تداعيات الامن السيبراني العراقي الراهنة وآفاق المستقبل

أ.د. حيدر علي حسين
hyder_iraq@uomustansiriyah.edu.iq
سرى غضبان غيدان
suraghedain@gmail.com
الجامعة المستنصرية – كلية العلوم السياسية

الملخص :

يركز هذا البحث على أستشراف مستقبل الامن السيبراني في العراق في ظل التحولات الرقمية ،والذي أستندنا فيه الى الواقع العالمي والحالي ،في ظل التحولات التكنلوجية المتسارعة ، نعيش بعالم أفتراضي فوضوي رقمي هائل ، حيث يتجه الامن السيبراني في العراق نحو أهمية متزايدة في ظل التطورات التكنلوجية ،مع توسع في الخدمات الرقمية ،ومايصاحبها من تزايد في حجم التهديدات السيبرانية ،والتي باتت تطال المؤسسات الحكومية والبنية التحتية ، كما ان هناك فجوة في الكوادر الفنية في المجال السيبراني ،وبالمقابل الجهود الحكومية العراقية واضحة ، في التوجه نحو التحول الرقمي ،صياغة أطر قانونية تنظيمية للامن السيبراني ، مع الانفتاح الاقليمي والعالمي ، للاستفادة من تجارب الدول ذات البيئة المتشابهة ،وأستثمار من تجارب الدول المتقدمة تكنلوجياً ،لاسيما وان العراق يتجه نحو رقمنة الخدمات كافة ،مع خلق بنية تحتية سيبرانية قوية وآمنة ،والتوجه نحو تعزيز وبناء القدرات ، وبناء مراكز الرصد والاستجابة للحوداث السيبرانية ،والسعي نحو أقرار وتفعيل قانون جرائم المعلومات العراقي ،بما يتوائم مع الفضاء الرقمي العالمي الواسع .

الكلمات المفتاحية :الامن السيبراني ،الفضاء الرقمي ،العراق ،تعزيز القدرات .

Abstract:

This research focuses on anticipating the future of cybersecurity in Iraq in light of digital transformations, which we relied on the global and current reality, in light of the rapid technological transformations. We live in a huge digital, chaotic virtual world, where cybersecurity in Iraq is heading towards increasing importance in light of technological developments, with the expansion of digital services, and the accompanying increase in the volume of cyber threats, which now affect government institutions and infrastructure. There is also a gap in technical cadres in the cyber field. In contrast, the Iraqi government's efforts are clear, in the direction of digital transformation, formulating legal and regulatory frameworks for cybersecurity, with regional and global openness, to benefit from the experiences of countries with a similar environment, and investing in the experiences of technologically advanced countries, especially since Iraq is heading towards digitizing all services, while creating a strong and secure cyber

infrastructure, and moving towards strengthening and building capabilities, and building monitoring and response centers for cyber incidents. ...and striving to enact and implement the Iraqi Information Crimes Law, in line with the broader global digital landscape.

Keywords: cybersecurity, digital space, Iraq, capacity building.

المقدمة :

شهد الفضاء الرقمي تقدم وتسارع تكنلوجي واسع ، وباتت التكنلوجيا متداخلة وبشكل معقد في حياتنا اليومية ،بالمقابل زادت التهديدات السيبرانية ،ويعد المشهد السيبراني العراقي من مشاهد الاداء وأنعكاس لكمية التحديات والفرص والتي يتعرض لها الفضاء الرقمي العراقي ،فالاداء العراقي يعتمد على عوامل عديدة قائمة على مواكبة حجم التطور والتقدم التكنلوجي في الفضاء الرقمي ،والاستثمار المتزايد بالبنى التحتية الرقمية ، بالاضافة الى حجم التحديات المتصاعدة ،فالمشهد السيبراني العراقي قائم على التقييم وتعزيز البنى التحتية الرقمية والتحول نحو خلق ودعم الامن السيبراني العراقي ،بما يتناسب مع تعزيز الامن الوطني العراقي ،في ظل عصر معلومات شائك محفوف بالمخاطر والتحديات ، لاسيما أن التوجه الوطني العراقي قائم على تحسين قدرات المؤسسات بالقطاعين العام والخاص،والاعتماد على حلول تقنية وأستراتيجية ،وتطبيق خطوط الحماية بشكل كامل،والعمل بأتجاه خلق بنية آمان رقمية متطورة قادرة على احتواء التهديد الرقمي المتزايد.

أهمية البحث :

تكمن الاهمية العلمية والعملية للبحث في تسليط الضوء على طبيعة التحولات التكنلوجية في الفضاء الرقمي ،وما يتمخض عنها من تحديات سيبرانية داخلية وخارجية مستقبلية، وما تؤثره على الامن الوطني العراقي ، مما ادى الى لفت الانظار في ضرورة مواجهة التحديات بالإضافة الى الدعم الحكومي ، في مجال التحول الرقمي وبالمقابل دفع صناع القرار والمخططين الاستراتيجيين والمتخصصين والاكاديميين ،الى تبني التخطيط الاستراتيجي المستقبلي لمواجهة التحديات واحتوائها .

أشكالية البحث :

ينطلق البحث من أشكالية مؤداها من مساءلة فلسفية مفادها أن التقدم التكنولوجي، بوصفه تجليًا لحداثة متسارعة، لا يفضي بالضرورة إلى تعزيز الأمن، بل يعيد إنتاج أنماط جديدة من الهشاشة البنيوية في الفضاء الرقمي. وفي هذا السياق، تبرز مفارقة جوهرية تتمثل في أن تعاظم القدرات التقنية يقابله تصاعد موازٍ في التهديدات السيبرانية، بما يضع الدولة أمام تحدي إعادة تعريف مفهوم الأمن الوطني خارج حدوده التقليدية.

ومن ثم، تتمحور الإشكالية حول الكيفية التي يمكن من خلالها للعراق أن يؤسس مقاربة استراتيجية متكاملة للأمن السيبراني، قادرة على التوفيق بين متطلبات التحديث التكنولوجي وحدود البنية التحتية، وإكراهات الإطار التشريعي، وإشكالات بناء رأس المال البشري، بما يضمن تحقيق السيادة الرقمية وصون الأمن الوطني في أفق التحولات المستقبلية. وعليه يمكن طرح التساؤلات التالية :

١- ما التحديات التي تواجه إعداد وتأهيل الخبرات الوطنية في هذا المجال؟ وكيف يمكن تعزيز التنسيق بين المؤسسات الحكومية والقطاع الخاص في مواجهة التهديدات الرقمية؟

٢- ما السيناريوهات المحتملة لمستقبل الأمن السيبراني في العراق؟

٣- كيف يمكن للعراق الانتقال من موقع رد الفعل إلى موقع المبادرة في إدارة المخاطر السيبرانية

فرضية البحث :

يقوم البحث على فرضية مفادها (إذا تبنّى العراق استراتيجية وطنية شاملة للأمن السيبراني مدعومة بتطوير البنية التحتية الرقمية، وتعزيز القدرات البشرية والتشريعية، فإن أداءه المستقبلي في مجال الأمن السيبراني سيتحسن بشكل ملموس، مما يعزز قدرته على مواجهة التهديدات السيبرانية وحماية أمنه القومي الرقمي، وأن العراق يمتلك إمكانات كامنة لتطوير منظومة أمن سيبراني فعّالة، رغم التحديات المرتبطة بالبنية التحتية والتشريعات والكفاءات البشرية؛ وأن تبني مقاربة استراتيجية شمولية قائمة على تحديث البنية الرقمية، وتطوير الإطار القانوني، والاستثمار في رأس المال البشري، وتعزيز التكامل المؤسسي، من شأنه أن يحوّل التهديدات الرقمية من عامل إضعاف إلى محفّز لبناء قدرة سيبرانية وطنية مرنة، بما يدعم تحقيق السيادة الرقمية ويعزز الأمن الوطني في المستقبل.

منهجية البحث :

اعتمد البحث على المنهج التحليلي والذي يقوم على تحليل التقدم التكنلوجي وماله من تأثير على زيادة التهديدات ومايؤوله ذلك على الامن الوطني والقومي العراقي في ظل نظام عالمي تكنلوجي متسارع ،وكذلك المنهج الاستشرافي الذي يستشرف مستقبل الاداء العراقي في مجال الامن السيبراني .

المبحث الأول

تقييم المشهد السيبراني العراقي المعاصر

بدا العراق منذ سنين عدة في التحرك نحو صياغة سياسية واستراتيجية تخص الامن السيبراني العراقي ، وتعزيز الاداء العراقي السيبراني ،مع وجود أدراك الى حجم التحديات السياسية والامنية والاقتصادية التي عاصرها العراق في السنوات الاخيرة ، فالمشهد العراقي مازال متجهاً نحو البناء والتطوير والاحتواء الرقمي ،ولايمكن التغافل عن كمية الاستثمارات البشرية والفنية التي تم اعتمادها من قبل العراق في هذا المجال ،بالاضافة الى الاطر القانونية والفنية والسياسية والتكنلوجية والدعم والعمل مع القطاعين العام والخاص على حد سواء،ترجمت وثيقة السياسات العراقية في أمن المعلومات والاتصالات، والاستراتيجية الوطنية العراقية للامن السيبراني، حالة الإدراك والاستجابة العراقي في الفضاء الرقمي الواسع، وكان التحرك نحو محاور عديدة، تمثلت في بناء بنية تحتية رقمية آمنة، والاستثمار في مراكز البيانات المحلية، والتعاون البناء المستمر بين الأجهزة الامنية ووضع استراتيجية عمل مشتركة، بالاضافة الى تعزيز الدفاعات السيبرانية الأمنية، والتوجه نحو سياسة تعاون اقليمية ودولية، قائمة على تعزيز التعاون في هذا المجال، قادرة على مواجهة الاختراقات والهجمات العابرة للحدود، والاستثمار المستمر للخبرات الوطنية العراقية، ورفع الوعي والتثقيف السيبراني عن طريق زيادة التوعية، والتأكيد على بناء القدرات.

ويكون التقييم صادر من الاتحاد الدولي للاتصالات(IIU) *، والذي يعد مبادرة من الاتحاد، وتكون من خلال مجموعة متنوعة من الخبراء والمساهمين في البلدان والمنظمات الدولية، ويكون التقييم عن طريق جمع البيانات من مختلف البلدان الملتزمة بالأمن السيبراني.

ويكون التقييم عن طريق الرقم القياسي العالمي للأمن السيبراني (GCI) (Global Cyber security Index) ، وهو مؤشر مركب للمؤشرات، يحدد مستوى التزام الدول بالأمن السيبراني، ويكون الالتزام بالأمن السيبراني في إطار ركائز خاصة ببرنامج الأمن السيبراني العالمي، والأهداف الرئيسية لقياس التقييم كالتالي:

١. التقدم بالأمن السيبراني وفق منظور اقليمي وعالمي.

*الاتحاد الدولي للاتصالات أو International Telecommunication Union (ITU) هو وكالة متخصصة تابعة لـ الأمم المتحدة، تُعنى بتنظيم وتنسيق شؤون تكنولوجيا المعلومات والاتصالات على مستوى العالم، ووضع المعايير التقنية، وتحسين البنية التحتية للاتصالات .للمزيد انظر:الموقع الرسمي :https:www.itu.int

٢. نوع ومستوى الالتزام السيبراني للدول مع مرور الوقت داخل البلد ومع البلدان الأخرى.
٣. فجوة الالتزام ما بين بلد وبلد آخر، وتكون على أساس المشاركة مبادرات الأمن السيبراني.

ويعتمد الاتحاد الدولي للاتصالات (Itu) الى خمسة ركائز اساسية من خلالها يتم تقييم عمل ومستوى الدول في مجال الأمن السيبراني وهي:

(الاطار القانوني،الاطار التنظيمي، الاطار الفني ،تطوير القدرات ،التعاون)

ويعد التقييم والرقم القياسي العالمي للأمن السيبراني، أفضل مجال لتحسين ورفع مستوى الأداء لدى الدول، ويعمل على ضبط الالتزام الوطني، ومعرفة التحديات، وتحديد وضع الدولة في الفضاء الرقمي، والعمل على تنسيق الممارسات، وتعزيز الثقافة العالمية، كما يهدف التقييم والرقم القياسي الى توضيح الامثلة الناجحة للدول في هذا المجال.

والعراق عضو في الاتحاد الدولي للاتصالات (IIU)، يعمل على زيادة وتعزيز مواطن القوة، ومعالجة نقاط الضعف، والاستفادة من تجارب الدول الأعضاء المتقدمين في مجال الأمن السيبراني، ودعم السياسات السيبرانية الوطنية.

ومن النقاط الاساسية التي أكد عليها العراق في مجال الفضاء الرقمي، هو النظر في الأمور الاتية:

١. مواصلة تطوير فريق (السيرت CERT) الوطني، كأحد اهم مقومات القوة في الفضاء الرقمي.
٢. اعداد وتنفيذ استراتيجية وطنية، وتطبيقها من خلال خطة واضحة.
٣. تحسين وتعزيز قدرات الأمن السيبراني في المؤسسات الحكومية والقطاع الخاص.
٤. المشاركة في النشاط الاقليمي والدولي، وارساء مبدأ التعاون، وتبادل الممارسات الجيدة، والعمل على تحسين ودعم قدرة التأهب والاستجابة.
٥. شمول وتنوع القوة العاملة في مجال الأمن السيبراني، لاسيما النساء والشباب.

*فريق السيرت هو اختصار لـ Computer Emergency Response Team، ويُعرف بأنه فريق متخصص في التعامل مع حوادث الأمن السيبراني والاستجابة لها للمزيد انظر:

https://www.cert.org

وفي حلول عام ٢٠٢٠م، وصل عدد البلدان التي لديها استراتيجية وطنية خاصة بالأمن السيبراني الى (١٢٧) دولة، وبلغ عدد البلدان المتقدمة في هذا المجال الى (٦٠) بلداً متقدماً، وأحد اهم نقاط القوة التي تعتمدها البلدان المتقدمة في مجال الأمن السيبراني، هو أتباع خطة أنمائية، مع وضوح الاهداف المتعلقة بحماية البنية التحتية الرقمية، وتجنب قدر الإمكان الحوادث المتعلقة بشبكات الكهرباء، وتنقية المياه، وأنظمة النقل، والعمل على تقليل المخاطر، ولنجاح اي استراتيجية وطنية خاصة بالأمن السيبراني، لابد من زيادة الانفاق المالي، وبات الاستثمار المالي في الأمن السيبراني، ضرورة ملحة لا مفر منها على الإطلاق.

وكان الاتجاه الاكثر تأكيداً في العراق، هو حماية البنية التحتية الرقمية الوطنية العراقية، والتي تكون عن طريق وضع إطار زمني لإدارة المخاطر، وتحديدها والتوجه نحو تقليل استيراد التكنلوجيا، واستخدام المنتجات والخدمات التكنلوجية الموثوق بها.

ومن اهم نقاط القوة التي يركز عليها العالم بشكل عام، والعراق بشكل خاص في مجال الأمن السيبراني، والفضاء الرقمي ككل، هو تعزيز التعاون الاقليمي والدولي ، وتوقيع مذكرات التفاهم، وحضور الاجتماعات والندوات، وتبادل الخبرات التدريسية، لاحتواء خطر هذه الهجمات والعمل على محاربتها.

والذي جمع الدول كافة نحو مبدأ تعزيز التعاون في القضاء الرقمي هو المصلحة المشتركة التي يجمع الدول، والتي تعد المحفز الاستراتيجي للحراك الدولي الرقمي، والتكامل الأمني التكنلوجي العالمي.

وعليه توجه العراق نحو تقرير التعاون مع الدول والمنظمات الدولية، كنوع من مرتكزات القوة الرقمية، ففي عام ٢٠١٦ عمل العراق على تدريب موظفين من فريق الاستجابة للحوادث السيبرانية، بالتنسيق مع حلف شمال الاطلسي (NATO)، الدورات تستهدف المتخصصين العاملين في أجهزة الدولة، لرفع مستوى الخبرة التقنية الوطنية، وتعزيز القدرات الدفاعية العراقية لمواجهة اي تحديات سيبرانية.

وفي عام ٢٠١٧ أطلق الاتحاد الاوربي بعثة استشارية في العراق لدعم القطاع الأمني، وكانت أحد جوانبه الأمن السيبراني، وكانت هذا التعاون بمذكرة تعاون من عام (٢٠١٧ – ٢٠٢٤)، بميزانية تصل الى (٧٠) مليون يورو، ويعد هذا التعاون، ترجمة لالتزام العراق الأمني السيبراني لتطوير القدرات السيبرانية، ومكافحة التهديدات الالكترونية.

وظل العراق يركز على نقاط القوة التي تعزز الأمن السيبراني الوطني، والتأكيد على التعاون الدولي الذي بات يمثل انعكاس لالتزام العراق بتحسين المجال الرقمي الوطني العراقي، ففي ٥ آذار ٢٠١٩م، انعقد في بغداد مؤتمر "العراق الالكتروني والأمن السيبراني"، وبالتعاون مع المجلس الدولي للاستشارة الالكترونية (Ec-Council) التابع لمفوضية الاتحاد الاوروبي، والذي يتعلق بمتابعة قضايا الأمن السيبراني، كان

للهدف من هذا المؤتمر هو رفع مستوى العراق في مجال الدفاع السيبراني الوطني، ووضع إستراتيجية تكتيكية للحكومة العراقية، ورسم مستقبل الحكومة الالكترونية الوطنية، وسبل مواجهة الهجمات، وكيفية الدفاع عن البيانات، وكان يعد هذا المؤتمر أحد أهم خطط الحكومة العراقية التي تعمل على تعزيز الأمن السيبراني العراقي.

وفي عام ٢٠١٩ شارك العراق بالاجتماعات المنعقدة في الجمعية العامة التابعة للأمم المتحدة في نيويروك، واصبح العراق عضواً في "الفريق العامل المقترح العضوية لتكنلوجيا الاتصالات والمعلومات" (OEW)، والذي تشكل بموجب قرار الجمعية العامة للأمم المتحدة على هامش اعمال الدورة (٧٣) المرقمة (٢٧/٧٣) في عام ٢٠١٨م، وكان العراق يشارك في الاجتماعات والمقترحات .

كما اقترح العراق بإنشاء نقطة اتصال دولية برعاية الأمم المتحدة، مهمتها إدارة القوانين والتشريعات لرفع المستويات، وحسب درجة المخاطر التي تواجهها البلدان بما يضمن أمن الفضاء السيبراني العالمي.

وفي الوقت ذاته يعمل فريق الاستجابة للحوادث السيبرانية في العراق (CERT) من خلال موقعه على (Face Book)، والقناة الخاصة بالفريق على تطبيق التيلكرام (Telegram) على زيادة التوعية، والتنويه الى أهم اعمال الفريق في هذا الجانب، سنتطرق الى اهم أعمال الفريق في عام ٢٠٢٤، وعام ٢٠٢٥ وكالآتي:

١. اعطاء وتوضيح مفهوم الهندسة الاجتماعية: وفي حالة اختراق يقوم بها (الهكر او المهندس الاجتماعي)، سرقة المعلومات الرقمية الخاصة بالترخيص عن طريق طرح الاسئلة او طلب الهاتف بحجة نفاذ الشحن، او اتصال ضروري، وتعد هذه الحالة من اكثر الحالات انتشاراً لاختراق المعلومات والبيانات الشخصية، ويعمل فريق السيرت على اعطاء ورش وندوات توعية، خاصة بالهندسة الاجتماعية، في المؤسسات الحكومية والوزارات والجامعات.
٢. الاشارة الى مفهوم التصيد الاحتيالي: وهو عملية الاختراق عن طريق ارسال رابط مما يقوم بتنزيل برامج ضده، بالتالي سيؤدي الى سرق معلوماتهم، مع اعطاء خطوات لتجنب حالات التصيد والاحتيال[١].
٣. اجراءات وتدابير امنية قام بها الفريق الوطني للاستجابة للأحداث السيبرانية، لضمان حماية أمن المعلومات ضد محاولات الاختراق، تجاه منصة أور الخاصة ببيانات المرور العامة[٢].

٤. استضافة الفريق العراقي للأمن السيبراني نخبة من المختصين في مجال الأمن السيبراني، في إطار توجه الحكومة العراقية نحو التوجه الرقمي، واحتضان المواهب البارزة في تجمع Arab Hack Team، مع التأكيد على ضرورة احتضان المواهب الفنية الشابة، مع تعزيز الوعي بالقوانين المحلية، والمضي نحو تطوير القدرات الفنية، مع مناقشة وتحديد خارطة التعاون بين فريق الاستجابة العراقي والمواهب المحلية، مع ضرورة انشاء منصة للتدريب وورش عمل لغرض تبادل المعلومات وتأهيل جيل عراقي جديد من خبراء الأمن السيبراني، بالاضافة الى برامج دعم خاص للنساء لتعزيز دورهن في هذا المجال الحيوي، ويمثل هذا التوجه خطوة، نحو بناء بيئة رقمية آمنة ومستدامة في العراق قادرة على مواجهة التحديات السيبرانية المتزايدة.

٥. تحديد الثغرات الامنية التي تأتي من كلمات المرور الضعيفة المكونة ان لا تقل عن (١٨ حرفاً)، وان تحتوي على أحرف كبيرة، واحرف صغيرة، وارقام، ورموز ويستغرق المهاجم هنا مدة (٧) كوادر ليون ستة لاختراقك، والـ (١) كوادر ليون يساوي مليون مليار سنة.

٦. مشاركة الفريق العراقي للأمن السيبراني في الحدث السنوي "Security Day 2024"، والذي اقيم في بغداد، وكان هذا الحدث انطلاقه حول تبادل وتعزيز الخبرات، ومعرفة أهم التقنيات والتحديات في مجال الأمن السيبراني، بالإضافة الى مناقشة مستقبل العراق في المجال الرقمي .

٧. تقدم العراقي بالتصنيف الدولي السيبراني، وحسب مؤشر (GCI) العالمي وهو مؤشر يصدر من الاتحاد الدولي للاتصالات (IIU)، مما يعكس ويترجم مدى تحسن الأداء والاستجابة السيبرانية، وتقدم فريق السيرت الى المستوى الرابع عالمياً.

٨. وبالإضافة الى ذلك فإن أحد اهم المجالات التي اضافها الأمن السيبراني الى الاقتصاد العالمي، هو طلب المتخصصين والكفاءات واصحاب الخبرات في وظائف حماية المعلومات والانظمة مثل[١]:

(محللي أمن المعلومات، مهندسي الشبكات الآمنة، مستشاري الأمن السيبراني، متخصصين الحماية من التهديدات المتقدمة) ،ومن المتوقع ان ينمو سوق الأمن السيبراني بمعدل نمو سنوي مركب يتراوح الى (١٠-١٥%) خلال السنوات القادمة

المبحث الثاني

الاتجاه المستقبلي في استراتيجية الأمن السيبراني العراقي

يعد الامن السيبراني العراقي، جزءاً اساسياً من بيئة الأمن الوطني العراقي، وبات أحد الركائز الاساسية في المنظومة للتقنية الأمنية، كما أن آليات مواجهة التحدي تقع على عاتق المنظومة الأمنية العراقية، وفق مكونات القوة، وطريقة توظيفها، وتوجه الدولة اليوم في ظل فضاء رقمي واسع هو كيفية رفع مستوى حماية أمن البيانات والمعلومات، مع توفير خدمات الدعم، والاستجابة لحوادث أمن المعلومات في المؤسسات الحكومية، فالرؤية المستقبلية لوضع العراق اليوم تتمحور حول اتجاهين، اما التركيز على عناصر القوة وتوظيفها، لمواجهة التحديات والاختراقات المتزايدة، أو عدم مواجهة التحديات، وما يصاحبهُ في تراجع القوة السيبرانية العراقية.

وعلى هذا الاساس يمكن تقسيم المبحث الى محورين وكما يلي:

اولاً:حالة الارتقاء بالقوة السيبرانية العراقية والقدرة على مواجهة التحديات

تعد حالة الارتقاء هو هدف استراتيجي في ظل المتغيرات التكنلوجية السريعة، ضمن بيئة التهديدات الرقمية، فإذا أردنا الارتقاء والوصول الى المستوى العالمي المرتفع، لابد من وضع استراتيجيات سيبرانية تنسجم مع السياسة الوطنية، مع تحديد الرؤية الاستراتيجية الواضحة، لتمكن العراق من ان يكون رائداً في مجال الأمن السيبراني على المستوى الاقليمي ثم العالمي خلال الـ (١٠) سنوات القادمة، والهدف الاساسي للارتقاء هو حماية السيادة الرقمية العراقية، مع بناء اقتصاد رقمي آمن.

فاذا أردنا الارتقاء باستراتيجية القوة في المن السيبراني، لابد ان تكون الاستراتيجية تمثل العلاقة المحسوبة بين الوسائل المتخذة والغايات والتي تحمل مميزات وهي:

١. تكون متوازنة ومتوافقة بين الوسائل والغايات، ولا تعتمد على الفرضيات الكثيرة.
٢. تكون اهدافها سياسية عسكرية اقتصادية قانونية واخلاقية.
٣. يجب ان تكون صالحة لأي موقف، لنجاح المهام والوصول الى الاهداف المراد تحقيقها.

والاستراتيجية بشكل عام، هي تخطيط مستقبلي، لكن يستند الى الحاضر، ويحتاج الى الماضي، في ابعاد الزمن الثلاثة، وذلك لأسباب عدة منها:

١. الاستراتيجية بحاجة الى الدوافع التاريخية، لتحقيق الاهداف، وتحفيز القدرات، وبناء نظام معرفي وقيمي.

٢. لا يمكن معرفة متغيرات الحاضر والمستقبل، دون الرجوع الى التاريخ، مع دراسة البيئة الداخلية والخارجية.

٣. لا ينجح التخطيط العلمي والمستقبلي دون معرفة المعطيات واهم التطورات.

فالتخطيط يعكس سلسلة الاجراءات، مع إمكانية تطوير البرامج الاساسية، وتوظيفها للمستقبل.

الخطة المقترحة للأمن السيبراني العراقي سبق وان صدرت استراتيجية الأمن السيبراني العراقي، من قبل أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، لفرض تهيئة الاستعداد الوطني، واتخاذ الاجراءات الاستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء العراقي، وحماية البنية التحتية للمعلومات والاتصالات حيث تتألف هذه الاستراتيجية من مراحل زمنية متعددة، مراحل قصيرة، ومتوسطة، وطويلة الأمد، لمعالجة المخاطر والتهديدات، ومواجهة التحديات التي يواجهها العراق في الفضاء السيبراني، والتي تؤثر على الارض الوطني العراقي، ومن هذهِ التهديدات هي:

(الارهاب الالكتروني،الجريمة الالكترونية،الصراع السياسي للتجسس السيبراني ،إساءة معاملة الأطفال واستغلالهم عبر الانترنيت)

وعند وضع استراتيجية للأمن السيبراني، لابد من ترتيب الاولويات، وتحديد القطاعات المستهدفة مثل القطاع الاقتصادي، والاجتماعي، والسياسي، لتحقيق الأهداف الشاملة للدولة، وتحديد الموارد المادية الخاصة بتنفيذ البرامج، لتحقيق النتائج المرجوة، في مدة زمنية محددة[١].

ولابد من تحديد الخطوات الاساسية، لمواجهة التحديات والارتقاء بالأمن السيبراني العراقي، من اهم الخطوات[٢]:

١. رفع الوعي الأمني عن طريق التدريب، ووسائل الاعلام خصوصاً للموظفين، والتركيز على تدريب العاملين في الأجهزة الامنية وخصوصاً العاملين بالأجهزة الأمنية فإن تدريب الملاكات يعد تنفيذ لاستراتيجية المواجهة الأمنية.

٢. اعتماد تقنيات الرقابة الالكترونية في الأنظمة المصرفية.

٣. انشاء منظومة الدفاع الرقمي الالكتروني ضد الاقتراحات الإضرابية.

٤. تعميم ثقافة الأمن السيبراني لدى عامة الشعب. والقيام بالحملات الوطنية لمحو امية المعلوماتية– الرقمية والقيام بالتعبئة والدعم للمواطنين لمواجهة جرائم الانترنيت.
٥. تشجيع الابحاث التخصصية والأكاديمية لبناء كوادر عالية الاحتراف في ميادين الأمن المعلوماتي الرقمي.
٦. بناء خلايا عالية للتخصص والاحتراف لمتابعة اخر مستجدات والتحديثات وتقديم التوصيات لصناع القرار الأمني.

واذا أردنا الوصول الى حالة الارتقاء في الأمن السيبراني لابد من تبني التطورات التكنلوجية الرقمية باتخاذ تدابير وقائية لمواجهة التحديات، ومكافحة القضايا السيبرانية، فمن الممكن الارتقاء عن طريق تأثير الأمن السيبراني التنظيمي، وتقيمه عن طريق إداء الموظفين، والامتثال لسياسات تنظيمية، ومدى التزام العاملين في المؤسسات تجاه قضايا الأمن السيبراني.

فالعراق اذا ارد الوصول الى حالات الارتقاء بالأمن السيبراني، عليه معالجة القوانين والتشريعات السيبرانية كخطوة اولى وبالغة الأهمية، كما دعت منظمة العفو الدولية الى سحب قانون جرائم المعلومات العراقي.

فالعراق يتقدم بالأمن السيبراني في المجال المصرفي، والعملاء على وعي بالبرامج والمعايير والأصول المعلوماتية بالجانب المصرفي، والتقييمات إيجابية، من ناحية السياسات والمعايير والامتثال لها.

ومن اكبر التحديات التي على العراق مواجهتها، هو التبني السريع للتكنلوجيا والتحول الرقمي، لكن التقييمات ايجابية نوعاً ما في هذا المجال، فبالاضافة الى التوجه نحو سياسة الامتثال وتعزيز المعايير، الا انه اذا اراد العراق الارتقاء لابد من تعزيز وعي الموظفين وسلوكهم تجاه الأمن السيبراني، مع تبني مفهوم الأمن السيبراني المؤسسي، والذي يركز على حماية الاصول الرقمية والمعلومات الحساسة للمؤسسات من التهديدات الرقمية، وتشير التقارير الى ان العراق يعزز هذا المجال، والاهتمام الزائد خاصة مع التبني السريع للتكنلوجيا الرقمية.

واذا اراد العراق الارتقاء بالأمن السيبراني في السنوات القادمة، لابد من اعتماد نظرية "النظام الديناميكي"*، لفهم التغيير في المؤسسات فيما يتعلق بالأمن السيبراني من متطور الأعمال وتكنلوجيا المعلومات.

والتوجه نحو بناء القدرات البشرية، عن طريق التدريب والتوعية، والالتزام بمعايير إجراءات الاستجابة للحوادث، وتطوير القدرات الحكومية، مع اتخاذ التدابير القانونية[١].

بالإضافة الى الشراكات بين القطاعين العام والخاص، مع رفع مستوى البحث والتطوير في هذا المجال.

ولحماية الأمن الوطني العراقي، لابد من الارتقاء بمستوى الأمن السيبراني، ومن اهم التحديات التي من الواجب علاجها، هي تطوير القدرات، حيث تشكل الأخطاء البشرية في المجال الرقمي، من اهم التحديثات التي تجعل الدولة معرضة للاختراق[٢].

فلابد من التوجه نحو الاستراتيجية الاستباقية، في الكشف عن التهديدات الرقمية

وأوصت كل الدراسات المستقبلة حول حالة العراق، باستكشاف دور الموظفين، وتدريبهم وتوعيتهم، مع تأثير الهيكل التنظيمي للمؤسسة، وكيفية ممارسة القيادة، فالأمن السيبراني المؤسسي ذا أهمية بالغة في العراق، وحيث انهُ يتأثر بعوامل بشرية، وتنظيمية، وتقنية، وعلى الرغم من التحسن المتوسط، الا ان هناك لايزال مجال للتحسين، ورفع مستوى الوعي، ومن الممكن تبني استراتيجيات شاملة، قائمة على تعزيز التعاون، وبتبادل الخبرات والمعلومات، لمواجهة التهديدات السيبرانية المتزايدة فبات الأمن السيبراني المؤسسي ركيزة اساسية لنجاح الاستراتيجية السيبرانية العراقية، ومن خلال اتباع الخطوات التالية:

١. تحليل دور الأمن السيبراني المؤسسي في أماكن العمل الرقمية في العراق.
٢. عينة الدراسة تتكون من أماكن العمل الرقمية في العراق التي تتبع العديد من ممارسات الأمن.
٣. جمع بيانات الموظفين في أماكن العمل الرقمية في العراق.

كما اذا أراد العراق التوجه نحو التقدم في مجال الأمن السيبراني عليه التوجه نحو بناء القدرات الأمنية، فالقدرات الأمنية عنصراً حاسماً تعمل على تمكين الدول والأفراد من الدفاع عن انفسهم في الفضاء الرقمي، والتصدي للجرائم الالكترونية وتكون هذه العمليات على مستويات مختلفة وجوانب عدة.

١- على المستوى الوطني

٢- على مستوى المؤسسات.

٣- على مستوى الأفراد.

وفي ضوء ذلك إذا اراد العراق التقدم فعليه اتباع سياسة استباق التهديدات، من خلال التحليل والمراقبة المستمرة، والبقاء في صدارة المهاجمين من خلال توقع خطوات المهاجمين، فالدولة التي تريد ان تتقدم لا يمكنها الانتظار حين يقع الهجوم، لابد ان تكون متقدمة بخطوة، فلابد من التفكير وتوقع بما يفعله الخصم، وعلى ماذا ينوي؟ مع الاستعداد لكل الاحتمالات، وهنا ستكمن القدرة على أستباق التهديد، والذي سيسمح ان تكون القدرة على اتخاذ إجراءات أستباقية يمكن ان تنجح في منع وقوع الهجوم، وهو شيء لا يمكن ان يتم أتخاذهُ او فعلهُ مرة واحدة، بل حالة مستمرة ضرورية فعالة للوصول الى حالة الأمن السيبراني، ويتم تنفيذ "استراتيجية دفاع أستباقية" للبقاء في صدارة التهديدات السيبرانية، حيث تبنى على عقلية استباقية، تفكر ما يمكن القيام به، لتعزيز الدفاعات قبل وقوع الهجوم، وقائمة على الاستفادة من دمج التقنيات الحديثة مثل الذكاء الاصطناعي، والتعليم الآلي، فالاستراتيجية الاستباقية تتطلب من الدولة ان تكون في حالة تأهب في جميع الاوقات، والبحث المستمر عن طرق لتحسين الوضع الآمني.

خلاصة القول ان الارتقاء بالقوة السيبرانية في العراق، ومواجهة التحديات، بات من الأمور الحيوية اللازمة، في ظل تحولات رقمية متسارعة، العراق مازال في طور بناء بنية تحتية رقمية متكاملة، لكنها قادرة على دعم وتعزيز الأمن السيبراني، بجهود متفرقة، ودعم فريق الاستجابة، والجهات الأمنية المسؤولة، ولنجاح استراتيجية الارتقاء لابد من التعاون ورفع الوعي، وتنسيق الجهود الوطنية ضمن اطار أكثر شمولية، مدرك لحجم المخاطر الرقمية.

ثانياً :حالة ضآلة الأداء السيبراني وتراجع القدرة على مواجهة التحديات

شكل الاندماج في الفضاء الرقمي خطراً كبيراً على الدول بشكل عام، ويعاني المشهد السيبراني في العراق من تحديات معقدة، تتراوح بين التأثيرات الاقتصادية، والأمنية، والتقنية، والاجتماعية، ومن أهم التحديات التي تؤدي الى تراجع القدرة هي ضعف الوعي السيبراني، فالتعليم التكنلوجي في العراق محدوداً، وهنالك صعوبات تواجه العراق في بناء مشهد سيبراني قوي، وهنالك نقاط ضعف في البنية التحتية الرقمية، والمعاملات الرقمية، كما ان سابقاً لم يكن لدى الحكومة إستراتيجيات واضحة نطاقها، ولابد من أستثمار استراتيجي قادر على تطوير المهارات الرقمية، ويشكل نقص الوعي على إتاحة الثغرات، التي تمكن المهاجمون من اختراقها.

ويمكن إدراج المعوقات التي تواجه الأمن السيبراني الوطني العراقي والتي اذا لم تعالج من الممكن يتراجع المشهد السيبراني العراقي وكما يلي:

١- **الافتراضات assumptions:** تعتمد اغلب المؤسسات اليوم في الدفاع الرقمي بالعراق على الافتراضات، والمزودة من قسم تكنلوجيا المعلومات، أو مستشاري الأمن السيبراني، وغالباً ما تكون هذهِ الافتراضات مضللة، او لتحقيق هدف معين.

٢- **الفجوة الرقمية:** وهو التفاوت الرقمي بين الدول .

٣- **مفهوم عمل المؤسسة والمخاطر والتهديد .**

٤- **إدارة البيئة السيبرانية:** لابد من ان تكون الأدارة تحت اكثر من دولة، للتقليل من الهيمنة، ولحصول الارتقاء السيبراني، لابد من وقف السيطرة والتحكم في مقدرات الشعوب المعلوماتية والاتصالات، والقطاع العسكري والأمني والثقافي، لذا تتطلع الدول الى جعل شبكة الانترنت تحت إشراف الأمم المتحدة، من خلال هيأة دولية، لفرض المراقبة على شبكة الانترنت وإدارتها، وهو الذي أكدت عليه (القمة العالمية الثانية المعلومات التي عقدت في تونس عام ٢٠٠٥م).

ولابد للعراق ايضاً وقف استيراد التكنلوجيا واذا ظل الاعتماد على التكنلوجيا المستوردة سيتراجع المشهد السيبراني العراقي.

كما اذا أراد العراق ان يرتقي بالمشهد السيبراني المستقبلي، فلابد من توثيق الاستراتيجية، فالتوثيق يلعب الدور الحاسم، الذي يضمن الكفاءة، والتوحيد بين العمليات،

ومن التحديات التي تعيق التقدم بالمشهد السيبراني لأي دولة، هو أن نطاق التكنلوجيا والمعلومات والاتصالات، أسع وبات خارج نطاق الفضاء الحكومي الرسمي، كما أن معظم القدرات التي وفرتها التكنلوجيا والمتوفرة حالياً هي تجارية، وبعضها غير قانوني وقد تصل بعض البرامج مثل (Sky Grabber) الروسي، بتكلفة (٢٦) دولار فقط، والقادر على التقاط مقاطع الفيديو والصور، كما تعد استخبارات الاشارات أحدى أهم التهديدات المستقبلية التي تواجه العراق، والتحدي الأكبر للمشهد الأمني السيبراني العراقي.

وأدت تكنلوجيا المعلومات والاتصالات الى إتجاه الفراد بنقل ولائهم الوطني الى الولاء لقضايا اخرى، خاصة الجماعات الارهابية التي تكيف نفسها مع المتغيرات في وسائل التواصل الاجتماعي، وطريقة إرسال المعلومات، عن طريق التكنلوجيا المتاحة، والتي تفوق في قدرتها قدرة الحكومات من ناحية التأثير على الرأي العام والمواطنين[١]، كما توجد معايير للارتقاء بالمشهد المستقبلي بالأمن السيبراني والتي هي

صادرة في عام ٢٠١٨، من منظمة المعايير الدولية، حيث توفر هذه المعايير إطار الأمن السيبراني ويركز على الوظائف التالية:

١. التجديد ويشمل (إدارة الاصول، بيئة الاعمال، الحوكمة، تقييم المخاطر، استراتيجية تقييم المخاطر، إدارة المخاطر).
٢. الحماية ويشمل (التوعية والتدريب، الوقاية، الصيانة، التغذية، إجراءات وعمليات حماية المعلومات، التحكم في الوصول).
٣. الكشف ويشمل (المراقبة الامنية المستمرة، عمليات الكشف).
٤. الاستجابة وتشمل (التحليل، التخفيف، الاتصالات).
٥. الاسترداد ويشمل (التحسينات، وتخطيط الاسترداد).

والعراق بحاجة الى الارتقاء في المشهد السيبراني المستقبلي، وبحاجة الى تطبيق المعايير الدولية، للنهوض بواقع الأمن السيبراني، واستحداث معاهد وطنية لوضع معايير الأمن السيبراني العراقي، مع تطبيق المعايير الدولية في استراتيجية الأمن السيبراني العالمي والتعاون مع المنظمات الدولية، لاسيما وان التحديات تتزايد كلما تقدمنا بالتكنلوجيا، واتجهنا نحو التحول الرقمي، لاسيما التهديدات تطال كل القطاعات، واهمها الانتخابات إذا كان التصويت الكتروني.

وبات وجود استراتيجية فعالة مطبقة بشكل صحيح، وتطبق عن طريق هيئة وطنية معنية بالأمن السيبراني، حيث أصبح الأمن السيبراني بشكل جزءاً اساسياً من أية سياسة وطنية أمنية للدولة، وصناع القرار اليوم يصنفون مسائل الحماية والدفاع السيبراني أولوية في سياسات الدفاع الوطني، ولاسيما بعد ان اعلنت اكثر من (١٣٠) دولة حول العالم عن تأسيس أقساماً خاصة بدراسة ووضع استقراءات وسيناريوهات مستقبلية خاصة بالحروب السيبرانية، وضمنت داخل فرق الأمن الوطنية، وباتت تضاف هذهِ الاجراءات الى الجهود الأمنية التقليدية، لمحاربة الجرائم الالكترونية، والاحتيال الالكتروني، والأوجه الأخرى للمخاطر السيبرانية.

وفي ظل التسارع الرقمي، اصبح الأمن السيبراني أحد الأعمدة الاساسية لحماية البيانات، والبنى التحتية الرقمية، فسيناريو التراجع يمكن ان يكون ناتج من، النقص في الكوادر الفنية المتخصصة، وغياب السياسات الوطنية الماطرة بإطار تنظيمي واضح داخل المؤسسات، فغالباً السياسات غير محدثة، والاعتماد على الانظمة التكنلوجية القديمة الغير محدثة، بالتالي غير قادرة على صد الهجوم، فالسياسة والاستراتيجية

لابد ان تكون محدثة مدعومة، مصحوبة بآليات تنفيذ فعالة، والقضاء على حالة التراجع من ناحية التنسيق بين المؤسسات عند وقوع الازمات.

الخاتمة :

يُعد الأمن السيبراني اليوم أحد المقومات الأساسية للحفاظ على استقرار الدول وحماية مؤسساتها الحيوية، ولا يختلف الوضع في العراق عن بقية دول العالم، بل تزداد فيه الحاجة إلى بناء قدرات سيبرانية متينة نتيجة التحديات الأمنية والتكنولوجية التي يواجهها. وقد أظهرت الدراسة أن الأداء السيبراني العراقي لا يزال في طور التشكّل، ويعاني من مشكلات جوهرية تتعلق بضعف البنية التحتية، وقلة الكفاءات المتخصصة، وغياب تشريعات ناظمة، فضلاً عن عدم وجود استراتيجية وطنية واضحة وشاملة للأمن السيبراني.

إن تحسين الأداء السيبراني في العراق يتطلب إرادة سياسية جادة، واستثمارات حقيقية في مجالات التعليم والتدريب وبناء القدرات، إلى جانب تطوير الأطر القانونية والتنظيمية، وتعزيز التعاون الإقليمي والدولي. ومن دون هذه الخطوات، سيظل العراق عرضة للتهديدات السيبرانية المتزايدة، مما قد يؤثر سلباً على أمنه القومي وتقدّمه الرقمي في المستقبل.

لذلك، فإن النهوض بالأمن السيبراني في العراق يجب أن يكون جزءاً أساسياً من استراتيجية الدولة الشاملة للتحول الرقمي، بما يضمن حماية المصالح الوطنية في الفضاء الإلكتروني، وتحقيق السيادة الرقمية.

الاستنتاجات :

١. الاعتماد الكبير على التكنلوجيا المستوردة مما يزيد من احتمالية وجود الثغرات، التي تعرض البرامج للاختراق.
٢. وجود توجه حكومي حقيقي للتحول الرقمي، وتحسن واقع الأمن السيبراني، وبالتعاون مع الجهات الامنية المتخصصة، لوضع استراتيجيات لحماية الفضاء الرقمي.

زيادة الوعي والتدريب نحو تعزيز وبناء القدرات خصوصاً بالجانب الاكاديمي والجامعات، وجدية الجامعات في إقامة الورش، ودورات التوعية، نحو بناء جيل قادر مع تحديات الفضاء الرقمي.

المصادر بالعربية والإنكليزية :

١- الاتحاد الدولي للاتصالات (IIU) على الرابط: https://www.itu.int تاريخ الزيارة ٢٠٢٥/٣/٣
٢- بلا، ما هو المؤشر العالمي للامن السيبراني؟ بحث منشور، المركز الوطني للأمن السيبراني National Cyber Secirity Center، المملكة الهاشمية الاردنية، ٢٠١٩، متاح على الرابط: https://www.safeonlin.jo/AR/ تاريخ الزيارة: ٢٠٢٥/٣/٣.

٣- الاردن في مؤشر الأمن السيبراني العالمي (GCI)، ورقة حقائق، المنتدى الاقتصادي الاردني، المملكة الهاشمية الاردنية، ٢٠٢٢، ص٤.
٤- مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، المجلد٢، العدد٢٠، ٢٠٢٠، العراق، ص٥٦-٥٨.
٥- يخة حسن الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، كلية القانون: جامعة الشارقة، المجلد ١٧، العدد١، ٢٠١٩، الامارات العربية المتحدة، ص٧٤٠-٧٤١.
٦- حازم حمد موسى الجنابي، الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، "مقارنة بين المعضلة الأمنية والمكتبة الأدائية"، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد ٥٧، العدد٥، الجزائر، تاريخ النشر: ٢٠٢٠/١٢/١٧، ص٥٦١.
٧- بلا، تحديث المؤشر الوطني للأمن السيبراني (NSCI)، تقرير منشور، إدارة الدفاع الوطني، المديرية العامة لأمن ونظم المعلومات، تاريخ النشر: ٢٠٢٣/١٢/٢٩، المملكة المغربية، متاح على الرابط: https://www.dgssi.gov.ma/ar تاريخ الزيارة: ٢٠٢٥/٣/٤.
٨- صلاح مهدي هادي الشمري، زيد محمد علي، الأمن السيبراني كمرتكز حديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية – جامعة النهرين، العدد ٦٢، ٢٠٢٠، العراق، ص٢٨٣.
٩- باسم علي خريسان، الأمن السيبراني في العراق: قراءة في مؤشر الأمن السيبراني العالمي لعام ٢٠٢٠، مركز البيان للدراسات والتخطيط، العراق، ٢٠٢١، ص١٠
١٠- بعثة الاتحاد الاوروبي الاستشارية في العراق، تقرير صادر من بعثة الاتحاد الاوروبي والعراق، تاريخ النشر: ٢٠٢١/١١/١٨، متاح على الرابط: http://www.eeas.europa.eu/iraq/ تاريخ الزيارة ٢٠٢٥/٣/٥.
١١- ما هي الهندسة الاجتماعية، توعية سيبرانية، الفريق العراقي للاستجابة للحوادث السيبرانية IQCERT، تاريخ النشر ٢٠٢٤/٤/٣، متاح على الرابط: Tem/Cert-gov-iq الزيارة: ٢٠٢٥/٤/٤.
١٢- ما هو التصيد الاحتيالي؟ الفريق العراقي للأمن السيبراني، تاريخ النشر: ٢٠٢٤/٤/٤، متاح على الرابط: https://facebook.com/Cert.gov.iq تاريخ الزيارة: ٢٠٢٥/٤/٤.
١٣- بيان، الفريق العراقي للأمن السيبراني IQ.CERT، تاريخ النشر: ٢٠٢٤/٥/١٨، متاح على الرابط: Tem/Cert-gov-iq تاريخ الزيارة: ٢٠٢٥/٤/٤.
١٤- اجتماع جمع نخبة من تجمع Arab Hack Team والخريف العراقي للأمن السيبراني، تاريخ الاجتماع، ٢٠٢٤/٥/٢٤، الفريق العراقي للأمن السيبراني، متاح على الرابط: Tem/cert-gov-iq تاريخ الزيارة: ٢٠٢٥/٤/٤.
١٥- كم هو الوقت المستغرق لاختراقك؟، الفريق العراقي للأمن السيبراني IQ.CERT ، تاريخ النشر: ٢٠٢٤/٦/٧، متاح على الرابط: https://facebook.com/cert.gov.iq تاريخ الزيارة: ٢٠٢٥/٤/٤
١٦- ورشة عمل، الامن السيبراني في التحديات وعصر التكنلوجيا، رئاسة الوزراء: المجلس الأعلى للشباب ومستشارية الامن القومي فريق الاستجابة للحوادث السيبرانية، كلية المأمون الجامعة، ٢٠٢٥/٣/١٧
١٧- تيري، ديبل، استراتيجية الشؤون الخارجية، منطق الحكم الامريكي، ترجمة وليد شحاذة، دار الكتاب العربي، العراق، ٢٠٠٩، ص٧١٨-٧١٩.
١٨- نجاح محمود، التاريخ والاستراتيجية والعقل العربي، مجلة الفكر السياسي، العدد (١٦)، دمشق، اتحاد الكتاب العرب، سوريا، ٢٠٢٢، ص٣.
١٩- بوب جارات وآخرون، كيف نفكر استراتيجية: فن إعادة اكتشاف المسارات والاتجاهات الصحيحة، ترجمة: عبد الرحمن توفيق، مركز الخبرات المهنية، مصر، ١٩٩٨، ص٧٢-٧٣.
٢٠- علي ابراهيم المعموري، الأمن السيبراني واثره على الأمن الوطني بعد ٢٠٠٥، رسالة ماجستير (غير منشورة)، جامعة بغداد، كلية العلوم السياسية، العراق، ٢٠١٩، ص١٥٠-١٥٣.
٢١- نظرية النظام الديناميكي، بحث منشور، ٢٠١٥، متاح على الرابط: https://www.sciencedirect.com تاريخ الزيارة: ٢٠٢٥/٤/١٨.
٢٢- ** الاتمتة في كشف التهديدات الرقمية: (Threat Detection Automation in Cyber): اي استخدام الانظمة الذكية والبرمجيات لتحليل البيانات الرقمية والمراقبة بشكل تلقائي دون تدخل بشري، واكتشاف البرامج الخبيثة

والهجمات الالكترونية باسرع وقت ممكن. للمزيد انظر: Cuide to cyber Threat information sharing, October 2016, Nist, on link: https://www.nist.gov تاريخ الزيارة: ٢٠٢٥/٤/١٨.
٢٣- حسن هادي لذيذ، اساسيات استراتيجية الأمن السيبراني القوية، مكتبة نور، ٢٠٢٢، العراق، متاح على الرابط: https://noor-book.com تاريخ الزيارة: ٢٠٢٥/٤/٢٧، ص٣.
٢٤- مجموعة مؤلفين، استخبارات الاشارة للجميع، مؤسسة رافد، الولايات المتحدة الامريكية، ٢٠١٧، ص٥.
٢٥- شادي عبد الوهاب، حروب الجيل الخامس: التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم، دراسات المستقبل، مركز المستقبل للابحاث والدراسات المتقدمة، الامارات العربية المتحدة، ٢٠١٧، ص١٤-١٥.
٢٦- الشبكة الدولية للانترنت، لمحة حول على الأمن السيبراني، متاح على الرابط: http://www.tra.gov.Ib/Cybersecurity-in-few-words-AR . تاريخ الزيارة: ٢٠٢٥/٤/٢٧.
27- Nazem etal, Cyber Security Determinates in iraq's Digital work Place: Attitude, Policy and Compliance Roles International Journal of Cyber Criminology (Diamond open Access Journal), Vol 17 Issue 2 July – December 2023, Iraq, D.3.
28- Amnesty International (2019), International Journal of Research in Business and Social Science, 9, 23, London, 2019, P. 88.
29- (1) M. Fareed Mahdi, Shared Cyber Security Responsibilities in the Banking Sector: A case study of the Republic of Iraq, university of Thi-Qar, 1/12/2024, Iraq, p130.
30- T. Lee A Comprehensive analysis of challenges and strategies in enhancing Cyber security for The defense industry, school of Helms, Liberty University, doctor of philosophy, 2024, USA, p.130.
31- Information technology – security techniques – Cyber security and IEC standards, first edition, 2018 on link: www.sis.se/sed-80001536
32- http://www.itu.int/en/ITU-D/CyberSecurity/pages/global-CyberSecurity-index-asex. تاريخ الزيارة: ٢٠٢٠/٤/٢٧
33- -١Cyber security spending for critical Infrastructure to surpass us $105 Billion in 2021, 10Feb 2021, research, on link: https://www.abiresearch.com/press/Cybersecurity
34- M. Radif, Internal and External Factors to Adopt a Cyber Security strategy in Iraqi organizations, university of Al-qadsiyal, webology, volume19, Number1, January, 2022, Iraq, p.p. 7-8.