رسالة ماجستير، غير منشورة، جامعة كربلاء، كلية الإدارة والاقتصاد، كلية إدارة الاعمال، ٢٠٢٢، ص٤٠.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات القانونية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات قانونية
في دار الكتب والوثائق ٦٨٢ لسنة ١٩٩٩
رقم الإيداع الدولي ISSN 2223-8190

٤٩.منى الاشقر جبور، الامن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، ٢٠١٢، ص٧-٨.

٥٠.منى عبد الله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (١١١)، (مصر: ٢٠٢٢)، ص٩.

٥١.ناصر عبد الخالق، إدارة الأزمات الرقمية وأمن الفضاء الإلكتروني، ط١، دار أسامة للنشر، عمّان، ٢٠٢٢، ص١٣٥.

٥٢.هاني يوسف الكبيسي، الأمن الوطني في البيئة الرقمية، ط١، مركز البيان للدراسات والتخطيط، بغداد، ٢٠٢١، ص٩٣.

٥٣.هشام خليل، مؤشرات التنافسية الرقمية في الشرق الأوسط، ط١، مركز دراسات الخليج، الدوحة، ٢٠٢١، ص٨٢.

٥٤.هشام خليل، مؤشرات التنافسية الرقمية في الشرق الأوسط، مصدر سبق ذكره، ص٨٣.

٥٥.هيئة الأمن السيبراني الإستونية، دليل مؤشر NCSI للجاهزية الوطنية، ط١، وزارة الاقتصاد الرقمي، تالين، ٢٠٢٠، ص٥٥.

٥٦.وليد عبد الجبار الربيعي، الذكاء الاصطناعي والأمن الوطني، ط١، دار الأكاديميون للنشر، عمّان، ٢٠٢١، ص١٢١.

٥٧.يوسف أحمد الخطاب، القوة السيبرانية في العلاقات الدولية، ط١، دار صفحات للدراسات والنشر، دمشق، ٢٠٢٠، ص٦٣.

٥٨.يونس مؤيد يونس مصطفى، العراق بين ضرورات التحول الرقمي وتحديات المحافظة على امنه الوطني، مجلة فرسان الرد السريع للدراسات الأمنية، العدد (٢)، فرقة الرد السريع، وزارة الداخلية العراقية، ٢٠٢٤، ص١٢٣-١٢٤.

٥٩.يونس مؤيد يونس مصطفى، العراق بين ضرورات التحول الرقمي وتحديات المحافظة على امنه الوطني، مصدر سبق ذكره، ص١٢٩.

Semi-annual Quarterly journal issued by Department of law Studies In Bayt Al-Hikma
No.of deposit at Library and Archives(694)1999
ISSN.2223-8190
Info@baytalhikma.iq

Iraq's Position in International Cybersecurity Indicators After 2020

A Comparative Analytical Study

Lect.Dr.Alaa AbdulRazaq Abdul Qader(*)

Abstract

This study examines Iraq's position in international cybersecurity indicators after 2020 as a proxy for national readiness to protect the digital domain and critical infrastructure amid accelerated digital transformation. Using a comparative analytical approach, it links the conceptual foundations of cybersecurity to the measurement logic of key international benchmarks, particularly the Global Cybersecurity Index (GCI), the National Cyber Security Index (NCSI), and ITU assessment frameworks. The study diagnoses Iraq's cybersecurity capacity across legal, institutional, technical, and human-capital dimensions, highlighting structural gaps that constrain performance: the absence of a comprehensive national cybersecurity law, fragmented mandates and coordination, limited incident response and early-warning capabilities, aging digital infrastructure, and shortages of specialized expertise.

(*) Ministry Of Education