مجلة إكليل للدراسات الانسانية
التصنيف الورقي: العدد 25 /آذار/2026
المجلد(7)- العدد(1)-الجزء(2) IASJ–Iraqi Academic Scientific Journals

قدرات العراق السيبرانية بين التحديات والمعالجات

م.د. علي عبد المطلب صادق
مركز الدراسات الاستراتيجية والدولية
جامعة بغداد

الكلمات المفتاحية: العراق، الأمن السيبراني، التهديدات السيبرانية

الملخص:

يتناول البحث مدارات الفضاء السيبراني وما ينطوي عليه من تعقيدات تتطور بسرعة فائقة، بحيث لانبالغ إذا قلنا بأنه لاتوجد دولة تستطيع بمفردها مسايرة التطور التكنلوجي للقوة السيبرانية، ومن الواضح أن التهديدات السيبرانية باتت تتخذ طابعا وطنيا ودوليا يطال المنشآت الحيوية في الدولة لجهات عدة رسمية أو غير رسمية، ومنفردة أو جماعية، وكذلك أعمال القطاع الخاص لغرض إستهداف التأثير على الاقتصاد الوطني والدولي وسبل عيش المواطنين سيما بعد الانتشار المطّرد في إستعمال شبكة المعلومات الالكترونية الدولية (الانترنيت)، ولم يكن العراق بمعزل عن تلك التهديدات التي شكلت بمجموعها تحديا للأمن السيبراني العراقي في نواحي البنية المادية والتقنية والبشرية المطلوبة للتصدي لأي تهديد سيبراني، وبعد إدراك تلك التحديات صار العراق يسعى باستمرار إلى مواكبة التطورات التكنلوجية السيبرانية، وبناء استراتيجية أمن سيبراني منطلقا من مبدأ ضمان أمن العراق وحماية وجوده في الفضاء السيبراني وحماية بنية المعلومات الوطنية الحيوية.

المقدمة:

يتخذ موضوع الأمن السيبراني مكانة هامة عند جميع الدول، ومع تنوع فواعل التهديدات السيبرانية تعددت سبل مواجهتها وطنيا ودوليا، وبسبب سهولة استعمال الفضاء السيبراني وقابلية التعرض للخصوم صار الفضاء السيبراني ميدانا فريدا لتحقيق مكاسب سياسية واقتصادية واجتماعية وثقافية عبر إيقاع أكبر ضرر ممكن في الطرف المقابل، ويمكن القول أن التحدي الأكبر للتهديدات السيبرانية يكمن في صعوبة تحديد مصدر الهجوم السيبراني، مما أدى الى تصاعد مسارات الحرب السيبرانية بين الدول بعد أن أصبحت المعرفة والتكنلوجيا وبنك المعلومات هي الاسلحة المستعملة في الحروب المعاصرة بدلا من الاسلحة التقليدية، وبالتالي أصبح الفضاء السيبراني ساحة صراع تخوضها الدول وفواعل أخرى تتجاوز الحدود التقليدية وسيادة الدولة، ولم يكن العراق بعيدا عن تعقيدات المشهد السيبراني

وتموضعه مابين مواجهة التحديات وتبني المعالجات في كل ما يتعلق بالفضاء السيبراني، ومع تزايد التعاملات والخدمات الالكترونية داخل العراق تعقدت تحديات الأمن السيبراني في استهداف المعلومات والتعاملات البينية في شتى القطاعات وتعرضها لخطر الاختراق والتخريب المتعمد من قبل هجمات سيبرانية تعرقل الاداء الحكومي الحيوي، ومن هنا صار لزاما على العراق التفاعل مع القوى الاقليمية والدولية تفاعل إيجابي لصد التهديدات السيبرانية، وامكانية الانضمام الى التحالفات التي تشكل منظومة أمن سيبراني مشترك.

أهمية البحث:

تظهر أهمية البحث في مدى امتلاك الدولة العراقية إمكانيات مواجهة التهديدالت السيبرانية، ومن المهم لصانع القرار العراقي معرفة مكانة العراق في مضمار الفضاء السيبراني الذي ماانفك عن التطور المتسارع، وتأكيد أن من يمتلك أعلى تكنلوجيا معلوماتية يمتلك فضاء سيبرانيا أكثر أمانا.

هدف البحث:

يعرّف البحث بالفضاء السيبراني وتهديداته وتحدياته وإمكانية معالجتها في المستوى الوطني، كما يهدف الى بيان أبعاد التهديد السيبراني والمكامن التي يستهدفها أي هجوم سيبراني محتمل، سواء في القطاعات الرسمية للدولة أو غيرها من مصالح القطاع الخاص، وبالنتيجة يكون الهدف هو الدولة وقوتها السياسية والاقتصادية والاجتماعية.

مشكلة البحث:

تنبع إشكالية البحث من جوهر القوة السيبرانية ذاتها، إذ لاقناعة مطلقة في التمكن من امتلاك قوة سيبرانية مطلقة لأي طرف، وعليه تستثار إشكالية الضعف السيبراني باستمرار، وهذا يشجع على إثارة تساؤلات عدة، أهمها كيف تستطيع الدولة الوصول لأعلى جاهزية عند مواجهة التحديات السيبرانية؟، وهل يمكن للدولة اللجوء الى بدائل لمواجهة التهديد السيبراني عوضا عن مواجهته لوحدها؟، وما هي الآليات أو الاستراتيجيات التي يمكن للدولة أن تتبناها في هذا المجال؟

فرضية البحث:

يفترض البحث أن مواجهة التحديات السيبرانية هو أمر لابد منه، مادام الفضاء السيبراني متاحا لفواعل رسمية وغير رسمية، وظاهرة ومستترة، وهذا دفع جميع الدول ومنها العراق الى التوجه نحو بناء رؤية واقعية وعملية لمعالجة تلك التحديات، وهذا يتطلب تطوير قدرات مادية وتقنية وبشرية لمواجهة تطورات التهديدات السيبرانية.

محتويات البحث:

ينطوي البحث على اربع مطالب انتظمت في مبحثين حمل المبحث الاول عنوان (مفهوم القدرات السيبرانية) وفيه مطلبين الاول (القدرات السيبرانية في المستوى الوطني)، والثاني

(القدرات السيبرانية في المستوى الدولي)، وجاء المبحث الثاني تحت عنوان (تحديات ومعالجات الأمن السيبراني العراقي) وتضمن مطلبين الاول (تحديات الأمن السيبراني العراقي)، والثاني (معالجات تهديدات الأمن السيبراني العراقي)، ثم الخاتمة والاستنتاجات والتوصيات.

المبحث الاول: مفهوم القدرات السيبرانية

توسعت استعمالات مفاهيم الفضاء السيبراني مع توسع استعمالات تقنيات التواصل الالكتروني وتقنيات تكنلوجيا المعلومات، ومع تباين توظيف قدرات الدول في مجال الامن السيبراني ما بين وسائل الهجمات السيبرانية وآليات الحماية من التهديدات السيبرانية صار لزاما على الباحثين التميز بين قدرات الهجوم وقدرات الدفاع، إذ لم تعد دولة بعينها يمكنها إحتكار القدرات السيبرانية في الدفاع والهجوم معا من دون النظر الى ساحة التنافس السريع بين الدول لتطوير قدراتها السيبرانية، فما أن تعلن دولة أنها تمكنت من تطوير قدراتها السيبرانية تعلن دولة غيرها بأنها تجاوزت تلك الامكانيات وغادرتها الى تقنيات سيبرانية أكثر تعقيدا، وعلى هذا المنوال تستمر الدول في تطوير آليات تحدي التهديدات السيبرانية، ومن أجل الاطلاع على مفاهيم القدرات السيبرانية ومعرفة حدودها قسمنا هذا المبحث على مطلبين:

المطلب الاول: القدرات السيبرانية في المستوى الوطني.

المطلب الثاني: القدرات السيبرانية في المستوى الدولي.

المطلب الاول: القدرات السيبرانية في المستوى الوطني

يشير مصطلح القدرة السيبرانية أو التحكم بالفضاء السيبراني الى ضبط الاشياء والسيطرة عليها عن بعد[1]، ويعرف بأنه الفعل المستخدم عبر الشبكات الالكترونية بهدف السيطرة على أو التعطيل لبرامج الكترونية أخرى[2]، ويمكن وصف الفضاء السيبراني بأنه عالم معلوماتي افتراضي موازي ومتداخل مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، ويحمل ذلك التداخل بعدا تكامليا ينطوي على مزايا مفيدة وعيوب خطيرة بمديات واسعة ربما تكون غير متوقعة الحصول، وأن تعاون حقيقي أو صراع فعلي يدور في الفضاء السيبراني[3].

تعد الدولة القوة القانونية الرئيسة المخولة بممارسة سلطتها على الافراد في الفضاء السيبراني، من خلال توظيفها وسائل إدارة شبكات الاتصال وأمنها وتطويرها و...غيرها، وترتكز سياسة الدولة داخليا في مجال الفضاء السيبراني على تنظيم وتوجيه التمكن من استعمال روابط الشبكة العنكبوتية (الانترنيت) والبحث في المواقع الالكترونية، فالدولة هي الفاعل المحوري الرئيس الذي يتحكم بالعالم الافتراضي السيادي كما هو الحال في العالم الواقعي، لذلك يجب أن تتمتع الدولة بميزة استدامة التحكم والسيطرة على الفضاء السيبراني الوطني، وأن تكون مؤهلة ماديا ومعلوماتيا لخوض أي صراع سيبراني محتمل مثلما هي مستعدة دائما لأي مواجهة عسكرية قد تخوضها[4]، وتتوقف مسائل تحديد طبيعة الفضاء السيبراني لأي دولة على مدى إدراك وجاهزية الدولة نفسها لحفظ معلوماتها الوطنية لكل قطاعاتها السياسية والاقتصادية

والاجتماعية والثقافية والعسكرية والأمنية و...غيرها، ويتطلب ذلك تحليل دلالات قدرتها في السيطرة على الفضاء السيبراني الوطني في حالات السلم والحرب والدفاع والهجوم، ويمكن قياس دلالات السيطرة والتحكم بالفضاء السيبراني من خلال نتائج ومعطيات ثلاث عناصر يمكن تلخيصها بما يأتي[5]:

1 – العنصر المادي. يشمل الملاكات البشرية المتخصصة، والمعدات الحاسوبية المادية الملموسة، ومستوى التطور التكنلوجي لأجهزة الحاسوب، وتقنيات الربط والتوصيل بين الاجزاء المادية.

2 – العنصر البرامجي. يشمل مجموعة البرامجيات التشغيلية والتطبيقات البرمجية المستعملة.

3 – العنصر المعلوماتي. يشمل البنى التحتية المعلوماتية، وجميع المعلومات الوطنية المسجلة الكترونيا بكل تفاصيلها وطبيعتها وشخوصها، وكل ما يتعلق بقواعد البيانات قيد البحث والمحفوظة والمؤرشفة.

تتمظهر الاستراتيجية السيبرانية في المستوى الوطني في التخطيط لجميع العمليات السيبرانية بطريقة حكيمة في جميع مؤسسات وقطاعات الدولة تفاديا للتهديدات السيبرانية الداخلية والخارجية لتحقيق أمن الدولة والوصول إلى مبتغاها، ويجب أن تتمتع الاستراتيجية السيبرانية لأي دولة بالمرونة والدقة والاستجابة للمعطيات الآنية ومستجدات المواجهة السيبرانية، ومن هنا تتصف الاستراتيجية السيبرانية الناجعة بأنها قادرة على الحصول على النتائج المرجوة عن طريق استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أن لها القدرة على استعمال الفضاء السيبراني لخلق مزايا تنفرد بها الدولة، وقدرتها على التأثير في الاحداث المتعلقة بالبيانات التشغيلية الأخرى، وتحويل مسار المواجهة لصالحها عبر وسائل سيبرانية، وأن تستوعب مجموعة عناصر السيطرة والتحكم بالفضاء السيبراني[6].

لقد أثر الفضاء السيبراني في الهوية الوطنية للدولة، وذلك بسبب سحب الافراد من المجتمع الوطني الجماعي والعمل في إطار الوحدة الوطنية نحو مجتمع فرداني يقلل من فرص الاندماج والتواصل الوطني المستمر، إذ ساهم الفضاء السيبراني بتعزيز التواصل الافتراضي الذي ساهم في إنتاج هوية سيبرانية منسلخة عن طابعها الوطني الحقيقي مؤثرا بذلك في بنية الهوية الوطنية ومكوناتها وتزعزع فكرة الوطن المرتبط بالحيز الجغرافي والتأريخي[7]، وهذا يتطلب من الدولة بذل قدرات أكبر وأوسع للسيطرة على الفضاء السيبراني، بعد ظهور تحولات جديدة طالت مفهوم قوة الدولة وسيادتها، وظهور مفهوم جديد أطلق عليه (القوة الالكترونية)، التي أدت الى توزيع القوة بين عدد أكبر من الفاعلين من غير الدولة الوطنية، بعد أن كانت الدولة هي المحتكر الوحيد للقوة، مما جعل قدرة الدولة على الهيمنة في هذا المجال موضع شك بسبب التطور المتسارع لتطبيقات تكنلوجيا المعلومات، لاسيما مع زيادة تأثير الفاعلين الخارجيين على الأداء السياسي الوطني، واستعمال الفضاء السيبراني لاعتبارات إختراق الأمن الوطني[8]، ومن هنا قدم مركز بلفر للعلوم والشؤون الدولية في جامعة هارفارد كينيدي في الولايات المتحدة الامريكية

سبعة أهداف رئيسة تشجع الدولة على امتلاك قدرات الفضاء السيبراني في المستوى الوطني لحماية أمنها السيبراني وحفظ سيادتها الرقمية، وتتمثل هذه الاهداف بما يأتي[9]:

1 – مسح ومراقبة المجموعات المحلية من خلال قيام الدولة برصد واكتشاف وجمع المعلومات الاستخبارية عن التهديدات المحلية والجهات الفاعلة داخل جدودها.

2 – تعزيز القدرات الدفاعية السيبرانية الوطنية لحماية الاصول والانظمة الالكترونية الحكومية وتحسين مرونة المواجهة.

3 – التحكم في بيئة المعلومات ومعالجتها وازدواجية ضبط المعلومات المنبثقة في الفضاء السيبراني، مع الحفاظ على خصوصية الاستخدام الالكتروني وحرية التعبير.

4 – انتزاع المعلومات الاستخبارية من الخصوم، كالمعلومات السرية عن الاتفاقيات، والخطط العسكرية السرية واتصالات كبار الشخصيات الحكومية.

5 – تحقيق مكاسب اقتصادية وتجارية تعزز النمو الوطني، عبر النشاط السيبراني في قطاعات الصناعة الانتاجية والتكنلوجيا الحديثة.

6 – مواجهة وتعطيل البنية السيبرانية للخصوم لاضعاف قدرة الخصم عند المواجهة كشكل من أشكال الدفاع الشرعي عن النفس.

7 – مشاركة الدولة في النشاطات والمناقشات السياسية والقانونية والفنية المتعلقة بالفضاء السيبراني مع الدول الاخرى، والمساهمة في تحديد معايير استعمال الفضاء السيبراني بما لايلحق الضرر بالسيادة الوطنية.

المطلب الثاني: القدرات السيبرانية في المستوى الدولي

أصبح امتلاك القدرات السيبرانية في مجال العلاقات الدولية أحد مفاتيح القوة في هذه العلاقات، وبات يمثل مجالا لهيمنة الدول بعضها على بعض سواء بطريقة مباشرة أو غير مباشرة، وتحولت القوة العسكرية من قوة استخدام الاسلحة الى قوة الذكاء البشري، ولذلك يتبين أن الأمن السيبراني يعد قضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال الذي أحدث تحولات تدريجية في مفهوم امتلاك القوة ظهرت مع نهاية الحرب الباردة على مستوى التفكير الاستراتيجي، إذ تطورت واتسعت الرؤيا حول العلاقات الدولية واصبحت أكثر ديناميكية، واصبح مفهوم الامن أكثر شمولا واتساعا واصبح الباحثون في حقل العلاقات الدولية وحقول الدراسات الاستراتيجية والامنية يركزون بشكل متزايد حول أثر القدرات التكنلوجية على الامن القومي والدولي ويشمل ذلك تأثيرها في المفاهيم ذات الصلة كالقوة والسيادة والحوكمة العالمية والاممية، وقد ارتبط مفهوم القدرات السيبرانية في المستوى الدولي بظهور الامن السيبراني ومواجهة الهجمات السيبرانية عبر انحاء العالم[10]، ويتمثل الدور الدولي في تعزيز القدرات السيبرانية في التعاون المشترك بين الدول والمنظمات الدولية وكل الجهات المختصة من أجل تأمين الفضاء السيبراني وحماية البنية التحتية الرقمية، والحد من التهديدات

السيبرانية التي يمكن أن تؤثر على الامن السيبراني الدولي، وتشمل الجهود الدولية في هذا المجال محاور عدة أهمها التعاون الدولي متعدد الاطراف لمواجهة التهديدات السيبرانية العابرة للحدود من خلال تبادل المعلومات، كما تؤدي المنظمات الدولية دورا حيويا في تحديد سياسات الامن السيبراني وتنسيق الاستراتيجيات العالمية في الفضاء السيبراني، كذلك تساهم الدول المتقدمة في مجال القدرات السيبرانية في دعم الدول النامية في هذا المجال من خلال برامج تدريبية ومبادرات رفع قدرات الحكومات والشركات، فضلا عن وضع أطر قانونية وتنظيمية مشتركة لمواجهة التهديدات السيبرانية واستخدامات الفضاء السيبراني، وحماية البنية التحتية الحيوية كشبكات الكهرباء والنقل والاتصالات عبر استراتيجيات أمنية مشتركة وتعاون دولي في رصد وتقييم المخاطر التي تهددها، والاستجابة للطوارىء السيبرانية الدولية بسرعة وفاعلية، والبحث والابتكار عبر تعزيز البحث العلمي والتقني في مجال القدرات السيبرانية[11].

لايقتصر السعي الى امتلاك القدرات السيبرانية في المستوى الدولي على الدول فقط، بل تؤدي فواعل أخرى من غير الدول دورا مهما في مجال الفضاء السيبراني، لما تملكه من أدوات وتقنيات تكنلوجية متاحة يمكن توظيفها لتحقيق اهدافها، ومن تلك الفواعل ما يأتي[12]:

1 – الشركات متعددة الجنسية. تمتلك الشركات متعددة الجنسيات موارد مالية ضخمة وفروع كثيرة في العديد من دول العالم، مما يتيح لها السيطرة والتحكم في العمليات البرامجية واستكشاف المستفيدين من خدماتها، لذا تؤدي تلك الشركات دورا في صراعات الفضاء السيبراني، وربما يوفر لها هذا الدور مصادر كبرى من المعلومات قد تعجز عن تحصيلها بعض الدول، وقد تمتلك بعض الشركات قدرات سيبرانية تفوق ما تمتلكه بعض الدول، خصوصا الشركات المتخصصة بتطبيقات التواصل الاجتماعي أو التبادل التجاري أو المراسلات الالكترونية أو تبادل البيانات، مثل شركات (جوجل، ميتا، مايكروسوفت، آبل،آمازون)، إذ تسمح خوادم تلك الشركات امتلاك قواعد البيانات العملاقة في فضائها السيبراني الخاص بها، والتواصل المباشر مع المستخدمين، مؤثرة بذلك ومتحكمة في رغبات وثقافة وافكار المجتمعات بشكل عروض ترويجية أو عمليات تجارية ربحية أو...غيرها[13].

2 – المنظمات غير الحكومية. يتمتع الفضاء السيبراني بقابلية استيعاب كل مستخدم مهما كانت توجهاته واهدافه، إذ يستفيد المستخدم من قابلية التخفي التي يتيحها المدى الواسع للفضاء السيبراني، وهذا يجعل من الصعب الكشف عن كثير من المنظمات التي تمتلك قدرات سيبرانية تؤهلها للقيام بتهديدات سيبرانية قد يتعرض لها المستفيد أو أن يكون متورطا في جريمة سيبرانية وهو لايعلم، ومنها انتحال شخصية موقع الكتروني رسمي، أو انتحال شخصية سياسية أو اقتصادية معروفة، أو القيام بهجوم على موقع شركات منافسة والتلاعب بمنتوجاتها، أو استعمال بطاقات إئتمان وتداولها في إطار أعمال مشبوهة تقوم بها المنظمة، أو العبث بالانظمة

الالكترونية العامة بوساطة فيروسات بهدف التخريب، ناهيك عن الجرائم غير الاخلاقية لابتزاز الشخصيات العامة[14].

3 – الافراد. يعد الفرد فاعلا هاما في الفضاء السيبراني لما له القدرة على ضخ المعلومات والمراسلات وتحشيد الآخرين واستقطاب المستخدمين حول العالم، فمواقع التواصل الاجتماعي ومن خلال الفضاء السيبراني تؤدي دورا كبيرا في استثارة الرأي العام، كما يوجد أفراد مختصون في أعمال القرصنة أو الجرائم السيبرانية وسرقة المعلومات والبيانات الشخصية والتلاعب فيها واستغلالها في عمليات الابتزاز والتشهير، فضلا عن إختراق أفراد مجهولي الهوية عبر الفضاء السيبراني لأنظمة الكترونية رسمية تنطوي على بيانات ومعلومات سيادية تخص دولة معينة للتأثير في سياساتها[15].

يثير التوسع في استعمال القدرات السيبرانية في الهجوم والدفاع في المستوى الدولي تغيرا واضحا في نمط الصراع ومجاله واشخاصه والآثار الناجمة عنه، ويطرح هذا التغير تساؤلات تتعلق بالقوة وخرق سيادة الدول وتجاوز مباديء القانون الدولي الانساني، ومع تنامي وتنوع أشكال التهديدات السيبرانية يواجه التنظيم الدولي المعاصر تحديا كبيرا يتطلب تنسيقا أكبر وتكييفا للهجمات السيبرانية تحت ظل القانون الدولي العام، فالهجمات السيبرانية تشكل تهديدا للمباديء الرئيسة في القانون الدولي مثل إحترام سيادة الدول لما فيه من إختراق لمعلومات وطنية سرية، وتقوض مبدأً أساس هو الامتناع عن استعمال التهديد باستعمال القوة بسبب الاضرار البالغة التي تؤثر في سير عمل الحكومات والخدمات في الدولة التي تتعرض لمثل تلك الهجمات، فالفضاء السيبراني يختلف عن العالم المادي الطبيعي في جوانب عدة منها: إنعدام جغرافيا المكان الطبيعي بما يشكل فسحة جديدة إستثمرتها الحركة العلمية والثقافية (الرقمية) المعاصرة في مجالي التهديدات السيبرانية وارتكاب جرائم تمس سيادة الدول، واصبح الفضاء السيبراني مسرحا حقيقيا لهجمات من نوع جديد تتنازع فيه الاطراف الدولية وتتسابق نحو إستغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من أشكال سباق التسلح[16].

المبحث الثاني: تحديات ومعالجات الأمن السيبراني العراقي

تمثلت قدرات العراق السيبرانية في جانبين هما التحديات والمعالجات، ففي مجال التحديات السيبرانية يواجه العراق يوم بعد يوم مزيدا من تحديات مواجهة تهديدات الامن السيبراني بسبب حداثة بناه التحتية في مجال الفضاء السيبراني نسبيا، وتهافت القوى الخارجية في جعل العراق ساحة للاختراق الامني التقليدي والتكنلوجي، وتطلب ذلك بذل جهود حثيثة لإيجاد قواعد أساسية تعالج التهديدات السيبرانية بشتى الوسائل المتاحة بعناصرها البشرية والتكنلوجية أم بادواتها المادية والبرامجية، ولتوضيح ذلك أكثر قسمنا هذا المبحث على مطلبين:

الاول: تحديات الامن السيبراني العراقي.

الثاني: معالجات تهديدات الأمن السيبراني العراقي.

المطلب الاول: تحديات الأمن السيبراني العراقي

يتجسد التحدي الأكبر للعراق في مجال تحديات الأمن السيبراني في إنكشاف العراق سيبرانيا أمام باقي الدول، إذ أن إطلاق واشاعة المعلومات من أكثر من جهة رسمية دون ضابط وفي مختلف القطاعات السياسية والاقتصادية والاجتماعية، فضلا عن الامنية والتجارية بدعوى تبني الشفافية والمكاشفة أمام الرأي العام يمثل فرصة سهلة لجمع كم هائل من المعلومات حول البلد، خصوصا وأن العراق يعاني ضعفا في مجالات تقنيات حماية المعلومات والتطور التكنلوجي والحوسبة، ولايمتلك قدرات التمكن والتكيف المطلوب لمواجهة التحديات المتسارعة التي يفرضها الفضاء السيبراني، إذ أن العراق لازال يمر بمرحلة بناء منظومة الامن السيبراني الوطني ومازالت الفجوة قائمة مع تطور تقنيات الامن الالكتروني وما تفرضه تعقيدات تكنلوجيا المتغيرات الجديدة في بيئة الامن السيبراني دوليا[17]، وأن التهديدات السيبرانية المحتملة على البنية التحتية في العراق باتت تمثل تهديدا حقيقيا أكثر من أي وقتا مضى، فالبنية التحتية الحيوية التي تمثل شبكات الكهرباء والمياه والنقل والاتصالات والحسابات الالكترونية الرسمية والنظام المالي فضلا عن استهداف البيانات الشخصية للمواطنين كلها تعد أهداف متاحة للهجمات السيبرانية، وبتعطيلها تتعطل الحياة اليومية للمواطنين وتضطرب معها التعاملات البينية بكل أشكالها، مما يزيد التحديات السياسية والاقتصادية والاجتماعية في البلد[18].

لقد طور الفضاء السيبراني وسائل مبتكرة للابتزاز كالتهديد بالوثائق المزورة والصور الشخصية التي يتم تزييفها الكترونيا بدرجة يصعب التفريق بينها وبين الصور الحقيقية، فضلا عن تحديات اختراق الحواسيب الشخصية وسرقة بطاقات الإئتمان الشخصية والمعاملات التجارية الالكترونية، وقد مثل الابتزاز الالكتروني تحديا واضحا للفضاء السيبراني العراقي، إذ يتم من خلاله الحصول على معلومات سرية أو صور شخصية أو تسجيلات فيديوية لمواطنين عراقيين يتم استغلالها لأغراض إبتزاز مالي أو القيام باعمال غير قانونية، وأعمال أخرى تعد من أشد الجرائم خطورة على الأمن الوطني العراقي، كونها جرائم تهدد أمن المجتمع وحقوق الانسان من خلال اختراق الخصوصية وتسببها بآثار نفسية واجتماعية يصعب معالجتها، ونتيجة التفاعل الكبير مع منصات التواصل الاجتماعي سجلت السلطات القضائية في العراق في السنوات الاخيرة كثير من حالات الابتزاز الالكتروني كان معظم ضحاياها من النساء، وفي ذات السياق تصاعدت عمليات الاختراق الالكتروني والتجسس مع إتساع استعمال الفضاء السيبراني، وكان الهدف الرئيس من تلك العمليات الحصول على المعلومات الخاصة بالخطط العسكرية الدفاعية والهجومية ودراسات وابحاث استراتيجية ومعلومات استطلاعية واستخباراتية، وغالبا ما يقوم الارهابيون باستعمال برامج التجسس على الشبكات والانظمة الالكترونية لتخريب البنى التحتية وزعزعة الأمن ونشر الخوف والرعب وتهديد الاشخاص والسلطات العامة فضلا عن الترويج

بوجود بيئة سياسية غير مستقرة[19]، وفي هذا الاطار تواجه العملية الانتخابية في العراق تحديا في حماية نزاهة الانتخابات السياسية في العصر الرقمي، فمع تطور تكنلوجيا الاتصالات أصبحت العملية الانتخابية عرضة لهجمات سيبرانية تعمل على تحريف نتائج الانتخابات وزعزعة ثقة المواطنين بجدوى الاقتراع النيابي ومصداقية النظام الديمقراطي عموما، ومع تزايد الاعتماد على الانظمة الالكترونية وإدخال مفاهيم الحوكمة الرقمية في إدارة العملية الانتخابية، أصبحت العملية الانتخابية في العراق أكثر عرضة للتهديدات السيبرانية، مما يشكل تحديا حقيقيا أمام الرأي العام الوطني والدولي في ضمان النزاهة والشفافية الانتخابية، لاسيما تحت ظل ضعف البنية التحتية للأمن الرقمي في العراق، ويتجسد هذا التحدي في آلية نقل نتائج التصويت عبر منظومة الاتصال الفضائي (VSAT) ليكون إحدى نقاط الضعف أمام هذا التحدي، ورغم اعتماد هذه المنظومة كبديل احترازي عن شبكة الانترنيت للحد من مخاطر الاختراق، إلا أنها لاتتضمن الحماية المطلقة، خصوصا في مواجهة هجمات سيبرانية ذات قدرات متقدمة للتلاعب بالبيانات الانتخابية، مما يحتم على المفوضية العليا المستقلة للانتخابات في العراق وجهاز الامن الوطني العراقي تعزيز اجراءات الحماية السيبرانية، وتبني استراتيجية وطنية متكاملة تشمل تأسيس مراكز بحثية متخصصة في أمن البيانات الانتخابية أثناء التصويت وبعده[20].

تشير الشواهد الواقعية الى أن الجهود الوطنية في مجال مكافحة التهديدات السيبرانية وما ينتج عنها من جرائم مازالت دون المستوى المطلوب، سواء من حيث إيجاد محاكم متخصصة أو دوائر تحقيق تكون مساندة للقضاء ومتخصصة في النظر في هذا النوع من الجرائم، أو من حيث الاهتمام بالجانب التدريبي لملاكات الامن العام أو القضاة، لاسيما وأن الجرائم المعلوماتية تعد من الجرائم التي تحتاج الى معرفة فنية دقيقة من عند التعامل مع مرتكبيها، كما أن الجانب التشريعي في مكافحة جرائم المعلوماتية يعتريه القصور في العديد من المحاور، خصوصا فيما يتعلق بالاجراءات الجزائية للتعامل مع هذا النوع من الجرائم، ومن بين ما يجب أن تعالجه منظومة القوانين السيبرانية ما يتعلق بالامن والدفاع الالكتروني، واسماء النطاقات التجارية الالكترونية، وانواع الجرائم الالكترونية وطبيعتها، وحقوق الملكية، وقوانين الخصوصية الشخصية، وحرية التعبير، وحدود التعامل مع الحد الفاصل بين ماهو حق شخصي وحرية تسمح بها القوانين وبين ما هو أمن سيبراني يمس أمن الدولة ومصالحها وسلامة مواطنيها[21].

إن تحدي عدم وجود تشريعات معاصرة ومحددة لمواجهة التهديدات السيبرانية في العراق شجع مخترقي الفضاء السيبراني العراقي على تنفيذ أنشطتهم التخريبية دون التخوف من مواجهة جزاءات قانونية جادة توازي مستوى العمل التخريبي الحاصل، وأدى ذلك الى العجز في بعض الحالات عن تطبيق القانون على المخترقين لتحقيق العدالة، مما يزيد من التهديدات ويقلل من فاعلية الاستجابة، لذلك يجب تحسين استجابة الامن السيبراني في العراق من خلال تعزيز

إصدار تشريعات فاعلة وشاملة تعالج جوانب عدة من الامن السيبراني بما في ذلك الوقاية من الهجمات السيبرانية قبل حدوثها وتفعيل العقوبات المناسبة في حال وقوع اختراق سيبراني، وفي تعزيز الجانب التشريعي طرح مجلس النواب العراقي أواخر عام 2023م مشروع قانون جرائم المعلوماتية بعد فشل الدورات النيابية السابقة تقديم هكذا مشروع قانون طيلة السنوات السابقة[22]، وفي خطوة هامة صادق العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة عام 2010م، من أجل تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظا على أمن الدول العربية ومصالحها وسلامتها وسلامة مجتمعاتها وافرادها، وأن تلتزم كل دولة طرف في هذه الاتفاقية بتبني الاجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الاتفاقية وذلك إذا ما ارتكبت الجريمة كليا أة جزئيا[23].

المطلب الثاني: معالجات تهديدات الأمن السيبراني العراقي

حددت مستشارية الامن الوطني في العراق استراتيجية الامن السيبراني للدولة، واوضحت أن العراق ليس بعيدا عن التهديدات السيبرانية التي تتمثل في الجريمة الالكترونية والتجسس السيبراني والارهاب الالكتروني واساءة معاملة الاطفال واستغلالهم عبر الانترنيت، ووضعت الدراسة ثلاث مراحل زمنية يتم من خلالها تحديد وتقييم الضعف الهيكلي في نظم المعلومات الوطنية، وبالتالي تقديم آليات جديدة تعالج هشاشة الامن السيبراني في البلاد، وخصصت المرحلة الاولى من الدراسة لزيادة الوعي بالامن السيبراني ومدتها سنة واحدة يجري خلالها تقديم مسودات قوانين تخص هذه المرحلة، أما المرحلة الثانية ومدتها ثلاث سنوات فتتضمن بناء البنية التحتية وتعزيز قدرات باحثي أمن المعلومات، أما المرحلة الثالثة ومدتها خمس سنوات تتضمن تطوير الاعتماد على الجهد الذاتي من حيث تكنلوجيا المعلومات ومراقبة آليات الامتثال والاستجابة للخطط والمعايير القياسية الموضوعة للأمن السيبراني العراقي، وقد مثلت هذه الدراسة محاولة هامة تسهم في بناء أساس الأمن السيبراني في العراق وتجعله مؤهلا للدخول في تصنيفات الدول في مجال امتلاك القدرات السيبرانية والامن السيبراني[24]، والى ذلك أشارت استراتيجية الامن الوطني العراقي 2025-2030 (العراق أولاً) بأن هذه الاستراتيجية تعد وثيقة وطنية أساس لتعزيز وتفعيل منظومة إدارة المصالح الوطنية العليا للدولة العراقية، وحماية كيانها من التحديات والمتغيرات التي تهددها من الداخل والخارج، وتأمين مصالحها الحيوية، وتهيأة المتطلبات الملائمة لتحقيق اهدافها الاستراتيجية ومصالحها وعلاقاتها الاقليمية والدولية، من أجل تعزيز الأمن والاستقرار والسيادة والازدهار بموجب المادة (110) من الدستور العراقي[25].

يرتكز بنيان فاعلية القدرات السيبرانية في الاساس على محورين أساسيين هما الادارة الناجحة والحوكمة، فالادارة الناجحة في إطار الفضاء السيبراني تعني حسن إدارة المعلومات وتحليل

مستوى جاهزية منظومة الامن السيبراني من حيث التكامل الاستراتيجي، وتوسيع استراتيجية الامن السيبراني وتقليل المخاطر، والقدرة على إستيعاب شكل التهديد السيبراني وتسهيل اتخاذ القرارات السليمة لمواجهة الهجمات الالكترونية ضد الدول، وعلى الرغم من عدم وجود انموذج واحد متفق عليه لإدارة الامن السيبراني، إلا أن المتفق عليه عالميا أن تحسين فاعلية ادارة الامن السيبراني يعد أمرا ضروريا لحماية البنى الحيوية الاساسية لأي دولة، أما الحوكمة في إطار الامن السيبراني فتشير الى المباديء والقواعد الادارية واساليبها المتبعة في جهة ما لضبط سلطات اتخاذ القرار وتحديد أصحاب المسؤولية والمحاسبة على تنفيذ المهام والواجبات ذات العلاقة بالحماية من الهجمات الالكترونية، أو سوء استعمال الاصول المعلوماتية، فضلا عن ضمان استمرارية العمليات التشغيلية في حال وقوع حوادث أو كوارث، فالهدف من حوكمة الامن السيبراني توجيه سلوكيات وقرارات الافراد ومراقبتهم وارشادهم بما يحسن ويرفع من كفايتهم السيبرانية، وتسهيل عمل الجهات ذات العلاقة من خلال التعاون وتنسيق الجهود[26].

يمكن تطوير قدرات العراق السيبرانية عبر فواعل عدة أهمها ما يأتي:

1 – تثقيف المجتمع.

يقوم على حماية الافكار والمعتقدات والثوابت الاجتماعية من التلاعب والتحريف من خلال بث الافكار التخريبية والتحريضية عبر الفضاء السيبراني، وأن فاعلية الحفاظ على الثوابت الوطنية الجامعة والعادات والتقاليد والقيم المشتركة تعزز وتؤمن بلورة مصدر إجتماعي رئيس مضاف لمصادر القوة الوطنية الاخرى عند مواجهة تهديدات داخلية أو خارجية، ويوسع من قاعدة الشعور بالمسؤولية الوطنية لدى الافراد، وأن تثقيف المجتمع بالفضاء السيبراني ومخاطر استعماله والتحول الى مجتمع رقمي واعي ينسجم تماما مع الثقافة الرقمية المعاصرة بجانب الدور الثقافي التقليدي الذي يلازم سلوك كل مجتمع، إذ أن الدور الثقافي الرقمي الواعي يسهم في حصانة المجتمع من الاطروحات الثقافية الدخيلة في عصر التطور التكنلوجي وثورة المعلومات والاستعمال المطّرد لوسائل التواصل الاجتماعي، وصراع قيم الفكر والثقافة والتعليم والاعلام والفنون والادب، وكلها تتطلب المواجهة عبر فاعلية تمكين الشعب من إستيعاب أهمية ممارسة منظومة القيم الوطنية الخاصة به في دولته المستقلة[27].

2 – تطوير المؤسسات الرسمية للدولة.

يتضمن توسيع الشراكات الدولية عبر التعاون مع المنظمات الدولية لتبادل الخبرات والاستعمال الأمثل للقدرات السيبرانية، مع تعزيز الشراكات مع القطاع الخاص عبر التعاون مع شركات التكنلوجيا لتطوير حلول تقنية تساهم في في الحد من مخاطر التهديد السيبراني والاختراق والابتزاز الالكتروني، وتعزيز البنية التحتية للقدرات السيبرانية من خلال العمل على بناء بنية تحتية قوية تحمي المستخدمين، فضلا عن إنشاء مراكز تعليم وتدريب تقدم برامج تعليمية وتدريبية تعزز مهارات الأمن الرقمي بين المواطنين سيما أصحاب الوظائف الهامة ومنتسبي

الاجهزة الامنية، مع تكثيف الجهود الحكومية في توعية مكونات المجتمع الرئيسة عموما، والتعريف بأفضل الممارسات الكفيلة بجعل الفضاء السيبراني بيئة يستعملها مختلف مكونات المجتمع سيما الشباب منهم، وتشجيع الاستثمار التكنلوجي المتخصص ورصد موازنات جيدة تخص البحث والتطوير في مجالات الامن السيبراني وتكنلوجيا المعلومات[28].

3 – تطوير عمل مؤسسات المجتمع المدني.

تحت ظل تطور الفضاء السيبراني المتسارع والاعتماد المتزايد على وسائل التواصل الاجتماعي وتبادل المعلومات أصبح الامن السيبراني أمرا بالغ الاهمية للمجتمع المدني ومؤسساته غير الحكومية، وتنعكس هذه الاهمية من خلال توعية العاملين بمؤسسات المجتمع المدني والافراد كإحدى الفئات المستهدفة في إطار إستراتيجية وطنية شاملة للامن السيبراني تهدف إلى إعداد ملاكات قادرة على مواجهة التهديدات السيبرانية، وينبغي معها زيادة الوعي بالامن السيبراني لشريحة أوسع من المجتمع، خصوصا الفئات الضعيفة تقنيا التي تجهل مخاطر االتواصل عبر روابط مجهولة أو المشاركة بمعلومات شخصية قد تعرضهم للابتزاز أو إختراق الحسابات الشخصية، وعدم التردد من الابلاغ عند التعرض للابتزاز الرقمي، ويمكن لمنظمات المجتمع المدني أن تكون خط الدفاع الاول عبر إنشاء خطوط إتصالات ساخنة وسرية للابلاغ، وتقديم الدعم القانوني والنفسي للضحايا وتنظيم ورش توعية تفاعلية للنشأ الجديد، فضلا عن أهمية بناء شراكات حقيقية بين منظمات المجتمع المدني والجهات الامنية والقانونية لضمان الاستجابة والتعامل الحساس مع الضحايا[29].

4 – تطوير قطاع التعليم.

إن الاهتمام الكبير بمجال الامن السيبراني أدى الى تحركات سريعة في تعزيز مجالات التعليم المعاصر في أعلى المستويات، لذلك تم تأسيس كليات متخصصة في إختصاص الامن السيبراني إنبثقت عنها هيئات لتدريب وتأهيل الطلاب لاستعمال أساسيات الامن السيبراني واعتماد مبادرات دورية للتدريب والتأهيل على حماية مصالح الدولة الحيوية وامنها الوطني والبنى التحتية الحساسة، ومع تقدم تقنيات الاتصالات وشبكات المعلومات المعاصرة تبلورت أهمية بناء نظومة متكاملة من الاحتياجات الحساسة لصيانة ممتلكات الدولة المرتبطة بتكنلوجيا المعلومات، مما ألزم بضرورة تأهيل ملاكات متخصصة في مجال أمن المعلومات وجعل الجامعات والكليات والمعاهد تتبنى مسؤولية خلق جيل محترف لتقنيات الامن السيبراني[30].

تكمن فاعلية تطوير قطاع التعليم في مواجهة تهديدات الامن السيبراني من خلال تضمين مفاهيم الامن السيبراني بمقررات التعليم ذات الاختصاص، وتوعية ملاكات وطلاب قطاع التعليم عموما باهمية تطوير قدرات استعمال تكنلوجيا المعلومات ترافقها دورات تدريبية بالشراكة مع الجامعات وتشكيل فرق قانونية متخصصة بقضايا الاحتيال الالكتروني، وعقد دورات حول آليات التعامل الآمن مع شبكة الانترنيت والمنصات التعليمية واستشارة الخبراء

ومتخصصي الامن السيبراني لفحص الاجهزة والبرمجيات بصفة مستمرة ووضع دليل تفاعلي يتضمن أسس ومباديء أخلاقيات الامن السيبراني ومفاهيمه، وكذلك الالتزام بالضوابط الاساسية للامن السيبراني الصادرة عن الهيئات الوطنية[31].

الخاتمة:

تسعى جميع الدول الى تطوير قدراتها السيبرانية باستمرار في مجالي الهجوم والدفاع على حد سواء، ومن هذا المنطلق سعى العراق الى تعزيز إمكانياته التقنية المتعلقة بالفضاء السيبراني بعد التوسع الملحوظ في استعمال التبادل الرقمي والتواصل الالكتروني في المستوى الرسمي وغير الرسمي، ومن الواضح مواجهة العراق تحديات عدة في هذا المجال شكلت بمجموعها عقبة في تطوير الأمن السيبراني، وأبرز تلك التحديات ضعف البنية المادية والبشرية المطلوبة للتعامل مع الفضاء السيبراني، وتراجع دور الاستجابة للتطورات المتسارعة في مجال تكنلوجيا المعلومات والأمن المعلوماتي، ومحدودية المؤتمرات وورش العمل والندوات الوطنية والدولية على حد سواء التي تعنى بالأمن السيبراني، ومع ذلك يستمر العمل المؤسسي لمواجهة تلك التحديات من خلال فواعل عدة أهمها تطوير منظومة الامن السيبراني في المؤسسات الرسمية وغير الرسمية، ورفع الوعي الامني والمسؤولية الوطنية والاجتماعية في حماية المعلومات، وتثقيف أفراد المجتمع بالتطورات الحاصلة في تكنلوجيا المعلومات والفضاء السيبراني خصوصا في قطاع التعليم.

الاستنتاجات:

1 – يعد الفاعل الرقمي في عالمنا المعاصر من أهم مؤثرات التواصل بين الدول، وصارت منصات التواصل الالكتروني وتبادل المعلومات والبيانات في الصعيدين الرسمي وغير الرسمي الجزء الرئيس في النسق الدولي الذي تستعملها الوحدات الدولية القليدية وفواعل أخرى تتمتع بالشخصية الاعتبارية وأخرى غير قانونية علبرة للحدود.

2 – أصبح الاختراق السيبراني هو التهديد الاكثر شيوعا بين دول العالم، بسبب إمكانية الوصول الى المعلومات بسرعة وسهولة وفي أي وقت وعدم تحديد مصدر التهديد السيبراني بدقة إلا بعد فوات الاوان.

3 – يمكن مواجهة التهديدات السيبرانية من خلال تطوير البنى التحتية الرقمية وتكنلوجيا المعلومات وتجتمع هنا ثلاثية العامل البشري الكفوء والمكونات المادية المتطورة وتطبيقات البرامجيات الحمائية التي تشكل بمجموعها قوة تصطف بمواجهة أي تهديد سيبراني.

4 – ترسخت القناعة لدى الدول ومنها العراق ان الفضاء الالكتروني يشكل متغير استراتيجي جديد ربما يحسم مصير كثير من التهديدات والتحديات التي تواجهها على الصعيد الدولي، وأن الدول تعي تماما الخصائص والسمات التي يمتاز بها هذا المتغير المعاصر واستعماله كسلاح غير تقليدي خلال مراحل الصراع والمواجهة.

الهوامش:

(1)رمزي منير البعلبكي، قاموس المورد الحديث انكليزي-عربي، دار العلم للملايين، بيروت، 2008، ص307 .

(2) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، 2018، ص12.

(3) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الانسانية، المجلد8، العدد2، مركز بابل للدراسات الحضارية والتاريخية، جامعة بابل، بابل،٢٠١٨ ، ص141.

(4) علي محمود سلمان النداوي، الفضاء السيبراني ودوره في صياغة وتوجيه مسار القوة في العلاقات الاقتصادية الدولية نماذج من دول مختارة للمدة 2010-2020، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021، ص33-34.

(5) احمد عبدالجبار عبدالله، تطور مفهوم القوة في عصر المعلوماتية القوة الامريكية أنموذجا، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد،2021 ، ص10.

(6) محمد اكرم محسن ومروان سالم علي، السيبرانية: الماهية الخصائص الفواعل الابعاد الاستراتيجية، مجلة حمورابي للدراسات، العدد43، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2022 ، ص388.

(7) تارا عمر محمد، الهوية وإعادة صياغتها في المجتمع السيبراني أسباب ونتائج، مجلة قضايا سياسية، العدد80، كلية العلوم السياسية، جامعة النهرين، بغداد، 2025 ، ص813.

(8) تغريد معين حسن المشهدي، الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، المجلد2019، العدد30، كلية التربية للبنات، جامعة الكوفة، الكوفة، 2019 ، ص245.

(9) هبة جمال الدين محمد العزب، الامن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد24، العدد1، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، القاهرة، 2023 ، ص197.

(10) اسراء شريف جيجان، الامن السيبراني الصيني دراسة في الدوافع والتحديات، مجلة قضايا سياسية، العدد65، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021 ، ص38-39.

(11) محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنومعلوماتية والفضاء السيبراني، مجلة دراسات اقليمية، العدد44، مركز الدراسات الاقليمية، جامعة الموصل، الموصل، 2020 ، ص154-155.

(12) محمد رحمن عبود الجبوري، أثر التهديدات السيبرانية في الأمن المجتمعي ايران السعودية دراسة مقارنة، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد، 2023 ، ص42047.

(13) هديل حربي ذاري، قوة الفضاء السيبراني ساحة صراع جديدة بين القوى الدولية والاقليمية في القرن الحادي والعشرين، مجلة قضايا سياسية، العدد72، كلية العلوم السياسية، جامعة النهرين، 2023 ، ص346.

(14) محمد أكرم محسن ومروان سالم علي، توظيف الفواعل من غير الدول للقوة السيبرانية واثرها على الامن الدولي، مجلة المعهد، العدد15، معهد العلمين للدراسات العليا، الكوفة، 2023 ، ص540.

(15) عماد خليل ابراهيم ونجوان هاني محمود، استخدام القوة السيبرانية في سياسات الدول الكبرى، المجلة العراقية للعلوم السياسية، العدد10، الجمعية العراقية للعلوم السياسية، بغداد، 2024 ، ص23.

(16) احمد عبيس نعمة وزهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، جزء أول، المجلد12، العدد44، كلية القانون، جامعة الكوفة، 2020 ، ص57.

(17) مهند جبار عباس وهيثم كريم صيوان، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة العراق انموذجا، مجلة قضايا سياسية، العدد70، كلية العلوم السياسية، جامعة النهرين، بغداد، 2022 ، ص160.

(18) علي صباح محمد، تحديات الامن السيبراني على الاستقرار الامني في العراق، مجلة دجلة للعلوم الانسانية، المجلد7، العدد2، جامعة دجلة، بغداد، 2024 ، ص157.

(19) شيماء تركان صالح، الامن الوطني العراقي والتهديدات السيبرانية الارهاب السيبراني انموذجا، مجلة تكريت للعلوم السياسية، المجلد4، العدد33، كلية العلوم السياسية، جامعة تكريت، صلاح الدين، 2023 ، ص234.

(20) فاضل عباس صباح، الامن السيبراني وأثره على الاستقرار السياسي في العراق بعد عام 2003 دراسة تحليلية، مجلة قضايا سياسية، العدد 82، كلية العلوم السياسية، جامعة النهرين، بغداد، 2025 ، ص223.

(21) دلالي جيلالي وبلبشير يعقوب، رهانات الامن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، المجلد37، العدد1، كلية القانون الكويتية العالمية، الكويت، 2021 ، ص556-557.

(22) رعد خضير صليبي، تعزيز الامن السيبراني في العراق التحديات والفرص، مجلة دراسات دولية، العدد99، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2024 ، ص519.

(23)الوقائع العراقية، العدد4292، بغداد، 2013.

(24) علي قاسم خيرالله، دور الامن السيبراني في مكافحة التطرف، وقائع مؤتمر مواجهة التطرف في ظل الازمات العالمية الراهنة، المؤتمر العلمي الرابع عشر 24-25 آذار 2024، المجلد1، العدد7، مركز المستنصرية للدراسات العربية والدولية، الجامعة المستنصرية، بغداد، 2024 ، ص187.

(25)الايجاز التعريفي لاستراتيجية الامن الوطني العراقي 2025-2030 العراق أولاً، مستشارية الامن القومي، رئاسة الوزراء، جمهورية العراق، بغداد، 2025 .

(26) مصطفى ابراهيم سلمان الشمري، الامن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد10، العدد1، كلية القانون والعلوم السياسية، جامعة ديالى، ديالى، 2021 ، ص159-160.

(27) نور علي صكب، الامن الوطني العراقي في ظل الاختراق السيبراني أمن المعلومات، مجلة كلية القانون والعلوم السياسية، العدد11، كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، 2021 ، ص386.

(28) مريم محمد حسين ومصطفى صادق عواد، الامن السيبراني والتنشئة الاجتماعية، المجلة العراقية للعلوم السياسية، العدد 13، الجمعية العراقية للعلوم السياسية، بغداد، 2024 ، ص182.

(29) بشرى العزاوي، الامن السيبراني مسؤولية مجتمعية لمواجهة التهديدات الرقمية، متاح على شبكة المعلومات الالكترونية الدولية (الانترنيت) على الرابط: https://www.azzaman-iraq.com/content.php?id=109846

(30) نوال بنت عيسى محمد اليحيائي، اهمية الامن السيبراني في العملية التعليمية والقيم الدينية، مجلة جامعة المدينة العالمية المحكمة، العدد 48، كانون الثاني، 2024 ، ص220.

(31) عائشة عبيد الله مبارك قويضي العازمي، واقع الامن السيبراني في التعليم وعلاقته بالامن النفسي من وجهة نظر المعلمات بدولة الكويت، المجلة الدولية لنشر البحوث والدراسات، المجلد5، العدد 59، عمان، ايلول، 2024 ، ص48-49.

قائمة المصادر والمراجع باللغة العربية :

أولاً- الوثائق:

(1)الوقائع العراقية، العدد4292، بغداد، 2013.

(2)الايجاز التعريفي لاستراتيجية الامن الوطني العراقي 2025-2030 العراق أولاً، مستشارية الامن القومي، رئاسة الوزراء، جمهورية العراق، بغداد، 2025 .

ثانياً- القواميس:

- رمزي منيرالبعلبكي، قاموس المورد الحديث انكليزي-عربي، دار العلم للملايين، بيروت، 2008.

ثالثاً- الكتب والاطاريح والمجلات العلمية:

(1) احمد عبدالجبار عبدالله، تطور مفهوم القوة في عصر المعلوماتية القوة الامريكية أنموذجا، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد،2021.

(2) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، 2018.

(3) احمد عبيس نعمة وزهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، جزء أول، المجلد12، العدد44، كلية القانون، جامعة الكوفة، 2020.

(4) اسراء شريف جيجان، الامن السيبراني الصيني دراسة في الدوافع والتحديات، مجلة قضايا سياسية، العدد65، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021.

(5) تارا عمر محمد، الهوية وإعادة صياغتها في المجتمع السيبراني أسباب ونتائج، مجلة قضايا سياسية، العدد80، كلية العلوم السياسية، جامعة النهرين، بغداد، 2025.

(6) تغريد معين حسن المشهدي، الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، المجلد2019، العدد30، كلية التربية للبنات، جامعة الكوفة، الكوفة، 2019.

(7) دلالي جيلالي وبلبشير يعقوب، رهانات الامن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، المجلد37، العدد1، كلية القانون الكويتية العالمية، الكويت، 2021.

(8) رعد خضير صليبي، تعزيز الامن السيبراني في العراق التحديات والفرص، مجلة دراسات دولية، العدد99، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2024.

(9) شيماء تركان صالح، الامن الوطني العراقي والتهديدات السيبرانية الارهاب السيبراني انموذجا، مجلة تكريت للعلوم السياسية، المجلد4، العدد33، كلية العلوم السياسية، جامعة تكريت، صلاح الدين، 2023.

(10) عائشة عبيد الله مبارك قويضي العازمي، واقع الامن السيبراني في التعليم وعلاقته بالامن النفسي من وجهة نظر المعلمات بدولة الكويت، المجلة الدولية لنشر البحوث والدراسات، المجلد5، العدد 59، عمان، ايلول، 2024.

(11) علي صباح محمد، تحديات الامن السيبراني على الاستقرار الامني في العراق، مجلة دجلة للعلوم الانسانية، المجلد7، العدد2، جامعة دجلة، بغداد، 2024.

(12) علي محمود سلمان النداوي، الفضاء السيبراني ودوره في صياغة وتوجيه مسار القوة في العلاقات الاقتصادية الدولية نماذج من دول مختارة للمدة 2010-2020، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021.

(13) عماد خليل ابراهيم ونجوان هاني محمود، استخدام القوة السيبرانية في سياسات الدول الكبرى، المجلة العراقية للعلوم السياسية، العدد10، الجمعية العراقية للعلوم السياسية، بغداد، 2024.

(14) فاضل عباس صباح، الامن السيبراني وأثره على الاستقرار السياسي في العراق بعد عام 2003 دراسة تحليلية، مجلة قضايا سياسية، العدد 82، كلية العلوم السياسية، جامعة النهرين، بغداد، 2025.

(15) محمد اكرم محسن ومروان سالم علي، السيبرانية: الماهية الخصائص الفواعل الابعاد الاستراتيجية، مجلة حمورابي للدراسات، العدد43، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2022.

(16) محمد أكرم محسن ومروان سالم علي، توظيف الفواعل من غير الدول للقوة السيبرانية واثرها على الامن الدولي، مجلة المعهد، العدد15، معهد العلمين للدراسات العليا، الكوفة، 2023.

(17) محمد رحمن عبود الجبوري، أثر التهديدات السيبرانية في الأمن المجتمعي ايران السعودية دراسة مقارنة، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، 2023.

(18) محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنومعلوماتية والفضاء السيبراني، مجلة دراسات اقليمية، العدد44، مركز الدراسات الاقليمية، جامعة الموصل، الموصل، 2020.

(19) مريم محمد حسين ومصطفى صادق عواد، الامن السيبراني والتنشئة الاجتماعية، المجلة العراقية للعلوم السياسية، العدد 13، الجمعية العراقية للعلوم السياسية، بغداد، 2024.

(20) مصطفى ابراهيم سلمان الشمري، الامن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد10، العدد1، كلية القانون والعلوم السياسية، جامعة ديالى، ديالى، 2021.

(21) مهند جبار عباس وهيثم كريم صيوان، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة العراق انموذجا، مجلة قضايا سياسية، العدد70، كلية العلوم السياسية، جامعة النهرين، بغداد، 2022.

(22) نوال بنت عيسى محمد اليحيائي، اهمية الامن السيبراني في العملية التعليمية والقيم الدينية، مجلة جامعة المدينة العالمية المحكمة، العدد 48، كانون الثاني، 2024.

(23) نور علي صكب، الامن الوطني العراقي في ظل الاختراق السيبراني أمن المعلومات، مجلة كلية القانون والعلوم السياسية، العدد11، كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، 2021.

(24) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الانسانية، المجلد8، العدد2، مركز بابل للدراسات الحضارية والتاريخية، جامعة بابل، بابل،٢٠١٨ .

(25) هبة جمال الدين محمد العزب، الامن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد24، العدد1، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، القاهرة، 2023.

(26) هديل حربي ذاري، قوة الفضاء السيبراني ساحة صراع جديدة بين القوى الدولية والاقليمية في القرن الحادي والعشرين، مجلة قضايا سياسية، العدد72، كلية العلوم السياسية، جامعة النهرين، 2023.

رابعاً- المؤتمرات:

- علي قاسم خيرالله، دور الامن السيبراني في مكافحة التطرف، وقائع مؤتمر مواجهة التطرف في ظل الازمات العالمية الراهنة، المؤتمر العلمي الرابع عشر 24-25 آذار 2024، المجلد1، العدد7، مركز المستنصرية للدراسات العربية والدولية، الجامعة المستنصرية، بغداد، 2024.

خامسا- شبكة المعلومات الدولية (الانترنيت):

-بشرى العزاوي، الامن السيبراني مسؤولية مجتمعية لمواجهة التهديدات الرقمية، متاح على شبكة المعلومات الالكترونية الدولية (الانترنيت) على الرابط: https://www.azzaman-iraq.com/content.php?id=109846

قائمة المصادر والمراجع باللغة الانكليزية :

First - Documents:

(1)Iraqi Gazette, Issue 4292, Baghdad, 2013.

(2)Briefing on the Iraqi National Security Strategy 2025-2030, Iraq First, National Security Advisory, Prime Minister's Office, Republic of Iraq, Baghdad, 2025.

Second - Dictionaries:

-Ramzi Munir Al-Baalbaki, Al-Mawrid Modern Dictionary, English-Arabic, Dar Al-Ilm Lil-Malayin, Beirut, 2008.

Third - Books, Theses, and Scientific Journals:

(1)Ahmed Abdul-Jabbar Abdullah, The Evolution of the Concept of Power in the Information Age: American Power as a Model, Unpublished Doctoral Dissertation, College of Political Science, University of Baghdad, Baghdad, 2021. (2) Ahmed Abis Naama Al-Fatlawi, Cyber Attacks, Zain Legal Publications, Beirut, 2018.

(3)Ahmed Abis Naama and Zahraa Emad Mohammed Kalantar, Adapting Cyber Attacks in Light of International Law, Kufa Journal of Legal and Political Sciences, Part 1, Volume 12, Issue 44, College of Law, University of Kufa, 2020.

(4)Israa Sharif Jijan, Chinese Cyber Security: A Study of Motives and Challenges, Political Issues Journal, Issue 65, College of Political Science, Al-Nahrain University, Baghdad, 2021.

(5)Tara Omar Mohammed, Identity and its Reconstruction in Cyber Society: Causes and Consequences, Political Issues Journal, Issue 80, College of Political Science, Al-Nahrain University, Baghdad, 2025.

(6)Taghreed Mueen Hassan Al-Mashhadi, The Military Impact of Cyber Security on the Geopolitics of the State, Journal of Geographical Research, Volume 2019, Issue 30, College of Education for Girls, University of Kufa, Kufa. 2019.

(7)Dalali Jilali and Belbachir Yaqoub, National Cybersecurity Stakes in Light of Digital Transformation: A Reading in the Foundations of Knowledge and the Legislative Strategy for Confrontation, Kuwait International Law School Journal, Vol. 37, No. 1, Kuwait International Law School, Kuwait, 2021.

(8)Raad Khudhair Salibi, Enhancing Cybersecurity in Iraq: Challenges and Opportunities, International Studies Journal, No. 99, Center for Strategic and International Studies, University of Baghdad, Baghdad, 2024.

(9)Shaima Turkan Saleh, Iraqi National Security and Cyber Threats: Cyberterrorism as a Model, Tikrit Journal of Political Science, Vol. 4, No. 33, College of Political Science, Tikrit University, Salahaddin, 2023.

(10)Aisha Obaid Allah Mubarak Qwaidhi Al-Azmi, The Reality of Cybersecurity in Education and its Relationship to Psychological Security from the Perspective of Female Teachers in the State of Kuwait, International Journal for Publishing Research and Studies, Vol. 5, No. 59, Amman, September. 2024.

(11)Ali Sabah Mohammed, Cybersecurity Challenges to Security Stability in Iraq, Dijlah Journal of Human Sciences, Volume 7, Issue 2, Dijlah University, Baghdad, 2024.

(12)Ali Mahmoud Salman Al-Nadawi, Cyberspace and its Role in Shaping and Directing the Course of Power in International Economic Relations: Case Studies from Selected Countries for the Period 2010-2020, Unpublished Doctoral Dissertation, College of Political Science, Al-Nahrain University, Baghdad, 2021.

(13)Imad Khalil Ibrahim and Najwan Hani Mahmoud, The Use of Cyber Power in the Policies of Major Powers, Iraqi Journal of Political Science, Issue 10, Iraqi Association for Political Science, Baghdad, 2024.

(14)Fadhil Abbas Sabah, Cybersecurity and its Impact on Political Stability in Iraq after 2003: An Analytical Study, Political Issues Journal, Issue 82, College of Political Science, Al-Nahrain University, Baghdad, 2025.

(15)Mohammed Akram Mohsen and Marwan Salem Ali, Cybersecurity: (16) Muhammad Akram Mohsen and Marwan Salem Ali, The Use of Cyber Power by Non-State Actors and its Impact on International Security, Journal of the Institute, Issue 15, Al-Alamein Institute for Graduate Studies, Kufa, 2023.

(17)Muhammad Rahman Aboud Al-Jubouri, The Impact of Cyber Threats on Societal Security: Iran and Saudi Arabia – A Comparative Study, Unpublished Doctoral Dissertation, College of Political Science, University of Baghdad, 2023.

(18)Muhammad Wael Al-Qaisi, The Future of Global Strategic Security in Light of Techno-Informational Challenges and Cyberspace, Regional Studies Journal, Issue 44, Regional Studies Center, University of Mosul, Mosul, 2020.

(19)Maryam Muhammad Hussein and Mustafa Sadiq Awad, Cybersecurity and Socialization, Iraqi Journal of Political Science, Issue 13, Iraqi Association for Political Science, Baghdad. 2024.

(20)Mustafa Ibrahim Salman Al-Shammari, Cybersecurity and its Impact on Iraqi National Security, Journal of Legal and Political Sciences, Volume 10, Issue 1, College of Law and Political Science, University of Diyala, Diyala, 2021.

(21)Muhannad Jabbar Abbas and Haitham Karim Siwan, Cyber Warfare: Challenges and Strategies for Confrontation – Iraq as a Model, Journal of Political Issues, Issue 70, College of Political Science, Al-Nahrain University, Baghdad, 2022.

(22)Nawal Bint Issa Muhammad Al-Yahyaei, The Importance of Cybersecurity in the Educational Process and Religious Values, International University of Madinah Journal, Issue 48, January 2024.

(23)Nour Ali Sakab, Iraqi National Security in Light of Cyberattacks: Information Security, Journal of the College of Law and Political Science, Issue 11, College of Law and Political Science, Iraqi University, Baghdad, 2021.

(24)Noura Shloush, Cyber Piracy in Cyberspace: The Escalating Threat to State Security, Journal of the Babylon Center for Studies Humanity, Volume 8, Issue 2, Babylon Center for Civilizational and Historical Studies, University of Babylon, Babylon, 2018.

(25)Heba Gamal El-Din Mohamed El-Azab, Cybersecurity and the Transformation of the International System, Journal of the Faculty of Economics and Political Science, Volume 24, Issue 1, Faculty of Economics and Political Science, Cairo University, Cairo, 2023.

(26)Hadeel Harbi Dhari, Cyber Power: A New Arena of Conflict Between International and Regional Powers in the 21st Century, Political Issues Journal, Issue 72, Faculty of Political Science, Al-Nahrain University, 2023.

Fourth - The Conference:

References:

-Ali Qasim Khairallah, The Role of Cybersecurity in Combating Extremism, Proceedings of the Conference on Confronting Extremism in Light of Current Global Crises, 14th Scientific Conference, March 24-25, 2024, Volume 1, Issue 7, Al-Mustansiriya Center for Arab and International Studies, Al-Mustansiriya University, Baghdad, 2024.

Fifth - The International Information Network (Internet):

- Bushra Al-Azzawi, Cybersecurity: A Societal Responsibility to Confront Digital Threats, available on the International Information Network (Internet) at the following link: https://www.azzaman-iraq.com/content.php?id=109846.

Iraq's cyber capabilities between challenges and solutions

Dr. Ali AbdulMuttalib Sadiq

Center for Strategic and International Studies

University of Baghdad

ali.a@cis.uobaghdad.edu.iq

Keywords: Iraq, cybersecurity, cyberthreats

Summary:

This research addresses the orbits of cyberspace and the complexities it entails, which are evolving at an extremely rapid pace. It is no exaggeration to say that no single country can keep pace with the technological development of cyberpower. It is clear that cyber threats have taken on a national and international character, targeting vital state facilities from various official and unofficial entities, individually or collectively, as well as the activities of the private sector. These threats impact the national and international economy and the livelihoods of citizens, especially after the steady spread of the use of the international electronic information network (the Internet). Iraq has not been isolated from these threats, which collectively pose a challenge to Iraqi cybersecurity in terms of the physical, technical, and human infrastructure required to confront any cyber threat. Recognizing these challenges, Iraq has continuously sought to keep pace with cybertechnological developments and develop a cybersecurity strategy based on the principle of ensuring Iraq's security, protecting its presence in cyberspace, and protecting its vital national information infrastructure.