سياسات الامن الوطني العراقي
في ظل التحديات العالمية للأمن السيبراني

ا.م.د. عباس فاضل علوان
كلية العلوم السياسية - جامعة الكوفة
abassf.aljboori@uokufa.edu.iq

سياسات الامن الوطني العراقي
في ظل التحديات العالمية للأمن السيبراني

ا.م.د. عباس فاضل علوان
كلية العلوم السياسية - جامعة الكوفة
abassf.aljboori@uokufa.edu.iq

ان الامن السيبراني هو من الموضوعات المهمة في عالم اليوم، وهو موضوع يجمع بين اكثر من تخصص، فهو موضوع امني، واقتصادي، وسياسي، سواء كان داخلي او دولي، ونظرا لان الكثير من المرافق اصبحت تدار بواسطة الخصائص الرقمية وعبر منظومات الانترنت، كما ان المواطن اصبح يتعامل مع المؤسسات، ومع مصالحه بطريقة رقمية، وبصورة متزايدة، لهذا فان القطاع الرقمي، لا يمكن ان يترك من دون تنظيم، في ظل وجود امكانية للأضرار بالمصالح العامة والخاصة عبر استخدام ادوات تدخل للخصائص الرقمية، وتقوم بسرقة البرامج والبيانات او اتلافها او تغييرها، او استخدامها على نحو يضر بالمالك الاصلي للبرامج والبيانات، اتجهت الدول الى وضع سياسات للأمن السيبراني، واعتبرته جزء من الامن الوطني، للتعامل مع حالات اختراق الاجهزة، او تعطيلها او سرقة محتواها او الاضرار بمالك الاجهزة الرقمية والبيانات والبرامج. ويأتي هذا الاتجاه، نظرا لخطورة التعاملات الرقمية، من حيث اضرارها المادية المباشرة، والاضرار بالثقة العامة، والاضرار المرتبطة بضعف قدرة الدولة عن التعامل مع حفظ مصالح المؤسسات والافراد، والمشكلة البحثية التي ينطلق منها البحث، تتعلق بالسؤال: كيف ينتهي العالم السيبراني الى وضع مخاطره ضمن سياسات الامن الوطني؟ ان البحث، ينتهي الى تحليل مفهوم الامن السيبراني، والصلة التي تربطه بالأمن الوطني، ثم يتم البحث بالأمن السيبراني في العراق، وابرز التحديات التي يعاني منها، ليكون قادرا على الاستجابة للتحديات والتهديدات السيبرانية في عالم اليوم.

الكلمات المفتاحية: الامن، السيبرانية، الامن الوطني، الامن السيبراني، العراق، التهديدات السيبرانية.

Iraqi National Security Policies in Light of Global Cybersecurity Challenges

Assistant Professor Abbas Fadhil Alwan

College of Political Science

University of Kufa

Cybersecurity is one of the important topics in today's world, and it is a topic that combines more than one specialization, as it is a security, economic, and political topic, whether internal or international, and given that many facilities are now managed by digital features and via Internet systems, and that citizens are increasingly dealing with institutions and their interests in a digital manner, the digital sector cannot be left without regulation, in light of the possibility of harming public and private interests through the use of tools that interfere with digital features, and steal, damage, or change

programs and data, or use them in a way that harms the original owner of the programs and data. Countries have moved towards developing cybersecurity policies, and considered it part of national security, to deal with cases of hacking devices, disabling them, stealing their content, or harming the owner of digital devices, data, and programs. This trend comes due to the danger of digital transactions, in terms of their direct material damage, harm to public trust, and harm associated with the weakness of the state's ability to deal with preserving the interests of institutions and individuals. The research problem from which the research is based is related to the question: How does the cyber world end up placing its risks within national security policies? The research ends with an analysis of the concept of cyber security, and the relationship that links it to national security, then the research is conducted on cyber security in Iraq, and the most prominent challenges it suffers from, to be able to respond to cyber challenges and threats in today's world.

Keywords: Security, Cyber, National Security, Cyber Security, Iraq, Cyber Threats.

المقدمة

ان تحليل موضوع سياسات الامن الوطني انما يظهر الاهمية له، فدول العالم تتجه الى تحليل هذه السياسات لأنها تسهم بحفظ الامن والاستقرار في الدولة، والمبني على وجود مؤشرات وتقديرات الى جانب وجود اختصاصات وواجبات على الدولة ومؤسساتها ان تقوم بها تجاه الدولة والمجتمع والافراد.

ان سياسات الامن الوطني انما هي من ابرز السياسات، لان الدولة تشعر انها مسؤولة عن حفظ السلم والامن والاستقرار، في وجه اي تحدي او تهديد. والتحديات والتهديدات التي تتعرض لها الدولة والمجتمع ومصالح الافراد او وجودهم، انما تعد من التحديات والتهديدات الي يتم تسليط الضوء عليها، من اجل كبحها وانهاءها او في اقل تقدير اضعاف تأثيرها.

ويبرز من بين التحديات او حتى التهديدات للأمن الوطني، التحديات السيبرانية، واي قصور في اجراءات الامن السيبراني اي ضعف الاجراءات التي تتبعها الدولة لمواكبة التغيرات والتحولات في الامن السيبراني اي امن المصالح والمنظومات والبيانات التي ترتبط بالسيبرانية، انما تعد من بين الاخطاء المهمة التي تؤثر على امن الدولة، بسبب تزايد الربط الكبير للمصالح العامة والخاصة بالسيبرانية، في وقت تحمل السيبرانية فرص فأنها تحمل ايضا تهديدات وتحديات خطرة، ان تم اختراق المنظومات وبياناتها، واستهداف المصالح العامة والخاصة التي تقف خلفها.

ان العراق ما زال في خط الشروع الاول في موضوع السيبرانية، واخذ ربط المصالح العامة والخاصة بالمنظومات السيبرانية يزداد، من اجل تسهيل الاجراءات ومواكبة التحولات العالمية، وهو ما يفيد ان البنية السيبرانية يمكن ان تتعرض للخطر، ومن ثم تتعرض المصالح التي تستخدمها او تستفيد منها للخطر. ومن ثم يتطلب الامر البحث في موضوع سياسات الامن الوطني السيبرانية المعتمدة من قبل البلد.

اهمية البحث والهدف منه:

ان اهمية البحث في موضوع سياسات الامن الوطني انها واحدة من اهم السياسات التي تبنى على تعقب كل ما يهدد مصالح الدولة، سواء كمصالح عامة او خاصة حتى يشعر الجميع (من في الدولة) ان هناك حماية جمعية لهم، وتلك السياسات تتعقب كل تحدي او تهديد يتعرض له الامن في الدولة، واستعراض تلك التحديات والتهديدات انما يوضح لصناع السياسات العامة في شق الامن الوطني ان هناك اولويات يجب التركيز عليها، خاصة في مجال الامن السيبراني.

والهدف من هذا البحث هو اعطاء تركيز على التحديات والتهديدات التي اخذت تصيب مصالح مستحدثة للدولة، وفقا للقواعد لعامة، فالأصل ان الدولة عليها ان تضع سياسات للأمن الوطني، وتهدف لحماية كل من المصالح العامة والخاصة، والسيبرانية هي قدرة الدولة والمؤسسات والافراد على ابتداع اساليب للوصول والادارة والتنظيم والعمل بطرق مبتكرة وسريعة، واحداث ضرر فيها انما يظهر ان الدولة غير قادرة على حماية المصالح العامة والخاصة.

علما ان التهديد السيبراني هو تهديد متعدد الابعاد ومتعدد المستويات محليا ودوليا لعدم وجود الحدود في التأثير.

حدود البحث :

اما حدود البحث فانه يتقيد بالاتي: مكانيا فانه يشير الى موضوع السيبرانية، وهو ما لا يتقيد بأبعاد محددة فهو موضوع مركب : سياسي وقانوني وامني واقتصادي وثقافي، ويتسع للأبعاد الوطنية والدولية، وهنا سيتم الاشارة الى التحديات العالمية ويتم الاشارة الى الابعاد والتحديات في شقها السياسي، وموضوعيا فان البحث يربط بين الامن السيبراني والامن الوطني، بوصف الاول انما يمثل اجراءات تدخل في نطاق الموضوع الثاني.

اشكالية البحث:

ان الاشكالية تدور حول التحديات التي يطرحها التعرض للمصالح العامة (كل ما يتعلق بالمؤسسات الحكومية المختلفة) والخاصة (الشركات والافراد) في المجال او الفضاء السيبراني او الرقمي، وما يجب على سياسات الامن الوطني القيام به للارتقاء الى مرتبة تأكيد حماية تلك المصالح الوطنية في ظل البيئة العالمية التي يمتد اليها العالم او الفضاء السيبراني.

وهذه الاشكالية تطرح الحاجة للإجابة عن عدة تساؤلات وهي:

ما مفهوم الأمن السيبراني وأبعاده؟

ما هي التحديات السيبرانية، وهي تحديات تكاد تكون عالمية؟

ما هي العلاقة بين الأمن السيبراني والأمن الوطني؟

ما هو واقع الأمن السيبراني في العراق؟

ما هي التحديات والتهديدات السيبرانية العالمية التي تواجه العراق؟

فرضية البحث:

نفترض هنا انه في عالم اليوم يزداد استخدام السيبرانية نتيجة التقدم في التكنولوجية الرقمية، ونطاق حضور تلك التقنيات عالمي، وفي ظل الامتداد العالمي فان هناك تحديات للأمن السيبراني تفرض حضورها على الدول وبضمنه العراق كمتغير مستقل، وطالما ان على تلك الدول

ان تتعامل مع مصادر التحدي او التهديد وتحجيمها وانهائها فان ذلك يفرض على الدول وبضمنها العراق تطوير سياسات الامن الوطني لتكون اكثر شمولا كمتغير تابع. وان العراق يتجه لزيادة استخدام السيبرانية في المصالح العامة والخاصة وهو ما يتطلب حماية تلك المصالح ضمن اجندات سياسات الامن الوطني.

المنهج:

ان تناول الاشكالية السابقة سيتم معها استخدام المنهج التحليلي الوصفي.

الهيكلية:

سيتم تقسيم وتناول هذا البحث عبر الموضوعات التالية، الى جانب المقدمة والخاتمة:

اولا– مفهوم الأمن السيبراني وأبعاده، وسيتم فيه تناول : تعريف الأمن السيبراني وأهدافه، والتحديات السيبرانية على المستوى العالمي، والعلاقة بين الأمن السيبراني والأمن الوطني

ثانيا– واقع الأمن السيبراني في العراق، وسيتم فيه تناول موضوع تحليل الوضع القائم للأمن السيبراني في العراق

ثالثا– التحديات العالمية للأمن السيبراني، ومتطلبات حماية الامن الوطني العراقي، وسيتم فيه البحث في موضوعات التحديات العالمية للأمن السيبراني، وسيتم فيه استعراض التحديات والتهديدات السيبرانية التي تواجه العراق، والتحديات التقنية التي تواجه اشكالية الامن السيبراني ومنها ضعف البنية التحتية والتكنولوجيا المتطورة، والتحديات المؤسسية: نقص التنسيق بين الجهات الحكومية والقطاع الخاص، والتحديات القانونية المتمثلة بغياب التشريعات الحديثة،

رابعا– تقييم السياسات والآليات المتبعة في العراق لمواجهة التهديدات السيبرانية، ويتم فيه الاشارة الى تقييم السياسات والآليات المتبعة في مواجهة التهديدات السيبرانية.

اولا- مفهوم الأمن السيبراني وأبعاده

ان الخطوة الاولى في التعامل مع العلوم الاجتماعية يتطلب الشروع بتحديد الاطار المفاهيمي والنظري، والاشارة او البحث في مفهوم الامن السيبراني وعلاقته بالأمن الوطني، يتطلب الاشارة الى معنى الأمن السيبراني وأهدافه، ان الامن السيبراني هو احد الموضوعات التي تطورت في العصر الذي اخذت تنتقل فيه المصالح لحفظ ومعالجة البيانات واداء الاعمال والتعبير عن نفسها من خلال الخصائص الرقمية، وهي منظومة تشمل: الاجهزة والبرامج والمعلومات واجهزة الربط الشبكي والانترنت، ومن خلالها يتم ضمان اداء الاعمال من قبل مزود الخدمة ووصولها الى المستفيد من دون حاجة لانتقاله للحصول على ذات الخدمة.

وبعيدا عن المعنى اللغوي او التوسع بالتعاريف المعطاة للمعاني، فان لفظ الامن اصطلاحا انما يشير الى التحرر من الخوف، وتجنب الضرر، او اي حالة غير مرغوب بها[1]، بينما تشير كلمة السيبرانية الى عدة دلالات، فهو يستخدم بمعنى العالم الافتراضي او الرقمي، ويشير اصطلاحا الى نطاق او مجال يتم انشاءه من قبل اجهزة الحاسوب او الهواتف الذكية باستخدام البرامج المخصصة للتعامل مع بيانات محددة (معلومات او اموال) او لإدارة عمل او نشاط بصيغة آلية وعن بعد، ويتم ربطه عبر الانترنت ليكون فضاء عالمي، او فضاء محلي ان كانت منظومة الانترنت وطنية، وهذا العالم يشهد تطورات كبيرة بفعل تطوير خصائص الذكاء الاصطناعي، واخذت كل المصالح العامة (مؤسسات الحكومات والمنظمات الحكومية الدولية،...) والخاصة (الشركات والافراد والمنظمات غير الحكومية،...) تربط نفسها بالعالم الافتراضي من خلال مواقع تقدم الخدمة للمستفيدين (برامج التعليمية او ادارة او خدمة او تنظيم الانتاج او تقديم استشارات او اي مجال اخر) [2].

ان الأمن السيبراني انما يعد من المجالات الحيوية التي تزايدت أهميتها في العصر الراهن بعد ان ازداد ربط مجالات الحياة المختلفة ومنها الادارية والصناعية والخدمية والمالية والتجارية رقميا، وهو ما تطلب: تخزين البيانات رقميا، ووضع انظمة ادارة وعمل للأنشطة لكي تكون المؤسسات والمصالح قادرة على تعريف نفسها رقميا، ويكون المستفيد قادر على الدخول الى الانظمة والتفاعل والحصول على الخدمة التي يرغب الوصول اليها، في ظل وجود الحواسيب وانظمة الوصول الشبكي والبرامج وانظمة حماية الأنظمة والشبكات والبيانات من الهجمات والتهديدات الإلكترونية. كل ما تقدم انما يتم شمله بإجراءات الأمن السيبراني بوصف الاخيرة انما هي مجموعة من التقنيات والإجراءات التي تهدف إلى ضمان سرية المعلومات، وسلامة المعلومات وسلامة الاجهزة والربط وسلامة استمرار الخدمة، وطالما ان بقاء الموقع الالكتروني واستمرار تقديم الخدمة واستمرار المحافظة على البيانات والاجهزة والربط الشكي انما هي مصالح، سواء كانت مصالح عامة او خاصة، وطالما ان من مهام الدولة المحافظة على تلك المصالح، باعتبارها جزء من مسؤوليتها، اذا يجب ان ترتقي اجراءات الحكومة الى ربط الامن السيبراني بالأمن الوطني، وعد الاخلال بالأمن السيبراني اخلالا بالأمن الوطني، لان استمرار السيبرانية يفيد استمرار مصالح محمية من الدولة، ومن ثم ظهور الدولة بوصفها نظام قانوني، ونظام مستقر، وتتمتع المصالح فيه بحماية، سواء كانت تلك المصالح بنية تحتية او مؤسسات صناعية او مالية او خدمية او ادارية او تعليمية او حتى سياسية، او مصالح خاصة لشركات او لأفراد[3].

ويرى البعض ان الامن السيبراني انما هو اجراءات لحماية كل من : البيانات والبرامج والحواسيب والربط الشبكي والمنفعة المتحققة من وجود البرامج والبيانات وطرق ادارة المصالح (عامة كانت او خاصة)[4].

بعبارة اخرى، ان الامن السيبراني انما هو اجراءات يتم استخدامها لضمان الحماية، ويتم تفعيلها عندما يكون هناك تحدي او تهديد للمقومات الاساسية التي يبنى عليها الامن السيبراني: تهديد البيانات، والبرامج والاجهزة والخدمة التي تطرح للمستفيدين والربط الشبكي بين الاجهزة وغيرها مما يمكن ان تستوعبه السيبرانية.

ان الهدف من وجود الامن السيبراني انما يرتبط بحماية المصالح، فالأطراف الحكومية انتقلت في ادارة الانتاج والخدمات من الادارة والخدمة المادية القائمة على الوجود المباشر، الى الادارة والانتاج الرقمي، الذي يمكن ان يحدث عن بعد، ويتم فيه تغذية الحواسيب والتلفونات الذكية، بالبيانات والبرامج المناسبة، ويتم ايجاد ربط بين تلك الحواسيب والبرامج والبيانات وبين اجهزة اخرى، ولا يتوقف الامن السيبراني على حماية البيانات او الاجهزة او البرامج او ادارة المصلحة او الانتاجية او تقديم الخدمة، انما تشمل كل ما تقدم، لان الواقع الرقمي يجب ان يماثل الواقع المادي، وحمايتهما واجب في كل الحالات، والامر نفسه ينسحب على المصالح الخاصة سواء للشركات وحتى الافراد، فالواقع المادي اخذ ينسحب ويتجه ليكون واقع رقمي او افتراضي، ويبقى المستفيدين من التعامل مع الافراد والشركات يتعاملون مع المخرجات، او الخدمة، والامن السيبراني عليه حماية ذلك الوجود. وفي كل الحالات، المصالح العامة او الخاصة فان السيبرانية انما تفيد ان المصلحة تحولت الى حالة افتراضية يتم تلمسها بالمخرجات، والبرامج تتطور وتتيح بنفس الوقت امكانية الاختراق واحداث اضرار بتلك المصالح سواء بوقف الخدمات او الاضرار بقواعد البيانات (كمعلومات او كأموال) او الاضرار بالبرامج المستخدمة، وبالنتيجة فان الاضرار يصيب المصلحة، وهنا فان من واجب الاجراءات الامنية ان تتدخل لتحمي المصلحة الموجودة عامة او شخصية. ويرتبط بما تقدم فان على الامن السيبراني ان يضمن استمرار منظومة المصالح الموجودة، وتلك المصالح اليوم تعتمد على تكنولوجيا المعلومات والتطورات الموجودة فيها، من حيث سرعة العمل والوصول للمستفيدين ان كان المشروع والمصلحة عامة وخدمية وانتاجية، او سرعة الانجاز والخزن ان كانت المصلحة شخصية تضمن السرية للمتعاملين مع تلك التكنولوجية الرقمية.

ومن اهداف الامن السيبراني هو التصدي للهجمات السيبرانية، وبعضها هجمات اجرامية واخرى هجمات سياسية واخرى هجمات تفرضها لعبة المنافسة واحيانا تأتي كأمر طارئ، وفي كل الاحوال فان على الاجراءات ان تضمن المصلحة التي تقف خلف العالم الرقمي الذي تدور حوله، من اي هجمات تحدث سواء كانت بصيغ: الفيروسات، والبرمجيات الخبيثة، وعمليات الاختراق،، والأمن السيبراني يهدف إلى منع هذه الهجمات، ويتم ذلك عن طريق استخدام تقنيات متعددة وفقا للتطور الحاصل في التكنولوجيا الرقمية، مثل: جدران الحماية، وبرامج مكافحة الفيروسات، الى جانب أنظمة الكشف عن التسلل لمراقبة ومنع الأنشطة الضارة. ويأتي هذا في اطار واجب التصدي للهجمات السيبرانية، وهذا الواجب يقع اولا على ذوو العلاقة المباشرة، سواء كدفاع من خلال منع التسلل او بصيغة الجوم وهو واجب الدولة بوصفها مسؤولة عن ضمان الامن العام والحماية لكل المصالح التي تقع على اراضيها، بما يحفظ الثقة بالدولة ومؤسساتها[5].

ان على المصالح العامة والخاصة ان تركز على موضوع الوعي ضد مخاطر التهديدات والهجمات السيبرانية، وان تعزز الوعي بأهمية الامن السيبراني، وهي الخطوات الاولى التي تقلل من مخاطر الاختراق، لان الاصل ان الهجمات موضوع مطروح، سواء وقعت الهجمات لأغراض جنائية او لأغراض سياسية او كنوع من التحدي او لأي سبب اخر، الا ان الهجمات لا تعني حصول الاختراق لان الامر يعتمد على الوعي بالهجمات ومخاطر الاختراق، وعلى الانظمة والاجراءات المعتمدة في ضمان الامن، ثم على قوة الردع الذي تكفله الدولة لحماية المصالح العامة والخاصة على اراضيها او تحت سيادتها، مهما كان مصدر الهجوم السيبراني[6].

ان موضوع اعتماد اجراءات للأمن السيبراني يماثل توفر اجراءات للدفاع في الاحوال التقليدية، وهذا الاتجاه يتطلب بناء خبرات تتناسب وحجم ونوع التحديات التي يطرحها العالم او الفضاء السيبراني، فهو اولا عالم يصعب تتبعه ظاهريا، وعالم مفتوح بلا حدود جغرافية، واحيانا يظهر افراد يربكون عمل دول، او العكس عندما تقوم دول بتتبع افراد، وفي كل الاحوال فان الامر يتوقف على حالة تنافس في الغالب تعتمد على من يقوم بتطوير برامج وتقنيات يمكن استخدامها للحماية او الهجوم، واجراءات الامن لدى الطرف الاخر، في خضم هذا الحال تبرز تحديات عدة في العصر السيبراني الذي يكاد يكون سمة لعالم اليوم، ولعل ما يعظم من حضور التحديات او التهديدات ان هناك اعتماد يتزايد على الرقمية او العالم الافتراضي في ظل تطورات التكنولوجيا الرقمية[7].

بقدر ما يوجد العالم الرقمي او الافتراضي فرص للدول بقدر ما يفرض تحديات على الدول، وعلى المصالح العامة والخاصة، لان تلك المصالح تستثمر ما متاح من تطورات في حفظ ومعالجة البيانات، وفي بناء البرامج التي تستخدم البيانات لتحقيق منفعة (الانتاج او الادارة او التنظيم او اي غرض اخر) وتستخدم البرامج اجهزة الحاسوب والتلفون، وتستخدم الربط الشبكي، وتصل الى المستفيدين الذين يستخدمون برامج وتطبيقات محددة للحصول على المنفعة، وكل ما تقدم يمكن الدخول عبره ببرامج مضادة يمكن الوصول من خلالها الى البيانات وتغييرها او سرقتها او اجراء اي تلاعب اخر بها، وهو ما يفرض تطوير تكنولوجية رقمية اخرى لزيادة الامن، والعملية هنا مستمرة، والدولة تتدخل عندما يتطلب الامر توفير مظلة اكبر من المظلة الذاتية للحماية السيبرانية.

ان العالم السيبراني اليوم عالم متطور، يزداد الاستثمار فيه الى مستويات مهمة، وهو مجال يسمح بالنمو لأنه عالم لا يوجد به حدود، وربما تتفوق فيه شركات او مجموعة مجهزون على دول، وكلما تفوق طرف على اطراف اخرى في مجال التقنيات الرقمية فانه يعرض الانظمة السيبرانية للانكشاف، ومن ثم تجد المصالح والدول نفسها امام تحديات شبه دائمة، ووجه الخطورة اليوم ان هناك تعظيم لخيار ربط كل شيء ومنه البنية التحتية والادارة والامن والتعليم والصحة والانتاج بالاتمتة وبالعالم الرقمي، واي قدرة على النفوذ لقواع البيانات والبرامج التي تستخدمها انما يفيد بقدرة المخترق على تجميد او ايقاف العمل وربما جعل المنظومة تعمل بطريقة مغايرة والى الضد من الغاية من وجودها. وربما يبرز التهديد هنا من دول او من شركات متنافسة او من افراد لدوافع مختلفة.

ويبرز تحدي اخر يتمثل في كون الغطاء التشريعي ما يزال منقوص ليواكب التغيرات في عصر التطورات التكنولوجية الرقمية[8]. فالتشريعات تحتاج الى مدة لكي يتم اقرارها في حين ان العالم الرقمي يتغير بسرعة كبيرة، والنقص التشريعي هنا يتيح فرصة للنفوذ الى المنظومات او البرامج او البيانات وسرقتها او تغييرها او اتلافها او تغيير وظائفها، للأضرار بالمستخدم او بالمستفيد.

واحد ابرز التطورات اليوم التي تعظم من امكانية حصول ضرر اكبر للتهديدات السيبرانية هو نمو استخدامات الذكاء الاصطناعي، فهذا التطور يتيح امكانية اكبر للاختراق، لأنه يمكن اكتشاف نقاط الضعف، بصورة سريعة عبر عمليات متعددة، ومن ثم هناك امكانية اكبر للاختراق ومن ثم تهديد المصالح المحية بإجراءات الامن السيبراني[9].

وهذا الامر يدفع للبحث عن موضوع اخر مهم الا وهو : العلاقة بين الأمن السيبراني والأمن الوطني، بوصف الاخير هو اجراءات تتبعها الدولة لحماية المصالح العامة والخاصة لكل ما يعد واقع ضمن سيادة الدولة، انطلاقا من مسؤولية الدولة، وطالما ان السيبرانية هي طريقة لإدارة المصالح، الحيوية منها والسيادية والخاصة، فان التعرض لتلك المصالح في العالم الافتراضي فأنها تحرك مسؤولية الدولة نفسها لتكون قادرة على حفظ تلك المصالح[10].

ان مسؤوليات الدولة واسعة، فهي تبدأ بضمان مظلة الحماية والاستقرار والسلم الداخلي، وتعزيز الرفاهية، وتعزيز المكانة، وضمان ان تكون الدولة مدافعة عن كل المصالح الواقعة ضمن نطاق السيادة، وبضمنه حماية البنية التحتية والبيانات وحماية هوية الدولة والسلم الاهلي وحماية الافراد وغيرها، وبحكم ان كل ما تقدم اتجه للسيبرانية، فان حماية تلك المصالح انما يرتبط بواجبات الدولة تجاه المصالح المختلفة الموجودة داخل الدولة.

ثانيا- واقع الأمن السيبراني في العراق

ان تحليل الوضع القائم للأمن السيبراني في العراق يوضح اولا ان العراق مستهلك للسيبرانية وليس منتج لها، فالأجهزة (الحاسوب والهواتف الذكية) والبرامج انما هي منتجات لشركات اجنبية، وهذا يعد اول السلبيات التي يعاني منها البلد.

دخل العراق في المجال السيبراني بشكل خجول ومتأخر، بعد ان اخذ العالم يتجه بسرعة الى التطبيقات السيبرانية في كل المجالات، ليتسع الفضاء السيبراني، ويضم اغلب التطبيقات الامنية والاقتصادية الصناعية والمالية والادارية والخدمية، والشخصية، في حين كانت التطبيقات في العراق محدودة، وحتى اغلب المواقع التي تم انشائها كانت عبارة عن صفحات محدودة وغير تفاعلية ولا تقدم خدمة متكاملة او انها تعطي معلومات عامة وليس عبارة عن برامج تفاعلية تقدم خدمات متكاملة للمتعاملين معها.

وتحت الضغوط في الواقع العالمي اخذت السيبرانية تفرض حضورها على كل القطاعات، واصبح لزاما على المؤسسات ايجاد ربط سيبراني وادارة سيبرانية الى جانب الواقع المادي القائم، والاشكالية هنا ان العراق اربط مباشرة بالأنترنت العالمي وليس عبر منظومة وطنية، في ظرف ان الاجهزة والبرامج والشبكة المستخدمة للأنترنت هي اجنبية وليس انتاج وطني. وهو ما يبقي موضوعات محدودة ضمن الحيز الوطني (المعلومات والخدمة والادارة) وهو ما جعل البلد في مراتب متاخرة نسبيا عالميا.

ان اهم المؤشرات التي تقيس الواقع السيبراني في العالم هي[11]:

1) المؤشر العالمي للأمن السيبراني (ITU) والذي يضم 83 مؤشر تتوزع على خمسة محاور كل منها له 20 نقطة، وهي: القانوني والتقني والتنظيمي والقدرات والتعاون ويعطى لكل محور 20 نقطة (والذي تضعه الوكالة المتخصصة في تكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة والاتحاد الدولي للاتصالات).
2) مؤشر "NCPI" هذا المؤشر يصدره مركز بيلفر للعلوم والشؤون الدولية التابع لجامعة هارفرد، وهذا المؤشر يضمّ 29 مقياسا تتجمع حول ثماني اهداف وهي (القدرة المالية، المراقبة، الاستخبارات، الى جانب كل من التجارة والدفاع ومراقبة المعلومات والتدمير)، وابرز تلك المؤشرات هي: " الهجمات الإلكترونية، وقوانين حماية البيانات، والمعايير الفنية، وحوكمة الإنترنت، والبحوث الإلكترونية، والجرائم الإلكترونية، والإنفاذ، واستخدام المعرفة المتاحة للجمهور عن القدرات الإلكترونية".

وحسب مؤشر القوة السيبرانية يقع العراق في مراتب متأخرة حسب البيانات المتاحة، فهو وقع بالمرتبة 159 عام 2017 والمرتبة 129 عاليا من مجموع 193 دولة في العام 2019 في المؤشر العالمي للأمن السيبراني ثم حصد المرتبة 107 في الاعوام 2020 والمرتبة 129 عام 2021[12]. والمرتبة 107 عام 2023 واكثر جوانب الخلل الموجودة هي المرتبة بضعف القدرات، فحسب المؤشر جاءت نقاط العراق كالاتي: " التدابير القانونية 11.2 نقطة، والتدابير الفنية 9.6 نقطة، اما التدابير التنظيمية 15.7 نقطة، في حين ان تطوير السعات والقدرات 8.3 نقطة، اما تدابير التعاون 8.1 نقطة، وبلغ مجموع نقاط العراق 53 من 100 نقطة[13].

ولإجراء تحول في العراق بما يناسب الواقع العالمي والعراقي، والتعامل مع: الدخول السريع للسيبرانية، والتعامل مع التحديات والتهديدات الموجودة، اتجه العراق الى تسريع ادخال المؤسسات والمصالح العامة بالسيبرانية، ووضع اطر وتشريعات تنظم موضوع السيبرانية وانشاء مؤسسات واقسام معنية بهذا الموضوع، وبقصد التعامل مع الوقائع الجديدة، انشا العراق عام 2017 فريق استجابة الحوادث السيبرانية، الا انه لم يعالج الاحتياجات الفعلية لقطاع السيبرانية، وتم اعداد سياسات عامة للأمن السيبراني عام 2020، وتم انشاء اول مركز للأمن السيبراني في وزارة الداخلية عام 2022، كما اصدر استراتيجية للامن السيبراني من قبل مستشارية الامن الوطني، ويمكن تتبع بعضا من تلك الاجراءات، فمثلا انشأ العراق :

1. فريق الاستجابة للحوادث السيبرانية (CERT)، للتعامل مع الرقمي العراقي السيبراني وفحص الثغرات وتقييم المواقع الحكومية من الناحية الامنية. الى جانب حماية البنية

التحتية للأنترنت والمواقع الرسمية ونشر الوعي والدعم للحماية في الفضاء السيبراني ولتعزيز ثقة المواطن بالمؤسسات الحكومية والدولة، ويعمل على الاستجابة للحوادث الامنية، وتلقي البلاغات عن الحوادث السيبرانية...[14].

2. اما في وزارة الداخلية فقد تم انشاء مركز الامن السيبراني في العام 2022، وذلك بهدف ايجاد وتعزيز الثقة في التقنيات الرقمية للوزارة وحماية البيانات من التهديدات السيبرانية والحد من اساءة استخدام تكنولوجيا المعلومات والاتصالات ومنع الاختراق[15].

ان ما تقدم يظهر ان العراق قد شرع باعتماد الاجراءات السيبرانية اي التوسع باستخدام الحواسيب والهواتف الذكية والبرامج التي تستخدم بيانات محددة وترتبط بالانترنت وتتجه الى مستخدمين محددين يطلبون خدمة محددة، سواء في المصالح العامة او الخاصة، وحدثت تطورات مهمة خلال مدة قصيرة، ومن ثم فان موقع العراق بمؤشرات الامن السيبراني يعد طبيعيا، لان البلد ليس منتجا للتقنية السيبرانية، وان البلد استمر طيلة المدة السابقة بتنفيذ الاعمال عبر الطرق التقليدية، ومن ثم فان التحول الرقمي يحتاج لكي يحقق الغاية منه الى بعض الوقت، ونجاح اجراءات الامن السيبراني يحتاج الى الاستمرارية والتطور.

ثالثا- التحديات العالمية للأمن السيبراني، ومتطلبات حماية الامن الوطني العراقي

ان تحليل الواقع القائم للأمن السيبراني في العراق، يلاحظ ان هناك نقص مركب، فاستعراض التحديات والتهديدات السيبرانية التي تواجه العراق، وهي تحديات مفتوحة، ليس بالضرورة ان ترتبط او ان تكون محلية المصدر، يلاحظ انها تتوزع على عدة مستويات[16].:

أ. التحديات التقنية: ضعف البنية التحتية والتكنولوجيا المتطورة وان هناك صعوبة في تحديث مستدام للأنظمة السيبرانية.

ب. التحديات المؤسسية: نقص التنسيق بين الجهات الحكومية والقطاع الخاص.

ج. التحديات القانونية: غياب التشريعات الحديثة المتكاملة، والعراق يحتاج الى تشريعات أكثر شمولية لحماية النظام السيبراني في البلد، والعمل على مكافحة الجرائم السيبرانية بما يتماشى مع الواقع السيبراني (تم تقديم قانون الجرائم المعلوماتية للتصويت عليه في مجلس النواب وتم قراءته قراءة اولى في تموز 2011 ولم ينتقل بعدها للقراءة الثانية).

بعبارة اخرى، ان هناك اشكالية مركبة تجعل موضوع السيبرانية في العراق موضوع حديث، وينمو الا ان هناك تحديات فيه.

ان هناك منافسة عالمية في المجال الرقمي او السيبراني بين شركات ودول عدة حول العالم، للاستفادة من مزايا هذا التحول، وهو ما يجعل كل العالم اشبه بقرية صغيرة، وهو ما نشط في الوقت نفسه فاعلين مختلفين للقيام بهجمات او اختراقات للأنظمة السيبرانية لمصالح عامة او خاصة عبر العالم لغايات مختلفة، ومنها الحصول على البيانات (معلومات او اموال او اسرار صناعية او امنية ،...) او اتلافها او استبدالها او تغيير وظيفة البرامج والمواقع التي تعمل عليها، او لاي غاية اخرى: جنائية او سياسية او مرتبطة بالمنافسة او لأي اعتبار اخر، فان من يقوم بتلك الانشطة في الاختراق والهجوم لديه طرق مختلفة، ليحقق الغاية من الهجوم.

ان الامن السيبراني يشير الى جهود واجراءات مهمة، وطالما انه يحمي مصالح مهمة، وطالما ان الامن الوطني موضوع مهم ووظيفته توفير مظلة الدولة لحماية كل ما يقع تحت حدود الدولة او تحت سيادتها، فان الارتباط بين الموضوعين مهم بل وتزداد الاهمية والتعقيد كون الامن السيبراني يستهدف المصادر المتعددة ومنها الخارجية التي تحاول احداث الضرر، ان العراق استطاع ان يتعامل مع تحديات مختلفة منذ العام 2003، الا انه اغلبها كان تهديدات صلبة وليس افتراضية او سيبرانية، ووضع التهديدات السيبرانية واجراءات الامن السيبراني ضمن اجراءات الامن الوطني موضوع مهم جدا، وهنا توجد عدة مبادئ يتوجب الاخذ بها وهي[17].:

1- وجود وعي لدى جميع القطاعات التي تستخدم السيبرانية في حفظ واستخدام البيانات وايصال الخدمة او تنفيذ اعمال وانتاج عبر هذه التقنيات لفهم المخاطر التي تهدد المنظومات السيبرانية، وكيف يمكن ان ينتهي اي هجوم او اختراق او اساءة استخدام او حفظ البيانات الى نتائج تحاكي ما يحصل على الواقع المادي.

2- في الامن السيبراني فان الجميع يتحمل المسؤولية، لان الاختراق والهجوم في العالم المادي يأتي عبر الهجوم الخارجي ليتعامل مع جوانب حماية معروفة اما في العالم الافتراضي فان الهجوم يأتي عبر الانترنت والربط الشبكي والبرامج ويحدث في حالة وجود خلل لأنظمة الحماية.

3- وينبغي ايضا فهم خصائص الانترنت باعتباره مشاركة تطوعية يعتمد على الركائز التكنولوجية الرقمية، وطالما ان المصالح يجب ان تدخل للأنترنت وتقدم خدمات سيبرانية باعتبارها افضل وسيلة لعرض المصالح وادامة الخدمات والانتاجية وبما يضمن سرعة الوصول الى المستفيدين فانه يتوجب ان يكون الامن السيبراني وبروتوكولات استخدام المواقع ضمن الاجراءات التنظيمية لأنشاء اي موقع سيبراني لأي مصلحة عامة او

خاصة، فالفضاء السيبراني انما هو فضاء تشغيل اي نقل العمل من صفته المادية الى الافتراضية لتقليل الوقت والجهد وضمان سرعة الانجاز، ويتوجب على كل مصلحة اعتبار ان الامن السيبراني للموقع والمصلحة انما يمثل اولوية قصوى للوجود والاستمرار.

4- ويتطلب ايضا بناء سياسات وأنظمة للحماية، مثل: إنشاء جدران الحماية وبرامج مكافحة الفيروسات الى جانب أنظمة كشف التسلل والوقاية منها، والعمل على وضع برامج التشفير وكلمات المرور في عمليات تسجيل الدخول. الى جانب الالتزام بمعايير مثل الابلاغ عن الهجمات والامتثال للمعايير الوطنية في الحماية السيبرانية.

ان حجم الارتباط بين الامن السيبراني والامن الوطني في عالم اليوم، كون متطلبات حماية البنية والتعاملات السيبرانية انما هي مسؤولية للدولة مثلها مثل اي تحدي مادي يصيب المصالح، ولهذا اخذ البلد يضع الامن السيبراني ضمن سياسات الامن الوطني، بعد سلسلة من الاختراقات التي تعرضت لها مواقع حكومية تقدم اما البيانات والارشادات او الخدمات الاخرى للمواطنين ومنها موقع مجلس النواب في حزيران 2016 وموقع وزارة الاتصالات في تشرين الاول 2016 وموقع المفوضية العليا المستقلة للانتخابات في شباط 2017 وغيرها[18].

واصدرت مستشارية الامن القومي في العراق استراتيجية الامن السيبراني العراقي، وتناولت الاهداف التي يتوجب على العراق تحقيقها، في ضوء الفرص والتهديدات التي تشمل هذا العالم، وتتحدث الاستراتيجية عن وجوب الاستعداد للتهديدات الامنية السيبرانية ووجود اطار تشريعي وتنظيمي وتنفيذ المعايير المعتمدة في المؤشر العالمي للسيبرانية، وان البلد يحتاج كمرحلة اولى الى معالجة المخاوف الفورية ثم بناء البنية التحتية ثم الاعتماد على الذات[19].

كما اخذ الجهد الوطني العراقي يهتم بموضوع اخر الا وهو تنظيم الجهد المؤسسي للتعامل مع الواقع السيبراني، باعتبار ان كل المؤسسات الحكومية تلتقي تحت عنوان الدولة العراقية، وان هناك مسؤوليات تقع على كل القطاعات الحكومية للعمل على تعزيز الاجراءات والحماية السيبرانية.

رابعا- تقييم السياسات والآليات المتبعة في العراق لمواجهة التهديدات السيبرانية

بعد الاشارة الى ان الامن السيبراني انا يمثل جزء مرتبط بالأمن الوطني، وان الاخير من مسؤولياته ضمان الاجراءات الكفيلة بإيصال المصالح المختلفة العامة والخاصة التي تستخدم الانترنت ان بياناتهم والاجهزة والربط الشبكي والمواقع كلها محمية مهما كان مدر التهديد والتحدي.

ان تحليل الوضع الراهن للأمن السيبراني في العراق[20] يلاحظ ان الاتجاه للسيبرانية اصبح امر ملزم على كل المصالح في ظل الارتباط بين قوة الدولة ووجوب اكمال البنية التحتية السيبرانية، وفي ظل الارتباط بين السيبرانية الوطنية والسيبرانية على النطاق العالمي، اي انه لا يمكن الابتعاد عن العالم الافتراضي العالمي[21].

الا ان الخلل المهم هو الجانب التقني لان العراق ليس منتج او مطور للمعدات والبرامج السيبرانية انما مستهلك لها، كما لا توجد منظومة انترنت وطنية داخلية لكبح مصادر التهديد الخارجي ومن ثم فان ذلك يحدث مشاكل مركبة للأمن السيبراني العراقي، فأولا من السهل على المهاجمين استهداف واختراق المنظومات الوطنية رغم كل اجراءات الامن والسلامة، وثانيا فان استمرار الارتباط بالسيبرانية انما يجعل مصالح عديدة منكشفة ويحتاج الامر الى بذل جهود لتعزيز اجراءات الامن السيبراني والعمل على تطوير معدات سيبرانية من انتاج وطني.

بهذا، فان الامر رغم انه يفتح فرص للتوسع في قطاع الاعمال والانشطة العامة والخاصة، الا ان التحديات والتهديدات تبدو كبيرة خاصة ان مصدر التهديد قد لا يكون مستخدم محلي انما قد يكون مستخدم عبر الحدود في ظل عالم مفتوح، وفي ظل تطور برامج الذكاء الاصطناعي وامكانية الاختراق للمواقع الالكترونية[22]، يبدو ان التهديد والتحدي يتعظم لإجراءات الامن السيبراني، طالما ان السيبرانية كأجهزة وبرامج وانترنت هي ليس انتاج وطني انما مستوردة، وان الدول والمنظمات والافراد المتعاطين لحالات الاختراق والهجوم السيبراني يمتلكون قدرات كبيرة.

واسباب الاختراق او الهجوم متعددة كما تم الاشارة اليه، فهي اما الحصول على المعلومات او تغيير المعلومات او اتلاف المعلومات او التأثير في الاداء، وما اسعف العراق في السنين السابقة ان المواقع الالكترونية انما كانت مواقع شكلية محدودة وليس مواقع حقيقية من حيث قيمتها السيبرانية، اما بتزايد الربط السيبراني عراقيا، فان التحدي سيزداد ويفرض على كل المصالح وعلى الدولة نفسها تسريع اجراءات وضمانات حماية قطاع السيبرانية.

وتقييم السياسات والآليات المتبعة في مواجهة التهديدات السيبرانية، يلاحظ انها ما تزال محدودة، ورغم ذلك يزداد التقدم في كل الجهود، ويحتاج البلد الى بذل الجهد في مجال التشريعات والسياسات الحكومية، وبذل الجهد في مجال تطوير الآليات والمؤسسات الحكومية، وضمان الاستجابة للحوادث السيبرانية، والاستفادة من التعاون الدولي، والتوعية والتدريب.، ووجوب تحول المؤسسات السيبرانية اي الناشطة في مجال تكنولوجيا المعلومات الى ان تكون منتجة للأجهزة والمعدات والبرامج السيبرانية. ويحتاج العراق الى انفاق الاموال ليس الى شراء بنية تكنولوجيا المعلومات انما الشروع بدعم البحث والتطوير السيبراني ليحدث انتقال حقيقي في مجال الامن السيبراني[23].

الخاتمة:

في ختام هذا البحث، فان الملاحظ ان الامن الوطني للدولة هو مفهوم شامل يبحث في كل حالة تهديد ويوفر حماية للمصالح المحمية بحكم القانون سواء كانت عامة او خاصة، فالدولة ملزمة ان تضع سياسات تضمن تحقيق الاستقرار والامن في الدولة.

ان مفهوم المصالح والاعمال اخذت بفعل التطورات في التكنولوجية الرقمية تتحول من العالم الواقعي المادي الى عالم افتراضي، ففي ظل العالم الرقمي او ما يعرف بالسيبرانية فان العالم يتحول بسرعة ليقوم بأداء نفس الاعمال بسرعة وبكفاءة اعلى وبجهد اقل، والوصول الى شريحة اكبر من المستخدمين للنشاط والمنفعة، بفعل السيبرانية، وهي ثورة في الحياة بكل اوجهها، وتتطلب معدات محدودة الا انها مهمة ومنها: اجهزة الحواسيب والتلفونات الذكية والبرامج والربط الشبكي والانترنت، وبيانات، والمحافظة على تلك البنية، انما يحتاج الى اجراءات، فلا يمكن تصور ان تقوم المصالح بالوصول الى القطاعات الانتاجية والخدمية والادارية والانتاجية المختلفة من دون ضمانات للحماية، بحكم ان الموقع الالكتروني الذي يربط بتلك المصلحة سيتفاعل ويمكن الوصول اليه في فضاء عالمي وليس ضمن فضاء محلي او محدود، وهو ما يتطلب اجراءات حماية على مستويين:

أ. المستوى الاول مرتبط بإجراءات اصحاب المصلحة، اي المؤسسات الحكومية والشركات والافراد، عبر تفعيل بروتوكولات وبرامج خاصة للحماية

ب. المستوى الثاني الاجراء الوطني الذي يضمن توفير حماية الدولة وتدخلها ان تعرضت اي مصلحة محمية للاختراق والهجوم والضرر، باعتبار ان الدولة مسؤولة عن توفير مظلة الحماية.

ان البحث في هذا الموضوع اوضح ان دخول العالم للعالم الرقمي كان متدرج ينمو كلما نمت الثورة في التكنولوجيا الرقمية، باعتبار الدول المعنية هي دول منتجة ومستهلكة في الوقت نفسه للتكنولوجيا الرقمية، وان من مصلحتها لتسريع العمل هو دخول المصالح المختلفة لهذا القطاع، لتضمن قدرة تنافسية اعلى، ورضا المستفيدين او المستخدمين بشكل اكبر، ثم اخذت الدول الاخرى تدخل في القطاع الرقمي، والعراق كان من الدول المتأخرة نسبيا في دخول العالم الرقمي، وهو ما يستلزم وجود مواقع واجهزة وبرامج تكون قادرة على اداء العمل بشكل تلقائي، في كل الاوقات، ومواقع تفاعلية، اي توفر بنية تحتية قوية في المجال الرقمي.

ان الشروع في التسيس للعالم السيبراني، انما يعين ظهور مزيد من الفرص، لان المواطن او المستفيد من الخدمات الادارية والخدمية والانتاجية ستكون رقمية اي تختزل الانتقال المادي، وبضمنه نقل الافراد والاموال، والحصول على الخدمة بغض النظر عن الوقت، هذا التحول يتطلب الى جانب البنية التحتية السيبرانية، يتطلب اتقان المعايير الفنية، والانفتاح على فرص كبيرة، تحضى بدعم من يتلقى الخدمة، الا انه سيكون امام تحدي كبير، لان نقل البيانات من طابعها الورقي (معلومات او اموال او غيرها) الى الطابع الرقمي، في ظل وجود اجهزة وبرامج مصنعة من قبل شركات اجنبية، وغياب منظومات الربط الشبكي والانترنت الوطني المغلق لتوفير حماية للبيانات والاستخدام، يفيد ان السيبرانية في العراق مفتوحة على السيبرانية العالمية، والاخيرة فيها الكثير من محترفو الجرائم السيبرانية الجنائية، او ذات الطابع السياسي او التنافسي الاقتصادي او التجاري او الصناعي او المالي، او حتى لهواة الانترنت، وهو ما سيعرض المواقع للاختراق او توفير ضمانات عالية للأمن السيبراني.

الاستنتاجات:

توصل البحث الى عدد من الاستنتاجات وهي:

1) ان الامن الوطني انما هو مسؤولية الدولة تجاه كل المصالح العامة (المؤسسات الحكومية والاموال العامة والاعمال والانشطة المختلفة التي تؤديها مؤسسات الدولة) والخاصة (شركات وافراد، وكل ما يتعلق بمعلوماتهم واموالهم وطرق تنفيذ الاعمال ووصولهم الى الغير)، وهو ما يستلزم من الدولة التدخل لحماية تلك المصالح.
2) ان كل ما تعلق بالمصالح على ارض الدولة، والواقعة ضمن سيادتها، انما يقع على الدولة عبء توفير الحماية، ومن ثم فان سياسات الامن الوطني لا تمتد للمصالح المادية فقط انما اصبح لزاما عليها ان تمتد لتغطي المصالح السيبرانية، وهو ما يلقي على الدولة

ومؤسسات الامن الوطني مسؤولية كبيرة لان التهديد والتحدي قد لا يكون قادم من بيئة داخلية، وغالبا ان مصدر التهديد والتحدي غير معلوم. والاكثر منه ان مصادر التهديد والتحدي هي مصادر لديها احترافية في مجال الاختراق والهجوم السيبراني خاصة في ظل الذكاء الاصطناعي.

3) ان الأمن السيبراني انما هو اجراءات تعتمدها المصالح المختلفة بما يحفظ لها القدرة على الوجود والاستمرار واداء العمل والتفاعل والمحافظة على البيانات. والامن السيبراني يتطلب امتلاك برامج متقدمة الى جانب الاحترازات التي تمنع تسهيل مهمة الاختراق.
4) يعاني العراق من ضعف البنية التحتية السيبرانية رغم ان لديه عدد كبير من المؤسسات التعليمية المعنية بتكنولوجيا المعلومات، فالعراق مستهلك للمعدات الرقمية او السيبرانية وليس منتجا لها، ومن ثم يستلزم منه انشاء مواقع لحفظ البيانات (معلومات واموال وبرامج لتشغيل وتوفير الخدمات المختلفة) وهو ما يطرح تساؤلات عن كيفية حفظ تلك التعاملات والبيانات والاجهزة المختلفة.
5) اتجه العراق الى تطوير بعضا من الاجراءات التي يمكن ان تؤسس لقاعدة في مجال الامن السيبراني مستقبلا، وذلك ادراكا منه ان العالم القادم هو عالم سيبراني، ويصعب انعزال المؤسسات المختلفة والافراد عن التعاملات السيبرانية.
6) يحتاج العراق الى جانب انشاء المؤسسات والمراكز المعنية بالأمن السيبراني الى مزيد من التعشيق للسيبرانية في سياسات الامن الوطني. لان الاخيرة هي المسؤولة عن الحماية والامن، وعليها ان تستوعب كل التحولات وتستفيد من الفرص المتاحة، وتتعامل مع سقف مرتفع ومفتوح من التهديدات والتحديات السيبرانية.

التوصيات:

يوصي البحث في ختامه بالاتي:

1) في ظل التحديات المتزايدة التي يواجهها العراق، بحكم الامر الواقع، في مجال الأمن السيبراني، ان من الضروري العمل على اكثر من مسار، الاول الزام كل المصالح باعتماد برامج حماية من الاختراق والهجمات السيبرانية، والزام الشركات المصنعة للأجهزة التي يستخدمها العراق ان توفر ضمانات للحماية السيبرانية في تلك الاجهزة.
2) من الضروري ان تستمل منظومة التشريعات المتعلقة بالأمن السيبراني، وان يغطي ذلك اجراءات ترتبط بحالات الاختراق من اطراف خارجية لا تخضع لسيادة الدولة، وهو ما

يستلزم عقد اتفاقيات تعاون سيبرانية وجنائية مع دول العالم ثنائية ومتعددة الاطراف لضمان التعقب لمصادر الهجوم والاختراق وردعه.

المصادر:

1- عبد القادر دندن و آخرون, العلاقات الدولية في عصر التكنولوجيات الرقمية تحولات عميقة..مسارات جديدة، عمان، مركز الكتاب الاكاديمي، 2021، ص239.
2- فارس العمارات، جرائم العصر من الرقمية إلى السيبرانية، عمان، دار الخليج للنشر والتوزيع، 2023، ص122.
3- الضوابط الاساسية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، تاريخ الدخول 23 كانون الاول 2024، على الرابط: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf
4 - علي زياد العلي، المرتكزات النظرية في السياسة الدولية، القاهرة، دار الفجر للنشر و التوزيع، 2017، ص224.
5- للتوسع ينظر:
علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، القاهرة، العربي للنشر والتوزيع، 2022، ص164-166.
6- عادل عبدالصادق، الرقمنة والمرونة السيبرانية:حالة المنطقة العربية، القاهرة، المركز العربي لأبحاث الفضاء الالكتروني، 2021، ص19.
7- فارس العمارات, ابراهيم محمد الحمامصة، الامن السيبراني (المفهوم وتحديات العصر)، عمان، دار الخليج للنشر والتوزيع، 2022، ص129.
8- سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني دراسة في ضوء احكام القانون الدولي العام، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية, المجلد 14, العدد 3 ج1، 2022، ص536.
9- أحمد عبد المجيد عبد العزيز منصور، خدعة القرن العشرين، الذكاء الاصطناعي والامن القومي، القاهرة، وزارة الاعلام - الهيئة العامة للاستعلامات اللغة:العربية، 2025، ص75.
10- مروان قبلان، واخرون، الأمن القومي العربي وتحديات الأمن الإقليمي، الدوحة، المركز العرب، ي للأبحاث ودراسة السياسات 2023، ص391.
11- ينظر بشان تلك المؤشرات:
Julia Voo, Irfan Hemani, Daniel Cassidy , National Cyber Power Index 2022, Belfer Center for Science and International Affairs Harvard Kennedy School September 2022, P: 9-12.
وكذلك: حروب المستقبل.. ما هي الدول الخمس الأقوى سيبرانيًا؟، تاريخ الدخول 22 كانون الثاني 2025، على الرابط: https://www.usawtiq.com/
12- علاء عبيس راضي الجبوري، الهجمات السيبرانية والأمن الوطني العراقي: بين المواجهة والإدارة، بغداد، مركز البيان للدراسات والتخطيط، شباط 2025، ص9.
13- ينظر:
Global Cybersecurity Index 2024 5th Edition, International Telecommunication Union, FAB 2025, IN: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

14- فريق الاستجابة للحوادث السيبرانية العراقي: CERT، تاريخ الدخول 22 تشرين الثاني 2024، على الرابط: https://cert.gov.iq/cert/
15- مركز الامن السيبراني، تاريخ الدخول 22 تشرين الثاني 2024، على الرابط: https://moi.gov.iq/?page=6295
16- مصطفى علي الطائي، تحديات النظام السيبراني في العراق،، تاريخ الدخول 22 تشرين الثاني 2024، على الرابط: https://jaredaiq.net/News/5780
17- ينظر:
Cyber Security Regulations What are Cyber Security Regulations?, fab 2025, IN: https://www.bitsight.com/glossary/cyber-security-regulations
18- يسرى ستار بيركة، الامن السيبراني واثره على الامن الوطني العراقي، مجلة المستنصرية للدراسات العربية والدولية، العدد الخاص بالندوة العلمية السنية الاولى، المجلد 10، اجامعة المستنصرية، 2024، ص2018.
كذلك: صلاح مهدي هادي، . زيد محمد علي اسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العرقية، قضايا سياسية, العدد 62، جامعة النهرين، 2020، ص279.
19- استراتيجية الامن السيبراني العراقي، تاريخ الدخول 2 كانون الاول 2024، على الرابط: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

20- هشام شبر، تنظيم الجهد المؤسساتي والوزاري المشترك إزاء الأمن السيبراني في العراق، بغداد، مركز البيان للدراسات والتخطيط، شباط 2024، ص4-6.
21- ماجد صدام سالم، الامن السيبراني العراقي واثره في قوة الدولة، مجلة العلوم التربوية والانسانية، العدد 18، الامارات العربية المتحدة، كلية الامارات للعلوم التربوية والنفسية،2022، ص75-77.
22- عادل عبد الصادق، الذكاء الاصطناعي بين الأمننة والعسكرة والحوكمة، المركز العربي لأبحاث الفضاء الالكتروني، 2023، ص40.
23- حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني ((مقاربة بين المعضلة الأمنية والمكنّة الأدائية))، المجلة الجزائرية للعلوم القانونية و السياسية، جامعة بن يوسف بن خدة الجزائر، المجلد 57، العدد 5، ديسمبر 2020، ص553-557,