استراتيجية الامن السيبراني العراقي

م.د ايناس مجبل دليان
جامعة بغداد / مركز الدراسات الأستراتيجية والدولية

Iraqi Cyber Security Strategy

Dr. Enas Majbel Dalian
University of Baghdad/Center for Strategic and International Studies

المستخلص : تسارع استخدام التكنولوجية الرقمية في ادارة مختلف مرافق الحياة، العامة والخاصة، واصبحت الكثير من مؤسسات الدولة، وحتى المصالح الفردية، يتم ادارتها: الكترونيا. وتلك المصالح اخذت تدرك ان التطورات التكنولوجية والوقائع القائمة تتطلب ذلك والاستفادة من الفرص الكثيرة التي يتيحها التحول نحو الادارة الالكترونية.

ان التطور التكنولوجي، لم يكن ذو شق ايجابي فقط، انما ظهر هناك: شق سلبي، يرتبط بهجمات التي يمكن ان تتعرض لها تلك المصالح، يستخدمها افراد أو منظمات اجرامية، أو حتى مؤسسات استخبارية، معادية، تهدف إلى الاضرار بالمصالح المستهدفة. وهو ما يرتبط، بادارة الصراع الحديث، وتحويله إلى: حرب سيبرانية. ولهذا، اخذت تلك المصالح، سواء كانت افراد أو مؤسسات أو دول، تعمل على تفعيل ما يعرف بالامن السيبراني، باعتباره الاداة التي تقابل التطورات التكنولوجية السيبرانية .

ان موضوع الامن السيبراني هو: من الموضوعات التي تشغل اهتمامات العديد من دول العالم، نظرا لمخاطر استخدام الهجمات السيبرانية، لتخريب المواقع، أو سرقة البيانات، ومن ثم تعطيل المصالح العامة، أو الخاصة. ولهذا، اتجهت اغلب الدول، ومنها: العراق، إلى وضع استراتيجية متخصصة، لحماية البيانات، والتعامل مع الهجمات السيبرانية، والجرائم السيبرانية.

في هذا البحث، تم التعامل مع اشكالية، وهي: ان هناك اهمية لانشطة كبح التهديدات، والجرائم، السيبرانية، والتي تمثل: تهديد لامن الدولة. وهو ما يطرح اشكالية مضمونها: كيف تعامل العراق مع التهديدات والتحديات السيبرانية؟

ان البحث تعامل مع الموضوع، من خلال دراسة موقع العراق في مؤشر الامن السيبراني العالمي،والتحديات التي تواجه البلد، ودراسة: مقومات استراتيجية الامن الوطني السيبراني.

الكلمات المفتاحية: العراق، السيبرانية، التهديدات، استراتيجية، الامن الوطني، التعاون الدولي، مؤشر الامن السيبراني.

Abstract: The use of digital technology has accelerated in the management of various aspects of life, both public and private. Many state institutions, and even individual businesses, are now managed electronically. These businesses have begun to realize that technological developments and existing realities require this and to take advantage of the numerous opportunities offered by the shift to e-governance.

Technological development has not only had a positive aspect; rather, there has also been a negative aspect related to attacks that these businesses may be subjected to, used by individuals, criminal organizations, or even hostile intelligence agencies, aiming to harm the targeted interests. This is linked to the management of modern conflict, transforming it into a cyberwar. Therefore, these businesses, whether individuals, institutions, or countries, have begun to implement what is known as cybersecurity as a tool to counter cybertechnological developments.

The topic of cybersecurity is a topic of concern to many countries around the world, given the risks of using cyberattacks to sabotage websites, steal data, and thus disrupt public or private interests. Therefore, most countries, including Iraq, have developed a specialized strategy to protect data and address cyberattacks and cybercrimes.

This research addresses the importance of activities to combat cyber threats and crimes, which represent a threat to state security. This raises the question: How has Iraq dealt with cyber threats and challenges?

The research addressed this issue by examining Iraq's position in the Global Cybersecurity Index, the challenges facing the country, and the components of a national cybersecurity strategy.

Keywords: Iraq, cyber, threats, strategy, national security, international cooperation, cybersecurity index.

المقدمة

يعد موضوع الامن السيبراني من بين الموضوعات الحديثة، التي يتزايد اهتمام الدول بها لاعتبارات متعددة، وذلك لان العالم الحديث والمستقبلي انما يعتمد على ربط وتسيير اعمال مؤسساته على المنظومات الشبكية والرقمية، وتلك الشبكات والمنظومات: بيانات، أو ادارة منشات ومرافق، أو اموال،.. لا يمكن تركها من دون حماية، في ظل التوجهات العالمية، لاجهزة الاستخبارات، لادارة الصراعات عبر مجموعات متخصصة بالحروب السيبرانية، وفي مجموعات الهكر، وكلها تهدف اما إلى تخريب البيانات أو سرقة محتوياتها، وغيرها مما يضر بالمرافق العامة، ومن ثم يضر بالثقة بالاجرات الحكومية، ويضر من ثم بالامن الوطني للدولة.

طور الاتحاد الدولي للاتصالات التابع للأمم المتحدة ما عرف باسم: المؤشر العالمي للامن السيبراني، عام 2005، ويضع فيه اهم مرتكزات الامن السيبراني الواجب اتباعها، والاجراءات الواجب اعتمادها، ومن ثم يقيس موقع الدول على المؤشر، وهو ما يعد خطوة متقدمة للدفع بالتنافس بين الدول في هذا الموضوع المهم والذي اخذ يؤثر على حياة عدد ليس بالقليل من الدول والمؤسسات وحتى الافراد، نتيجة الاستهداف وغياب أو ضعف اجراءات الحماية.

العراق من بين الدول التي اخذت تهتم بموضوع السيبرانية والامن السيبراني، فوضع استراتيجية متخصصة بالامن السيبراني تهتم بعدة نقاط وهي: الرؤية للامن السيبراني، والاستعدادات الواجب اتخاذها، والاطار التشريعي لتجريم الجرائم السيبرانية، وتعزيز القدرات السيبرانية، وكيفية التعاون في الاطار الدولي، وذلك بقصد تقليل فرص التعرض للهجمات السيبرانية.

مع ذلك، ان مستوى التهديدات السيبرانية في العراق ومعه كل دول العالم مرتفع، خصوصا مع وجود شبكات محترفة سواء من افراد أو مدعومة بطرق شتى من اجهزة مخابرات، تحاول اختراق الأنظمة والأجهزة والتطبيقات والبيانات، في الدول والمؤسسات والافراد المستهدفة، وهو ما استدعى تطوير استراتيجيات للامن السيبراني لحماية الشبكات من اي تهديدات أو اختراقات.

اهمية البحث: ان البحث في موضوع الامن السيبراني، مثله مثل البحث في موضوع الامن الوطني للدولة، فالمصالح اخذت تنتقل بسرعة من كونها مادية إلى كونها سيبرانية، واعمال المؤسسات التي كانت تدار ماديا اصبحت تدار عبر الشبكات، ويمكن من خلال التعرض للشبكات احداث اضرار كبير بالمؤسسات، طالما ان الجزء الاكبر من عمل المؤسسات التابعة للدولة أو للافراد أو حتى مصالح الافراد، وحماية تلك المصالح يوازي حماية المصالح المادية، بل ربما ان التعرض لمؤسسة ما ان يعرض المصالح الحيوية للدولة للخطر ان كانت تحوي اسرار عسكرية أو امنية، ولهذا تلجأ العديد من الدول إلى: وضع مبادئ وقواعد لحماية الامن السيبراني، واستراتيجيات للتصدي لاي مخاطر، يمكن ان تحدث وفقا لقواعد منظمة للاجراءات الحكومية، باعتباره تهديد للامن الوطني للدولة.

اهداف البحث: من البحث في هذا الموضوع يرتبط بدراسة الامن السيبراني وتوضيح اهميته، وتقديم تعريف له، إلى جانب دراسة موقع العراق في مؤشر الامن السيبراني العالمي، والتحديات التي تواجه البلد، والعمل على تحديد عناصر ومقومات استراتيجية الامن الوطني السيبراني المتبعة في العراق، وبضمنه دراسة كيفية ادارة البيانات وتامينها والحصول على الدعم والتعاون الدولي، وغيره من المضوعات التي ارتبطت بدراسة هذا الموضوع.

الاشكالية وتساؤلات البحث: ان الاهمية التي تنطوي عليها، انشطة كبح التهديدات، والجرائم، السيبرانية، التي تمثل: تهديد لامن الدولة، انما يطرح اشكالية مضمونها: كيف تعامل العراق مع التهديدات والتحديات السيبرانية؟

تطرح هذه الاشكالية، عدة تساؤلات، فرعية، سيتم الاجابة عنها في متن البحث وهي:

ما هو تعريف الامن السيبراني ؟ وما واهميته؟

ما موقع العراق في مؤشر الامن السيبراني العالمي؟ وما هي التحديات التي تواجه العراق سيبرانيا؟ ما هي عناصر ومقومات استراتيجية الامن الوطني السيبراني العراقية؟

الفرضية: نفترض هنا، انه كلما ازدادت التحديات والتهديدات السيبرانية، وكلما تطور العالم سيبرانيا، كلما كانت هناك حاجة عراقيا إلى تطوير استراتيجية توضح: التحديات والتهديدات، وما يتطلبه العراق تشريعيا، والاجراءات الحكومية التي يتوجب اتباعها للتعامل مع تلك التهديدات والتحديات.

المنهجية: يعتمد البحث على المنهج التحليلي النظمي، لدراسة ما يرتبط باستراتيجية الامن الوطني السيبرانية للعراق، وتحليل المشكلة البحثية المعتمدة.

الهيكلية: تم تقسيم البحث إلى ثلاثة مباحث فلا عن المقدمة والخاتمة وكالاتي:

المبحث الاول: تعريف الامن السيبراني واهميته .

البمحث الثاني: موقع العراق في مؤشر الامن السيبراني العالمي والتحديات التي تواجهه .

المبحث الثالث: عناصر ومقومات استراتيجية الامن الوطني السيبراني: ادارة البيانات وتامينها والحصول على الدعم والتعاون الدولي .

المبحث الاول: تعريف الامن السيبراني واهميته

ان تعريف الامن السيبراني (Cybersecurity) يبدء من تعريف الامن، وواجبات الدولة، والتطور التكنولوجي وكيف انتهى إلى تطوير وظائف الدولة، واسهم بتغيير مجرى الحياة بالكثير من جوانبها.

لقد اخذت الدول تتطور عبر عدة قرون، لتاخذ وظائف كونها المسؤولة عبر السلطات والمؤسسات داخلها عن التمثيل للمجتمع، وحفظ الحقوق وتعزيز الرفاهية للافراد داخلها، والاهم القدرة على حماية الامن للمصالح الموجودة على ارضها والتي تفرض الدولة سيادتها عليها. وللدولة القدرة على توظيف الموارد المختلفة حتى تصل إلى الاهداف التي تريدها، بشرط ان يكون هناك فصل بين المصالح العامة للدولة ومصالح الحكام، والتي ان تصاعدت لتغلب مصالح الدولة تتجه الاخيرة إلى تصاعد مؤشرات ضعف الاستقرار فيها.

وطورت الدول استراتيجيات للامن الوطني فيها لحماية مصالح الدولة والجماعات داخلها، سواء ما ارتبط منها بالسيدة والامن والاستقرار والرفاهية، وحفظ الحقوق، فالدول تدرك ان عليها مسؤوليات كبيرة مقابل ان تفرض حضورها وواجباتها على المجموعات الداخلية، وعليها التزامات لتكون قادرة على التمثيل الخارجي للمجموعات داخلها[1].

لقد اخذت متغيرات عديدة ومنها التكنولوجيا تدخل إلى مختلف اوجه الحياة لتعيد تقديمها، اجتماعيا واقتصاديا وسياسيا وامنيا، اي حدثت بيئة جديدة، وفرضت انماط من التفاعلات جديدة، ومن ثم اجبرت الدول على اعتماد معايير واجراءات جديدة للتفاعل، بما يتناسب وما اصبحت التكنولوجيا تفرضه في مختلف اوجه الحياة.

لقد كان الامن إلى مرحلة قليلة مضت يعبر عن الاجراءات التي تعتمد للوصول إلى مرحلة الشعور بالاستقرار، وان المصالح محفوظة، من قبل الدولة وقائيا، وان الاخيرة ستتخذ الاجراءات المناسبة لردع اي اختراق للاجراءات وتعريض المصالح للضرر. تلك المفاهيم اخذت تتغير، خاصة بعد ان اصبح جزء من اتفاعلات وجزء من مصالح الدولة سيبرانيا. بعبارة اخرى، استطاع البعض تطوير بنية لادارة البيانات وحفظها الكترونيا، والتوصل إلى قدرة لان تدار المؤسسات الكترونيا من دون الحاجة للحضور المادي، وطالما ان الاصل ان المؤسسة هي موجودة الا ان بياناتها تحولت من ورقية إلى الكترونية، وان اموالها تحولت من ورقية إلى الكترونية، وان ادارتها تحولت من حضورية إلى الكترونية، فان التعرض لقدرة المؤسسة على ان تعمل أو سرقة بياناتها أو اتلافها أو سرقة اموالها أو تعطيل قدرتها على العمل، سواء كانت مؤسسة عامة أو خاصة انما يفيد بان الامن الوطني تعرض للضرر. ويستوجب ان تكون االدولة حاضرة لمعرفة من قام بهذا، وكيف، وقبلها ان تقوم الدولة بالاعمال الوقائية لتامين المصالح العامة والخاصة والفردية، وتوفر مظلة اجراءات للردع وللتعقب والمسائلة ان حدث شيء يضر بالمصالح المحمية بموجب القانون

[1] - حسن الحاج علي أحمد واخرون، الأمن القومي العربي وتحديات الأمن الإقليمي، الدوحة، المركز العربي للأبحاث ودراسة السياسات، 2023، ص32-33.

سواء كانت مصالح مادية مباشرة أو مصالح سيبرانية طالما ان الاصل انها مصالح تتبع الدولة ومؤسساتها ومؤسسات تتمتع بحماية الدولة أو مصالح افراد يتبعون الدولة وتوفر لهم حمايتها[1]

ان المعنى السابق يفيد ان الامن هو واحد بفكرته، الا ان ادواته تتغير، ومن ثم لا يمكن عزل الامن الوطني بمفهومه الاعتيادي عن الامن بمفهومه السيبراني، لانه في الحالتين يقصد به تتبع الدولة لاجراءات وقائية لحماية مصالح محمية بموجب القانون، والاتجاه إلى اجراءات الردع والعقاب عند نجاح التعرض لتلك المصالح والتسبب بضرر فيها ولمن يتعامل معها.

ان الامن السيبراني (Cybersecurity) انما يقصد به بحسب البعض: امن الشبكات وامن المعلومات، وجعل الفضاء السيبراني آمن للتعاملات المحمية من قبل الدولة[2].

ويذهب البعض للقول انما يقصد بالامن السيبراني بانه: " حزمة الاجراءات التي تتووخى تامين وحماية الشبكات واجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به، ومن التعطيل أو العرقلة في الخدمات التي تقدمها بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، هو: مجموعة من المهام مثل: تجميع وسائل وسياسات واجراءات امنية ومبادئ توجيهية ومقاربات لادارة المخاطر وتدريبات وممارسات فضلى، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين، يمكن تعريف الامن السيبراني انطلاقا من اهدافه بانه: النشاط الذي يؤمن حماية الموارد البشرية وتلمالية للدولة، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي ترتتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع إلى ما كان عليه باسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج وبحيث لا تتحول الاضرار إلى خسائر دائمة" [3].

---

[1] - عادل عبدالصادق، الاقتصاد الرقمي وتحديات السيادة السيبرانية، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2020، ص85.

[2] - فراس جمال شاكر محمود، الحروب المعلوماتية.. في المجال الأمني والعسكري أمريكا والصين، القاهرة، العربي للنشر والتوزيع، 2022، ص231.

[3] - منى لاشلاقر جبور، الامن السيبراني التحديات ومستلزمات المواجهة، القاهرة، المركز العربي للابحاث القانونية والقضائية، 2012، ص3-4.

وايضا: نور علي صكب،، الامن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)، مجلة كلية القانون والعلوم السياسية، العدد 11، المجلد 20، الجامعة العراقية، 2021، ص10-11.

بعبارة اخرى، ان الامن السيبراني انما يقصد به حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، وبكل ما تتضمنه مكوناتها من: أجهزة وبرمجيات وبيانات، وما يرتبط به من خدمات، من أي نشاط: اختراق أو تعطيل أو تعديل أو استخدام أو استغلال غير مشروع للاجهزة والبرامج والبيانات.

اما البحث في اهمية الامن السيبراني، فانه يتاتى من طبيعة التطورات التكنولوجية، وحقائق الواقع العالمي الراهن واحتمالاته القادمة، فالتطورات التكنولوجية انتهت الى جعل اغلب التعاملات تتم عبر اطر الكترونية، وادارة اغلب الانشطة الكترونيا ومنها الانتاج والتسويق والحماية وحتى الامور المالية، والتعامل مع المستفيدين من المؤسسة او المتعاملين معها، وغيره، وتحويل الانشطة من مادية الى انشطة رقمية يترتب عليه تغيير في يئة العمل واجراءات الامن وغيره، وهو ما يطرح موضوع كيفية حماية البيئة الرقمية، بالمعلومات والبرامج التي تحويها واجراءات العمل داخلها، وهو ما يطلق عليه بالامن السيبراني. ان الكثير من المؤسسات قد طورت لها انظمة واجراءات امن خاصة بها، يمكن ان تسهم بحفظ الحقوق التي ترتبط بالتعاملات السيبرانية، فاذا كان لتطور التكنولوجي قد فرض نفسه واوصل التعاملات الى السيبرانية فان التطور نفسه يلزم بان يتم حماية الحقوق والتعاملات السيبرانية من اي استهداف يمكن ان تتعرض له، من افراد او منظمات اجرامية او مؤسسات مخابراتية لدول اخرى، لان تلك المؤسسات والمنظمات يمكنها ان تقوم باستغلال التطور التكنولوجي وتطور برامج اختراق، فتستهدف البيانات او البرامج او الاموال بالتعطيل او السرقة او الاتلاف، وهو ما يجعل نظام الامن السيبراني مهم في التعاملات السيبرانية.

المبحث الثاني: موقع العراق في مؤشر الامن السيبراني العالمي والتحديات التي تواجهه

ان اهمية الامن السيبراني دفعت الدول والمؤسسات إلى تامين الحماية المناسبة للاجهزة والبرامج والبيانات والاموال، من اي اختراق أو تعامل غير مشروع أو سرقة أو اتلاف أو اي اجراء اخر غير مسموح به ضد تلك البنية المحمية بموجب القانون.

والدول تتباين في اجراءاتها المعتمدة لتوفير الامن السيبراني، نظرا لان موضوع الامن السيبراني هو موضوع ناشأ وما يزال ينتطور بسرعة كبيرة بفعل تطور التقنيات، والاهم من هذا ان موضوعه عرضة للتنافس وليس للصراع لانه يعتمد على ادخال المعرفة بالقطاعات المخلفة، وانتاج اجهزة وبرامج وتحليل بيانات ومنظومات شبكية لاستخدام ما تقدم، فالدول والمؤسسات تعمل من اجل ان تستفيد من التطور التكنولوجي، وكلما اتجهت الدول والمؤسسات إلى التعاملات الرقمية كلما حققت فاعلية اكبر الا انها بالوقت نفسه تعرض نفسها لتهديدات اكبر، لان الاجهزة معرضة للاختراق، والبرامج التي تستخدم لحفظ وتحليل البيانات، والاموال يمكن سرقتها وسرقة من ثم البيانات والاموال، والربط الشبكي يسمح بتعريض مجموعة اكبر للضرر، بل ان الضرر يمكن ان يمتد ليصيب مؤسسة بالكامل، ويتوقف أو يتضرر المتعاملين معها لتصبح القضية قضية امن وطني ان كانت تلك المصالح تعبر عن ثقة المتعاملين بها ومعها بالدولة واجراءاتها، فالاختراق ليس للمؤسسة لذاتها انما الاختراق لاجراءات الدولة في توفير وقاية لاعمالها واعمال المؤسسات الخاصة ولاعمال الافراد من الاختراق والاضرار بمصالحهم.

ان ما تقدم دفع الاتحاد الدولي للاتصالات (ITU) إلى وضع عدد من المعايير تحت عنوان: مؤشر الأمن السيبراني (Global Cybersecurity Index) ومختصره: (GCI)، والذي يوضح موقع الدول في العالم بحسب قوة الاجراءات الوقائية لحفظ امن الاجهزة والبرامج والربط الشبكي والبيانات والاموال للدولة ومؤسساتها ومصالح الافراد المتعاملين سيبرانيا، أو اجراءات الردع والتتبع والمسائلة في حال تعرض المواقع والبيانات للهجوم والتعطيل والسرقة والاتلاف أو اي تجراء اخر غير مصرح به، وتوفر له الدولة الحماية، وذلك التقرير تم وضعه عام 2005، وتم تطويره ليكون قادرا على ان يعطي صورة شاملة لموقع الدولة في الامن السيبراني[1].

[1] - فرح يحيي زعاترة، التهديدات السيبرانية على الأمن القومي الأمريكي، القاهرة / العربي للنشر والتوزيع، 2023، ص69.
وايضا: فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني، عمان، دار الخليج للنشر والتوزيع، 2023، ص137-138.
وللتوسع ينظر مثلا:
انعام عبد الرضا سلطان العكّابي، الدور الدولي في تعزيز الامن السيبراني في ضوء التحديات المعاصرة، المجلة العراقية للعلوم السياسية، العدد 9، الجمعية العراقية للعلوم السياسية، 2023، ص267-269.

ان تتتبع موضوع مؤشر الامن السيبراني، فان موقع العراق فيه، يوضح ان المؤشر يعتمد في تقييم موقع الدولة على خمسة ركائز متنوعة؛ فالمؤشر لا ينظر إلى تطبيق محدد للسيبرانية الواجب حمايته انما ينظر اليه من زاوية انه تطبيقات متعددة، تتطلب اجراءات شاملة ومتنوعة، وتلك الركائز هي[1]:

1. التدابير القانونيّة، اي ان تنجح الدولة في وضع تشريعات وقوانين، تتعامل مع الجرائم الإلكترونية.
2. التدابير التقنيّة، اي ان تمتلك الدول إجراءات وتدابير تكنولوجية وتقنية يمكن من خلالها اكتشاف الهجمات الإلكترونية والرد عليها، واهم تلك التدابير هي وجود هيئة وطنية متخصصة في مجال الأمن السيبراني، نظرا لخصوصية الجرائم السيبرانية.
3. التدابير التنظيميّة، وتتضمن وجود خطة واضحة وهدف استراتيجي قابل للتنفيذ، ويمكن تتبع قياس الانشطة والاجراءات التي تم اعتمادها.
4. تنمية القدرات، وهنا يتوجب على الدول اعداد لقدرات البشرية والمؤسسية، والعمل على تعزيز المعرفة والوعي بالأمن السيبراني والاجراءات التي تتخذها الدولة لتحقيق هذا الغرض، وتوفر الموارد التي تُتيح البحث والتطوير والتدريب في مجالات الأمن السيبراني.
5. التعاون، ان مفهوم الأمن السيبراني هو مفهوم واسع ويتطلب ايجاد تعاون متعدد مع المؤسسات المحلية، والجهد الدولي، بما يؤمن للدولة امتلاك قدرات كبح وردع التهديدات الموجودة.

[1] - عادل عبد الصادق، الرقمنة والمرونة السيبرانية:حالة المنطقة العربية، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2021، ص30-31.
وايضا: زياد عبدالتواب، مؤشرات الأمن السيبرانى، مركز الاهرام للدراسات السياسية والاستراتيجية، تاريخ الدخول 12 اب 2024، على الرابط : https://www.siyassa.org.eg/News/18495.aspx

وتتبع مواقع الدول في المؤشر العالمي للامن السيبراني يلاحظ انه في العام 2020 كانت الولايات المتحدة بالمرتبة الاولى تليها الصين ثم بريطانيا ثم روسيا ثم المانيا ثم فرنسا ثم كندا واليابان وثم استراليا عاشرا، وفي العام 2022 كان ترتيب اقوى الدول في اجراءات الامن السيبراني الشاملة هي: الولايات المتحدة ثم الصين ثم روسيا ثم بريطانيا ثم استراليا ثم هولندا وكوريا الجنوبية وفيتنام وفرنسا وايران [1]، اما في العام 2023 فان الترتيب اصبح: الولايات المتحدة وبريطانيا والسعودية واستونيا وكوريا الجنوبية وسنغافورة واسبانيا وروسيا [2]، والتغير في المراتب العالمية انما يعكس حجم التنافس بين الدول، وحجم الاستثمار في بنية الامن السيبراني فيما بينها نظرا لتعقد البنية السيبرانية وتوسع مهامها.

الى جانب ما تقدم، صدر عن مركز بيلفر للعلوم والشؤون الدولية بجامعة هارفارد، مؤشر اخر للقوة السيبرانية، يختصر تحت اسم: "إن سي بي آي" (NCPI)، وصدر بنسختين للعام 2020 و 2022، ويقوم بتصنيف قدرات 30 دولة وفقا لقدراتها وإمكانياتها السيبرانية، وهذا المؤشر يتكونن من 29 مؤشرًا فرعيا، واهمها: القدرة على صد الهجمات الإلكترونية، ووجود قوانين حماية البيانات، ووجود المعايير الفنية، وحوكمة الإنترنت، ووجود نظام للبحوث الإلكترونية، والقدرة على كبح الجرائم الإلكترونية، والقدرة على الإنفاذ إلى المنظومات السيبرانية وتوفير الحماية والردع، واستخدام المعرفة المتاحة للجمهور عن القدرات الإلكترونية، وغيرها، ويتم تقييم هذه المؤشرات عبر ثمانية أهداف، من وجهة نظر واضعوا المؤشر، وهي: القدرة المالية التي يتم انفاقها على الاجراءات السيبرانية، والمراقبة، والاستخبارات، والتجارة، والدفاع، ومراقبة المعلومات، ونوايا الدولة وقدرتها في ادارة الحرب الإلكترونية والدفاع، وكل ذلك ياتي في ظل الدينامية التي تتناول موضوع الامن السيبراني والمؤشرات المرتبطة به[3].

---

[1] - خالد وليد محمود، عن مؤشر القوة السيبرانية الوطني 2022، تاريخ الدخول 12 اب 2024، على الرابط: https://www.aljazeera.net/opinions/2022/10/12

[2] - وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات، تاريخ الدخول 12 اب 2024، على الرابط: https://x.com/mfu46/status/1409974694061674500?lang=ar

[3] - خالد وليد محمود، عن مؤشر القوة السيبرانية الوطني 2022، مصدر شبق ذكره.
وايضا: إبراهيم سيف منشاوي، تحولات القوة: دمج القدرات السيبرانية في تقرير التوازن العسكري 2020، مركز المستقبل للأبحاث والدراسات المتقدمة، تاريخ الدخول 14 اب 2024، على الرابط :
https://futureuae.com/ar-AE/Mainpage/Item/6159 8A-2020

ان تحليل مكانة العراق على صعيد الامن السيبراني يلاحظ الاتي:

الجدول (1): موقع العراق في مؤشر الامن السيبراني العالمي لسنوات مختارة

ت	2019	2020	2021	2022	2023	2024
الترتيب	107	129	159	127	165	150
عدد الدول في المؤشر	182	182	182	193	176	182

الجدول من عمل الباحث بالاعتماد على:

الجدول يوضح، ان البلد ما يزال يعاني [1]، فهو احتل المرتبة 107 عالميا عام 2019 من مجموع 182 دولة، ثم احتل المرتبة 129 عالميا عام 2020، من مجموع 182 دولة، ثم المرتبة 165 عالميا من مجموع 176 دولة عام 2023، واحد ابرز الاسباب لذلك الموقع المتاخر هو عدم وجود مؤسسة معنية بالامن السيبراني تضمن توفير مظلة لحماية الاجهزة والبرامج والربط الشبكي والبيانات والاموال لمستخدميها فقط، وغياب المظلة التشريعية أو برامج لتطوير القدرات، .. حتى العام 2022 [2].

وايضا: خالد وليد محمود، لمغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية، مركز المتوسط للدراسات الاستراتيجية فيسبوك تويتر واتساب تيلقرام، تاريخ الدخول 14 اب 2024، على الرابط:
https://mediterraneancss.uk/2024/05/07/cyber-capabilities-united-states-of-america-china/
الامن السيبراني في العراق، مركز رواق بغداد، تاريخ الدخول 14 اب 2024، على الرابط:
https://rewaqbaghdad.org/uploads/files/shares/pdf/taqdeer_mawkif/64c7ab39eb14c.pdf
كذلك: العراق في مقدّمة الدول الأسوأ بالأمن السيبراني على المستوى العالمي، تاريخ الدخول 14 اب 2024، على الرابط : https://yaqinnews.net/?p=26916
And: International Telecommunication Union, ITU, IN:
https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[1]- حمزة محمود شمخي، مؤشر الامن السيبراني وموقع العراق فيه، جامعة كربلاء، كلية الادارة والاقتصاد،، تاريخ الدخول 14 اب 2024، على الرابط: https://business.uokerbala.edu.iq/wp/archives/20636

[2]- الامن السيبراني في العراق، مركز رواق بغداد، تاريخ الدخول 14 اب 2024، على الرابط:
https://rewaqbaghdad.org/uploads/files/shares/pdf/taqdeer_mawkif/64c7ab39eb14c.pdf
وايضا: العراق في مقدّمة الدول الأسوأ بالأمن السيبراني على المستوى العالمي، تاريخ الدخول 14 اب 2024، على الرابط: https://yaqinnews.net/?p=26916

لقد انتهى البعض ومنذ وقت مبكر إلى وجوب ان يضع استراتيجية مناسبة للامن السيبراني، فمع الاتجاه العالمي لتطبيق اجراءات للامن بهذا الشان، فعلى البلد ان يضع استراتيجية للأمن السيبراني الوطني، تعتمد على الركائز التالية"[1]:

1) تطوير إستراتجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة
2) إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات
3) ردع الجريمة السيبرانية
4) ايجاد قدرات وطنية لادارة الحواسيب الالية
5) تحفيز ثقافة وطنية للامن السيبراني.

ولقد حرصت الحكومة العراقية على تعزيز الأمن السيبراني، اذ تم في العام 2012م إطلاق الاستراتيجية الوطنية لضمان الأمن السيبراني، لغرض توضيح أولويات الأمن السيبراني لجميع مؤسسات الدولة وأفرادها، وذلك في شباط 2022 بعد ان عقدت جلسة مجلس الأمن الوطني، وتم فيها: اقرار إستراتيجية الامن السيبراني العراقي (2022 – 2025) .

المبحث الثالث: ناصر ومقومات استراتيجية الامن الوطني السيبراني: ادارة البيانات وتامينها والحصول على الدعم والتعاون الدولي

في العام 2022 انتهت الحكومة العراقية إلى اقرار وجود استراتيجية للامن السيبراني بما يعكس اهمية هذا الشق من التفاعلات والمؤسسات، وما يتبعه من بيانات واموال واداء والاهم صورة البلد امام المجتمع الدولي.

اظهرت هذه الاستراتيجية الاهتمام بتوضيح أولويات الأمن السيبراني لجميع مؤسسات الدولة وأفرادها. وتضمنت الاستراتيجية عدة محاور وأهداف تساهم في رفع مستوى الأمن السيبراني للبلد،

[1] - علي زياد العلي، المرتكزات النظرية في السياسة الدولية، عمان، دار الفجر للنشر والتوزيع، 2017، ص226-227.
وللتوسع ينظر ايضا: انعام عبد الرضا سلطان العكّابي، الدور الدولي في تعزيز الامن السيبراني في ضوء التحديات المعاصرة، مصدر سبق ذكره، ص269.

والتي تم إعدادها من قبل: فريق الإستجابة للحوادث السيبرانية العراقي (IQ-CERT) [1]، والمختصين في هذا المجال في القطاعات المختلفة، والهدف منه تحسين صورة البلد امام البيئة الدولية، وتوفير الثقة للمتعاملين مع مؤسسات الدولة بان هناك اجراءات وقائية واجراءات ردع ومحاسبة لمن يتعرض للبنية السيبرانية الحكومية والخاصة، وهو ما سيساعد في تعزيز الثقة بالمؤسسات الوطنية من قبل المستثمرين والافراد، وستكون نتائجه ايجابية على كل القطاعات المتصلة بالفضاء السيبراني العراقي.

وقد تضمنت هذه الاستراتيجية عدة أهداف رئيسة، عبرت عن رؤية صناع السياسة لما يجب ان تكون علية البنية الامنية السيبرانية، والهدف من وجود الاستراتيجية المتمثل بايجاد خارطة طريق ومبادرات لحماية الامن السيبراني العراقي. واعتبرت الاستراتيجية ان الامن السيبراني انما يمثل جزء من الامن الوطني العراقي، وعملت الاستراتيجية على رصد نقاط الضعف في اجراءات الامن الوقائي المعتمدة، وانه من الواجب توفير المظلة التشريعية لحماية البيانات والاجهزة والبرامج المستخدمة وان تعمل الدولة على تطوير القدرات السيبرانية في البلد، وان يتجه العراق إلى تعزيز التعاون المتعدد الاطراف مع المجتمع الدولي[2].

بعبارة اخرى ان الاستراتيجية عكست التوجه العراقي لاظهار الاهتمام بهذا القطاع، وان العمل جاري على تطوير خطة وطنية فاعلة للأمن السيبراني في البلد، تماشياً مع المتطلبات العالمية التي تتطلب وجود هيئة مستقلة وخاصة بالأمن السيبراني، وعليه فان العراق انتهى إلى إنشاء: فريق الاستجابة للحوادث السيبرانية العراقي، إلى جانب مركز الأمن السيبراني في مستشارية الأمن القومي، وكل منهما يعكس الاطار الاداري والسياسي الذي يمكن ان يؤسس لبناء امن سيبراني

[1]- فريق الإستجابة للحوادث السيبرانية العراقي (IQ-CERT)، تاريخ الدخول 14 اب 2024، على الرابط: https://cert.gov.iq/cert

[2] -استراتيجية الامن السيبراني العراقي، مستشارية الامن الوطني 2022- 2025، امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات، تاريخ الدخول 14 اب 2024، على الرابط: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

متكامل في الاعوام القادمة. وان العمل جاري لإيجاد منظومة حقيقة للأمن السيبراني في العراق، وتطويرها بما يضمن حماية حقيقية للوطن من تهديدات الأمن السيبراني المختلفة.

ان على العراق، بموجب المعايير التي تضمنها المؤشر العالمي للامن السيبراني، وضع عدد من الاجراءات المتخذة لحفظ الامن السيبراني، على الصعد: الاجراءات القانونية والاجراءات التقنية والاجراءات التنظيمية والاجراءات على صعيد بناء القدرات والاجراءات على صعيد التعاون الدولي[1]، وبالفعل العراق يدرك أهمية الامن السيبراني، وبدء منذ العام 2022 اعداد الأرضية المناسبة من اجل حماية انظمته من اي تهديدات الكترونية، وما يزال يحتاج إلى وقت مناسب لكي يفعل اليات العمل ضمن استراتيجية الامن السيبراني المعتمدة .

ان الامن السيبراني يشمل مؤسسات الدولة الامنية بالمقام الأول، إلى جانب المؤسسات الاقتصادية والمالية، وتمتد إلى مختلف المؤسسات الخاصة والمصالح الفردية، في ظل تسارع الجهد الوطني لاستكمال الانتقال إلى الإجراءات الإلكترونية في مختلف التبادل الادارية والمالية[2]

[1] - ينظر مثلا:
ماجد صدام سالم، الامن السيبراني العراقي واثره في قوة الدولة، مجلة العلوم التربوية والانسانية، العدد 18، جامعة ميسان، 2022، على الرابط:
https://www.jeahs.com/index.php/jeahs/article/view/302
وايضا:
Global Cybersecurity Outlook - Cybersecurity Trends 2024, IN:
https://www.weforum.org/publications/global-cybersecurity-outlook-2024/?utm_source=google&utm_medium=ppc&utm_campaign=cybersecurity&gad_source=1&gclid=CjwKCAjw8rW2BhAgEiwAoRO5rBzc_ij2ibbBandvpTW7_geGwZU-wqbkXQYNnFEd3gxZVNRZEQN40hoCt4EQAvD_BwE

[2] - للتسع ينظر مثلا:
آيات فاخر محمد العلوي، الامن السيبراني العراقي: الواقع وآفاق المستقبل، المجلة السياسية والدولية، العدد 58، الجامعة المستنصرية، 2024، ص303.
وايضا: علي احمد عبد مرزوك، الأمن السيبراني درع التحول الرقمي العراقي (بين التحديات الراهنة وضرورات المستقبل)، المجلة العلمية لجهاز مكافحة الارهاب، العدد 6، المجلد 3، جهاز مكافحة الارهاب، 2023، ص309 وما بعدها.

الخاتمـــة

بعد دراسة موضوع التطورات العالمية وكيف انتهت إلى تحويل متزايد لاغلب الانشطة من واقعها المادي إلى واقع سيبراني، اي التحول العالمي المتسارع للسيبرانية، والتي تشمل اجراءات متعددة ومنها: حفظ البيانات والاموال، وادارة المؤسسات، ونقل اجراءات المؤسسات إلى الاجراءات الرقمية، سواء ما تعلق منها بالمؤسسات الحكومية، بكل عناوينها أو المؤسسات الخاصة، أو حتى ما ترتبط احيانا ببيانات واموال الافراد، فان العالم السيبراني اوضح انه عالم يسع للمزيد من الاجراءات، وانه الاسرع والاكفا للخزن والادارة، الا انه بالمقابل تضمن اشكالية خطرة، الا وهي انه بالوقت الذي استفادت مؤسسات وافرد من اتساع تطبيقات السيبرانية، فان هناك مجموعات وافراد، واحيانا تتم ادارتهم عبر منظومات استخبارية في دول العالم، تتجه إلى الوصول إلى قواعد البيانات المخزنة لسرقتها، أو اتلافها، أو التلاعب بها وتغيير محتوياتها، أو سرقة الاموال، أو نشر معلومات خاطئة أو اي شيء يتسبب بحدوث اشكالية للدول والمؤسسات الخاصة والافراد المستهدفون، على نحو يتسبب بتهديد جدي للمصالح العامة أو الخاصة أو يمثل تحديا لها، طالما ان التعامل مع منظومة شبكات وقواعد واجراءات، والتقنيات الرقمية قادرة على فتح تشفيرها واختراقها، وهو ما يفرض اعتماد اجراءات حماية وامن تتناسب مع اهمية المصالح المحفوظة في التعامل الرقمي.

اتجه المجتمع الدولي إلى وضع ما يعرف بالمؤشر العالمي للامن السيراني، ويوضح موضع الدولة في اجراءات الامن السيبراني ومدى انكشافها أو منعتها وقوتها، وذلك استنادا إلى مجموعة قواعد وبيانات واجراءات، وهو ما اعطى دافع لدول عديدة حول العالم لتعزيز اجراءاتها وسياساتها واسراتيجياتها لتطوير بنية الامن السيبراني فيها، وبضمنه صياغة استراتيجيات للامن السيبراني فيها.

اتجه العراق، بعد ان اخذت قطاعات عديدة فيه وبضمنه القطاعات الحكومية إلى الارتباط بالاجراءات السيبرانية، وادارة وخزن البيانات والاموال الكترونيا، سواء للمصالح الحكومية أو الفردية، إلى العمل على تعزيز اجراءات الامن السبراني خاصة ان البلد مستهلك للمعدات

السيبرانية وليس منتجا لها، وهو ما يعرض المصالح الوطنية العامة أو الخاصة، إلى احتمالية متصاعدة للاضرار والضرر بسرقة البيانات أو الاموال أو اتلافها، سواء من مجموعات افراد، أو من مجموعات تعمل تحت ظل اجهزة مخابراتية، وهو ما صدر باستراتيجية متخصصة للامن السيبراني في العام 2022 .

انتهى البحث إلى اثبات فرضيته وتحقيق الهدف منه في دراسة استراتيجية الامن الوطني السيبرانية للعراق، والتي تم وضعها لتعزيز اجراءات الامن، والخطوات التي سيشرع العراق بها لتعزيز قدراته في مواجهة التحديات والتهديدات السيبرانية.

وانتهى البحث إلى عدد من الاستنتاجات، وهي الاتية:

1) ان الامن السيبراني يقصد به الاجراءات التي تتخذها الدولة أو المؤسسة الخاصة لحفظ بياناتها من السرقة أو الاتلاف، وبما يعزز الثقة لدى العملاء المتعاملين مع الدولة أو تلك المؤسسات بالاجراءات التي تم اتباعها لحفظ المصالح والحقوق.
2) ان اهمية الامن السيبراني تاتي من كون التعاملات التي تقوم بها الدولة والمؤسسات والافراد تتحول بشكل متزايد إلى تعاملات سيبرانية، والمنظومة والشبكات السيبرانية هي عبارة عن خطوط اتصال، تختلف مستوى تشفيرها وحمايتها، ومن ثم فان اجراءات اختراقها ايضا يمكن تطويرها تقنيا، وهو ما يفتح مدخلا لمجموعات الهكرز: افراد وشبكات أو حتى لاجهزة استخبارية تعمل لذاتها أو عبر تلك الشبكات وتوظف تلك الشبكات الاحترافية، من اجل الاختراق والسرقة والاتلاف، طالما ان جزء من الصراع والحرب اصبح سيبرانيا، واجراءات الحماية والامن مقابل اجراءات الاختراق، يعطي للموضوع اهميته وحيويته.
3) تتجه اغلب الدول إلى صياغة اجراءات الامن والحماية عبر استراتيجيات متخصصة، لا تبتعد كثيرا عن كونها جزء من استرايجيات الامن الوطني، لان المصالح المحفوظة هي مصالح حيوية والتعرض لها يهز الثقة بالدولة

ومؤسساتها، لانه يسرق بياناتها أو يتلفها أو يسرق الاموال أو يعطل الدولة ومؤسساتها عن تنفيذ قدرتها على ادارة المرافق العامة، أو حماية المرافق والمصالح الخاصة.

4) ان موقع العراق في مؤشر الامن السيبراني العالمي ما زال منخفض، وذلك لان العراق يستهلك البيانات ويستهلك المعدات السيبرانية وليس منتجا أو مطورا لها، ومن ثم فانه يعد مكشوفا من الناحية الامنية سيبرانيا. بل ان ادخال القدرات السيبرانية في الحفظ والادارة للمرافق العامة ما زال ضعيفا، ويعكس هشاشة البنية التحتية السيبرانية ويعكس الضعف الموجود بهذا الجانب، رغم ان القدرات وانتشار السيبرانية في القطاع الخاصة ينمو بشكل اكبر من القطاع الحكومي.

5) يواجه العراق تحديات سيبرانية متعددة، الا انها تحديات ما تزال ناشئة لضعف ربط المصالح الحكومية بالسيبرانية، ورغم نمو تخصص السيبرانية والامن السيبراني الا ان الموضوع ما يزال ناشئ في العراق، ومع ذلك يحتاج البلد إلى الاهتمام وتعزيز هذا الموضوع واجراءاته خاصة مع التحول إلى حفظ البيانات والاموال الكترونيا، في عدة مؤسسات، ويبقى موضوع الحكومة الالكترونية وادارة المرافق العامة والخاصة الكترونيا موضوع يحتاج إلى وقت وبنية سيبرانية ليتم تطويره مستقبلا.

6) وضع العراق رسميا في العام 2022 استراتيجية للامن الوطني السيبراني، وتلك الاستراتيجية اعتمدت لها مقومات ترتكز على تحديد الهدف والرؤية، والاستعدادات لتطوير البنية للامن السيبراني، وما يحتاجه البلد لتعزيز اجراءاته القانونية للتعامل مع الجرائم والتهديدات السيبرانية، وما يحتاج البلد من تعاون دولي بهذا الشان.

وفي ختام هذا البحث، فان التوصيات التي تطرح هي:

1. يحتاج العراق إلى تطوير المنظومة السيبرانية الحقيقية، انتاجا وتطويرا، وذلك من خلال دعم حقيقي للبحث العلمي للباحثين لتطوير المنظومات الرقمية برامج واجهزة وشبكات، حتى يكون هناك منظومات وطنية لتقليل امكانية الاختراق الخارجية لقواعد البيانات أو اتلافها أو سرقتها، وبضمنه الاموال والمؤسسات والمصالح التي تدار الكترونيا.
2. يحتاج العراق إلى مراجعة حقيقية لاجراءات الامن السيبرانية، وفقا للمؤشرات العالمية، والابتعاد عن المراجعة الشكلية، اي الاقتراب من الاصل وهو: الشعور بالامن اسيبراني، وليس النظر بالاجراءات.

المصادر

اولا: الكتب العربية:

1. حسن الحاج علي أحمد واخرون، الأمن القومي العربي وتحديات الأمن الإقليمي، الدوحة، المركز العربي للأبحاث ودراسة السياسات، 2023
2. عادل عبد الصادق، الرقمنة والمرونة السيبرانية:حالة المنطقة العربية، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2021، ص30-31.
3. عادل عبدالصادق، الاقتصاد الرقمي وتحديات السيادة السيبرانية، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2020
4. علي زياد العلي، المرتكزات النظرية في السياسة الدولية، عمان، دار الفجر للنشر والتوزيع، 2017
5. فراس جمال شاكر محمود، الحروب المعلوماتية.. في المجال الأمني والعسكري أمريكا والصين، القاهرة، العربي للنشر والتوزيع، 2022
6. فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني، عمان، دار الخليج للنشر والتوزيع، 2023
7. فرح يحيي زعاترة، التهديدات السيبرانية على الأمن القومي الأمريكي، القاهرة / العربي للنشر والتوزيع، 2023
8. منى لاشلاقر جبور، الامن السيبراني التحديات ومستلزمات المواجهة، القاهرة، المركز العربي للابحاث القانونية والقضائية، 2012

ثانيا: المجلات والدوريات:

1) انعام عبد الرضا سلطان العكّابي، الدور الدولي في تعزيز الامن السيبراني في ضوء التحديات المعاصرة، المجلة العراقية للعلوم السياسية، العدد 9، الجمعية العراقية للعلوم السياسية، 2023
2) آيات فاخر محمد العلوي، الامن السيبراني العراقي: الواقع وآفاق المستقبل، المجلة السياسية والدولية، العدد 58، الجامعة المستنصرية، 2024
3) علي احمد عبد مرزوك، الأمن السيبراني درع التحول الرقمي العراقي (بين التحديات الراهنة وضرورات المستقبل)، المجلة العلمية لجهاز مكافحة الارهاب، العدد 6، المجلد 3، جهاز مكافحة الارهاب، 2023
4) نور علي صكب،، الامن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)، مجلة كلية القانون والعلوم السياسية، العدد 11، المجلد 20، الجامعة العراقية، 2021

ثالثا: مواقع شبكة الانترنت:

1. إبراهيم سيف منشاوي، تحولات القوة: دمج القدرات السيبرانية في تقرير التوازن العسكري 2020، مركز المستقبل للأبحاث والدراسات المتقدمة، تاريخ الدخول 14 اب 2024، على الرابط: https://futureuae.com/ar-AE/Mainpage/Item/6159 8A-2020
2. اسراتيجية الامن السيبراني العراقي، مستشارية الامن الوطني 2022- 2025، امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات، تاريخ الدخول 14 اب 2024، على الرابط: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf
3. الامن السيبراني في العراق، مركز رواق بغداد، تاريخ الدخول 14 اب 2024، على الرابط: https://rewaqbaghdad.org/uploads/files/shares/pdf/taqdeer_mawkif/64c7ab39eb14c.pdf
4. حمزة محمود شمخي، مؤشر الامن السيبراني وموقع العراق فيه، جامعة كربلاء، كلية الادارة والاقتصاد،، تاريخ الدخول 14 اب 2024، على الرابط: https://business.uokerbala.edu.iq/wp/archives/20636
5. خالد وليد محمود، عن مؤشر القوة السيبرانية الوطني 2022، تاريخ الدخول 12 اب 2024، على الرابط: https://www.aljazeera.net/opinions/2022/10/12
6. خالد وليد محمود، لمغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية، مركز المتوسط للدراسات الاستراتيجية فيسبوك تويتر واتساب تيلقرام، تاريخ الدخول 14 اب 2024، على الرابط: https://mediterraneancss.uk/2024/05/07/cyber-capabilities-united-states-of-america-/china
7. زياد عبدالتواب، مؤشرات الأمن السيبرانى، مركز الاهرام للدراسات السياسية والاستراتيجية، تاريخ الدخول 12 اب 2024، على الرابط: https://www.siyassa.org.eg/News/18495.aspx
8. العراق في مقدّمة الدول الأسوأ بالأمن السيبراني على المستوى العالمي، تاريخ الدخول 14 اب 2024، على الرابط: https://yaqinnews.net/?p=26916
9. فريق الإستجابة للحوادث الســـيبرانية العـــراقي (IQ-CERT)، تاريخ الدخول 14 اب 2024، على الرابط: https://cert.gov.iq/cert
10. ماجد صدام سالم، الامن السيبراني العراقي واثره في قوة الدولة، مجلة العلوم التربوية والانسانية، العدد 18، جامعة ميسان، 2022، على الرابط: https://www.jeahs.com/index.php/jeahs/article/view/302
11. وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات، تاريخ الدخول 12 اب 2024، على الرابط: https://x.com/mfu46/status/1409974694061674500?lang=ar

رابعا: المصادر الاجنبية:

1) Global Cybersecurity Outlook - Cybersecurity Trends 2024, IN: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/?utm_source=google&utm_medium=ppc&utm_campaign=cybersecurity&gad_source=1&gclid=CjwKCAjw8rW2BhAgEiwAoRO5rBzc_ij2ibbBandvpTW7_geGwZU-wqbkXQYNnFEd3gxZVNRZEQN40hoCt4EQAvD_BwE