ورقة سياسات

مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

الأمن السيبراني وحماية الاقتصاد العراقي
التهديدات السيبرانية واستراتيجيات المواجهة

د. نسرين رياض شنشول
د. أنور حامد حمد

سلسلة اصدارات مركز البيان للدراسات والتخطيط

مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

الأمن السيبراني وحماية الاقتصاد العراقي: التهديدات السيبرانية واستراتيجيات المواجهة

سلسلة اصدارات مركز البيان للدراسات والتخطيط / قسم الابحاث / الدراسات الاقتصادية

الاصدار / ورقة سياسات

الموضوع / الاقتصاد والتنمية، مكافحة التطرف والإرهاب

د. نسرين رياض شنشول/العلاقات الاقتصادية الدولية:كلية العلوم السياسية-جامعة النهرين
د. أنور حامد حمد/العلاقات الاقتصادية الدولية: كلية العلوم السياسية- جامعة النهرين

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌ، غيرُ ربحيٍّ، مقرُّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ، ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليلٍ مستقلٍّ، وإيجاد حلول عملية جليّة لقضايا معقدة تهمُّ الحقليْنِ السياسي والأكاديمي.

ملحوظة:

لا تعبّر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز، وإنّما تعبّر عن رأي كتابِها.

www.bayancenter.org
info@bayancenter.org
Since 2014

I. الملخص:

- منذ العام 2021، بدأت المؤشرات تعطي دلالات على ان العراق يتراجع في المؤشر العالمي للأمن السيبرانيGlobal Cybersecurity Index الصادر عن الاتحاد الدولي للاتصالات، وهذا يؤشر ان العراق يواجه تحديات في الهياكل التنظيمية للأمن السيبراني العراقي.

- العراق يُصنّف ضمن البلدان الناشئة (Nascent) في استخدام التقنيات لمواجهة الجريمة السيبرانية. ووفقاً لتطلعات العراق للتكامل الاقتصادي مع العالم، فإن ضعف البيئة التنظيمية في مجال مواجهة هذا النوع من الجرائم يعتبر من بين العوامل الرئيسية التي تعيق دخول العراق إلى المنصات العالمية للتبادل الرقمي، إلى جانب مخاوف الجهات الأجنبية المستثمرة من الدخول إلى السوق العراقي، خاصة في المشروعات ذات الاستخدام الرقمي والتكنولوجي المتقدم.

- لا يمكن معالجة وحوكمة الأزمات الهيكلية التي يعاني منها العراق، مثل الرقابة الصحية، والتدهور المناخي، وتوزيع المياه، وقياس مستويات التلوث، وتوسيع الشمول المالي، وغيرها من العناصر المساهمة في تحقيق التنمية المستدامة، ما لم يتم بناء منظومة رقمية محمية وقادرة على العمل بمستوى عالٍ من الموثوقية.

- يحتاج العراق إلى اتخاذ خطوات جادة في بناء الحكومة الإلكترونية، تشمل تطوير البنية التحتية الرقمية، وتعزيز الأمن السيبراني، واتخاذ تدابير أمنية فعّالة لمنع الاختراقات والوصول غير المصرح به إلى البيانات والحقوق.

- العراق بحاجة إلى اتخاذ تدابير لتبني تطبيقات حديثة، مثل تقنيات البلوكشين (Blockchain)، التي توفّر مستوى عالٍ من الأمان في التعاملات المالية من خلال تشفير البيانات ومنع التلاعب بها. ويمكن استخدام هذه التقنيات في حماية المدفوعات الرقمية، والعقود الذكية، والمعاملات المصرفية.

- تطوير أدوات استخدام الذكاء الاصطناعي في ابتكار حلول تتفاعل مع النظام البيئي التنظيمي، وتحليل البيانات الضخمة، واكتشاف الأنشطة المشبوهة في الأنظمة المالية، من شأنه أن يعزّز قدرات المؤسسات العراقية على التعرف على الهجمات قبل وقوعها واتخاذ إجراءات استباقية للحد من آثارها.

- تبني تشريعات قانونية فعّالة وتطوير إطار قانوني متكامل ينظّم الأنشطة الرقمية ويُطبَّق على كلٍّ من القطاعين الحكومي والخاص، إلى جانب تعزيز التثقيف وتنمية الوعي العام، بما يستلزم البحث عن حلول جديدة تتلاءم مع التطورات الأمنية المعاصرة، والابتعاد عن أساليب المعالجة التقليدية، بهدف إنشاء بنية معلوماتية متقدمة في العراق تواكب وتسهم في مجاراة التسارع التكنولوجي العالمي.

- تعزيز القدرات البشرية في مجال الأمن السيبراني من خلال إنشاء وتدريب وتطوير كوادر مهنية متخصصة في كلٍّ من القطاعين الحكومي والخاص، بما يؤهّلها لمواجهة التحديات السيبرانية بكفاءة وفعالية.

- إنشاء هيئة وطنية مستقلة للأمن السيبراني تتولى التنسيق بين الجهات الحكومية والمؤسسات الخاصة والهيئات الدولية، بهدف تبادل المعلومات المتعلقة بالتهديدات السيبرانية وتطوير استراتيجيات دفاعية فعّالة. كما يشمل ذلك التعاون مع منظمات دولية مثل EC-Council و Cisco و Microsoft لتنظيم ورش عمل تدريبية متخصصة.

- إدراج برامج دراسية متخصصة في الجامعات العراقية تُعنى بالأمن السيبراني وعلاقته بتطوير الآفاق الاقتصادية في العراق، حيث يمكن أن يسهم البحث العلمي في ابتكار حلول جديدة لحماية الأنظمة الرقمية. كما يُعد دعم الابتكار في قطاع التكنولوجيا المالية والتجارة الإلكترونية خطوة محورية لتعزيز الاقتصاد الرقمي في البلاد.

- تعزيز الشراكات مع المنظمات الدولية والهيئات الأمنية لتبادل المعلومات حول التهديدات السيبرانية والانضمام إلى المعاهدات الدولية لمكافحة الجرائم الإلكترونية.

II. المقدمة:

التهديدات الرقمية تمثّل أحد أبرز التحديات التي تواجه الدول في العصر الحديث، إذ أصبحت الأنظمة الإلكترونية مكوّناً أساسياً من مكوّنات البنية التحتية الاقتصادية. وفي العراق، يكتسب الاقتصاد الرقمي أهمية متزايدة في دعم وتطوّر مختلف القطاعات، مثل الصناعة والخدمات والتجارة. ومع ذلك، تواجه البلاد تهديدات متصاعدة من الهجمات السيبرانية التي تستهدف المعلومات المحمية، سواء كانت بيانات أفراد أو بيانات تعود إلى مؤسسات أو مجموعات أخرى، وتشمل بيانات حسّاسة، من بينها معلومات الأنظمة المالية والبيانات المتعلقة بالموجودات والعمليات اليومية للشركات والمؤسسات، ما يهدد بشكل مباشر استقرار الاقتصاد الوطني.

إن الأمن السيبراني يُمثّل مجموعة من الإجراءات والأنظمة المتكاملة التي تهدف إلى حماية الأنظمة المعلوماتية من الهجمات الإلكترونية. وفي ظل التحول الرقمي المتسارع الذي يشهده العراق، أصبحت البنية التحتية الرقمية أكثر عرضة للتهديدات التي قد تُلحق أضراراً جسيمة بالاقتصاد الوطني. ولا يقتصر الأمن السيبراني على حماية البيانات الشخصية فحسب، بل يشمل أيضاً حماية الأنظمة الاقتصادية الحيوية، مثل البنوك، والمؤسسات المالية، وشبكات الطاقة. وقد شهد العراق منذ عام 2003 تحولاً رقمياً متنامياً، جعله أكثر اندماجاً في الاقتصاد الرقمي العالمي، وبالتالي أكثر عرضة للهجمات السيبرانية. ومع ذلك، لا تزال البلاد تواجه تحديات كبيرة في بناء بنية تحتية رقمية متينة، وسنّ تشريعات حديثة، وتطوير كوادر متخصصة في مجال الأمن السيبراني، وهو ما جعل العراق من بين الدول الأكثر عرضة لهذه الهجمات، نتيجة الانفتاح المتزايد على العالم والتطور في المجالات التقنية والمعلوماتية.[1]

تُعد الاستراتيجية الوطنية للأمن السيبراني في العراق إطاراً يُراد من خلاله توفير تدابير متماسكة وإجراءات فعّالة لضمان أمن وحماية المعلومات في الفضاء السيبراني. وتركّز هذه الاستراتيجية على حماية البنية التحتية الحيوية للمعلومات، إلى جانب بناء ورعاية مجتمع إنترنت يتمتع بالموثوقية والأمان.[2]

1- مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد ا، المجلد 10، جامعة ديالى كلية القانون والعلوم السياسية، جمهورية العراق، 2021، ص 149.

2- وسن احسان عبد المنعم، احمد قيس احمد، تكنولوجيا المعلومات والأمن السيبراني، زمنية التطور وافتراضية الواقع وتخطي الحدود، دار ومطبعة الرفاه للطباعة والنشر، بغداد 2022، ص 89 -91.

تتسم البيئة العامة للأمن السيبراني في العراق بالضعف النسبي، إذ لا يزال يُصنَّف ضمن الدول الناشئة في مجال استخدام التقنيات الخاصة بمواجهة الجريمة السيبرانية. وتُعد هذه الجرائم خارج نطاق الأولويات المجتمعية في العراق، رغم التحذيرات الرسمية. فقد كشفت وزارة التخطيط أن النسبة الأكبر من الجرائم السيبرانية تُنفذ عبر مواقع التواصل الاجتماعي، وتشمل جرائم خطيرة مثل الاختطاف، والتهديد، وترويج المخدرات، والاحتيال، وسرقة المعلومات الشخصية، وغيرها من الانتهاكات التي تُهدد أمن الأفراد والمجتمع.[3]

بدأ تسجيل الإحصائيات الرسمية المتعلقة بالجريمة السيبرانية في العراق منذ عام 2006، وذلك نتيجة للانتشار السريع للإنترنت وتزامناً مع ظهور الجرائم السيبرانية بشكل واسع، مثل غسل الأموال، والقرصنة، والإرهاب الإلكتروني. وعند الرجوع إلى سجلات مكتب التحقيقات الجنائية العراقية، نلاحظ أن معدل الجرائم السيبرانية قد ارتفع بنسبة 2.2% خلال الفترة ما بين عامي 2006 و2011.

بهدف تطوير استراتيجية فعالة للأمن السيبراني في العراق، انعقد في العاصمة بغداد عام 2019 «مؤتمر العراق الإلكتروني والأمن السيبراني»، بالتعاون مع المجلس الدولي للاستشارة الإلكترونية (EC-Council) التابع للمفوضية الأوروبية، وهو مجلس يُعنى بمتابعة قضايا الأمن السيبراني على المستوى العالمي. وقد هدف المؤتمر إلى تحديث وابتكار العمليات الاستراتيجية والتكتيكية في مجال الأمن السيبراني للحكومة العراقية، ومناقشة مستقبل الحكومة الإلكترونية، والتهديدات السيبرانية المحتملة التي قد يتعرض لها العراق، وسبل التصدي لها. كما ركّز المؤتمر على تعزيز الوعي العام للحد من الجريمة السيبرانية، وحماية البيانات، وآليات التعامل مع الحوادث السيبرانية، واستعادة القدرة على العمل بعد التعرض للهجمات. وشهد المؤتمر تأكيداً على دور مجلس (EC-Council) في تقديم الدعم الفني والاستشاري للعراق، ويأتي هذا الحدث في إطار خطط الحكومة العراقية للاستثمار في التحول الرقمي وتعزيز قدرات الأمن السيبراني الوطنية. بالنسبة لعام 2021، نلاحظ ان العراق تراجع في المؤشر العالمي للأمن السيبراني Global Cybersecurity Index الصادر عن الاتحاد الدولي للاتصالات اذ حصل على المرتبة 159 عالميا في مؤشر الامن السيبراني من أصل 182 دولة بينما كان في المركز 107 في التقرير السابق، مما يدل على التحديات التي تواجه الهياكل التنظيمية للأمن السيبراني العراقي.[4]

3- مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مصدر سبق ذكره، ص ١٧١.

4- العراق يتراجع عالميا وعربيا في الأمن السيبراني، معلومة وردت على شبكة المعلومات الدولية (الانترنت)، متاحة على الموقع: https://shafaq.com /amp/ar مجتمع / العراق يتراجع - عالمياً وعربياً - في الأمن السيبراني.

III. التهديدات السيبرانية التي تواجه الاقتصاد العراقي

يعد العراق من الدول التي تواجه تهديدات سيبرانية متزايدة، تشمل هذه التهديدات: الهجمات على البنية التحتية الرقمية، واختراق الأنظمة المالية، وسرقة البيانات الحساسة، واختراق شبكات الإنترنت. وفي عام 2022 تم رصد زيادة كبيرة في الهجمات السيبرانية، خاصة تلك التي استهدفت القطاع المالي والبنية التحتية الحيوية.

تشمل التهديدات السيبرانية التي تواجه العراق: الهجمات على الأنظمة المالية، واختراق المؤسسات الحكومية، وسرقة البيانات الحساسة، بالإضافة إلى الهجمات التي تستهدف البنية التحتية الحيوية. ووفقاً لتقارير دولية، يشهد العراق تصاعداً في معدلات الجرائم السيبرانية، لا سيما في ظل توجهه نحو الاندماج في الاقتصاد العالمي، والمساعي الرامية إلى تسريع انتقال المعارف والمهارات التقنية إلى الداخل العراقي. ومن أبرز الأمثلة على هذه الهجمات، الهجوم السيبراني الكبير الذي استهدف النظام المصرفي في عام 2020، والذي أثّر على آلاف المستخدمين وأدى إلى تسرب بيانات حساسة. كما وقعت هجمات أخرى استهدفت قواعد البيانات الوطنية الخاصة بالأفراد. وتُعد مثل هذه الهجمات تهديداً مباشراً لثقة المواطنين والمستثمرين في النظام المالي العراقي، مما قد يترتب عليه تداعيات اقتصادية كبيرة.

1- الهجمات السيبرانية على البنية التحتية الحيوية

تتعرض البنية التحتية الحيوية في العراق، بما في ذلك شبكات الكهرباء والمياه والاتصالات، لهجمات إلكترونية متزايدة. وقد تؤدي هذه الهجمات إلى تعطيل الخدمات الأساسية، مما يؤثر بشكل مباشر على النشاط الاقتصادي، ويزيد من تكاليف تشغيل الأنظمة. وغالباً ما تستهدف هذه الهجمات الأنظمة التشغيلية لشبكات الخدمات الحيوية، وهو ما يتسبب في توقف الإمدادات الحيوية، ويؤثر سلباً على قطاعات الإنتاج الصناعي والتجاري. ونتيجة لذلك، تتزايد الأعباء الاقتصادية وتضعف قدرة الدولة على الحفاظ على الاستقرار الخدمي والتنموي.

2- اختراق البيانات والأنظمة المالية والمصرفية

في ظل التحول الرقمي الذي تشهده المؤسسات المالية في العراق، أصبحت الهجمات التي تستهدف البيانات المصرفية أكثر تعقيداً. هذه الهجمات تشمل سرقة المعلومات الشخصية وحسابات البنوك، وهو ما يؤدي إلى تدمير الثقة في القطاع المالي. وتشمل سرقة البيانات المالية، واختراق الحسابات المصرفية، والهجمات التي تطالب بالفدية المالية والتي تؤدي إلى خسائر مالية ضخمة، مثال الهجوم السيبراني على المصارف العراقية عام 2020، الذي أدى إلى تسريب بيانات حساسة لآلاف المستخدمين.

3- الهجمات التي تستهدف الشركات والمؤسسات الحكومية

تُعد المؤسسات الحكومية والشركات الكبرى أهدافاً رئيسية للهجمات السيبرانية، حيث يعتمد المهاجمون على أساليب متعددة مثل البرمجيات الخبيثة، والتصيد الاحتيالي، وأحياناً الفساد الداخلي للوصول إلى معلومات حساسة. وتؤدي هذه الهجمات إلى تسريب بيانات تؤثر بشكل مباشر على السياسات الاقتصادية والإدارة المالية، مما يشكّل تهديداً حقيقياً للأمن القومي. وغالباً ما تستهدف هذه الهجمات الوزارات والهيئات الاقتصادية الكبرى باستخدام تقنيات متقدمة لاختراق أنظمتها، وهو ما ينعكس سلباً على استقرار الدولة وقدرتها على إدارة الملفات المالية والاقتصادية بكفاءة.

4- الهجمات على التجارة الإلكترونية

مع تزايد الاعتماد على التجارة الإلكترونية في العراق، أصبحت الشركات الصغيرة والمتوسطة عرضة لهجمات سيبرانية تستهدف منصات الدفع الرقمي، مما يعرّضها لخسائر مالية فادحة ويقوّض ثقة المستهلكين في البنية الرقمية. وتؤثر هذه الهجمات بشكل مباشر على نمو الاقتصاد الرقمي، كما تؤدي إلى تراجع الاستثمارات في قطاع التكنولوجيا المالية (Fintech).

IV. العلاقة بين الأمن السيبراني والتنمية الاقتصادية

إن البيئة الإلكترونية الآمنة تؤدي إلى تعزيز ثقة المستثمرين في الاقتصاد العراقي، ويعد الأمن السيبراني أحد العوامل الأساسية التي تؤثر على بيئة الأعمال والاستثمار، حيث يسهم في خلق بيئة رقمية موثوقة تتيح للمستثمرين إمكانية ممارسة أنشطتهم بأمان. وفي الدول التي تمتلك أنظمة سيبرانية قوية، يتمتع المستثمرون بثقة أكبر في سلامة المعاملات المالية، وحماية بياناتهم، واستقرار الأسواق الرقمية، ويمكن أن يؤثر الأمن السيبراني على قرارات المستثمرين بواسطة:[5]

- حماية الأصول الرقمية: تجنب الشركات الاستثمارية في بيئات غير آمنة هو أمر ضروري، حيث يزداد القلق بشأن سرقة البيانات أو الهجمات السيبرانية التي قد تُلحق بها خسائر كبيرة.

- ضمان استمرارية الأعمال: يُفضّل المستثمرون الأسواق التي تمتلك نظم حماية متقدمة، تضمن استمرارية الأعمال دون انقطاع بسبب الهجمات الإلكترونية.

- الامتثال إلى المعايير الدولية: الدول التي تواكب المعايير العالمية للأمن السيبراني (مثل ISO 27001، Framework Cybersecurity NIST، GDPR) تجذب استثمارات أجنبية أكثر، لأن الشركات العالمية تحتاج إلى بيئة تتوافق مع هذه المعايير.

- سن تشريعات لحماية البيانات والاستثمارات الرقمية وفقاً للمعايير الدولية.
- تحفيز الشركات التقنية العالمية للاستثمار من خلال بيئة رقمية آمنة ومستقرة.

وعلى صعيد التحول الرقمي في العراق، يعتمد بشكل أساسي على مدى قوة منظومة الأمن السيبراني. إذ إن أي ضعف في الحماية الإلكترونية سيؤثر على نجاح مشاريع الحكومة الإلكترونية، والخدمات المالية الرقمية، والتجارة الإلكترونية. ومن هنا تأتي أهمية الأمن السيبراني في دعم مشاريع الحكومة الإلكترونية، كونها:[6]

5- اماني احمد وابو يوسف، واقع الافصاح عن تقرير ادارة مخاطر الامن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة، المجلة المصرية للدراسات التجارية، المجلد 13، العدد 2، 2021.
6- علي سعيد دبي، تأثير ضعف البنية التحتية الرقمية على الامن السيبراني في العراق، مقالة منشورة،2025على الرابط:https://www.researchgate.net/publication..

- تحتاج الحكومة الإلكترونية إلى بنية تحتية إلكترونية محمية تضمن عدم تعرض الخدمات الحكومية للاختراق أو التلاعب بالبيانات.

- ضعف الأمن السيبراني قد يؤدي إلى تعطيل الخدمات الرقمية أو سرقة البيانات الشخصية للمواطنين، مثال هجوم DDoS.

- رفض الخدمة الموزع الذي قد يؤدي إلى تعطيل الخدمات الإلكترونية للوزارات، وأنظمة الدفع الرقمي، والخدمات البنكية، ويعتمد الاقتصاد الرقمي على أنظمة الدفع الإلكتروني والتجارة الإلكترونية، مما يجعله هدفاً رئيسياً للهجمات السيبرانية.

- غياب التدابير الأمنية القوية قد يؤدي إلى اختراق حسابات العملاء وسرقة الأموال، مما يهدد ثقة المستخدمين في الاقتصاد الرقمي.

- استخدام تقنيات حديثة لتعزيز الأمن السيبراني، مثل تطبيق تقنيات Blockchain البلوكشين يوفر مستوى أمان عالٍ في التعاملات المالية من خلال تشفير البيانات ومنع التلاعب بها، ويمكن استخدام هذه التقنيات لحماية المدفوعات الرقمية، والعقود الذكية، والمعاملات المصرفية.

- كما يمكن استخدام الذكاء الاصطناعي في ابتكار الحلول التي تتفاعل مع النظام البيئي التنظيمي في تحليل البيانات الضخمة واكتشاف الأنشطة المشبوهة في الأنظمة المالية، والذي يمكنه تحسين قدرات المؤسسات العراقية في التعرف على الهجمات قبل وقوعها واتخاذ إجراءات استباقية.

٧. التحديات أمام تنفيذ استراتيجيات الأمن السيبراني في العراق

1- الافتقار إلى البنية التحتية التقنية المتطورة

تعاني العديد من القطاعات في العراق من بنية تحتية رقمية ضعيفة، مما يجعلها عرضة للاختراقات والهجمات السيبرانية، إلا أن البنية التحتية للأمن السيبراني لا تزال في مراحلها الأولى، والعديد من المؤسسات الحكومية والخاصة تفتقر إلى الأنظمة الأمنية الحديثة وتعتمد العديد من المؤسسات على أنظمة تكنولوجية قديمة، غير محدثة، وغير مؤمنة بشكل كافٍ، لذلك هناك حاجة إلى تحديث البنية التحتية الرقمية والاستثمار في أنظمة حديثة مقاومة للاختراقات.

2- التحديات القانونية

من أكبر التحديات التي تواجه العراق هي القوانين الحالية التي لا تغطي بشكل كامل قضايا الأمن السيبراني. كما أن هناك غياباً لتشريعات واضحة تتعلق بحماية البيانات والخصوصية. إن ضعف التشريعات والقوانين الحكومية الخاصة بالأمن السيبراني وحماية المعلومات يستوجب تبني تشريعات قانونية فعّالة، وتطبيقها على القطاعين الحكومي والخاص. وهذا يتطلب تنفيذ إجراءات أمنية محددة في الوزارات والمؤسسات، بالإضافة إلى القطاع الخاص، مما يعزز من الأمن المعلوماتي والسيبراني على حد سواء في العراق.

3- نقص الوعي العام

يعاني العديد من المستخدمين في العراق من نقص في الوعي الكافي حول مخاطر الإنترنت والتهديدات السيبرانية. ويتطلب الأمر تنظيم حملات توعية لتحسين سلوك الأفراد عند التعامل مع البيانات والأنظمة الرقمية. بالإضافة إلى ذلك، هناك ضعف في إدراك شركات تكنولوجيا المعلومات المحلية لحجم المخاطر الأمنية المعاصرة، مما يتطلب التثقيف وتنمية الوعي لديهم بأن التحديات الأمنية المعاصرة تختلف عن تلك التي كانت في المراحل السابقة. وهذا يستلزم البحث عن حلول جديدة مناسبة للتطورات الأمنية الحديثة، والابتعاد عن وسائل المعالجة التقليدية بهدف إنشاء بنية تحتية تكنولوجية متقدمة في العراق تواكب التطور السريع في العالم.

4-نقص الكفاءات

لا يزال العراق يعاني من نقص حاد في أعداد الكوادر الكفوءة والمهنيين المدربين في مجال الأمن السيبراني، مما يزيد من صعوبة مواجهة التهديدات المتزايدة. وينعكس هذا النقص على مخاوف التوسع في الأنشطة الاقتصادية التي تعتمد على نقل البيانات. ويُعد ضعف القدرات المهنية المحلية في مجال أمن المعلومات المتقدمة والأمن السيبراني من أبرز التحديات، مما يتطلب العمل الجاد على إنشاء وتدريب وتطوير كوادر مهنية محترفة في كل من القطاعين الحكومي والخاص، تكون مؤهلة لمواجهة التحديات السيبرانية بكفاءة وفاعلية.

VI. استراتيجيات المواجهة للأمن السيبراني في العراق

1- تطوير الإطار القانوني والتنسيق بين الجهات المعنية

يجب على العراق تطوير إطار قانوني قوي ينظم الأنشطة الرقمية، والتنسيق بين الجهات الحكومية والمؤسسات الخاصة والهيئات الدولية من أجل تبادل المعلومات المتعلقة بالتهديدات وتطوير استراتيجيات دفاعية. فضلاً عن تحديث القوانين المتعلقة بالأمن السيبراني وتوسيع إطار حماية البيانات الشخصية، ويشمل تطوير الإطار القانوني والتشريعي، تحديث القوانين العراقية بما يتماشى مع المعايير الدولية، مثل GDPR وNIST Cyber security Framework. وانشاء هيئة وطنية مستقلة للأمن السيبراني لتنظيم هذا القطاع.

2- تعزيز التعليم والتدريب في مجال الأمن السيبراني

يحتاج العراق إلى تعزيز القدرات البشرية في مجال الأمن السيبراني من خلال إقامة برامج تدريبية على مستوى الأفراد والمؤسسات، يمكن تقليل الفجوة المعرفية والمهارية في هذا المجال الحيوي. وإنشاء هذه البرامج التدريبية يأتي لتحسين مهارات القوى العاملة في مجال الأمن السيبراني وتشمل:

- إدراج برامج دراسية متخصصة في الجامعات العراقية.
- التعاون مع منظمات دولية مثل: EC-Council وCisco وMicrosoft لعقد ورش عمل تدريبية.

اما أهمية البحث العلمي في تطوير الأمن السيبراني فتتضح كما يلي:

- يمكن للبحث العلمي أن يساعد في اكتشاف حلول جديدة لحماية الأنظمة الرقمية في العراق.
- تعزيز الأبحاث في الجامعات العراقية سيساهم في إعداد كوادر محلية قادرة على مواجهة التهديدات السيبرانية.
- إطلاق مراكز بحثية متخصصة في الجامعات العراقية لدراسة الهجمات السيبرانية وتطوير أنظمة حماية مبتكرة.
- توفير تمويل حكومي ومؤسسي لدعم المشاريع البحثية في الأمن السيبراني.

3- تقنيات الوقاية المتقدمة

يجب على العراق استثمار التقنيات المتقدمة مثل الذكاء الاصطناعي والتحليل القائم على التنبؤ للكشف المبكر عن الهجمات السيبرانية، هذه التقنيات تستطيع تحليل الأنماط السلوكية للأجهزة وتحديد المخاطر المحتملة في وقت مبكر، مما يساعد على اتخاذ الإجراءات الوقائية المناسبة. ذلك بواسطة تعزيز التعاون مع شركات التكنولوجيا العالمية للحصول على تقنيات متقدمة وتشمل:

- تطبيقات الذكاء الاصطناعي والتعلم الآلي في اكتشاف التهديدات الإلكترونية والتصدي لها.
- الاستثمار في التشفير المتقدم وتقنيات كشف الاختراقات (IDS/IPS).

4- التعاون الإقليمي والدولي

بما أن الهجمات السيبرانية يمكن أن تتجاوز الحدود الوطنية، ينبغي على العراق تعزيز التعاون مع الدول الأخرى، وخاصة في المنطقة، لمكافحة هذه التهديدات بشكل جماعي وتشمل:

- تعزيز الشراكات مع المنظمات الدولية والهيئات الأمنية لتبادل المعلومات حول التهديدات السيبرانية.
- الانضمام إلى المعاهدات الدولية لمكافحة الجرائم الإلكترونية.

٥- تطوير البنية التحتية والاستثمار في التكنولوجيا الحديثة

يتطلب تأمين الأنظمة المالية والبنية التحتية الرقمية في العراق استثماراً كبيراً في التقنيات الحديثة مثل التشفير المتقدم والتحليل البياني، لحماية البيانات المالية والمصرفية من الهجمات الإلكترونية، فضلاً عن بناء أنظمة حماية متقدمة باستخدام تقنيات حديثة مثل الذكاء الاصطناعي والتعلم الآلي وتشمل:

- تحديث أنظمة الحكومة الإلكترونية وضمان تأمينها ضد الاختراقات.
- دعم الابتكار في قطاع التكنولوجيا المالية والتجارة الإلكترونية لتعزيز الاقتصاد الرقمي.

6- تطوير الخطط الوطنية

اتخاذ الخطوات العملية التي تشمل تطوير خطة وطنية لمكافحة الهجمات السيبرانية تشمل جميع القطاعات، إلى جانب تشجيع إنشاء مركز لتنسيق الأمن السيبراني يشمل مختلف الجهات الحكومية والخاصة، وهذا سيعمل على:

- رصد التهديدات السيبرانية والاستجابة السريعة للهجمات.
- وضع سياسات الأمن السيبراني وإجراء التدريبات الوطنية.

7- الربط بين الأمن السيبراني والنمو الاقتصادي الرقمي

تشير العديد من الدراسات إلى أن الاستثمار في الأمن السيبراني يمكن أن يكون له تأثير إيجابي على الاقتصاد الرقمي من خلال حماية الأنظمة الاقتصادية، ويتم تعزيز ثقة المستثمرين والمواطنين في الخدمات الرقمية، مما يؤدي إلى مزيد من الاستثمارات في قطاعات مثل التجارة الإلكترونية والخدمات المالية الرقمية.

من المهم أن يُعزّز العراق تعاونه مع المجتمع الدولي في مجال الأمن السيبراني، سواء من خلال توقيع اتفاقيات مع منظمات دولية متخصصة، أو عبر المشاركة في تدريبات ومشاريع مشتركة تهدف إلى بناء القدرات وتعزيز الجاهزية السيبرانية. كما يتطلب الأمر زيادة الاهتمام بالشؤون السيبرانية على المستوى الوطني، ويشمل ذلك تأسيس كليات وأقسام علمية متخصصة في مجال الأمن السيبراني، فضلاً عن بناء مؤسسات ووحدات سيبرانية تُحاكي ما هو معمول به في الدول المتقدمة. ويُعدّ تشريع القوانين والدخول في اتفاقيات دولية من شأنه دعم وتطوير منظومة الأمن السيبراني في العراق بشكل مستدام.

وترتيباً على ذلك، يمكن القول إنه في إطار تدعيم الأمن السيبراني عبر تكنولوجيا المعلومات، يتكوّن الإطار التكنولوجي للأمن السيبراني في العراق من العناصر الآتية:[7]

1- تطوير وبناء إطار تكنولوجي وطني للأمن السيبراني، والذي يحدد بدوره متطلبات السيطرة على الأمن السيبراني العراقي.

2- العمل على إنشاء برنامج وطني لتقييم وإصدار شهادات للمنتجات ونظم الأمن السيبراني.

7- علاء السالمي، المدخل الى الأمن السيبراني، دار الذاكرة للنشر والتوزيع، بغداد، ط1، ص 301.

VII. الخاتمة

يُعد الأمن السيبراني ركيزة أساسية للحفاظ على استقرار الاقتصاد العراقي في ظل التحولات المتسارعة التي يشهدها العالم الرقمي. إذ إنّ التصدي للتهديدات الرقمية يتطلب تنسيقاً فعالاً بين الجهات الحكومية، من خلال تبني استراتيجيات أمنية قوية وشاملة، تشمل تطوير الأطر التشريعية، وتعزيز التعاون بين القطاعين العام والخاص، وإطلاق حملات توعية مجتمعية، والاستثمار في البحث العلمي، فضلاً عن تنمية القدرات البشرية، واعتماد تقنيات حديثة لرصد الهجمات السيبرانية والتصدي لها. ورغم التحديات العديدة التي يواجهها العراق في هذا المجال، فإنّ الاستثمار الاستراتيجي في الأمن السيبراني يمكن أن يسهم بشكل كبير في بناء مستقبل رقمي أكثر أماناً واستقراراً، ويعزز من قدرة الاقتصاد الوطني على الصمود في وجه التهديدات المتزايدة. ويستلزم ذلك استمرار التنسيق بين الحكومة والقطاع الخاص للعمل جنباً إلى جنب على تطوير حلول مبتكرة وشاملة لمواجهة التحديات السيبرانية المتصاعدة. إن مستقبل الاقتصاد العراقي بات مرتبطاً ارتباطاً وثيقاً بحماية البيانات والبنية التحتية الرقمية، ما يجعل من الأمن السيبراني أولوية وطنية لا غنى عنها لضمان نمو الاقتصاد الرقمي، وجذب الاستثمارات الأجنبية، وتحقيق التنمية المستدامة.

VIII. المصادر

- العراق يتراجع عالميا وعربيا في الأمن السيبراني، معلومة وردت على شبكة المعلومات الدولية (الانترنت)، متاحة على الموقع: https://:com.shafaq/ar/amp مجتمع / العراق يتراجع - عالميا وعربيا - في الأمن السيبراني.
- اماني احمد وابو يوسف، واقع الافصاح عن تقرير ادارة مخاطر الامن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة، المجلة المصرية للدراسات التجارية، المجلد 13، العدد 2، 2021.
- علاء السالمي، المدخل الى الأمن السيبراني، دار الذاكرة للنشر والتوزيع، بغداد، طا، ص 301.
- علي سعيد دبي، تأثير ضعف البنية التحتية الرقمية على الامن السيبراني في العراق، مقالة منشورة، 2025على الرابط:

https//:www.researchgate.net/publication..

- مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد ا، المجلد ١٠، جامعة ديالى كلية القانون والعلوم السياسية، جمهورية العراق، 2021.
- وسن احسان عبد المنعم، احمد قيس احمد، تكنولوجيا المعلومات والأمن السيبراني، زمنية التطور وافتراضية الواقع وتخطي الحدود، دار ومطبعة الرفاه للطباعة والنشر، بغداد 2022.

لِدولةٍ فاعلةٍ ومجتمعٍ مُشارِك

www.bayancenter.org
info@bayancenter.org