وقائع المؤتمر العلمي الثامن
العراق 2050

في جامعة النهرين

بتاريخ 2025/04/20

قضايا سياسية

Political Issues

ملحق العدد ٨٠

E-ISSN: 2790-2404
P-ISSN: 2070-9250

العراق (2050)

وقائع المؤتمر الدولي الثامن

لكلية العلوم السياسية / جامعة النهرين
عقد بتأريخ 2025/4/20

الإشراف العام

أ.د. أسامة مرتضى السعيدي

إعداد وتحرير

م.د. محمد محي الجنابي

م.د. مصطفى صادق عواد

م.م. محمد مجيد حسين

م.م. زهراء كريم جاسم

مبرمج. رؤى عبد الحسين

لجان مؤتمر (العراق 2050)

المؤتمر الدولي الثامن لكلية العلوم السياسية / جامعة النهرين

عقد بتأريخ 2025/4/20

اولاً _ اللجنة التحضيرية :	
أ.د اسامة مرتضى باقر	عميد كلية العلوم السياسية
أ.د خضر عباس عطوان	رئيس قسم السياسة الدولية
أ.د علي حسين حميد	رئيس قسم الاستراتيجية
أ.د عباس سعدون رفعت	معاون العميد للشؤون الادارية
أ.د مصطفى حسين عبد الرزاق	رئيس قسم العلاقات الاقتصادية الدولية
أ.د سلمان علي حسين	مقرر قسم السياسة الدولية
أ.م.د حيدر زهير جاسم	معاون العميد للشؤون العلمية والدراسات العليا
أ.م.د استبرق فاضل شعير	رئيس قسم النظم السياسية والسياسات العامة
أ.م.د سولاف مصحب مهدي	مسؤول شعبة ضمان الجودة والاداء الجامعي
م.د زيدون سلمان محمد	مسؤول شعبة الشؤون العلمية
م.د محمد محي محمد	مدير تحرير مجلة قضايا سياسية
م.د محمد حميد محمد	مقرر قسم العلاقات الاقتصادية الدولية
م.د عبد الامير سليم عباس	أمين مجلس الكلية
م.د ايلاف نوفل احمد	مسؤول شعبة التسجيل
م.د.مصطفى صادق عواد	قسم النظم السياسية /مسؤول وحدة التوظيف والتأهيل
م.م مهدي علي وداعة	امانة مجلس الكلية

ثانياً _ اللجنة العلمية :		
أ.د قاسم محمد عبد	أ.د اسراء علاء الدين نوري	أ.م.د. احسان عدنان عبد الله
أ.د سلام عبد الجليل حسن	أ.د قاسم شعيب عباس	أ.م.د عصام اسعد محسن
أ.د احمد عبدالله ناهي	أ.د سهاد اسماعيل خليل	أ.م.د نسرين رياض شنشول
أ.د شيماء عادل فاضل	أ.د ياسر علي ابراهيم	أ.م.د زينب عبدالله منكاش
أ.د هشام حكمت عبد الستار	أ.د.إيضاح نعمان خزعل	أ.م.د ربا صاحب عبد مرزوق
أ.د عماد صلاح عبد الرزاق	أ.د علي حسين حميد /مقرر اللجنة	أ.م.د. صلاح مهدي هادي
أ.د محمد كريم كاظم	أ.د رياض مهدي عبد الكاظم	أ.م.د رواء طه درويش
أ.د هيثم كريم صيوان	أ.د صدام عبد الستار رشيد	أ.م.د محسن حساني ظاهر
أ.د وسن احسان عبد المنعم	أ.د. اخلاص قاسم نافل	أ.م.د همام خضير عبد مطلك
أ.د عامر هاشم عواد	أ.د فراس عبد الكريم محمد علي	ا.م.د. هناء جبوري محمد
أ.د كاظم علي مهدي	أ.د علي فارس حميد	أ.م.د ميثم حميد ناصر
ا.د.عبد العظيم جبر حافظ	أ.د الاء طالب خلف	ا.م.د.شيماء تركان صالح
أ.د احمد غالب محي	ا.د.مصطفى حسين عبد الرزاق	ا.م.د.سرى موفق جعفر
أ.د ارشد مزاحم مجبل	أ.م.د مصطفى فاروق مجيد	

ثالثاً _ اللجنة المالية :
م.م. خبيب منذر عباس / وحدة صندوق التعليم العالي / رئيساً
م.م.سعد رويس / قسم الاستراتيجية / عضواً
م.م. قمر ثامر جاسم / شعبة التدقيق / عضواً
إكرام فهمي اعجمي / مسؤولة شعبة الشؤون الادارية / عضواً

رابعاً _ اللجنة الاعلامية :
أ.م.د ندى عمران علي
م.د انمار علي ابراهيم
م.د سديف محمد كامل
م.م علي صباح محمد
م.م نشوان علاء حسين

خامساً _ لجنة الاستقبال :		
أ.د سعد محمد دخيل	م.م غفران جاسم جبر	م.م سجى فاضل عباس
أ.م.د رونق ناطق محمد	م.م سعد رويس	م.م. مصطفى ياسين طه
أ.م.د دنيا علي عبد الحسن	م.م نور مشتاق	م.م. محمد معن محسن
م.د شذى عبد الرضا عبد المجيد	م.م عبدالله محمد قاسم	م.م. هيثم عقيل محمود
م.د. علي محمد أمنيف	م.م نور سمير	سجاد محمد جاسم
م.د رفيف اياد	م.م مروة زياد طارق	عمر ثابت نعمان
م.د نبأ احسان شريف	م.م مفاز ابراهيم داوود	زينة سعد شمس الدين
م.د رنا احمد رجب	م.م نادية علي عبد الرضا	سرى عبد القادر خلف
م.د هناء رحيم زيدان	م.م قاسم محسن	نور الهدى عماد كاظم
م.م كاظم ناجي عبود	م.م عمار عايد كطوف	لينه ليث فارس
م.م صبا رشيد جبير	م.م هديل لطيف ياسر	رائد صبري حسن
م.م مها غافل حسين	م.م ميس محمود عداي	علي جابر محسن
م.م محمود جمال فتحي	م.م هدى عبد الحسين فياض	علي فاروق
م.م فرقان عبد حمود	م.م مها عباس فاضل	سيف سعد لعيبي
م.م نور هشام جليل	م.م عبد الرحمن محمد عيسى	علي محمد عواد
م.م علي عبد الرزاق شنشول	م.م تغريد رياض علي	م.م سجى فاضل عباس

جدول المحتويات

الأمن السيبراني العراقي: التحديات وسبل المواجهة

Iraqi cybersecurity: challenges and ways to confront them

م.م علي عبد المطلب صادق*
Ali AbdulMuttalib Sadiq

- **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 من جهات عدة رسمية أو غير رسمية، و منفردة أو جماعية، وكذلك أعمال القطاع الخاص للتأثير 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 تدارك 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.

- **الكلمات المفتاحية:** العراق، الأمن السيبراني، التهديدات السيبرانية، تشريعات الفضاء السيبراني.

- **Abstract:**

The research delves into the orbits of cyberspace and the complexities it entails that are developing at a very rapid pace, so that we would not be exaggerating if we said that no country can keep up with the technological development of cyber power on its own. It is clear that cyber threats have taken on a national and international character that affects vital facilities in the country from several official or unofficial parties, individually or collectively, as well as the work of the private sector to affect the national and international

(*) مركز الدراسات الاستراتيجية والدولية/ جامعة بغداد ali.a@cis.uobaghdad.edu.iq

economy and the livelihoods of citizens, especially after the steady spread of the use of the international electronic information network (the Internet). Iraq was not isolated from these threats, which together constituted a challenge to Iraqi cybersecurity in the aspects of the physical, technical and human infrastructure required to confront any cyber threat. After addressing these challenges, Iraq has been constantly seeking to keep pace with cybertechnological developments, and to build a cybersecurity strategy based on the principle of ensuring Iraq's security, protecting its presence in cyberspace, and protecting the vital national information infrastructure.

Keywords: Iraq, cybersecurity, cyber threats, cyberspace legislation.

- **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، 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 مايتعلق 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 اللجوء الى التحالف مع القوى الأكثر إمتلاكا لتقنية الأمن السيبراني، وهذا يؤدي بالعراق الى 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 تبيان 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.

- **الإشكالية:**

كيف يمكن للعراق تطوير وتعزيز قدراته السيبرانية لمواجهة التحديات الرقمية المتزايدة، وما هي المعالجات الفعالة لضمان الأمن السيبراني وحماية البنية التحتية الرقمية؟

- **الفرضية:**

يمكن للعراق تحقيق جاهزية سيبرانية عالية من خلال تطوير البنية التحتية الرقمية، وضع تشريعات فعالة، تعزيز الكوادر البشرية المتخصصة، وتبني استراتيجيات وطنية للأمن السيبراني، مما يساهم في الحد من المخاطر الرقمية وتحقيق الاستقرار الإلكتروني.

- **محتويات البحث:**

ينطوي البحث على ثلاث محاور، جاء المحور الاول تحت عنوان (ماهية الأمن السيبراني)، والثاني حمل عنوان (تحديات الأمن السيبراني العراقي)، أما المحور الثالث فقد جاء بعنوان (معالجات تهديدات الأمن السيبراني للعراق).

أولاً: ماهية الأمن السيبراني

تم تعريف الأمن السيبراني بانه مجموعة الادوات والسياسات والمفاهيم والضمانات الامنية والمباديء التوجيهية ونهج إدارة المخاطر والاجراءات والتدريب وافضل إستخدامات التكنلوجيا في مجال حماية البيئة السيبرانية للمؤسسات والمستخدمين، إذ تشمل الحماية تجهيزات الحواسيب وموظفي البيانات الالكترونية والتطبيقات والخدمات وانظمة الاتصالات والمعلومات المرسلة والمحفوظة في البيئة السيبرانية،

وكل ما من شأنه تحقيق الامن السيبراني والخواص الامنية للمؤسسة[1]، كما يعرف الأمن السيبراني بأنه أمن الشبكات والانظمة المعلوماتية والبيانات والمعلومات والاجهزة المتصلة بشبكة المعلومات الالكترونية الدولية (الانترنيت)، وهو المجال الذي يتعلق باجراءات ومقاييس ومعايير الحماية المطلوب اتخاذها أو الالتزام بها لمواجهة التهديدات والحد من آثارها، ويشير الأمن السيبراني الى مجموعة الاجراءات الواجب اتخاذها من قبل الاجهزة الامنية أو الاجهزة والمؤسسات الاخرى للمحافظة على سرية المعلومات الالكترونية ومنع الاختراقات الفيروسية الالكترونية من أجل ضمان وصول المعلومات الحاسوبية الى الجهات المختصة وفي الوقت نفسه ضمان عدم وقوعها في أيدي الاعداء والاصدقاء على حد سواء[2].

تعد إدارة المخاطر التي تتعرض لها أنظمة المعلومات أمرا أساسا لتحقيق الأمن السيبراني الفعال، وتعتمد المخاطر المرتبطة بأي هجوم سيبراني على ثلاث عوامل هي على التوالي: التهديدات (من هو المهاجم)، والثغرات الأمنية (التقاط الضعيفة التي يهاجمها)، والتأثيرات (ما يفعله الهجوم)، ومن الواضح أن الهجمات السيبرانية مستمرة ولكن معظمها محدودة التأثير، أما الهجوم الناجح منها فيحصل عندما يلامس بعض مكونات البنى التحتية الحيوية التي يتعامل معها القطاعين العام والخاص على حد سواء بشكل واسع، ويمكن أن تخلف تأثيرات كبيرة على الأمن الوطني والاقتصاد وسبل عيش وسلامة المواطنين، وعادة ما ينطوي الحد من مثل هذه المخاطر على إزالة مصادر التهديد ومعالجة الثغرات الأمنية وتقليل التأثيرات الناتجة عنها[3].

تقع على عاتق الدولة مسؤولية كبيرة لتحقيق الأمن السيبراني، ويصدق ذلك على وضع الإطار القانون المناسب بشكل خاص، ولاينبغي إقتصار عمل الدولة في هذا المجال على مجرد تعزيز وتشجيع البحث والتطوير في مجال الأمن عامة، بل يجب أن يتعدى ذلك إلى تعزيز ثقافة أمنية والامتثال لدواعي معايير الأمن بالمستوى الجزئي، والقيام بنفس الوقت بتقوية معايير إنفاذ القانون فيما يتصل بالجريمة السيبرانية، وهذا يثير مسائل الأنموذج الأساس والشراكة العامة–الخاصة لخطط العمل الوطنية والدولية لتأمين المعلومات، وفي المستوى الاستراتيجي من الضروري تأمين إدارة الوقاية ، والابلاغ، وتقاسم

(1) أوس مجيد غالب العوادي، الامن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، 2016، ص3.

(2) اسراء شريف جيجان، الامن السيبراني الصيني دراسة في الدوافع والتحديات، مجلة قضايا سياسية، العدد 65، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021، ص36.

(3) Congressional Research Service, Cybersecurity Issues and Challenges: In Brief C. R. (Ed.). (2016, August) متاح على شبكة الانترنيت على الرابط: https://crsreports.congress.gov.

المعلومات، والانذار، ومواجهة التحدي، ومن الضروري زيادة الوعي بافضل الممارسات في مجال الأمن وإدارة المخاطر، والمطلب المهم الآخر هو تنسيق النظم القانونية والتوفيق بينها وإنفاذ القانون الأمني، وصياغة التشريعات التعاونية المقترحة (الرسمية–غير الرسمية، والثنائية–متعددة الاطراف، والايجابية–السلبية، والوطنية–الدولية)[1]، ومن هذا المنطلق إهتم مركز (بيلفر) وهو مركز أبحاث بجامعة هارفرد يبحث في مجالات الأمن الدولي والدبلوماسية وقضايا البيئة والموارد، وسياسة العلوم والتكنلوجيا، إهتم بتقديم سبعة أهداف وطنية رئيسة يجب أن تضطلع بها الدولة لحماية أمنها السيبراني، قد تمثل بعضها تجاوزا على خصوصية الافراد وحقوق الانسان، بل قد يرتقي بعضها الى حد تهديد ركائز النظام الدولي بدلا من أن تتسم بالرشادة لدعم السلم والأمن الدوليين، وتمثلت تلك الاهداف السبع بما يأتي[2]:

1- مسح ومراقبة المجموعات المحلية عبر قيام الدولة برصد واكتشاف وجمع المعلومات الاستخبارية حول التهديدات المحلية والجهات الفاعلة داخل الدولة.
2- تعزيز الدفاعات السيبرانية الوطنية عبر حماية أصول الأنظمة الحكومية، وتحسين شبكة المعلومات الوطنية.
3- التحكم في بيئة المعلومات ومعالجتها، وازدواجية ضبط المعلومات من ناحيتي الباث والمستقبل، وتحكم الدولة بالمعلومات عبر استعمال الوسائل الالكترونية، وحفظ الخصوصية وحرية التعبير للمواطنين.
4- جمع المعلومات الاستخبارية من الدول الاخرى لحماية الأمن الوطني عبر قيام دولة ما بانتزاع أسرار وطنية من خصم اجنبي كالمعلومات السرية والوصول الى ملفات شديدة السرية كعمل إستباقي حمائي.
5- تحقيق مكاسب تجارية بما يخص قطاعات الصناعة والتكنلوجيا عبر التجسس الصناعي ضد الشركات الاجنبية لتيسير نقل التكنلوجيا.
6- السعي لتعطيل أو تدمير البنية التحتية للخصم وقدراته السيبرانية كشكل من اشكال الدفاع المشروع عن الأمن الوطني.

(1) حمدون توربة، دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، جنيف، 2006، ص15.

(2) هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 24، العدد 1، كانون الثاني، كلية الاقتصاد والعلوم السياسية، جامعة طرابلس، طرابلس، 2023، ص197.

7- تحديد القواعد والمعايير التقنية بالمستوى الدولي، أي مشاركة الدولة بالنشاطات القانونية والسياسية والفنية دوليا، وفي هذا مشاركة تدعم مرتكزات السلم والأمن الدولي.

لقد حددت معاهدة جرائم الفضاء السيبراني الصادرة عن مجلس الاتحاد الاوربي رقم (185) الصادر في بودابست 23 / تشرين الثاني من العام 2001، طبيعة وأهم أوجه جرائم الحاسوب والفضاء السيبراني، كما بينت المعاهدة ضرورة التعاون بين الدول الاعضاء من أجل مكافحة جرائم الفضاء السيبراني وحماية التشريعات القانونية المختصة، وعدت هذه المعاهدة رادعا أساس كونها تجرم الأفعال التي تشكل خطرا على السرية، وتحفظ نزاهة وجود أنظمة وشبكات وبيانات الحاسوب[1].

ثانياً: تحديات الأمن السيبراني العراقي

تتمثل التحديات التي يواجهها العراق لحماية أمنه السيبراني في تعدد توظيف الاطراف والفواعل الخارجية ونواياها الشريرة لضرب البنى الحيوية للدولة، إذ أن هذه التحديات لم تعد تقليدية مثل استعمال القوة العسكرية بشكل مباشر، بل أن الهدف هو الفضاء السيبراني الوطني واستهداف شبكات الحوسبة التي تدير وتوجه مؤسسات الدولة العراقية وبناها التحتية الحيوية المدنية والعسكرية، ومجالات الاعمال والتجارة والخدمات الحكومية والتعليم والصحة وغيرها من الانشطة السياسية والاقتصادية والاجتماعية، خصوصا مع تزايد التعاملات والخدمات الالكترونية داخل العراق، فمع هذا التصاعد المطّرد في استعمال شبكة الاتصالات الالكترونية الدولية (الانترنيت) 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 أو نشر برامج وفيروسات الكترونية تعطل تكنلوجيا الاتصالات والمعلومات الوطنية، وربما تدمير أنظمة التحكم الصناعي خصوصا في مرافق الطاقة والغاز الطبيعي والكهرباء والطيران والنقل وقواعد البيانات الوطنية فضلا عن اختراق البريد الالكتروني للمستخدمين وانكشاف واسع للمعلومات الشخصية أمام الهجمات السيبرانية[2]، وفي جانب التحدي السيبراني للمجال السياسي وتحت ضل التحول الديمقراطي والحرية الشخصية ومرافقة ذلك مع ثورة تكنلوجيا المعلومات،

(1) الاسكوا، نماذج تشريعات الفضاء السيبراني في الدول الاعضاء بالاسكوا، اللجنة الاقتصادية والاجتماعية لغربي آسيا، الامم المتحدة، نيويورك، 2007، ص33.

(2) مهند جبار عباس وهيثم كريم صيوان، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة العراق انموذجا، مجلة قضايا سياسية، العدد 70، كلية العلوم السياسية، جامعة النهرين، بغداد، 2022، ص158.

يواجه العراق تحدي قيام بعض الاشخاص أو الجماعات الارهابية من إنشاء مواقع في الفضاء السيبراني هدفها خلق معارضة وهمية للنظام السياسي القائم، ومحاولة نشر أخبار كاذبة أو تحريضية لإثارة السخط على النظام السياسي، أو تهديد شخصيات سياسية فاعلة بالقتل أو المساومة والتشهير عن طريق هتك أسرارهم وكشف معلوماتهم الشخصية وبياناتهم والتجسس على مراسلاتهم ومخاطباتهم الرسمية وغير الرسمية وتوظيفها للابتزاز أو التهديد لحملهم على تبني توجهات ومخططات الجماعات الارهابية[1].

يواجه العراق تحديات عدة تشكل 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، وكذلك ضعف مستوى التمويل المخصص لتطوير تقنيات الأمن السيبراني[2].

إن طبيعة التحديات التي يواجهها الأمن السيبراني تترافق مع تطورات أجيال الحرب النفسية، وبما أن أساليب التسلح الجديدة تعتمد بشكل كبير على المعرفة وتكنلوجيا المعلومات وتقنيات الكترونية شديدة التطور، فإن تمظهرات الأمن السيبراني والاعلام وعلاقتهما بصناعة الحرب النفسية وفق تحولات المشهد الاتصالي الجديد يتخذ بعدا موازيا للتطور التقني الفعال، ذلك أن الاعلام المفتوح والتدفق المعلوماتي الكبير جعل تحديات الحرب النفسية تتصدر الاولويات في الرصد والتحليل والمواجهة، واحدثت الحروب المعلوماتية تحت ظل التطور التقني تأثيرات سلبية كبيرة حول العالم، محققة بذلك أهداف استراتيجية لهذا النوع من الحروب وبشكل واسع[3].

بحسب التقرير الصادر عن شركة بوز ألن هاملتون (الشركة الامريكية الرائدة في مجال الادارة وتكنلوجيا المعلومات) فإن استمرار تطوير التكنلوجيا ونشرها في جميع أنحاء منطقة الشرق الاوسط

---

(1) أسعد طارش عبدالرضا وعلي ابراهيم مشجل المعموري، الامن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد العام 2003، مجلة دراسات دولية، العدد 80، كانون الثاني، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2020، ص168.

(2) باسم علي خريسان، الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي2020، مركز البيان للدراسات والتخطيط، بغداد، 2021، ص10.

(3) سهام حسن علي الشمري، تمظهرات الامن السيبراني والممارسة الاعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية رؤية نقدية علائقية، مجلة دراسات دولية، العدد 83، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2020، ص150.

وشمال افريقيا يواكبه باستمرار تنامي التهديدات السيبرانية، مثل عمليات الاحتيال لسحب البيانات وتعريضها للاختراق، ما يمثل تحديا سيبرانيا كبيرا للشركات والمنظمات بحيث سوف تحتاج الى تحويل مقاربتها للأمن السيبراني من مجرد التركيز على الامتثال الأمني الى تطوير ثقافة شاملة للأمن الاستباقي عبر النطاق الاوسع للمؤسسات، كما أظهر التقرير نفسه توقعات حول التهديدات السيبرانية لعام 2019م في منطقة الشرق الاوسط وشمال افريقيا التي بينت أهم توجهات التهديدات التي ينبغي أن تكون الدول والمنظمات في المنطقتين على علم بها لكي تتمكن من منع انتهاكات الأمن السيبراني، وتجنب الاضرار والخسائر الناجمة عن تلك الانتهاكات والحفاظ على الوعي الأمني بأعلى مستوياته[1].

ثالثاً: معالجات تهديدات الأمن السيبراني للعراق

بعد أن أدركت الحكومات أهمية تكوين نهج شامل للتصدي للهجمات السيبرانية تم وضع اجراءات وسياسات لتعزيز الامن السيبراني، ولما كان الفضاء السيبراني يتصل بالأمن الوطني، اتخذت الدول مسارات قانونية لضبط السيطرة على الفضاء السيبراني، وبما أن الفضاء السيبراني يشتمل على نشاطات الافراد والمؤسسات الحكومية صار لزاما على الدولة إصدار تشريعات قانونية تحكم التعاملات في هذا الفضاء وتحميه من الجرائم السيبرانية، وضرورة أن تكون هذه التشريعات مواكبة للمستجدات المعاصرة من ذكاء إصطناعي وغيره، وقد اتجهت العديد من الدول لإصدار تشريعات تنظم أمن المعلومات وتجرم الافعال الاجرامية الالكترونية[2].

تتصل استراتيجية الامن السيبراني عموما بكافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وابلاغها عبر وسائل الكترونية متاحة محمية من التهديدات الداخلية والخارجية ومن اولويات تلك الاستراتيجية مايأتي[3]:

1 – حماية وحفظ خصوصية الافراد.

2 – تأمين الخدمات الرقمية المقدمة للافراد.

---

(1) بلعسل بنت نبي ياسمين وعمروش الحسين، التهديدات الالكترونية والأمن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، المجلد 2، العدد 2، حزيران، المركز الجامعي مغنية، وزارة التعليم العالي والبحث العلمي، الجزائر، 2021، ص172.

(2) محمد زهير عبد الكريم، الارهاب السيبراني أزمة عالمية جديدة، مجلة قضايا سياسية، العدد 64، كلية العلوم السياسية، جامعة النهرين، بغداد، 2021، ص290.

(3) مصطفى عبد الكريم مجيد، الامن السيبراني وتأثيره على الامن الوطني، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2022، ص5.

3 – مرونة استعمال الخدمات المادية وغير المادية المعدة لمواجهة التهديدات السيبرانية.

4 – حفظ سلامة البنى التحتية الاساسية للجهات الحكومية.

5 – تنسيق الاستجابة السريعة في مواجهة التهديدات السيبرانية الطارئة.

6 – التأهب لإستمرارية تقديم الخدمات للافراد أثناء وبعد التهديد السيبراني.

تنطلق استراتيجية الأمن السيبراني في العراق (2022–2025) من مبدأ أساس هو ضمان أمن العراق وحماية وجوده في الفضاء السيبراني وحماية بنية المعلومات الحيوية وبناء مجتمع موثوق وآمن عن طريق تبني مجموعة من الاجراءات تعمل على حماية فضاء العراق السيبراني والدفاع عنه، وقد رصدت شركات أمنية متخصصة بالأمن السيبراني عام 2014م وجود حربا سيبرانية في العراق تم فيها استخدام وسائل التواصل الاجتماعي لحشد الرأي العام وتجميع المؤيدين للجماعات الارهابية ونشر الدعاية وجمع المعلومات الأمنية بوساطة مجموعة من قراصنة شبكة المعلومات الالكترونية الدولية (الانترنيت) يعملون على خداع الافراد عبر إرسال رسائل مشفرة وبرامج ضارة تخترق وسائل التواصل الاجتماعي، وما أن يتم فتحها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز وسرقة الملفات المخزنة في الجهاز أو استخدام كاميرا جهاز الحاسوب أو الميكرفون لمراقبة الشخص المستهدف[1]، ومن المعروف أن الحروب السيبرانية تنصب على الجانبين المدني والعسكري على حد سواء، وشجع ذلك الدول على تشكيل هيئات وطنية متخصصة بالأمن السيبراني، تضطلع بمهام إعداد إستراتيجية وطنية للأمن السيبراني وتنفيذها ووضع السياسات وآليات الحوكمة والارشادات المتعلقة بالأمن السيبراني مع شموليتها، ووضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، وتفعيل الاستجابة للحوادث والاختراقات، فضلا عن رسم السياسات والمعايير الوطنية للتشفير ورفع مستوى الوعي بالأمن السيبراني[2]، وهذا يوصلنا إلى نتيجة تفيد بأن تفاعلات الأمن السيبراني في العراق تقف أمام خيارين رئيسيين، الأول: السير الحثيث نحو إمتلاك تكنلوجيا أمن سيبراني متطورة تقنيا، إما منفردا أو عبر التحالف السيبراني مع الآخرين في إطار بناء أمن سيبراني متوازن، والآخر: الإذعان الأمني في المجال السيبراني للدولة الأقوى تقنيا في مواجهة مصدر التهديد السيبراني، وعليه يكون العراق جزءا من الدول المتفاعلة في المنطقة التي تواجه التهديد السيبراني

(1) مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، كلية القانون والعلوم السياسية، جامعة ديالى، ديالى، 2021، ص171.

(2) ساسوي خالد، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، 2020، ص51.

بالتحالف مع القوى الأكثر إمتلاكا لتقنية الأمن السيبراني، فالدولة الأقوى بالقدرات التقنية السيبرانية في الدفاع والهجوم تزيد من تفاعل القوى الأضعف للإذعان لها، ومعها يزداد ميل القوى التقليدية لمسايرة الدولة الاقوى، وكلما زادت القدرات السيبرانية لها زادت معها رغبة القوى الأضعف في التعاون معها، وهذا يفضي الى أن العراق يتفاعل مع القوى الاقليمية والدولية تفاعل إيجابي لصد التهديدات السيبرانية، ويلجأ إلى التحالفات التي تشكل منظومة أمن سيبراني مشترك[1].

لقد باشر فريق الاستجابة الالكتروني العراقي (CERT) مهامه في هذا الصدد وعمل على إيجاد التدابير والاجراءات لسد الفجوة الامنية السيبرانية ومعالجة أوجه الضعف الاساسية فيها، كذلك قام الفريق نفسه بتشكيل عدة فرق تعمل بشكل مستقل وبشكل منسق حيث تم تقسيم وتصنيف المجالات التي يجب العمل عليها بالشكل الذي يضمن إنتاجية الاستراتيجية الأمنية السيبرانية العراقية، وفي إطار زمني محدد إلى ثمانية أقسام وفقا للمعيار العالمي لإتحاد منظمة الاتصالات العالمية (ITU) وكذلك بما يضمن الارتقاء بمستوى العراق السيبراني العالمي، وأن الاقسام الثمانية هي على التوالي، الحكومة الفاعلة (العمل على تفعيل الحكومة الالكترونية بشكل يضمن راحة المواطنين)، والاطار التشريعي والتنظيمي (بناء القدرات التشريعية للجهات القانونية التنفيذية الوطنية)، والاطار التكنلوجي للأمن السيبراني (تحديد متطلبات السيطرة على الأمن السيبراني العراقي)، وتعزيز ثقافة الأمن السيبراني وبناء القدرات (تطوير آليات نشر المعلومات عن الأمن السيبراني في المستوى الوطني)، وتطوير الاعتماد على الذات (تعزيز مجتمع الابحاث في مجال الأمن السيبراني)، والامتثال والتنفيذ (وضع إطار معياري لتقييم مخاطر الأمن السيبراني)، والجاهزية لحماية الأمن السيبراني (وضع آليات فاعلة للابلاغ عن الحوادث السيبرانية)، والتعاون الدولي (التواصل مع منظمة الاتصالات العالمية، وتكوين شراكات مع فرق الاستجابة الالكترونية الدولية الأخرى)[2].

حدد مؤشر الأمن السيبراني العالمي (GCI) / (Global Cybersecurity Index)، وهو مؤشر يتم من خلاله وضع معايير لحالة الأمن السيبراني للدول عبر أنحاء العالم، ومرجع موثوق يقيس

(1) حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني مقاربة بين المعضلة الأمنية والمكنة الأدائية، مجلة دراسات دولية، العدد 83، مجلة دراسات دولية، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2020، ص120.

(2) استراتيجية الأمن السيبراني العراقي، اللجنة الفنية العليا لأمن الاتصالات والمعلومات، مستشارية الامن الوطني، بغداد، 2022، ص9.

مدى التزام الدول بمعايير الأمن السيبراني على مستوى العالم لرفع مستوى الوعي لأهميته وابعاده المختلفة، لأن للأمن السيبراني مجالا واسعا للتطبيق يشمل العديد من القطاعات المختلفة، واختيار البلدان الاكثر استعدادا لمواجهة الهجمات السيبرانية، إذ يتم إستعمال مؤشر الأمن السيبراني العالمي من خلال تقييم مستوى التنمية أو المشاركة في كل دولة ويعتمد على خمس ركائز هي: التدابير القانونية، والتدابير الفنية، والتدابير التنظيمية، وبناء القدرات، والتعاون، ثم يتم تجميعها في نتيجة إجمالية تبين معيار نجاح الدولة في مواجهة التحديات السيبرانية[1]، ومن اولويات هذه المواجهة تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة، والتشجيع على استعمال أجهزة وتقنيات وخدمات تكنلوجية موثوق بها عالميا، مع اتخاذ تدابير وطنية في إطار دولي مشترك والاستعداد الدائم للتصدي لجرائم المعلوماتية من خلال عقد اتفاقيات وبروتوكولات دولية لمواجهة تلك الجرائم والحد منها، ولايتم ذلك إلا من خلال استراتيجية موضوعة لهذا الغرض، وجعل مصالح الأمن الوطني والدولي هي الحافز لتقوية الأمن السيبراني في المستوى الدولي، وإدراك أن جميع الدول تتعاضد لتحقيق هدف شامل هو تحقيق التكامل الأمني عالميا[2].

تعتمد قدرة الدولة في منع الهجمات السيبرانية التي تطال البنية التحتية الحيوية لها على ما توفره من قوة عاملة متعلمة ومتخصصة وماهرة في مجال استعمال الشبكة الالكترونية الدولية (الانترنيت)، ويتحقق ذلك من خلال نظام تعليمي يتمكن من بناء هيكل نظمي يواكب التطورات المتسارعة في هذا المجال، بملاكات تتمتع بالكفاية والمقدرة على إكتشاف ومواجهة ومعالجة الهجمات السيبرانية، ويمكن الاستعانة بما توفره الادبيات والدراسات القائمة والتجارب الدولية والارشادات الاستراتيجية المتعلقة بكيفية تطوير القوى الوطنية العاملة في مجال الأمن السيبراني، وعليه تتحمل المؤسسات التعليمية تزويد الطلاب بالمعلومات المناسبة لهذا المجال، ومن هنا تظهر الحاجة الملحة لبناء استراتيجية وطنية لتعليم الأمن السيبراني، كما يمكن للحكومة والاوساط الاكاديمية العمل معا لمعالجة المتطلبات التعليمية للأمن السيبراني الوطني وتعزيز المبادرات التدريبية للمعلمين والبرامج الاكاديمية للأمن السيبراني، وفيما يخص الطلبة يجب إذكاء الوعي لهم بالأمن السيبراني وعلاقته بالأمن الوطني وبالأمن الشخصي عبر تثقيف الطلبة من خلال المقررات والمناهج الدراسية للجامعات، إنشاء مكتبة أمنية متخصصة بالأمن السيبراني

(1) تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد 30، كلية التربية للبنات، جامعة الكوفة، الكوفة، 2019، ص249.

(2) رعد خضير صليبي، تعزيز الامن السيبراني في العراق التحديات والفرص، مجلة دراسات دولية، العدد 99، تشرين الاول، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، بغداد، 2024، ص521.

والعلوم الأمنية، فضلا عن تكثيف عقد المؤتمرات والورش العلمية والحلقات النقاشية لزيادة الخبرات[1]، وقد عكفت بعض الحكومات أيضا على تكليف مجاميع من القراصنة المدنيين من القطاع الخاص الذين يمكن الاستعانة بجهودهم عند الحاجة، ويمكن لهذه الجهات الناشطة في مجال القرصنة إما أفرادا متخصصين في مجال التكنلوجيا المتقدمة أو قراصنة سابقين غير شرعيين يتم تكليفهم وتدريبهم لإستخدام مهاراتهم لتحقيق أهداف الأمن الوطني في مجال الأمن السيبراني، وقد تلجأ بعض الدول الى الاستعانة بوكلاء متخصصين من دول أخرى يعملون بالنيابة عنها، وهذه متغيرات تعكس التحول في استراتيجيات رد الفعل أزاء التهديدات السيبرانية وإعادة التفكير بالنهج الاستباقي لحرب المعلومات والعمل بفاعلية عند مواجهة تحديات تكنلوجيا متقدمة، ونتيجة للهجمات السيبرانية ظهرت شركات متخصصة في الأمن السيبراني الاحترافي لتنفيذ هجوم سيبراني مأجور كخطوة استباقية، أو بيع برامجيات متطورة تعمل كأسلحة الكترونية تعالج أي خرق سيبراني[2]، ومع إحتمالات زيادة توسع مجالات الصراع في المستقبل السيبراني في نواح عدة، ومع إفتراض أن كل عدو سيبراني في الفضاء الالكتروني يعمل على تحسين قدراته الهجومية، يسعى العديد منهم مثل (جماعات الجريمة المنظمة، والجيوش الالكترونية، والارهابيين) إلى أن يكونوا قادرين على إحداث تأثيرات طويلة الأمد وواسعة النطاق، سواء في سرقة الأموال أو المعلومات أو في تعطيل الخصوم، وعلى حد وصف تلك الاحتمالات يبدو أن هنالك ثلاث سيناريوهات يمكن التنبوء بها مستقبلا وهي كما يأتي[3]:

1 – أن يصبح الفضاء الالكتروني أكثر مرونة في مواجهة الهجمات السيبرانية مما هو متوقع، بحيث لايمكن حدوث عمليات هجوم سيبراني واسع النطاق.

2 – أن تتطور التقنيات الدفاعية السيبرانية وتكنلوجيا المعلومات لصالح المدافعين بقوة.

3 – أن يزداد تأير عمل المهاجمون السيبرانيون تحت ظل إنفلات تام من العقاب.

---

(1) سالي سعد محمد، الأمن السيبراني ودور الجامعات في تعزيزه لدى الطلبة، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 2022، ص4.

(2) أنسام فائق العبيدي، الأمن المجتمعي بين التحديات والتداعيات الأمنية السيبرانية والاستراتيجيات الاصلاحية المجتمعية، مجلة تكريت للعلوم السياسية، عدد خاص، كلية العلوم السياسية، جامعة تكريت، تكريت، 2023، ص358.

(3) Jason Healey,The Five Futures Of Cyber Conflict and Cooperation, Atlantic Council, Washington, 2011, pg3.

- **الخاتمة:**

يظهر من ثنايا البحث أن مسائل الأمن السيبراني لها الأولوية على الصعيد الدولي، وتأكدت العلاقة مابين إستيعاب التطورات التكنلوجية والسيطرة على الفضاء السيبراني، إذ تمنح القوة السيبرانية لمن يمتلكها سطوة المبادرة والتحكم بالفضاء السيبراني وتوظيفه لصالحه، وقد واجه العراق تحديات سيبرانية معقدة حثته على العمل بجدية لبناء استراتيجية أمن سيبراني يضع من خلالها معالجات فاعلة للتهديدات السيبرانية من منطلق حماية بنية المعلومات الحيوية الخاصة بالمؤسسات الرسمية وغير الرسمية، والتصدي للمخاطر السيبرانية وتوظيف الفضاء السيبراني لأهداف الأمن الوطني العراقي، والعمل على تأسيس مجتمع سيبراني موثوق، وقد تمحورت المعالجات السيبرانية العراقية حول الحوكمة الفاعلة ، والإطار التشريعي، وتطوير تكنلوجيا المعلومات، وبناء القدرات الدفاعية السيبرانية، والتأهب لحوادث الأمن السيبراني، والتشجيع على التعاون الاقليمي والدولي في مواجهة التهديدات السيبرانية، عبر المشاركة الفاعلة مع جميع هيئات الأمن السيبراني الدولية ذات الصلة، والمشاركة في جميع الفعاليات والمؤتمرات الدولية المتعلقة بالأمن السيبراني، ومن ذلك نستنتج مايلي:

1 – يقترن وجود أمن سيبراني عالي المستوى بوجود تكنلوجيا إتصالات متطورة تتسق والتسارع الحاصل في تقنيات المعلومات والتواصل الالكتروني.

2 – لايقتصر تعزيز آليات حفظ الأمن السيبراني على الدولة وحدها، بل يتطلب الامر التعاون الجاد مع أطراف اقليمية ودولية تتكاتف فيما بينها لتأمين الفضاء االسيبراني من التهديدات المتوقعة.

3 – تبنى العراق استراتيجية الأمن السيبراني (2022–2025)، وهي استراتيجية تعمل على تكوين استراتيجية منسقة تستجيب بشكل ديناميكي نحو التهديدات التي تواجه الأمن السيبراني الوطني، حيث أن الرؤية الوطنية للأمن السيبراني تتجه نحو مجتمع آمن وموثوق.

4 – هدفت استراتيجية الأمن السيبراني العراقية إلى حماية البنى التحتية المعلوماتية الوطنية في مختلف الاتجاهات، للارتقاء بالعراق نحو بيئة سيبرانية آمنة.

التوصيات:

لتحقيق أعلى جاهزية لمواجهة التحديات السيبرانية، يجب على الدولة العراقية تبني استراتيجية شاملة تشمل عدة محاور رئيسة، منها:

1 – بناء إطار تشريعي وتنظيمي قوي تساهم بشكل فعال في :

• سن قوانين وتشريعات واضحة تحكم الأمن السيبراني، مثل قانون الجرائم الإلكترونية وحماية البيانات.

• إنشاء هيئة وطنية للأمن السيبراني تكون مسؤولة عن وضع السياسات والإشراف على تنفيذها.

• فرض معايير أمنية على المؤسسات الحكومية والقطاع الخاص لضمان الالتزام بالإجراءات الوقائية.

2 – تطوير البنية التحتية الرقمية والأمنية:

• تحديث وتأمين مراكز البيانات الحكومية والبنية التحتية الرقمية الحرجة.

• تطبيق أنظمة كشف التهديدات والاستجابة للحوادث السيبرانية (مثل SOC – Security Operations Center).

• استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في رصد التهديدات السيبرانية والتعامل معها بفعالية.

3 – تعزيز القدرات البشرية والتدريب:

• إنشاء مراكز تدريب متخصصة في الأمن السيبراني وتأهيل كوادر محلية محترفة.

• إدراج الأمن السيبراني ضمن المناهج التعليمية في الجامعات والمعاهد التقنية.

• تنفيذ برامج توعية للمؤسسات والأفراد حول أهمية الأمن السيبراني وطرق الحماية من الهجمات.

4 – التعاون الدولي والإقليمي:

• الانضمام إلى الاتفاقيات والمنظمات الدولية المختصة بالأمن السيبراني، مثل الـ ITU والـ INTERPOL.

• تبادل المعلومات والخبرات مع الدول المتقدمة في مجال الأمن السيبراني.

• تطوير شراكات مع شركات التكنولوجيا العالمية لتعزيز الأمن السيبراني في العراق.

5 – إنشاء فرق استجابة للطوارئ السيبرانية (CERTs):

• تأسيس فرق مختصة بالاستجابة السريعة للهجمات السيبرانية.

• تطوير خطط طوارئ واختبارها بانتظام لمحاكاة سيناريوهات الهجمات المحتملة.

• تعزيز التعاون بين القطاعات المختلفة لضمان سرعة احتواء أي تهديد.

6 – تحفيز البحث والتطوير في الأمن السيبراني وهذه النقطة تحسب للباحث في ذلك:

• دعم الأبحاث في مجال الأمن السيبراني وتمويل الابتكارات المحلية.

• تشجيع إنشاء شركات ناشئة متخصصة في الأمن السيبراني وتقديم حوافز لها.

• استغلال الذكاء الاصطناعي والتقنيات الحديثة في تطوير حلول أمنية متقدمة.

7 – ومن أجل تحقيق أعلى جاهزية للأمن السيبراني في العراق يتطلب ذلك مزيجًا من التشريعات الصارمة، البنية التحتية المتطورة، الكوادر البشرية المؤهلة، والتعاون الدولي. الأمن السيبراني ليس مسؤولية جهة واحدة، بل يحتاج إلى تكاتف جميع القطاعات لضمان بيئة رقمية آمنة ومستقرة.

- **References:**

1-Aws Majeed Ghaleb Al-Awadi, Cyber Security, Al-Bayan Center for Studies and Planning, Baghdad, 2016.

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

3-Congressional Research Service, Cybersecurity Issues and Challenges: In Brief C. R. (Ed.). (2016, August) Available online at :https://crsreports.congress.gov

4-Hamdoun Turbah, Cybersecurity Guide for Developing Countries, International Telecommunication Union, Geneva, 2006.

5-Hiba Jamal Al-Din, Cybersecurity and the Transformation of the International System, Journal of the Faculty of Economics and Political Science, Volume 24, Issue 1, January, Faculty of Economics and Political Science, University of Tripoli, Tripoli, 2023 .

6-ESCWA, Cyberspace Legislation Models in ESCWA Member States, Economic and Social Commission for Western Asia, United Nations, New York, 2007.

7-Muhannad Jabbar Abbas and Haitham Karim Saywan, Cyber Warfare: Challenges and Confrontation Strategies: Iraq as a Model, Political Issues Magazine, Issue 70, College of Political Science, Nahrain University, Baghdad, 2022.

8-Asaad Taresh Abdulredha and Ali Ibrahim Mashjal Al-Maamouri, Cybersecurity and Its Role in the Spread of Terrorism in Iraq after 2003, International Studies Magazine, Issue 80, January, Center for Strategic and International Studies, University of Baghdad, Baghdad, 2020.

9- Bassem Ali Khreisan, Cybersecurity in Iraq: A Reading of the 2020 Global Cybersecurity Index, Al-Bayan Center for Planning and Studies, Baghdad, 2021.

10- Siham Hassan Ali Al-Shammari, Manifestations of Cybersecurity and Media Practice and Their Relationship to the Virtual Psychological Warfare Industry: A Critical Relational Perspective, Journal of International Studies, Issue 83, Center for Strategic and International Studies, University of Baghdad, Baghdad, 2020.

11- Balasal Bint Nabi Yasmine and Amroush Al-Hussein, Electronic Threats and Cybersecurity in the Arab World, Numerus Academic Journal, Volume 2, Issue 2, June, Maghnia University Center, Ministry of Higher Education and Scientific Research, Algeria, 2021.

12- Muhammad Zuhair Abdul Karim, Cyberterrorism: A New Global Crisis, Journal of Political Issues, Issue 64, College of Political Science, Al-Nahrain University, Baghdad, 2021.

13- Mustafa Abdul Karim Majeed, Cybersecurity and Its Impact on National Security, Hammurabi Center for Research and Strategic Studies, Baghdad, 2022.

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

15- Sassawi Khalid, Cyberwars and Global Security: Challenges and Confrontations, Unpublished Master's Thesis, College of Law and Political Science, Ziane Achour University, Djelfa, Algeria, 2020.

16- Hazem Hamad Musa, The Strategic Vision for Iraqi National Security in Cyberspace: An Approach between the Security Dilemma and the Performance Machine, Journal of International Studies, Issue 83, Journal of International Studies, Center for Strategic and International Studies, University of Baghdad, Baghdad, 2020.

17- Iraqi Cybersecurity Strategy, Supreme Technical Committee for Communications and Information Security, National Security Advisory, Baghdad, 2022.

18- Taghreed Moeen Hassan Al-Mashhadi, The Military Impact of Cybersecurity on the Political Geography of the State, Journal of Geographical Research, Issue 30, College of Education for Girls, University of Kufa, Kufa, 2019.

19- Raad Khadir Salibi, Enhancing Cybersecurity in Iraq: Challenges and Opportunities, Journal of International Studies, Issue 99, October, Center for Strategic and International Studies, University of Baghdad, Baghdad, 2024.

20- Sally Saad Mohammed, Cybersecurity and the Role of Universities in Enhancing It among Students, Hammurabi Center for Research and Strategic Studies, Baghdad, 2022.

21- Ansam Faiq Al-Obaidi, Community Security: Challenges, Cybersecurity Implications, and Community Reform Strategies, Tikrit Journal of Political Science, Special Issue, College of Political Science, Tikrit University, Tikrit, 2023, p. 358.

22- Jason Healey, The Five Futures of Cyber Conflict and Cooperation, Atlantic Council, Washington, 2011.