جامعة النهرين
كلية العلوم السياسية
قسم النظم السياسية
Ali.sabah@nahrainuniv.edu.iq

تحديات الامن السيبراني على الاستقرار الامني في العراق

علي صباح محمد
Ali sabah mohammed

الملخص:

يعد الأمن السيبر اني من أهم التحديات التي تواجه العالم الحديث، وخاصة في العراق. تز ايدت الهجمات السيبر انية على البنيةالتحتية الحيوية مثل شبكات الكهرباء والأنظمة المالية، مما أدى إلى تأثيرات كبيرة على الاستقرار الأمني والاقتصادي. العراق يواجه تحديات كبيرة في هذا المجال، تشمل نقص التكنولوجيا الحديثة، وضعف البنية التحتية التقنية، ونقص الوعي والتدريب بين المواطنين والمسؤولين، فضلاً عن المشاكل القانونية والتنظيمية والاقتصادية. تحسينالأمن السيبر اني يتطلب استثمارات كبيرة في التكنولوجيا والتدريب، بالأضافه إلى تطوير تشريعات قوية وتفعيل التعاون الدولي. من خلال هذه الجهود، يمكن تعزيز الأمن السيبر اني في العراق وضمان استقرار أكبر في المستقبل.

الكلمات المفتاحية:

(الامن السيبر اني , الاستقرار الامني , العراق , البنى التحتية)

Abstract

Cybersecurity is one of the most significant challenges facing the modern world, especially in Iraq. Cyberattacks on critical infrastructure such as power grids and financial systems have increased, leading to significant impacts on security and economic stability. Iraq faces substantial challenges in this area, including a lack of modern technology, weak technical infrastructure, and insufficient awareness and training among citizens and officials, in addition to legal, regulatory, and economic issues. Improving cybersecurity requires substantial investments in technology and training, along with developing robust legislation and enhancing international cooperation. Through these efforts, .cybersecurity in Iraq can be strengthened, ensuring greater stability in the future

المقدمــة

تعتبر التحديات السيبرانية من اهم القضايا في العصر الحالي، حيث اصبحت التكنولوجيا جزء لا يتجزء من حياتنا اليومية. في العراق، تواجه البلاد العديد من الصعوبات في مجال الامن السيبراني، مما يؤثر بشكل كبير على الاستقرار الامني. يمكن لهذه التحديات ان تكون ناتجة عن عوامل مختلفة مثل الهجمات الالكترونية المستمرة، ونقص في البنيةالتحتية السيبرانية، والتطور السريع للتكنولوجيا دون وجود الحمايه الكافية , الهجمات السيبرانية يمكن ان تستهدف البنيةالتحتية الحيوية، مثل شبكات الكهرباء والانظمة الماليه والقطاعات الحكومية، مما يؤدي الى تعطل الخدمات الاساسيه و اثارة الفوضى. بالاضافه الى ذلك، يمكن لهذه الهجمات ان تستغل الثغرات الامنية للتجسس وسرقة البيانات الحساسة، مما يشكل تهديدا على الامن القومي كما ان نقص الوعي والتدريب في مجال الامن السيبراني بين الافراد والمؤسسات يمثل تحديا اضافيا يحتاج العراق الى استراتيجيات فعاله لتعزيز الامن السيبراني، تشمل تطوير الكفاءات الوطنية وتحسين البنية التحتية.

أهميـة البحث

الامن السيبراني هو ممارسة حماية الانظمة والشبكات والبرامج من الهجمات الرقمية. تهدف هذه الهجمات عادة الى الوصول الى المعلومات الحساسه او تدميرها او تغييرها، و ايضا تعطيل العمليات العادية. في عالم اليوم، مع التوسع الهائل في استخدام التكنولوجيا والانترنت، اصبح الامن السيبراني اكثر اهميه من اي وقت مضى أهمية الامن السيبراني تكمن في حماية البيانات الحساسة، سواء كانت بيانات شخصية او مالية او حكومية. من دون اجراءات امنيه فعالة، يمكن للهجمات السيبرانية ان تتسبب في اضرار جسيمة، مثل فقدان المعلومات، وخسائر ماليه، و انتهاك الخصوصية، وتعطل الخدمات الحيوية. بالاضافه الى ذلك، يعزز الامن السيبراني الثقة بين المستخدمين في استخدام التكنولوجيا ويشجع على الابتكار والنمو الاقتصادي يعتبر الامن السيبراني عنصر اساسي في الحفاظ على الاستقرار والامان في العالم الرقمي الحديث، ويجب على الجميع، من افراد وشركات وحكومات، ان يكونوا واعين بالتحديات السيبرانية وان يعملوا معا لتطوير حلول امنية قوية وفعالة.

مشكلة البحث

تتمثل مشكلة البحث في تحديد وتحليل التحديات التي تواجه الأمن السيبراني في العراق وكيفية تأثيرهذه التحديات على الاستقرار الأمني والاقتصادي للبلاد. على الرغم من التقدم التكنولوجي السريع والتوسع في استخدام الإنترنت، يواجه العراق تهديدات سيبرانية متزايدة تؤثرعلى البنيةالتحتية الحيوية، مثل شبكات الكهرباء والأنظمة المالية، مما يؤدي إلى تأثيرات سلبية على الأمن الوطني والاجتماعي والاقتصادي. يشمل ذلك نقص التكنولوجيا الحديثة، ضعف البنيةالتحتية التقنية، قلة الوعي والتدريب، بالأضافه إلى التحديات القانونية والتنظيمية والاقتصادية. يتطلب تحسين الأمن السيبراني في العراق استثمارات كبيرة في التكنولوجيا والتدريب، وتطوير تشريعات قوية، وتعزيز التعاون الدولي. لذا، يسعى البحث إلى تقديم توصيات وحلول عمليهلمعالجة هذه التحديات وتعزيز الأمن السيبراني في البلاد.

فرضية البحث

يفترض هذا البحث أن التحديات المتعددة التي تواجه الأمن السيبراني في العراق، مثل نقص التكنولوجيا الحديثة، ضعف البنية التحتية التقنية، قلة الوعي والتدريب، والتحديات القانونية والتنظيمية والاقتصادية، تؤثر بشكل كبير على الاستقرار الأمني والاقتصادي للبلاد. ويعتمد البحث على الفرضية أن تحسينهذه الجوانب من خلال استثمارات في التكنولوجيا والتدريب، تطوير تشريعات قوية، وتعزيز التعاون الدولي، سيؤدي إلى تعزيز الأمن السيبراني وتحقيق استقرار أكبر في العراق.

منهجية البحث

ستعتمد منهجية البحث على المنهج الوصفي التحليلي لوصف وتحليل الوضع الحالي للأمن السيبراني في العراق، من خلال جمع البيانات الأولية عبر مقابلات مع خبراء الأمن السيبراني ومسؤولين حكوميين، واستخدام الاستبيانات لجمع آراء المتخصصين. كما سيتم جمع البيانات الثانوية من مراجعة الأدبيات والدراسات السابقة والتقارير الحكومية والدولية سيتم تحليل هذه البيانات باستخدام تقنيات التحليل الكمي والكيفي لاستخلاص الأنماط والتحديات الرئيسية. بالأضافه إلى ذلك، سيتم دراسة حالات سيبرانية سابقة في العراق وحالات من دول أخرى مشابهة لاستخلاص الدروس المستفادة. وفي النهاية، سيتم وضع توصيات وحلول عمليه لتعزيز الأمن السيبراني في العراق بناءً على نتائج التحليل.

المحور الاول : مفهوم الامن السيبراني والاستقرار الامني

تعد مفاهيم الأمن السيبراني والاستقرار الأمني من القضايا الحيوية في العصر الرقمي الحديث. الأمن السيبراني يشير إلى الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية التي قد تتسبب في أضرار كبيرة للبنى التحتية الحساسة والمؤسسات المختلفة. في الوقت الذي تتزايد فيه الاعتماد على التكنولوجيا في جميع جوانب الحياة، تزداد أيضاً التهديدات السيبرانية التي يمكن أن تؤدي إلى تعطيل الخدمات الحيوية وسرقة البيانات وانتهاك الخصوصية.

اولا : مفهوم الأمن السيبراني :

1. تعريف الأمن السيبراني: ان الامن السيبراني هو ممارسة حماية الانظمة والشبكات والبرامج من الهجمات الرقمية. يهدف الامن السيبراني الى منع الوصول غير المصرح به، واكتشاف التهديدات، والاستجابة للحوادث الامنية، واستعادة النظام بعد الهجوم. في العالم الرقمي المتزايد التعقيد، اصبح الامن السيبراني ضرورة لضمان سلامة البيانات والمعلومات الحساسة التي تعتمد عليها الحكومات والشركات والافراد.(1)

2. مكونات الأمن السيبراني(2)

1 - الحماية تتضمن الحماية تطبيق اجراءات وقائية لمنع الهجمات السيبرانية قبل حدوثها. هذا يشمل استخدام جدران الحماية، وبرامج مكافحة الفيروسات، وتشفير البيانات، وتحديث البرامج بشكل منتظم.

2 - الكشف : الكشف هو عملية رصد ومراقبة الانظمة لاكتشاف النشاطات المشبوهة او غير المعتادة. يستخدم الكشف تقنيات مثل انظمة اكتشاف التسلل، وتحليل السلوك، والتنبيهات المبكرة للكشف عن التهديدات المحتملة.

3 - الاستجابة: عندما يتم الكشف عن هجوم سيبراني، يجب على الفرق الامنية اتخاذ اجراءات فورية لاحتواء التهديد وتقليل الاضرار. يتضمن الاستجابة تحليل الحادث، وتطبيق اصلاحات، والتواصل مع الجهات المعنية.

4 - التعافي: التعافي يتضمن اعادة النظام الى وضعه الطبيعي بعد الهجوم. هذا يشمل استعادة البيانات من النسخ الاحتياطية، وتحديث السياسات الامنية، والتعلم من الحادث لتحسينالاجراءات الوقائية في المستقبل.

ثانيا : مفهوم الاستقرار الأمني:

1 - تعريف الاستقرار الأمني: الاستقرار الامني هو حالة من الامان والاستقرار داخل المجتمع، حيث تكون الهياكل الاساسية والخدمات الحيوية محمية من التهديدات والتدخلات التي قد تؤدي الى الفوضى او الضرر. يشمل الاستقرار الامني حماية الحدود، وضمان الامان الداخلي، والاستعداد لمواجهة الكوارث الطبيعية والبشرية.

2 - علاقة الأمن السيبراني بالاستقرار الأمني: في العصر الحديث، اصبح الامن السيبراني جزء لا يتجزأ من الاستقرار الامني. الهجمات السيبرانية يمكن ان تهدد الاستقرار الامني من خلال استهداف البنيةالتحتية الحيوية مثل شبكات الكهرباء والانظمة المالية. كما يمكن ان تؤدي الى فقدان الثقة في الحكومة والشركات، مما يساهم في زعزعة الاستقرار الاجتماعي والاقتصادي.(3)

3 – تاثير الأمن السيبراني على الاستقرار الأمني :

الامن السيبراني يؤثر بشكل مباشر على الاستقرار الامني من خلال حماية الانظمة والشبكات التي تعتمد عليها المجتمعات الحديثة(4) . الهجمات السيبرانية الناجحة يمكن ان تؤدي الى تعطل الخدمات الاساسية مثل الكهرباء والمياه والرعاية الصحية، مما يؤدي الى فوضى وعدم استقرار. بالأضافة الى ذلك، يمكن ان تؤدي الى خسائر مالية ضخمة، و انتهاك الخصوصية، والاضرار بالسمعة(5) .

ان الامن السيبراني يلعب دورا حاسما في الحفاظ على الاستقرار الامني في العصر الرقمي. بدون اجراءات امنية فعالة، يمكن للهجمات السيبرانية ان تؤدي الى فوضى وعدم استقرار، مما يؤكد على الحاجة الملحة لتطوير وتحسين استراتيجيات الامن السيبراني على مستوى عالمي ومحلي(6).

المحور الثاني : تحديات الأمن السيبراني في العراق

تعد تحديات الامن السيبراني من اهم القضايا التي تواجه العالم في الوقت الحالي. في ظل التطور التكنولوجي السريع و انتشار استخدام الانترنت بشكل كبير، اصبحت الهجمات السيبرانية تشكل تهديدا حقيقيا على مختلف القطاعات سواء كانت حكومية او خاصة الامن السيبراني ليس مجرد خيار بل هو ضرورة ملحة لحماية البيانات والمعلومات الحساسة التي يمكن ان تكون عرضة للسرقة او التلاعب. التحديات السيبرانية تشمل نقص التكنولوجيا الحديثة وضعف البنية التحتية وقلة الوعي والتدريب بين الافراد والمؤسسات. كما ان التشريعات القانونية لمواكبة هذا التطور غالبا ما تكون غير كافية، مما يزيد من صعوبة مواجهة هذه التهديدات. في هذا السياق، يعد تعزيز الامن السيبراني من خلال استراتيجيات فعالة واستثمارات مستدامة امر في بالغ الاهمية لضمان الامان الرقمي والحفاظ على استقرار المجتمعات والاقتصادات.

اولا: الوضع الحالي للأمن السيبراني في العراق:

تحليل الوضع الراهن للأمن السيبراني في العراق ان الوضع الراهن للأمن السيبراني في العراق يمكن وصفه بأنه غير متقدم ويحتاج الى الكثير من التطوير. العراق يواجه تهديدات سيبرانية مستمرة تتراوح من هجمات القرصنة الى البرمجيات الخبيثة. بينما هناك جهود مبذولة لتحسين الامن السيبراني الا انها غالبا ما تكون غير كافية مقارنة بحجم التهديدات الموجودة.

1 - تقييم للبنية التحتية الرقمية والأمنية: البنية التحتية الرقمية في العراق مازالت في طور النمو على الرغم من وجود بعض التحسينات في السنوات الاخيرة، الا ان البلاد تعاني من ضعف في الشبكات والانظمة التكنولوجية. البنية التحتية الامنية ايضا ليست على مستوى التحديات، حيث تفتقر الى التجهيزات والتقنيات الحديثة اللازمة لمواجهة الهجمات السيبرانية بشكل فعال(7).

2 - التحديات التقنية و نقص التكنولوجيا الحديثة: العراق يواجه نقصا كبيرا في التكنولوجيا الحديثة المتعلقة بالامن السيبراني. العديد من المؤسسات تعتمد على تقنيات قديمة وغير محدثة، مما يجعلها عرضة للهجمات السيبرانية. كما ان الاستثمار في التكنولوجيا الحديثة محدود، مما يعيق التقدم في هذا المجال(8).

3 - ضعف البنية التحتية التقنية:البنيةالتحتية التقنية في العراق تعاني من عدة مشاكل. الشبكات غالبا ما تكون بطيئة وغير مستقرة، وهناك نقص في مراكز البيانات المجهزة بشكل جيد. هذه الظروف تجعل من الصعب تطبيق حلول امنية متقدمة وحماية البيانات بشكل فعال.

ثانيا : التشريعات والقوانين المتعلقة بالأمن السيبراني:

العراق يفتقر الى تشريعات وقوانين واضحة وشاملة تتعلق بالامن السيبراني. القوانين الموجودة غالبا ما تكون قديمة وغير محدثة لتتماشى مع التهديدات الحديثة. هذا النقص في التشريعات يجعل من الصعب على السلطات التعامل مع الجرائم السيبرانية بفعالية.

1 - ضعف تنفيذ القوانين الموجودة: حتى مع وجود بعض القوانين المتعلقة بالامن السيبراني، فإن تنفيذها غالبا ما يكون ضعيفا. هناك نقص في الموارد والتدريب للجهات المسؤولة عن تطبيق هذه القوانين، مما يؤدي الى ضعف الرقابة وعدم القدرة على ملاحقة الجرائم السيبرانية بشكل فعال.

2 - تعزيز تنفيذ القوانين والرقابة : يجب تعزيز تنفيذ القوانين والرقابة لضمان ان جميع الجهات تلتزم بالاجراءات الامنية. هذا يشمل انشاء هيئات رقابية قوية، وتوفير الموارد اللازمة للجهات الامنية لتطبيق القوانين بفعالية . (9)

تحديات الامن السيبراني في العراق متعددة ومعقدة. يتطلب التعامل معها جهودا مشتركة من الحكومة والقطاع الخاص والمجتمع المدني. من الضروري تحسين البنيةالتحتية التقنية، وتعزيز الوعي والتدريب، وتطوير التشريعات والقوانين، وزيادة التمويل المخصص لهذا المجال. بدون هذه الجهود، سيبقى العراق عرضة للهجمات السيبرانية التي يمكن ان تؤثر بشكل كبير على استقراره الامني والاقتصادي.

ثالثا : الهجمات السيبرانية على البنية التحتية الحيوية:

الهجمات السيبرانية على البنيةالتحتية الحيوية في العراق تمثل تهديدا كبيرا للأمن الوطني. البنيةالتحتية الحيوية تشمل شبكات الكهرباء، المياه، النقل، والاتصالات، وهذه كلها تعتبر اهداف جذابة للهجمات السيبرانية مثلا اذا تم استهداف شبكات الكهرباء، يمكن ان يؤدي ذلك الى انقطاع التيار الكهربائي على نطاق واسع(10) مما يسبب فوضى واضطرابات كبيرة في الحياة اليومية للمواطنين. ايضا، الهجمات على انظمة النقل يمكن ان تعطل حركة المروروتؤثر على الامدادات اللوجستية، مما يزيد من التحديات الاقتصادية والأجتماعية في البلاد.

رابعا : تأثير الهجمات السيبرانية على الأمن الاقتصادي والاجتماعي:

الهجمات السيبرانية لها تأثير كبير على الامن الاقتصادي والاجتماعي في العراق. الهجمات التي تستهدف القطاع المالي يمكن ان تؤدي الى سرقة الاموال والمعلومات المالية الحساسة(11)، مما يضربثقة الجمهورفي النظام المالي ويؤدي الى خسائر اقتصادية كبيرة. بالأضافة الى ذلك، الهجمات التي تستهدف المؤسسات الصحية يمكن ان تعطل الخدمات الطبية وتؤدي الى ازمات صحية، مما يزيد من معاناة المواطنين. ايضا، الهجمات السيبرانية التي تستهدف البيانات الشخصية يمكن ان تؤدي الى انتهاك الخصوصية ونشر المعلومات الحساسة، مما يسبب قلقا اجتماعيا ويؤثر على الامن النفسي للمواطنين.(12)

التوصيات والحلول

1 - تعزيز البنية التحتية التقنية:استثمارفي التكنولوجيا الحديثة: من الضروري ان يستثمر العراق في التكنولوجيا الحديثة لتحسينالامن السيبراني. هذا يشمل استخدام انظمة متقدمة للحماية والكشف والاستجابة للهجمات السيبرانية. ايضا، يجب تحديث الاجهزة والشبكات بانتظام لضمان انها قادرة على مقاومة التهديدات الحديثة.

2 - تحسين البنية التحتية الرقمية:يجب تحسين البنيةالتحتية الرقمية في العراق لضمان استقرار وكفاءة الخدمات الالكترونية. هذا يشمل توسيع نطاق الشبكات، وتحسين سرعة الانترنت، وانشاء مراكز بيانات متطورة. تحسينالبنيةالتحتية الرقمية يساعد في تقديم خدمات اكثر امنا وفعالية للمواطنين والشركات.

3 - برامج تدريبية وتوعوية للمواطنين والمسؤولين:من الضروري تقديم برامج تدريبية وتوعوية للمواطنين والمسؤولين لزيادة الوعي بأهمية الامن السيبراني. هذا يشمل تعليم الناس كيفية حماية انفسهم من الهجمات السيبرانية وتجنب الوقوع في الفخاخ الالكترونية. ايضا، يجب تدريب الموظفين الحكوميين على كيفية التعامل مع التهديدات السيبرانية بشكل فعال.

4 - تشجيع التعليم الأكاديمي والبحث في مجال الأمن السيبراني: يجب تشجيع التعليم الاكاديمي والبحث في مجال الامن السيبراني لخلق جيل من الخبراء والمتخصصين. هذا يشمل دعم الجامعات والمعاهد لتقديم برامج دراسية متخصصة في الامن السيبراني، وتمويل الابحاث العلمية في هذا المجال.

5 - تحسين التشريعات والتنظيمات تطوير قوانين وتشريعات قوية تتعلق بالأمن السيبراني: من الضروري تطوير قوانين وتشريعات قوية تتعلق بالامن السيبراني لحماية البيانات والانظمة. يجب ان تكون هذه القوانين متوافقة مع المعايير الدولية وتغطي جميع جوانب الامن السيبراني، من حماية البيانات الشخصية الى التصدي للجرائم الالكتروني

6 - تعزيز تنفيذ القوانين والرقابة: يجب تعزيز تنفيذ القوانين والرقابة لضمان ان جميع الجهات تلتزم بالاجراءات الامنية. هذا يشمل انشاء هيئات رقابية قوية، وتوفير الموارد اللازمة للجهات الامنية لتطبيق القوانين بفعالية.

7 - زيادة التمويل والدعم: تخصيص موارد مالية كافية للأمن السيبراني يجب تخصيص موارد مالية كافية لتحسينالامن السيبراني في العراق. هذا يشمل تمويل المشاريع التقنية، وتحديث البنية التحتية، وتوفير التدريب والتعليم في هذا المجال. الاستثمار في الامن السيبراني يجب ان يكون من اولويات الحكومة لحماية البلاد من التهديدات السيبرانية.

8 - تشجيع التعاون الدولي والأقليمي في مجال الأمن السيبراني: من الضروري تشجيع التعاون الدولي والأقليمي في مجال الامن السيبراني. التعاون مع الدول الاخرى يمكن ان يوفر للعراق خبرات وموارد اضافية، ويساعد في تبادل المعلومات حول التهديدات السيبرانية. ايضا، يمكن ان يساهم في تطوير استراتيجيات مشتركة لمواجهة التهديدات السيبرانية على مستوى اقليمي ودولي.

الخاتمة

يواجه العراق تحديات كبيرة في مجال الأمن السيبراني تتطلب جهوداً متكاملة لتحسينالوضع الراهن. تشمل هذه التحديات نقص التكنولوجيا الحديثة، وضعف البنيةالتحتية التقنية، ونقص الوعي والتدريب بين المواطنين والمسؤولين، فضلاً عن القضايا القانونية والتنظيمية والاقتصادية. الهجمات السيبرانية المتزايدة تهدد البنيةالتحتية الحيوية وتؤثر سلباً على الأمن الوطني والاقتصادي والاجتماعي. من خلال الاستثمار في التكنولوجيا الحديثة، وتحسينالبنيةالتحتية الرقمية، وتقديم برامج تدريبية وتوعوية، وتطوير تشريعات قوية، وتعزيز التعاون الدولي، يمكن تعزيز الأمن السيبراني في العراق بشكل كبير. هذه الجهود المشتركة ستساهم في تحقيق استقرار أكبر وأمان رقمي أفضل للمجتمع العراقي، مما يتيح فرصاً للتنمية المستدامة والنمو الاقتصادي في المستقبل

الهوامش

(1) سامر مؤيد عبداللطيف، جبار سلمان حسين، دولة في الفضاء الرقمي، مكتبة عادل للطباعة والنشر، بغداد، 2016 ، ص75 .

(2) محمد علي الكناني ، مكزنات الامن السيبراني واهميتها في حماية المعلومات ، مجلة العلوم التقنية ، العدد 15 ، 2019 ،ص 13.

(3) احمد سالم الهلالي ، الاستقرار الامني والتحديات الامنية في العراق ، جامعة بغداد ، كلية العلوم السياسية ، 2021 ، ص 19 .

(4) نبيل بن عمر ، "الهجمات السيبرانية وتأثيرها على الأمن القومي الجزائري." مجلة الشؤون الدولية، العدد 14، 2020 ، ص 38.

(5) محمد العبدالله ، الاستقرار الامني في دول الخليج ، التحديات والفرص ، مجلة العلوم الامنية ، جامعة نايف العربية للعلوم الامنية ، 2018 ، ص8 .

(6) محمد عزوزي ، الامن السيبراني في الجزائر:الهجمات والتحديات ، مجلة الدفاع الرقمي ، العدد 9 ، 2021 ، ص 79 .

(7) محمد وحيد، مهدي حسن، علاء وجيه، دور الاقتصاد الخفي في التنمية المستدامة دراسة تحليلية، مجلة تكريت للعلوم الادارية والاقتصادية، المجلد 16، العدد خاص (ج2)، تكريت،(2020)، ص34 .

(8) محمد عبدالفتاح احمد ، التحديات الامنية السيبرانية في العراق : تحليل استراتيجي ، مجلة الدراسات الامنية ، العدد 5 ، 2019 ، ص 17 .

(9) مصطفى علاء الدين ، التحديات القانونية للامن السيبراني في الشرق الاوسط :دراسة حالة العراق ، مجلة القانون الدولي العدد 16 ، 2020 ، ص 22 .

(10) عبدالرزاق معوش ، التحديات التقنية للهجمات السيبرانية في الجزائر، جامعة وهران، كلية الحاسبات والمعلومات، مجلة الحاسبات والمعلومات، العدد 7، 2021، ص 12 .

(11) محمود عبدالله ، تحليل التحديات السيبرانية في العراق وتأثيرها على الأمن الوطني." مجلة تكريت للعلوم الادارية والقانونية، المجلد 12، العدد 3، 2020 ، ص 4 .

(12) محمد بن عيسى ، الهجمات السيبرانية وتاثيرها على الاقتصاد الجزائري ، مجلة العلوم والتكنولوجيا ، العدد 15 ، 2019 ، ص 7.