الأمن السيبراني العابر للحدود : نحو شراكة عراقية إقليمية قوية

م.م. نورا رياض الدباغ
مركز الدراسات الإستراتيجية و الدولية

الملخص

أدى التطور الكبير في استخدام التكنولوجيا الرقمية في مختلف مجالات الحياة، إلى أن تصبح التهديدات السيبرانية العابرة للحدود واحدة من أبرز التحديات التي تواجه الدول، خاصةً في منطقة الشرق الأوسط. يسلط هذا البحث الضوء على أهمية تعزيز الأمن السيبراني في العراق من خلال التعاون الإقليمي، مع التركيز على إستلهام تجربة رابطة دول جنوب شرق آسيا (ASEAN) بوصفها واحدة من التجارب الناجحة في التصدي للتحديات السيبرانية المشتركة.

يستعرض البحث واقع الأمن السيبراني في العراق والمنطقة، حيث يعاني العراق من ضعف البنية التحتية الرقمية، نقص التشريعات القانونية، قلة الكوادر البشرية المتخصصة، وتصاعد الهجمات السيبرانية التي تهدد مؤسساته الحيوية. كما يناقش البحث استراتيجيات وأدوات (ASEAN) في مواجهة التهديدات السيبرانية، مثل إنشاء مراكز الأمن السيبراني الإقليمية، وتوحيد التشريعات، وتعزيز بناء القدرات.

و لغرض تلافي ذلك يقترح البحث مجموعة من الأدوات والآليات لتعزيز الأمن السيبراني في العراق، ويخلص إلى أن تعزيز التعاون السيبراني العابر للحدود إقليمياً يُعد خيارًا استراتيجيًا يساهم في حماية البنية التحتية الرقمية للعراق، ودعم استقراره الرقمي، والمساهمة في استقرار المنطقة عموماً .

الكلمات المفتاحية : العراق ، الأمن السيبراني ، التعاون الإقليمي .

المقدمة :

مع توسع الإعتماد على التكنولوجيا الرقمية في مختلف جوانب الحياة اليومية، أصبح الأمن السيبراني يشكل جزءاً أساسياً من الأمن الوطني للدول. العالم اليوم يشهد زيادة غير مسبوقة في التهديدات السيبرانية التي تتسم بتعقيدها وإنتشارها عبر الحدود، مما يستدعي وضع إستراتيجيات شاملة لمواجهتها. العراق، مثل غيره من الدول، يواجه تحديات عديدة تتعلق بضعف البنية التحتية الرقمية، ونقص التشريعات الفعالة، وقلة الكفاءات البشرية المتخصصة. هذه العوامل تجعله عرضة للهجمات السيبرانية التي تستهدف مؤسساته الحيوية وتعرقل جهوده التنموية.

في هذا السياق، تبرز أهمية التعاون الإقليمي والدولي بوصفها وسيلة أساسية لتعزيز قدرات الأمن السيبراني. ومن التجارب الناجحة التي يمكن أن يستفيد منها العراق، تجربة رابطة دول جنوب شرق آسيا (ASEAN)، حيث نجحت دول هذه الرابطة في وضع إطار عمل مشترك لمواجهة التهديدات السيبرانية عبر إنشاء مراكز متخصصة، وتبادل المعلومات، وتطوير القدرات البشرية. يستعرض هذا البحث أهمية هذه التجربة في تعزيز التعاون السيبراني الإقليمي للعراق .

أهمية البحث :

من الناحية الأكاديمية يساهم في إثراء الدراسات المتعلقة بالأمن السيبراني الإقليمي ، و يسلط الضوء على تأثير التعاون السيبراني في حماية حقوق الأفراد والحد من الجرائم الإلكترونية العابرة للحدود.

إشكالية البحث :

كيف يمكن للعراق أن يطور شراكات إقليمية فعالة في مجال الأمن السيبراني ، للتصدي للتحديات الرقمية العابرة للحدود، وما هي الأدوات والآليات اللازمة لتحقيق ذلك؟

فرضية البحث

يمكن للعراق، من خلال بناء شراكات إقليمية استراتيجية، أن يلعب دورًا حيويًا في تعزيز الأمن السيبراني الإقليمي، عبر تبادل المعلومات، وتنسيق الجهود، وتطوير البنية التحتية الرقمية المشتركة.

منهجية البحث :

يعتمد هذا البحث على المنهج الوصفي التحليلي لدراسة واقع الأمن السيبراني في العراق والمنطقة، بالإضافة إلى المنهج المقارن لمقارنة التجارب الإقليمية والدولية الناجحة. كما يستند إلى المنهج الإستشرافي لإستقراء المستقبل وإقتراح حلول تعزز التعاون السيبراني العابر للحدود .

هيكلية البحث :

تم تقسيم البحث إلى ثلاثة مطالب رئيسة ، يتضمن المطلب الأول: واقع الأمن السيبراني في العراق والمنطقة الذي يناقش : التهديدات السيبرانية في المنطقة ، الواقع السيبراني في العراق و تحديات الأمن السيبراني في العراق والمنطقة . أما المطلب الثاني : دول جنوب شرق آسيا (ASEAN) أنموذجًا للتعاون السيبراني الإقليمي يتضمن : دور (ASEAN) في تعزيز التعاون السيبراني الإقليمي و إستراتيجيات التعاون السيبراني في (ASEAN) . أما المطلب الثالث : الأدوات والآليات اللازمة لتعزيز التعاون السيبراني الإقليمي للعراق ، ثم الخاتمة و الإستنتاجات و التوصيات .

المطلب الأول : واقع الأمن السيبراني في العراق والمنطقة :

أولاً : التهديدات السيبرانية في المنطقة :

يشهد الشرق الأوسط إرتفاعًا كبيرًا في حدة التهديدات السيبرانية ؛ بسبب التحول الرقمي المتزايد و البنية التحتية الحساسة التي تعتمد على التكنولوجيا. يمكن تصنيف هذه التهديدات إلى ثلاث فئات رئيسة :

- **التحديات التقنية:** حيث أن انتشار البرمجيات الضارة مثل "الفيروسات" و"الديدان" و"برمجيات الفدية" أصبحت تستهدف مؤسسات حيوية، كالمصارف وشبكات الكهرباء. العراق، بوصفه جزء من المنطقة، يعاني من ضعف في الحماية التقنية، مما يجعله عرضة لمثل هذه الهجمات ، فضلاً عن الهجمات الموزعة لمنع الخدمة (DDoS) و التي تزايدت بهدف تعطيل الخدمات الرقمية عن طريق إغراق الخوادم بكم هائل من الطلبات، مما يؤدي إلى شلل الأنظمة. هذه الهجمات غالبًا ما تُستخدم لأهداف سياسية أو اقتصادية. أما الهجمات المتطورة تعتمد فيها الجهات على أدوات سيبرانية متطورة تتجاوز الطرق التقليدية للاختراق، مثل : استغلال نقاط الضعف في الأنظمة التشغيلية وبرمجيات التحكم الصناعي (SCADA) [١].

- **الجرائم العابرة للحدود:** مثل الهجمات المنظمة تقوده جماعات سيبرانية دولية، بعضها مدعوم من دول، هجمات متقدمة تستهدف دول المنطقة ، في الغالب تكون هذه الجماعات مدفوعة بأهداف تجسسية أو لسرقة البيانات الحساسة. من جانب آخر هناك التجارة غير القانونية عبر الإنترنت التي تشتمل على تهريب المخدرات، الأسلحة، وحتى البشر عبر منصات رقمية سرية يصعب تتبعها، مما يشكل تهديدًا للأمن الإقليمي. ناهيك عن الابتزاز الرقمي: المتمثل بإ ستغلال المعلومات المسروقة أو تعطيل الأنظمة الحساسة لطلب فدية مالية ضخمة [٢].

(١) ماجد صدام سالم. "الأمن السيبراني العراقي وأثره على قوة الدولة ".*مجلة العلوم التربوية والإنسانية*، جامعة ميسان، العدد ١٨، ٢٠٢٢، ٧١.

(٢) رعد خضير صليبي، "تعزيز الأمن السيبراني في العراق"، *مجلة دراسات دولية*، مركز الدراسات الإستراتيجية والدولية، جامعة بغداد، العدد ٩٩ (٢٠٢٤): ٥١٦.

- **الأهداف الإقتصادية والسياسية :** مثل إستهداف البنية التحتية الحرجة مثل إستهداف شبكات الطاقة، محطات المياه، والأنظمة المالية. هذه الأنظمة تعد هدفًا جذابًا لجهات تسعى لإحداث ضرر واسع النطاق. بالإضافة إلى الهجمات على البيانات بهدف السعي للحصول على معلومات إستخباراتية، سواء كانت عسكرية أو اقتصادية، هو هدف رئيسي للعديد من الجهات السيبرانية ، خصوصاً في منطقة مليئة بالتوترات السياسية مثل منطقة الشرق الأوسط، تُستخدم الهجمات السيبرانية بوصفها وسيلة للحرب غير التقليدية بين الدول[٣] .

ثانياً : الواقع السيبراني في العراق :

يعاني العراق من ضعف البنية التحتية الرقمية بسبب هشاشة أنظمة الحماية التي تعتمدها المؤسسات فهي تقنيات قديمة وغير محدثة . مع غياب الإستثمار الكافي في تحديث الشبكات وتطوير مراكز بيانات محلية يعزز من تعرض الأنظمة للاختراق. بالتالي فإن ضعف الشبكات الوطنية يُسهل تنفيذ الهجمات السيبرانية، خاصة تلك التي تستهدف القطاع الحكومي [٤] .

من جانب آخر، رغم الجهود المبذولة إلا إن العراق يفتقر إلى إطار قانوني شامل يعالج الجرائم السيبرانية ، مما يعني ضعفاً في التشريعات القانونية السيبرانية . فغياب قوانين فعالة يُعيق ملاحقة الجرائم العابرة للحدود، مما يترك ثغرات يمكن للجهات الفاعلة استغلالها. بالتالي فإن ضعف التعاون مع الدول الأخرى لتسليم المجرمين السيبرانيين أو تبادل المعلومات حولهم يجعل العراق أكثر عرضة للتهديد [٥] . خصوصاً مع الاعتماد المتزايد على التكنولوجي يشهد العراق نموًا كبيرًا في إستخدام الخدمات الرقمية، مثل الخدمات المصرفية الإلكترونية والتعليم عبر الإنترنت، مما يزيد من حاجة البلاد لحماية هذه الأنظمة. فإن التحول الرقمي غير المدروس (إذا صح التعبير) يُعرض المؤسسات إلى مخاطر كبيرة بسبب غياب التخطيط الأمني السليم[٦] . فتلك الهجمات التي استهدفت أنظمة حكومية في السابق، مثل اختراق مواقع وزارات عراقية حساسة من جهة ، و تعرض البنوك العراقية لهجمات سيبرانية إستهدفت سرقة بيانات العملاء وتحويل الأموال من جهة ثانية ، و هجمات على أنظمة الطاقة ، أدت إلى تعطيل خدمات حيوية في بعض المناطق من جهة ثالثة .تسلط الضوء على الحاجة الملحة لتعزيز الأمن الرقمي في العراق ، لما لها من تأثيرات سلبية سواء كانت إقتصادية متمثلة بالخسائر المالية الكبيرة، التي تؤثر

---

(٣)سالم، "الأمن السيبراني العراقي"، ٧٨.

(٤) رعد خضير صليبي، "تعزيز الأمن السيبراني في العراق"،٥١٦.

(٥) إسراء نادر كيطان. "الجريمة الإلكترونية والحاجة لتشريع قانون مكافحتها." مقالة، الموقع الرسمي لمجلس القضاء الأعلى، ٣ ديسمبر ٢٠٢٤، https://sjc.iq/view.75479/.

(٦) زهير خضير عباس الزبيدي، وظفر عبد مطر التميمي. "العراق والأمن السيبراني .. الفرص والتحديات ".*مجلة واسط للعلوم الإنسانية*، جامعة واسط، العدد ١٨، ٢٠٢٢، ص. ١١.

على ثقة المستثمرين المحليين والدوليين من جانب ، أو إجتماعية تستهدف تزايد الشعور بعدم الأمان الرقمي لدى المواطن العراقي والشركات على حد سواء [٧] .

ثالثاً : تحديات الأمن السيبراني في العراق والمنطقة :

- غياب التنسيق الإقليمي : ضعف التعاون بين الدول المجاورة يُعيق عملية تبادل المعلومات حول التهديدات السيبرانية ، و عدم وجود آليات مشتركة للاستجابة السريعة لحالات الطوارئ السيبرانية[٨] .
- نقص الكوادر المتخصصة : بسبب قلة عدد المهندسين وخبراء الأمن السيبراني المؤهلين في العراق والمنطقة لإدارة الواقع السيبراني ، مما يشكل تحديًا رئيسيًا. ناهيك عن غياب برامج تدريب متخصصة ، ومراكز تأهيل لمواكبة التطورات التقنية[٩] .
- تصاعد الهجمات السيبرانية المرتبطة بالجماعات الإرهابية : مثل تنظيم "داعش" الذي بدأ يعتمد على تقنيات سيبرانية لتنفيذ هجماته أو نشر دعايته، مما يضيف بُعدًا جديدًا للتحديات الأمنية[١٠] .
- قلة الوعي المجتمعي : فإن ضعف الوعي عند الأفراد والمؤسسات بالمخاطر السيبرانية يجعلهم هدفًا سهلاً لتلك الهجمات ، كما أن ضعف الثقافة الأمنية الرقمية سيؤدي إلى تسرب البيانات بسهولة[١١] .

---

(٧)سالم، "الأمن السيبراني العراقي"، ٧٨.

(٨) علي زياد العلي. "التحديات غير المرئية للأمن الوطني العراقي." مركز البيان للدراسات والتخطيط، قسم الأبحاث، بغداد، ٢٦ يونيو ٢٠١٨، https://www.bayancenter.org/2018/06/4565/.

(٩) المصدر نفسه .

(١٠) الزبيدي والتميمي، "العراق والأمن السيبراني .. الفرص والتحديات"، ص. ١٢.

(١١)المصدر نفسه .

المطلب الثاني : دول جنوب شرق آسيا (ASEAN) أنموذجاً للتعاون السيبراني الإقليمي :

أولاً: دور (ASEAN) في تعزيز التعاون السيبراني الإقليمي:

إن رابطة دول جنوب شرق آسيا المعروفة بـ (ASEAN) تعد أنموذجًا بارزاً للتعاون الإقليمي في مجال الأمن السيبراني، حيث استطاعت دول الرابطة، التي تضم (١٠) دول ذات تنوع اقتصادي وتكنولوجي كبير، أن تطور إطارًا شاملًا للتعاون السيبراني يستند إلى الشراكة وتبادل المعلومات وبناء القدرات. هذه التجربة تقدم دروسًا قيمة للدول الأخرى، خاصة في المناطق التي تواجه تحديات أمنية مماثلة(١٢) .

حيث يمثل "مركز الأمن السيبراني الإقليمي" أحد أهم إنجازات (ASEAN) ، حيث أُنشئ ليكون منصة لتبادل المعلومات حول التهديدات السيبرانية الناشئة. يركز هذا المركز على تعزيز التنسيق بين الدول الأعضاء من خلال بروتوكولات استجابة مشتركة للحوادث السيبرانية، مما يضمن الاستجابة الفورية للهجمات، خاصة تلك التي تستهدف أكثر من دولة. بالإضافة إلى ذلك، ينظم المركز برامج تدريبية متقدمة تهدف إلى تأهيل خبراء أمن سيبراني محليين لديهم القدرة على التعامل مع التحديات التقنية المتطورة (١٣) .

ضمن إطار عمل (ASEAN) للأمن السيبراني، وضعت الرابطة إستراتيجية واضحة لتعزيز الثقة بين الدول الأعضاء وتوحيد الجهود لمواجهة التهديدات السيبرانية. ركزت هذه الإستراتيجية على توحيد السياسات الوطنية، ودعم التشريعات التي تغطي الجرائم الإلكترونية بشكل شامل، وإطلاق مشاريع مشتركة لتحسين البنية التحتية الرقمية. مثل هذه الجهود عززت قدرة الدول الأعضاء على التصدي للهجمات السيبرانية المتزايدة، وساهمت في دعم الاقتصاد الرقمي المزدهر في المنطقة(١٤) .

لم تكتفِ (ASEAN) بالتعاون الداخلي، بل وسعت جهودها من خلال بناء شراكات مع قوى عالمية مثل : الولايات المتحدة والصين والاتحاد الأوروبي. أسهمت هذه الشراكات في تعزيز القدرات التقنية للدول الأعضاء ونقل التكنولوجيا المتقدمة إلى المنطقة. كما استفادت الرابطة من التعاون مع منظمات دولية، مثل "الاتحاد الدولي للاتصالات"، في وضع معايير أمنية موحدة والتنسيق مع "المنتدى الاقتصادي العالمي" لتحليل التهديدات السيبرانية التي تواجه الاقتصادات الناشئة (١٥) .

---

(١٢) حميدة لحمر، وفريدة حموم. "التعاون الأمني في جنوب شرق آسيا، في مواجهة تهديدات الأمن السيبراني." مجلة طبنة للدراسات العلمية والأكاديمية، الجزائر، العدد ١، ٢٠٢١، ص. ٥٣٩.

(١٣) المصدر نفسه ، ص ٥٤٠ .

(١٤) المصدر نفسه ، ٥٣٧ .

(١٥)المصدر نفسه ، ٥٤٢ .

من أبرز النجاحات التي حققتها (ASEAN) في هذا المجال كان تنسيقها الفعّال للاستجابة لهجمات الفدية الكبرى، حيث تعرضت أنظمة المستشفيات والبنوك في المنطقة لهجمات معقدة. تمكنت الدول الأعضاء من احتواء هذه الهجمات عبر استجابة مشتركة وسريعة، مما قلل من حجم الأضرار الاقتصادية والاجتماعية. علاوة على ذلك، أطلقت الرابطة برامج لبناء القدرات، استهدفت تدريب الآلاف من المهندسين وخبراء الأمن السيبراني، مما رفع مستوى الجاهزية التقنية في المنطقة(١٦) .

رغم هذه النجاحات، واجهت (ASEAN) تحديات ملحوظة، أبرزها التفاوت في القدرات التقنية بين الدول الأعضاء. فعلى سبيل المثال، بينما تتمتع دول مثل سنغافورة وماليزيا ببنية تحتية متقدمة، تعاني دول أخرى مثل لاوس وكمبوديا من نقص في الموارد التقنية، مما يضعف الجهود الإقليمية المشتركة. كما أن الاختلافات في السياسات الوطنية المتعلقة بالأمن السيبراني تسببت في تعقيد وضع إطار قانوني موحد، وهو ما يشكل تحديًا إضافيًا أمام تحقيق التنسيق الكامل(١٧) .

ثانياً : إستراتيجيات التعاون السيبراني في (ASEAN) :

- إستراتيجية التعاون السيبراني (٢٠٢١-٢٠٢٥): تضمنت الاستراتيجية خمسة محاور رئيسة لتعزيز الفضاء السيبراني الآمن، منها بناء الجاهزية السيبرانية، تعزيز التنسيق في السياسات الإقليمية، تعزيز الثقة في الفضاء الرقمي، وبناء القدرات السيبرانية. تم دعم هذه المحاور بإنشاء فريق الاستجابة للطوارئ السيبرانية الإقليمي (ASEAN CERT) الذي يعمل كمنصة لتبادل المعلومات حول التهديدات السيبرانية والاستجابة لها، بالتوازي مع فرق (CERT) الوطنية في كل دولة عضو(١٨) .
- تعزيز القدرات وبناء الكفاءات: أطلقت (ASEAN) برامج تدريبية متعددة : مثل مركز ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)، الذي يركز على تطوير الإستراتيجيات السيبرانية والقدرات البحثية والقانونية. كما تم إجراء تدريبات إقليمية لمواجهة الهجمات السيبرانية، مع التركيز على بناء الخبرات التقنية مثل : التحليلات السلوكية والتحقيقات الرقمية(١٩) .

(16) Abdul Rahman, Muhammad Faizal. "How ASEAN's Cybersecurity Push Could Protect People and Economies." The Diplomat, November 2024. https://thediplomat.com/2024/11/how-aseans-cybersecurity-push-could-protect-people-and-economies/.

(17) Ibid.

(18)Regional Cooperation Mahusin, Mahirah, and Hilmy Prilliadi. "Strengthening ASEAN's Cybersecurity: Collaborative Strategies for Enhanced Resilience and." *ERIA Policy Brief*, no. 2024-06 (November 2024), p.2.

(19) Association of Southeast Asian Nations. ASEAN Cybersecurity Cooperation Strategy 2021–2025. Jakarta: ASEAN Secretariat, 2021.p 2.

- التعاون الدولي ووضع المعايير: تعاونت (ASEAN) في التعاون مع الأمم المتحدة لإعتماد معايير دولية لسلوك الدولة المسؤول في الفضاء السيبراني للحد من الحوادث السيبرانية[٢٠] . حيث إن إفتتاح مركز تدريب في سنغافورة للفرق الوطنية في رابطة دول جنوب شرق آسيا التي تستجيب لحوادث الأمن السيبراني في العام (٢٠٢٣) واحد من أبرز تلك المظاهر، إذ يعتقد العديد من الخبراء العالميين أن نموذج تعاون الأمن السيبراني في (ASEAN) يمكن أن يكون معيارًا جيدًا من الممكن للتجمعات الإقليمية الأخرى أن تتبعه[٢١] .
- التنسيق و السياسات المشتركة: أنشأت الرابطة لجنة التنسيق السيبراني (Cyber-CC) لتعزيز التنسيق بين الهيئات القطاعية في الدول الأعضاء. بهدف تحسين الردود العاجلة على الحوادث السيبرانية وتطوير إطار عمل تنظيمي موحد لضمان استدامة الأمن الرقمي[٢٢] .

تجربة (ASEAN) تقدم دروسًا مهمة يمكن للعراق والدول المحيطة به للاستفادة منها. يمكن أن يكون إنشاء مركز إقليمي للأمن السيبراني على شاكلة (ASEAN) خطوة محورية لتعزيز التعاون العربي في مواجهة التهديدات السيبرانية المشتركة. علاوة على ذلك، فإن تبني إطار عمل إقليمي موحد يعزز من قدرة الدول العربية على تبادل المعلومات وبناء القدرات التقنية. من الضروري أيضًا تعزيز الشراكات الدولية مع الدول المتقدمة للاستفادة من خبراتها في هذا المجال، مما يساهم في حماية البنية التحتية الرقمية وضمان استقرار الاقتصاد الرقمي في المنطقة[٢٣] .

(20)Roy-Choudhury, Amit. "What the World Can Learn from ASEAN's Cyber Cooperation." GovInsider. Accessed October 2023.https://govinsider.asia/intl-en/article/what-the-world-can-learn-from-aseans-cyber-cooperation-amit-roy-choudhury/.

(21) Association of Southeast Asian Nations 2021, p.3.

(22) Ibid.

(23) Abdul Rahman, 2024.

ثالثاً : تحديات تطبيق تجربة (ASEAN) في العراق:

العراق ، مثل العديد من الدول في المنطقة، يواجه تحديات متزايدة في مجال الأمن السيبراني، وقد أظهرت التجربة الإقليمية في (ASEAN) أهمية التنسيق القانوني والتعاون بين الدول لمواجهة التهديدات السيبرانية. ولكن تطبيق تجربة (ASEAN) في العراق يتطلب معالجة عدد من العوامل التي قد تؤثر على فاعلية هذا التعاون منها [٢٤] :

١. التحديات القانونية والتشريعية في العراق :

و ذلك عبر وجود إطار قانوني شامل يحكم الأمن السيبراني بشكل يتماشى مع المعايير الدولية. رغم وجود بعض التشريعات التي تعالج الجرائم الإلكترونية، فإن هذه القوانين تظل غير كافية لمواكبة التطورات التكنولوجية والتهديدات السيبرانية المعقدة ، على الرغم من تشريع (قانون الجرائم الإلكترونية) لعام (٢٠١٥) ، ولكن يواجه تحديات من حيث التنفيذ والتطبيق على أرض الواقع [٢٥].

٢. الحاجة إلى بناء الثقة بين الأطراف المعنية :

أحد أبرز جوانب التعاون السيبراني الإقليمي هو بناء الثقة بين الدول المعنية. في حالة العراق، فإن العمل على تهيئة بيئة قانونية وسياسية تشجع على التعاون مع الدول الأخرى في مجالات الأمن السيبراني. يعد بناء الثقة أمرًا بالغ الأهمية في تعزيز التعاون بين القطاعين العام والخاص، وكذلك بين الدول المختلفة [٢٦].

٣. تحديات السيادة والخصوصية :

من التحديات القانونية الرئيسية في تطبيق تجربة (ASEAN) في العراق هي مسألة السيادة الرقمية وحماية الخصوصية. إن التعاون السيبراني يتطلب تبادل البيانات والمعلومات بين الدول، وهو ما يثير مخاوف بشأن حماية الخصوصية وحماية السيادة الرقمية للدول. فإن الجرائمة السيبرانية بشكل عام تكون خطرة عابرة للحدود و تتطلب جهوداً كبيرة تتضمن التعاون بين عدة أطراف بغية التعرف على مرتكبيها . في العراق فيما يخص السيادة، قد تواجه الحكومة العراقية تحديًا في التنسيق مع دول أخرى بشأن تبادل المعلومات السيبرانية ، حيث تظل القضايا السياسية والأمنية في بعض الحالات عائقًا رئيسيًا. لذلك، من المهم أن يتم ضمان التنسيق مع إحترام السيادة الرقمية للعراق[٢٧].

---

(٢٤) رعد خضير صليبي، "تعزيز الأمن السيبراني في العراق"،٥١٧.

(٢٥) مصدر سبق ذكره ،٥١٩.

(٢٦) مصدر سبق ذكره ،٥١٧.

(٢٧) هاشم، فائز ذنون. "تأثير الإنترنت على مبدأ السيادة." مجلة كلية القانون، جامعة النهرين، بغداد، العدد ١٧، المجلد ٢ (٢٠١٥): ٣٤٦.

٤ . تطوير البنية التحتية والتدريب:

تعتبر البنية التحتية التقنية أحد الأبعاد الحاسمة في تطبيق تجربة (ASEAN) في العراق. يتعين على العراق تطوير وتحسين بنية تحتية سيبرانية تتسم بالمرونة، بحيث تكون قادرة على مواجهة التهديدات المتزايدة. كما ينبغي على العراق أن يستثمر في تدريب الكوادر المتخصصة في مجال الأمن السيبراني، حيث يعد تطوير الموارد البشرية أمرًا بالغ الأهمية لضمان التنفيذ الفعال لأي سياسات تتعلق بالأمن السيبراني. برامج التدريب المشتركة مع دول الجوار أو مع الوكالات الإقليمية والدولية يمكن أن تساعد في سد هذه الفجوة [٢٨] .

المطلب الثالث: الأدوات والآليات اللازمة لتعزيز التعاون السيبراني الإقليمي للعراق :

يمثل تعزيز التعاون السيبراني الإقليمي خطوة استراتيجية للعراق في مواجهة التحديات الرقمية العابرة للحدود، خاصة في ظل تصاعد الهجمات السيبرانية التي تهدد الأمن الوطني والإقليمي. لتحقيق هذا الهدف، يحتاج العراق إلى تبني مجموعة من الأدوات والآليات التي تساهم في بناء منظومة سيبرانية متكاملة قادرة على التصدي للتحديات المستجدة، وتعزيز شراكاته مع الدول الإقليمية.

أولى هذه الأدوات هي تطوير (البنية التحتية الرقمية الوطنية) التي تُعد الأساس لأي استراتيجية أمن سيبراني. مما يعني ضرورة أن تتضمن هذه الخطوة تحديث الأنظمة والشبكات القائمة لتواكب أحدث التقنيات، ما يساهم في تقليل نقاط الضعف التي قد تستغلها الجهات المهاجمة. كذلك، فإن إنشاء مراكز بيانات وطنية يمثل أولوية لتأمين المعلومات الحساسة وتقليل الاعتماد على مزودي الخدمات الأجنبية. من جهة أخرى، تحسين شبكات الإنترنت المحلية يُعد ضرورة ملحة لتقليل احتمالات الهجمات التي تستهدف تعطيل الخدمات الرقمية[٢٩] .

إن إنشاء (مركز وطني متخصص للأمن السيبراني) يُعد من الأدوات الرئيسة لتعزيز قدرة العراق على مراقبة التهديدات السيبرانية والاستجابة لها. يمكن لهذا المركز أن يكون هدفاً لتأسيس مركز إقليمي يشمل دول الجوار لاحقاً ، بما يعزز التنسيق وتبادل المعلومات والخبرات. ومن المهم أن يتم ربط هذا

---

(28)ASEAN Foundation. "Implementing Partner for ASEAN Cybersecurity Skilling Programme." Accessed December 15, 2024. https://wwwaseanfoundationorg.translate.goog/implementing_partner_for_asean_cybersecurity_skilling_programme?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=en&_x_tr_pto=wapp.

(٢٩) شيماء تركان صالح ، الأمن الوطني العراقي و التهديدات السيبرانية ... الإرهاب السيبراني أنموذجاً ، مجلة تكريت للعلوم السياسية ، جامعة تكريت ، العدد ٣٣ ، ٢٠٢٣ ، ص ٢٤٣ .

المركز بشبكات دولية مثل (فرق الاستجابة للطوارئ الحاسوبية) لضمان التواصل الفوري مع المجتمع السيبراني العالمي[٣٠] .

جانب آخر لا يقل أهمية هو تطوير الإطار التشريعي والتنظيمي. إذ يحتاج العراق إلى إقرار قوانين شاملة تغطي الجرائم السيبرانية بأنواعها، بما في ذلك الاختراق، الابتزاز، وسرقة البيانات. كما ويجب أن تكون هذه القوانين متوافقة مع المعايير الدولية، مثل اتفاقية الجرائم السيبرانية (بودابست)، لضمان التكامل مع الجهود الدولية في هذا المجال. كما يجب تسهيل التعاون القضائي بين العراق ودول المنطقة لتفعيل آليات تسليم المطلوبين ومشاركة الأدلة الرقمية بين الجهات القضائية[٣١] .

مع ضرورة بناء القدرات البشرية يمثل محورًا أساسيًا في تعزيز الأمن السيبراني. حيث يعاني العراق من نقص في الكفاءات المتخصصة، مما يتطلب إطلاق برامج تدريب وطنية بالتعاون مع الجامعات والمؤسسات التقنية لتأهيل جيل جديد من خبراء الأمن السيبراني. كما أن الشراكات الأكاديمية مع الجامعات الدولية والإقليمية يمكن أن تساهم في تقديم برامج دراسات عليا متخصصة، تسهم في سد الفجوة المعرفية. يمكن أيضًا تشجيع الشركات التقنية المحلية على تقديم حلول مبتكرة تُسهم في تحسين البنية التحتية السيبرانية[٣٢] .

على المستوى الإقليمي والدولي، يمكن للعراق تعزيز التعاون من خلال توقيع اتفاقيات ثنائية ومتعددة الأطراف مع دول الجوار لتنسيق الجهود في مواجهة التهديدات السيبرانية المشتركة. إنشاء منصة إلكترونية إقليمية لتبادل المعلومات حول الهجمات والتهديدات الناشئة يُعد خطوة مهمة في هذا السياق. من جهة أخرى، فإن التعاون مع منظمات دولية مثل "الاتحاد الدولي للاتصالات" و"المنتدى الاقتصادي العالمي" يمكن أن يوفر للعراق موارد تقنية وتمويلًا إضافيًا لتعزيز بنيته التحتية الرقمية[٣٣] .

لا يمكن إغفال أهمية تعزيز الوعي المجتمعي بوصفه جزءاً من استراتيجية الأمن السيبراني. يتطلب ذلك إطلاق حملات توعية وطنية لتعريف المواطنين والمؤسسات بأهمية الأمن السيبراني وسبل حماية البيانات الشخصية. إدراج مواد تعليمية حول الأمن الرقمي في المناهج الدراسية على مختلف المستويات يُعد خطوة مهمة لبناء وعي مبكر لدى الأجيال القادمة[٣٤] .

---

(٣٠)المصدر نفسه ، ٢٤٤ .

(٣١)المصدر نفسه ، ٢٤٠.

(٣٢) المصدر نفسه ، ٢٤٤ .

(33) *Tahawultech*. Last modified November 2024. https://www.tahawultech.com/features/cybersecurity-is-a-critical-necessity-for-iraqs-digital-evolution/.

(34) Ibid.

الخاتمة:

في الختام ، يمكن القول : إن التحولات الجذرية التي يشهدها العالم الرقمي، جعلت من الأمن السيبراني ضرورة إستراتيجية لا غنى عنها لضمان إستقرار المجتمعات وحماية المصالح الوطنية والإقليمية. وقد أظهرت الدراسة أن العراق يمتلك مقومات فريدة تؤهله للعب دور رئيسي في تعزيز الأمن السيبراني الإقليمي، خصوصًا في منطقة الشرق الأوسط التي تواجه تهديدات متزايدة بسبب تعقيدات الفضاء السيبراني وارتباطه بمصالح استراتيجية وأمنية متعددة الأبعاد.

تُظهر التحديات التي تواجه العراق، من ضعف البنية التحتية الرقمية إلى ضعف التشريعات القانونية الشاملة، أهمية التحرك الجاد نحو بناء إطار وطني وإقليمي متكامل للأمن السيبراني. ومع ذلك، فإن هذه التحديات ليست عوائق دائمة، بل يمكن تحويلها إلى فرص للتطوير من خلال تبني استراتيجيات متقدمة تركز على الاستثمار في التكنولوجيا، والتعاون الإقليمي والدولي، وبناء القدرات البشرية المتخصصة.

إن التعاون السيبراني العابر للحدود يُعد خيارًا استراتيجيًا لا يمكن للعراق تجاهله، حيث إنه يشكل وسيلة فعالة لمواجهة التحديات الرقمية المشتركة، مثل الجرائم الإلكترونية والهجمات السيبرانية الموجهة نحو البنى التحتية الحيوية. من خلال تعزيز شراكاته الإقليمية والدولية، يمكن للعراق أن يتحول إلى نموذج يُحتذى به في بناء أنظمة سيبرانية متطورة قادرة على التصدي للتهديدات العابرة للحدود، مع تعزيز الاقتصاد الرقمي وتحقيق التنمية المستدامة.

رغم أن الطريق نحو تحقيق هذا الهدف يتطلب جهودًا مستمرة، فإن التجارب الإقليمية الناجحة، مثل تجربة دول جنوب شرق آسيا (ASEAN)، تقدم دروسًا قيمة يمكن للعراق أن يستفيد منها. حيث إن إنشاء مراكز إقليمية للأمن السيبراني، وتطوير إطار قانوني موحد، وتبني سياسات قائمة على الشراكة والثقة المتبادلة، هي أدوات أساسية يمكن للعراق توظيفها لتعزيز مكانته بوصفه دولة محورية في مواجهة التحديات السيبرانية.

حيث يمثل الأمن السيبراني أحد الركائز الأساسية لاستقرار الدولة الحديثة وتنميتها. ومن خلال تبني نهج استراتيجي شامل ومتكامل، يمكن للعراق أن يضمن ليس فقط حماية فضائه الرقمي، بل أيضًا المساهمة الفاعلة في تعزيز أمن واستقرار المنطقة . إن نجاح العراق في هذا المجال لن يقتصر أثره على الداخل فحسب، بل سيمتد ليشمل تطوير منظومة إقليمية قوية قادرة على مواجهة التحديات المستقبلية وتعزيز التكامل الرقمي بين دول المنطقة.

الإستنتاجات :

١. تعاظم أهمية الأمن السيبراني في العصر الرقمي الذي أصبح عنصرًا أساسيًا في حماية المصالح الوطنية والإقليمية، مع تنامي التحديات التي تهدد البنى التحتية الرقمية للدول.

٢. تعدد و تتنوع التهديدات السيبرانية التي تواجه العراق والمنطقة لتشمل الجرائم الإلكترونية، الهجمات التقنية المتطورة، والابتزاز الرقمي، إضافة إلى استخدام الهجمات السيبرانية بوصفها أداة للحروب غير التقليدية بين الدول.

٣. إن ضعف البنية التحتية الرقمية العراقية مع أنظمة حماية قديمة، تجعله أكثر عرضة للهجمات السيبرانية، خاصة تلك التي تستهدف القطاعات الحيوية مثل : المؤسسات الحكومية والبنوك وشبكات الطاقة.

٤. رغم الجهود المبذولة، لا تزال التشريعات السيبرانية في العراق تحتاج إلى تطوير لمواكبة التطورات التكنولوجية والتهديدات الحديثة ، الأمر الذي يعيق الملاحقة القانونية للجرائم السيبرانية.

٥. يشكل نقص المهندسين وخبراء الأمن السيبراني تحديًا كبيرًا للعراق، مما يستدعي إطلاق برامج تدريبية مكثفة لتطوير الكفاءات المحلية القادرة على التصدي للهجمات السيبرانية بالتعاون مع جهات إقليمية فاعلة في هذا المجال .

٦. إن التجربة الإقليمية لرابطة دول جنوب شرق آسيا :(ASEAN) قدمت تجربة أنموذجية يمكن للعراق والدول العربية الاستفادة منه، لا سيما في إنشاء مراكز إقليمية للأمن السيبراني وتوحيد الجهود الرامية لمواجهة التهديدات العابرة للحدود.

٧. يمكن للعراق أن يلعب دورًا محوريًا في تعزيز التعاون الإقليمي في مجال الأمن السيبراني من خلال تبادل المعلومات وتنسيق الجهود مع دول الجوار، مما يعزز استقراره الرقمي والاقتصادي.

التوصيات :

١. تعزيز البنية التحتية الرقمية الوطنية عبر من خلال الاستثمار في تحديث الأنظمة والشبكات التقنية لتقليل نقاط الضعف التي تستغلها الهجمات السيبرانية.
٢. إنشاء مركز وطني بالشراكة مع جهات إقليمية للأمن السيبراني يتولى رصد التهديدات، والتنسيق مع مراكز مشابهة في دول الجوار، لضمان استجابة سريعة وفعالة.
٣. تطوير التشريعات القانونية السيبرانية عن طريق إقرار قوانين شاملة تتماشى مع المعايير الدولية، وتنظيم آليات لتسليم المطلوبين عبر التعاون القضائي الإقليمي.
٤. العمل على بناء و تطوير القدرات البشرية بإطلاق برامج تدريبية متخصصة بالتعاون مع الجامعات المحلية والدولية، وتطوير الكفاءات القادرة على إدارة التحديات التقنية.
٥. تعزيز الوعي المجتمعي من خلال حملات توعوية وطنية تهدف إلى تثقيف الأفراد والمؤسسات حول المخاطر السيبرانية وسبل الوقاية منها.
٦. إنشاء منصة إقليمية مشتركة لتبادل المعلومات تهدف إلى تسهيل التنسيق بين الدول لتتبع التهديدات السيبرانية والرد عليها بشكل جماعي.
٧. توسيع الشراكات الدولية بهدف الإستفادة من الخبرات والتقنيات المتقدمة التي تقدمها الدول والمؤسسات الدولية المتخصصة في الأمن السيبراني.

المصادر :

١. العلي، علي زياد. "التحديات غير المرئية للأمن الوطني العراقي." مركز البيان للدراسات والتخطيط، قسم الأبحاث، بغداد، ٢٦ يونيو ٢٠١٨، https://www.bayancenter.org/2018/06/4565/.

٢. الزبيدي، زهير خضير عباس، والتميمي، ظفر عبد مطر. "العراق والأمن السيبراني .. الفرص والتحديات." مجلة واسط للعلوم الإنسانية، جامعة واسط، العدد ١٨، ٢٠٢٢.

٣. صالح، شيماء تركان. "الأمن الوطني العراقي والتهديدات السيبرانية ... الإرهاب السيبراني أنموذجاً." مجلة تكريت للعلوم السياسية، جامعة تكريت، العدد ٣٣، ٢٠٢٣.

٤. صليبي، رعد خضير. "تعزيز الأمن السيبراني في العراق." مجلة دراسات دولية، مركز الدراسات الإستراتيجية والدولية، جامعة بغداد، العدد ٩٩ (٢٠٢٤).

٥. سالم، ماجد صدام. "الأمن السيبراني العراقي وأثره على قوة الدولة." مجلة العلوم التربوية والإنسانية، جامعة ميسان، العدد ١٨، ٢٠٢٢.

٦. لحمر، حميدة، وحموم، فريدة. "التعاون الأمني في جنوب شرق آسيا، في مواجهة تهديدات الأمن السيبراني." مجلة طبنة للدراسات العلمية والأكاديمية، الجزائر، العدد ١، ٢٠٢١.

٧. كيطان، إسراء نادر. "الجريمة الإلكترونية والحاجة لتشريع قانون مكافحتها." مقالة، الموقع الرسمي لمجلس القضاء الأعلى، ٣ ديسمبر ٢٠٢٤، https://sjc.iq/view.75479/.

٨. هاشم، فائز ذنون. "تأثير الإنترنت على مبدأ السيادة." مجلة كلية القانون، جامعة النهرين، بغداد، العدد ١٧، المجلد ٢ (٢٠١٥).

9. Abdul Rahman, Muhammad Faizal. "How ASEAN's Cybersecurity Push Could Protect People and Economies." The Diplomat, November 2024. https://thediplomat.com/2024/11/how-aseans-cybersecurity-push-could-protect-people-and-economies/.

10. Tahawultech. Last modified November 2024. https://www.tahawultech.com/features/cybersecurity-is-a-critical-necessity-for-iraqs-digital-evolution/.

11. ASEAN Foundation. "Implementing Partner for ASEAN Cybersecurity Skilling Programme." Accessed December 15, 2024. https://www.aseanfoundation.org/implementing_partner_for_asean_cybersecurity_skilling_programme.

12. Roy-Choudhury, Amit. "What the World Can Learn from ASEAN's Cyber Cooperation." GovInsider. Accessed October 2023.https://govinsider.asia/intl-en/article/what-the-world-can-learn-from-aseans-cyber-cooperation-amit-roy-choudhury/.

13. Association of Southeast Asian Nations. *ASEAN Cybersecurity Cooperation Strategy 2021–2025*. Jakarta: ASEAN Secretariat, 2021.

14. Mahusin, Mahirah, and Hilmy Prilliadi. "Strengthening ASEAN's Cybersecurity: Collaborative Strategies for Enhanced Resilience." *ERIA Policy Brief*, no. 2024-06 (November 2024).

15. Abdul Rahman, Muhammad Faizal. "How ASEAN's Cybersecurity Push Could Protect People and Economies." *The Diplomat*, November 2024. https://thediplomat.com/2024/11/how-aseans-cybersecurity-push-could-protect-people-and-economies/.