# تحديات الأمن القومي العراقي الأمن السيبراني أنموذجاً

م.د. صابرين ستار جبار *

يتناول البحث موضوع تحديات الأمن القومي العراقي تحدي الأمن السيبراني انموذجاً بوصفه أحد أبرز التحديات المعاصرة التي أفرزها التطور التكنولوجي المتسارع. فمفهوم الأمن القومي لم يعد مقتصراً على الأبعاد التقليدية العسكرية، بل امتد ليشمل الفضاء السيبراني الذي أصبح ميداناً جديداً للصراعات والتهديدات، خاصة مع الاعتماد المتزايد على الأنظمة الرقمية في إدارة مؤسسات الدولة والقطاعات الحيوية.

يستهدف البحث تحليل طبيعة التحديات السيبرانية التي تواجه العراق، كالهجمات الإلكترونية، والاختراقات الأمنية، وتسريب البيانات، فضلًا عن الجرائم الإلكترونية المنظمة التي تستهدف البنى التحتية الحيوية، مع بيان أبرز التحديات التي تعيق تحقيق أمن سيبراني فعال، ومن بينها ضعف البنية التحتية الرقمية، وقصور التشريعات القانونية، وقلة الكوادر المتخصصة، إضافة إلى محدودية الوعي المجتمعي بمخاطر الفضاء السيبراني، في الوقت ذاته العمل على تحليل مدى جاهزية العراق لمواجهة مثل هذه التهديدات.

فالتهديدات السيبرانية تمثل خطراً حقيقياً على الأمن القومي العراقي، مما يستدعي تبني استراتيجية وطنية شاملة متكاملة للأمن السيبراني هدفها بناء بيئة رقمية آمنة تحمي مصالح الدولة وتضمن استقرارها في ظل التحولات الرقمية المتسارعة.

**الكلمات المفتاحية: الأمن، السيبرانية، أبعاد الأمن القومي، التحديات، استراتيجية.**

## Iraqi National Security Challenges: Cybersecurity as a Model

**Dr.M. Sabreen Satar Jabbar**

This research addresses the challenges of Iraqi national security, with cybersecurity as a model, as one of the most prominent contemporary challenges brought about by rapid technological development. The concept of national security is no longer limited to traditional military dimensions; rather, it has expanded to include cyberspace, which has become a new arena for conflicts and threats, especially with the increasing reliance on digital systems in managing state institutions and vital sectors.

The study also seeks to analyze the nature of cyber challenges facing Iraq, such as cyberattacks, security breaches, data leaks, and organized cybercrimes targeting critical infrastructure. It further highlights the main obstacles to achieving effective cybersecurity, including weak digital infrastructure, inadequate legal legislation, a shortage of specialized personnel, and limited societal awareness of cyberspace risks. At the same time, it examines Iraq's level of readiness to confront such threats.

Cyber threats represent a real danger to Iraqi national security, which necessitates the adoption of a comprehensive national cybersecurity strategy aimed at building a secure digital environment that protects the state's interests and ensures its stability amid rapid digital transformations.

**Keywords: Cybersecurity,NationalSecurity Dimensions, Challenges, Strategy.**

* كلية الحكمة الجامعة .

## المقدمة

أصبح موضوع الأمن السيبراني في العراق يمثل ضرورة ملحة مع التسارع الكبير في التطورات التكنولوجية، والاعتماد المتزايد على الأنظمة الرقمية في إدارة القطاعات الحيوية. فالأمن السيبراني مثل عنصراً أساسياً في حماية استقرار هذه القطاعات وضمان استمرارية التقدم التقني بصورة آمنة ومستدامة.

وفي هذا السياق، تبرز الحاجة إلى دراسة معمقة لمختلف التحديات التي قد تواجه العراق، سواء كانت تهديدات سيبرانية عابرة للحدود أو جرائم إلكترونية متنامية، الأمر الذي يتطلب اعتماد استراتيجيات فعالة للتصدي لها والحد من آثارها. وفي الوقت نفسه، توفر التكنولوجيا الحديثة فرصاً مهمة يمكن استثمارها لتعزيز قدرات الأمن السيبراني وتطوير آلياته.

إلى جانب تنمية الجوانب الهيكلية وتحديثة البنية التشريعية، إذ إن تحسين البنية التحتية الرقمية وتحديث القوانين المرتبطة بالأمن السيبراني يسهمان بشكل مباشر في تعزيز مستوى الحماية. فمن خلال إدراك هذه التحديات والاستفادة من الإمكانات المتاحة، يمكن للعراق أن يؤسس لبيئة رقمية أكثر أماناً، ويحقق تقدماً مستداماً في مجال الأمن السيبراني يدعم مسيرته نحو التطور التكنولوجي.

يهدف البحث إلى تحليل واقع الأمن السيبراني في العراق، وتحديد أبرز التحديات التي تعيقه، مع دراسة مدى كفاءة الأطر التشريعية والبنية التحتية القائمة. محاولاً اقتراح الحلول والتوصيات العملية التي من شأنها ان تعزز مستوى الحماية السيبرانية وتحقيق بيئة رقمية آمنة تدعم التنمية التكنولوجية المستدامة.

## اشكالية البحث

تنطلق إشكالية البحث من تساؤل مفاده مدى قدرة البتى التحتية على مواجهة التحدي السيبراني للأمن والتصدي له، ليتفرع من ذلك أسئلة تتسائل عن قدرة التشريعات القانونية في حماية الفضاء السيبراني؟ وهل بالأمكان تحقيق التوازن بين الأمن السيبراني وحماية الحقوق والحريات؟

## فرضية البحث

يفترض البحث أن تعزيز الأمن السيبراني في العراق يعتمد بشكل أساسي على تطوير البنية التحتية الرقمية وتحديث الأطر التشريعية، وأن أي قصور في هذين الجانبين يؤدي إلى زيادة قابلية التعرض للتهديدات والهجمات الإلكترونية.

## منهجية البحث

اعتمد البحث على المنهج الوصفي التحليلي بعده منهجاً رئيساً لوصف واقع التحديات وتحليل أثرها مع الاستعانة بالمنهج الاستقرائي والاستنباطي بغية الوصول إلى النتائج المرجوة.

## المبحث الأول: ماهية الأمن القومي العراقي وأبعاده

يعد الأمن القومي من المفاهيم المهمة والرئيسة التي تعكس قدرة الدولة على حماية كيانها وضمان استقرارها في مختلف الظروف. ويشمل هذا المفهوم مجموعة من الأبعاد المتداخلة التي تهدف إلى مواجهة التحديات وتحقيق التوازن بين متطلبات الأمن والتنمية، لذا سنحاول في ثنايا هذا المبحث بيان ماهية الأمن وما ابعاده.

### المطلب الأول: ماهية الأمن(*) القومي

ان انتشار واستخدام مصطلح الأمن القومي يعود إلى ما بعد الحرب العالمية الثانية، أما جذوره فتعود إلى القرن السابع عشر بعقد معاهدة وستفاليا عام 1648، التي أسست لولادة الدولة القومية أو الدولة – الأمة "State–Nation". غير إن محاولات صياغة مداخل نظرية ومقاربات منهجية وبنى مؤسساتية تتبنى هذا المفهوم أي الأمن القومي فتعود إلى حقبة الحرب الباردة التي شكلت الإطار والمناخ الذي تحركت فيه تلك المحاولات [1].

فظروف الحرب الباردة دعت الولايات المتحدة الأميركية لتكون سباقه في الاهتمام بشأن الأمن القومي، إذ أصدرت

عام 1947 قانون "الأمن القومي"، والذي تأسس بمقتضاه "مجلس الأمن القومي"، واستحدث على أثره منصب مستشار الأمن القومي [2] ليصبح بعدها تعبير الأمن القومي متداولًا في الخطابات السياسية متضمنًا مصالح وأهداف الولايات المتحدة الأميركية العسكرية، والسياسية، والاقتصادية، على الصعيدين الداخلي والخارجي[3]

ونتيجة لتعدد الزوايا والرؤى التي ينظر بها إلى هذا المصطلح تعددت الرؤى الفكرية والاكاديمية لتعريفه، لكن في الإجمال يمكن تقسيمها إلى اتجاهين رئيسين، أولهما الاتجاه الضيق الذي اقتصر تعريفه للأمن القومي على الجانب العسكري فقط، إذ عرفت دائرة المعارف البريطانية الأمن القومي بأنه "حماية الأمة من خطر القهر على يد قوة أجنبية". [4]

وعرف (هانز مورغنثاو) الأمن القومي بأنه يساهم في حماية وحدة الإقليم الوطني ومؤسساته". وثانيهما الاتجاه الواسع، الذي شمل جوانب واهتمامات متعددة سياسية واقتصادية وعسكرية وثقافية وتنموية تحمل قيم وأهداف ومصالح الدول والمجتمعات، فعرف ارنولد وولفرز الأمن القومي إذ رأى بأنه "موضوعياً يرتبط بغياب التهديدات ضد القيم المركزية والمكتسبة، أما ذاتيا، فهو غياب الخوف من أن تكون تلك القيم موضع هجوم". [5]

وعلى صعيد النظام الدولي فالأمن القومي يعني " قدرة الدول والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي يرونها معادية. فالحد الأدنى للأمن هو البقاء، لكنه أيضا إلى حد معقول سلسلة من الاهتمامات الجوهرية حول شروط حماية هذا الوجود". [6]

وعلى صعيد المفكرين العرب عرف أمين هويدي الأمن القومي بأنه "الإجراءات التي تتخذها الدولة في حدود طاقتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة التغيير الدولي". [7] وكذلك تعريف (علي الدين هلال) للأمن القومي بأنه "تأمين كيان الدولة والمجتمع ضد الأخطار التي تحددها داخليا وخارجيا، وتأمين مصالحها وتهيئة الظروف المناسبة اقتصاديا واجتماعيا لتحقيق الأهداف والغايات التي تعبر عن الرضا العام في المجتمع". [8]

في حين جاء تعريف علي عباس مراد شاملا للمفهوم ومستوعبا لجميع مضامينه الآنية والمستقبلية، ومعبر عن أهدافه، وهذا ما اتفق معه الباحث، إذ عرف الأمن القومي بأنه "جملة المبادئ والقيم النظرية والأهداف الوظيفية، والسياسات العملية المتعلقة بتأمين وجود الدولة وسلامة أركانها، ومقومات استمرارها واستقرارها، وتلبية احتياجاتها، وضمان قيمها ومصالحها الحيوية، وحمايتها من الأخطار القائمة والمحتملة داخليا وخارجيا مع مراعاة المتغيرات البيئية الداخلية والإقليمية والدولية".[9]

لذلك فان الأمن القومي هو عملية حماية كيان الدولة من جهة، وتحقيق أهدافها ومصالحها من جهة أخرى له أربع متغيرات مستقلة بذاتها نظريًا، وتابعة لكونها إجراءات عملية مترابطة من برنامج بناء الدولة وقوة المجتمع، وهي:(العوامل الشخصية، العوامل التنظيمية، البيئة الداخلية، البيئة الخارجية،). [10]

وعلى أساس ما تقدم، لم يعد يقتصر مفهوم الأمن القومي ونطاق تدخله على مجال محدد دون مجال آخر، وجاء هذا نتيجة تعدد أداور الدولة وتفاعلاتها الداخلية منها والخارجية هذا من جهة، ونتيجة مدركات واهتمامات وأبعاد الأمن القومي ذاتها من جهة أخرى، والذي يسعى إلى تحقيق أهداف الدولة ومصالحها الحيوية، وبما إن هذه الأهداف والمصالح غير مقتصرة على مجال محدد، وإنما هي شاملة ومتعددة، كذلك فان الأمن القومي شامل ومتعدد.

وعليه فان الأمن القومي مفهوم مركب من اجتماع وتفاعل المصالح والأهداف والقيم والمبادئ النظرية العامة والثابتة،

والمواقف والسياسات والاستراتيجيات العلمية الخاصة والمتغيرة، ونتاج عن محصلة انجازاتهما، فالأمن القومي يشمل في طار ركنيه النظري والتطبيقي كل أوجه الحياة الإنسانية الطبيعية والاجتماعية، وكل نشاطاتها العسكرية، والاقتصادية، والسياسية، والثقافية، والعملية والتربوية .... الخ [11]

## المطلب الثاني: أبعاد الأمن القومي

لم يعد الأمن القومي يقتصر على بعد أو مجال واحد بعينه، سواء على البعد النظري أو البعد التطبيقي، بل تعددت مجالاته وأبعاده، وجاء ذلك لسببين رئيسيين، أولهما: اتساع نطاق الدراسات الأمنية بما يشمل جميع المجالات والنشاطات الإنسانية. وثانيا: تعدد وظائف الدولة ذاتها التي لم تعد تقتصر على مجال محددة بذاتها [12] لتكون أهم تلك الأبعاد هي:

1. البعد السياسي: في هذا البعد تهدف الدول إلى تعريف الأمن واستعمالاته بالشكل الذي يحتوي أهداف سياسية كبرى كحماية الكيان وصيانة المصالح الحيوية من التدخلات الخارجية وحتى من التدخلات الداخلية ليصبح الأمن القومي هو المدخل الرئيس الذي تتوقف عليه مخرجات السياسة الخارجية للدول. [13] ويرتبط بالبعد السياسي الأمن السياسي، والذي يعرف بأنه الجهود المبذولة في المحافظة على أسرار الدولة وسلامتها، والعمل على منع ما من شأنه إفساد العلاقة بين السلطة والشعب، أو تشويه صورة الدولة. [14]

2. البعد العسكري: يمثله الأمن العسكري، والذي يعد البعد الأكثر وضوحا لمفهوم الأمن القومي. فالأمن العسكري فرع من أفرع الأمن القومي، فالقوات المسلحة تمثل الدرع الواقي للدولة، وأهم عناصر قوتها، وهي وسيلة الحسم في أي صراع عندما تفشل الأدوات الأخرى. [15]

3. البعد الاقتصادي: يهدف هذا البعد إلى توفير الأوضاع الملائمة للوفاء باحتياجات الشعب، وتوفير سبل التقدم والرفاه [16] أي القيام على درجة مقبولة من الاستقلال الاقتصادي، ونجاح التنمية الاقتصادية المستقلة، والاعتماد على النفس، وفي حالة العلاقات الاقتصادية الدولية يمكن أن يكون الاعتماد المتبادل وليس التبعية الاقتصادية. [17]

4. البعد الاجتماعي: ويهدف إلى تطوير الأمن بالقدر الذي يعزز الشعور بالانتماء والولاء وتعزيز الهوية الوطنية. [18] وبذلك يمثل هذا البعد الحالة التي يكون فيها المجتمع متماسكا، وخاليا من كل مظاهر التردي [19]

5. البعد الثقافي – الأيديولوجي: أي القدرة في الحفاظ على الأنساق العقائدية، وتأمين الفكر والعادات والتقاليد والقيم من الثقافات الدخيلة أو الفاسدة. [20] وعليه فان هذا البعد يعبر عن قدرة الدولة، أو الأمة في الحفاظ على ثقافتها وتراثها، وأنماط السلوك، والاستهلاك، واللغة، والاعتزاز بالتاريخ، إلى غير ذلك [21]

6. البعد البيئي: ويتمثل بتوفير الأمان ضد التهديدات ومخاطر البيئة، ولاسيما التلوث البيئي والذي يمكن أن ينعكس سلبا على الأمن. [22]

## المطلب الثالث: التحديات التي تواجه الأمن القومي العراقي

تتمثل التحديات بمقدار المصاعب التي تواجه الدولة وتؤثر على مستوى تقدمها على الصعد كافة وعلى صعيد العراق يمكن تحديد التحديات التي تواجه أمنه القومي بما يلي:

1- التحدي الجيوبولتكي: والذي مثل تحدي مستمر وعلى وتير متذبذب فمنذ تأسيس العراق دولته الحديثة عاش في وضع جيوسياسي غير مستقر سببه الافتقار إلى الغمق الاستراتيجي والجغرافي.

2- التحدي الفكري والثقافي: عانى العراق من وجود رؤى فكرية لهوية وطنية جامعة لها القدرة على الاستمرار والبقاء إذ تصارعت على أرضه التيارات الفكرية المختلفة.

3- التحدي السياسي: العملية السياسية العراقية لم تنتج دولة قوية، كما ان نظامه الديمقراطي لا يزال في مرحلة التحول الأمر الذي حد من استعادة دوره الريادي.

4- التحدي الاجتماعي: إذ أسهم دستور العراق وتقاليد واعراف العملية السياسية في اضعاف الاندماج المجتمعي في التركيبة الاثنية العراقية، والذي صدح عوضًا عنه مفهوم المكون، والهويات الفرعية، والحركات المتطرفة، وتراجع بعض القيم المجتمعية الإيجابية [23]

5- التحدي الاقتصادي والمالي: الاقتصاد الريعي مع عمليات الفساد والجريمة المنظمة بما فيها غسيل الأموال وما شابه الوضع الاقتصادي العراقي من عمليات اختلاس كبرى جلها مثلت معوقات أمام بناء راسمالية وطنية.

6- التحدي السيبراني: مع التطورات التكنولوجية المتسارعة شكلت التهديدات السيبرانية بما تتضمنه من حروب الكترونية واختراقات وجريمة الكترونية وغيرها شكلت تهديدات كبرى للأمن القومي للدول لا سيمّا الدول التي تعاني من الضعف في البنى التحتية والفوقية.

## المبحث الثاني: السيبرانية ماهيتها وأهميتها للأمن القومي العراقي

ان التحديات السيبرانية من أفرازت التطورات التكنولوجية المتسارعة والخطرة التي تواجه الأمن القومي العراقي في العصر الرقمي، الأمر يستلزم البحث في ماهية السيبرانية وآليات مواجهة تحدياتها وهذا ما سيتم بحثه فيما يلي.

### المطلب الأول: ماهية السيبرانية والمفاهيم المقاربة لها

#### أولاً: ماهية السيبرانية

ان مصطلح السيبرانية اشتقت من لفظة سيبر cyber اليونانية الأصل، وقد اشتقت من كلمة kybernetes، بمعنى (الشخص الذي يدير دفة السفينة)، وقد تستخدم مجازاً لتعبر عن المتحكم[24] فهناك ايضاً من يرجع أصلها إلى منتصف القرن العشرين لعالم الرياضيات الأمريكي NorbertWiener، حيث استخدمها للتعبير عن التحكم الآلي[25] وهذا يعني أن مصطلح سيبر يعني الفضاء الالكتروني أو الفضاء السيبراني، أذ ظهر مع ظهور الانترنت، وقد ظهر حديثا بمعنى: مجمل القوانين السياسية، الأدوات، النصوص المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجية المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص[26]

هنالك العديد من التعاريف حول مصطلح الأمن السيبراني فهناك من يعرفه على أنه "أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والاجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات والحد من آثارها[27] ووفقاً لدراسة الاتحاد الدولي للاتصالات فإن الأمن السيبراني هو عبارة عن مجموعة من المهام مثل تجميع وسائل وأدوات وسياسات وإجراءات أمنية ومبادئ توجيهية وإرشادات وطرق إدارة المخاطر والتدريب وأفضل الممارسات والاستراتيجيات الأمنية ويمكن استخدامه لحماية البيئة السيبرانية والمؤسسات والمستخدمين[28] ويمكن تعريف الأمن السيبراني انطلاقاً من أهدافه ، بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية للدولة المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والاضرار ، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج، وكذلك لا تتحول الاضرار الى خسائر مستمرة[29] ويعرفه ريتشارد " Richard "كمرر بأنه " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة[30]

ومن الناحية الاجرائية يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات واجهزة الكمبيوتر في الفضاء السيبراني من مختلف التهديدات والهجمات والاختراقات التي تهدد الأمن القومي للدولة نفسها[31] وعليه يمكن تعريف الأمن السيبراني بأنه كل جهد يبذل على الصعيد القطاع الحكومي أو الخاص من أجل حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، أذ يشمل ذلك تحديد وتقييم المخاطر والتهديدات المحتملة، واتخاذ الإجراءات.

**ثانياً: المفاهيم المقاربة للسبرانية**

نتيجة أتساع مفهوم الأمن السيبراني وذلك بسبب التقدم الكبير في التكنلوجيا والتقنيات الحديثة وبعد انتهاء الحرب الباردة في مطلع تسعينيات القرن العشرين ظهرت عدة مفاهيم أخرى مقاربة منها على سبيل المثال كالآتي:

1- الفضاء السيبراني: ويفهم بأنه بيئة تفاعلية حديثة مادية ومعنوية تتكون من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات ويطلق عليها الذراع الرابعة للجيوش الحديثة، وقد أصبح ساحة لنقل الصراعات وتصفية الخلافات بكل أنواعها بين أطراف الصراع كافة[32]

2- **الحرب الافتراضية:** وتشمل الهجمات السيبرانية الهجمات على الأنظمة الحاسوبية، والتجسس الإلكتروني، والتلاعب في البيانات، وانتشار البرامج الضارة، والحملات الإعلامية الإلكترونية[33] فهي وسائل واساليب القتال التي تدور في الفضاء الالكتروني وفي بعض الاحيان ترتقي الى مستوى النزاع المسلح الذي يتعلق بالتطبيقات العسكرية للفضاء السيبراني[34]

3- **الجريمة السيبرانية:** هي الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراءاً بذلك، ولا تشمل فقط الجرائم التي ترتكب عن طريق الكمبيوتر ، بل تشمل أيضاً أية جريمة تتضمن استخدام أو استهداف الكمبيوتر[35]

4- **الإرهاب السيبراني:** استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة كالطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين وتخريبياً، لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب [36]

في العراق لا يقتصر الارهاب السيبراني على صورة واحدة ومعينة، فهو يبدأ من الجرائم الالكترونية باستخدام الانترنيت كنوافذ للتخطيط والتنفيذ وصولاً الى جرائم الاتجار بالبشر، ثم تجارة المخدرات وحتى الى ارتكاب الجريمة المنظمة والقرصنة الالكترونية وانتحال صفة عن الأشخاص، وجرائم الاحتيال المالي إضافة إلى تزوير البيانات، وهي من الجرائم السيبرانية الأكثر انتشاراً داخل العراق[37] وقد تعددت مخاطر الإرهاب السيبراني على الاقتصاد القومي منها ما يمكن التنبؤ بها وأخرى لا يمكن التنبؤ بها مثل عمليات غسل الأموال القانونية وإيجاد الجرائم المالية عبر الإنترنت وسرقة الأصول الفكرية .. الخ، كل هذه العمليات لها أثر اقتصادي قد يكون كفيلاً بتدمير أي دولة[38]

5- الفضاء السيبراني: ويعرف بأنه الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم، وعليه فإن الفضاء السيبراني هو الفضاء الافتراضي الذي يستخدم الالكترونيات والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل المعلومات عن طريق استخدام النظام الشبكي والبنية المادية المعنية[39] [40]

## المطلب الثاني: أهمية الأمن السيبراني

تبرز الأهمية الأسمى للأمن السيبراني بالقدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي،

وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية[41]

لقد أصبحت للمعلوماتية حضور في تأسيس سمة هذا العصر المتغير وسط تسيد تقنية المعلومات والاتصالات، وتستهدف تحقيق متغيرات سريعة على صعيد بناء المستقبل، وتتأثر قيادات الدولة ومفاصلها المختلفة، وبضمنها المؤسسات الأمنية بهذه الآلية الجديدة ومتغيراتها اللاحقة، مما يتطلب الأمر في هذه الحالة التدقيق في ماهية هذه المعلومات، ومدى دقتها وشموليتها وعلاقتها بالمواقف التي تستدعي اتخاذ القرار بشأنها.

## المطلب الثالث: العلاقة بين الأمن القومي والأمن السيبراني

أصبح الأمن الوطني لأية دولة وثيق الصلة بتكنولوجيا المعلومات والاتصال بحكم قدرتها في التأثير في أي مجتمع، إذ لها دور في توجيه الرأي العام وتعبئة الشارع وخير مثال على ذلك ما تعرضت له البلدان العربية منذ العام 2011 التي تأثرت بما يسمى (الربيع العربي) [42] علمًا ان هناك مجمعاً صناعياً الكترونياً آخذاً في الظهور، تماماً مثل المجمع الصناعي العسكري في الحرب الباردة[43]

كما اصبح الاقتصاد الرقمي والمجتمع الأكثر تقدماً في أي بلد يكون أكثر عرضة للتهديدات السيبرانية، وهذا يتطلب من الدول ذات الاقتصاد الرقمي والبنية التحتية الرقمية المتقدمة إيلاء المزيد من الاهتمام لحماية الفضاء السيبراني، لا سيما بعدما أصبح الأمن السيبراني مشكلة أمنية وطنية وجزءاً لا يتجزأ من منظومة الأمن الوطني لأية دولة، بل يجب أن تبنى استراتيجية الأمن الوطني السيبراني على استراتيجية الأمن الوطني، وتحتاج الدول إلى استراتيجيات مرنة وديناميكية للأمن السيبراني حتى تستطيع الرد على التهديدات السيبرانية، لاسيما وان الفضاء السيبراني دائم التغير والتطور وليس له حدود مادية، وهذا بدوره يفرض مسألة لا تخلو من الحساسية ألا وهي حماية البيانات مقابل مشاركة المعلومات، فالمواطنين لديهم حق مشروع في العيش في مجتمع مفتوح يتمتع بالتدفق الحر للمعلومات، وفي المقابل فإن الحكومات من واجبها حماية هذه المعلومات حفاظًا على الأمن والنظام العام، فمكافحة جرائم الإنترنت والحرب على الارهاب وغيرها تتطلب تبادل المعلومات وتفاعل يومي بين المواطنين والحكومة كونها أصبحت من الضرورات المعاصرة للأمن الوطني، ويمكن تقسيم الاستراتيجية الوطنية للأمن السيبراني على خمسة اقسام رئيسة وهي العسكرية أي الحرب السيبرانية، والجرائم السيبرانية، وحماية البنية التحتية الحيوية وادارة الأزمات والدبلوماسية السيبرانية، كما ان الدول تصوغ استراتيجية امنها السيبراني بشكل مستقل بناءً على أفكارها وتصوراتها الأمنية[44]

وعليه فإن التطورات المعاصرة فرضت نفسها على دول العالم ضرورة تبني استراتيجية وطنية للأمن السيبراني على ان يراعى فيها التوازن بين متطلبات الأمن الاساسية وبين احترام خصوصية المواطنين وطبيعة الثقافة السائدة في البلد، علمًا ان هذه الاستراتيجية لا بد ان تكون ذات نهج شمولي أي لا تقتصر على الحكومة فحسب، بل من الضروري اشراك جميع أصحاب المصلحة وهم: الحكومة والقضاء والاجهزة الامنية والمسؤولين عن البنية التحتية للأمن السيبراني من القطاع العام والخاص، ومجهزي خدمة الانترنت وتكنولوجيا

المعلومات، والمؤسسات التعليمية المختصة والمواطنين، فضلاً عن الهيئات الاقليمية والدولية المعنية بمجال الأمن السيبراني[45]

ومن اجل ضمان فاعلية ونجاح الاستراتيجية الوطنية للأمن السيبراني لا بد من توفر مجموعة من العناصر الاساسية لها ولعل أهمها: ضمان أعلى مستوى من التأييد والدعم الرسمي لها ماديًا ومعنويًا من قبل الحكومة، وتشكيل هيأة مختصة بالأمن السيبراني، وإشراك الهيئات الحكومية المعنية وضمان التعاون والتنسيق فيما بينها واشراك أصحاب المصلحة الآخرين لاسيما القطاع الخاص الموثوق بهم لضمان عمل البنى التحتية الأساسية للأمن السيبراني، وتخصيص موارد لها في ميزانية الدولة الوطنية وضرورة ان تتضمن الاستراتيجية خططاً قابلة للتنفيذ وأهداف قصيرة ومتوسطة وبعيدة المدى تسعى إلى تحقيقها، والإدارة الجيدة لمخاطر التهديدات السيبرانية لضمان استمرارية عمل هذه الاستراتيجية، ووضع خطة طوارئ لإدارة أزمات الأمن السيبراني، وتعزيز تبادل المعلومات بين القطاع الحكومي والخاص، وإجراء عمليات محاكاة وتدريبات عملية للأمن السيبراني، فضلاً عن تدريب كوادر مختصة وتنمية مهاراتهم، وتشجيع الابتكار والبحث والتطوير، ووضع قوانين واضحة تحد من الانشطة السيبرانية المحظورة معززة بقدرات تنفيذية تحد من الجريمة السيبرانية ومواءمة الاستراتيجية الوطنية للأمن السيبراني بخطط واستراتيجيات الأمن السيبراني الإقليمية والدولية[46]

وقد اكتسبت الصراعات السياسية والعسكرية والاقتصادية بين الدول بعدًا الكترونيا بحيث يصعب التنبؤ بحجمها وتأثيرها، بل ان الحروب التي تدور رحاها في الفضاء السيبراني أكثر أهمية من الأحداث التي تجري على أرض الواقع، ذلك ان الانجازات المذهلة للتجسس السيبراني اظهرت المكاسب الكبيرة لعمليات اختراق اجهزة الكومبيوتر مقارنة بارتفاع اشكال التجسس التقليدية التي تتطلب ذكاء بشري وارتفاع نسبة الخطورة، مما جعل التجسس السيبراني على الساحة العالمية مصدر قلق للدول على امنها الوطني، فالهجوم السيبراني ليس غاية في حد ذاته ولكنه وسيلة قوية لمجموعة متنوعة من الغايات من الدعاية إلى التجسس، ومن تعطيل الخدمات إلى تدمير البنية التحتية الحيوية [47]

وعليه فإن الأمن السيبراني يعد مشكلة للفرد والمجتمع على حدٍ سواء، ويتعين معالجتها من قبل السياسيين كونها امن وطني بالمقام الأول، إذ يتفق جميع السياسيين على أن الأمن السيبراني أمر مهم وينظرون إليه كمسألة تكنولوجية تحتاج إلى حل بشكل عام، فهو أكبر من مجرد مشكلة تكنولوجية ذلك أن القيم السياسية للدولة هي المقصودة في اي هجوم سيبراني، إذ ينظر إلى الجريمة السيبرانية على أنها تهديد محتمل في كل مكان، وسيترتب عليها تأثير مدمر على الحياة، وفي حالة عدم وضع حد لها ستكون المخاطر كبيرة، علمًا ان هناك مشكلة يجب ان تؤخذ بنظر الاعتبار ألا وهي ان عدم وضوح المجرم في الغالب سيعقد من صياغة الأمن السيبراني بطريقة فعالة، ذلك ان الهجوم السيبراني سيعده البعض عملاً شريراً او ارهابيا في حين يعده البعض الآخر بأنه عملا بطولياً اعتمادًا على وجهة النظر[48]

ولذلك أصبح الأمن السيبراني أكثر أهمية في أذهان صانعي القرار في الدول، ولهذا تم وضع عقائد متعلقة بالأمن السيبراني في جميع دول العالم تقريبا، ولكن واقع الحال يؤكد بأنه لا تزال هناك فجوة واضحة بين الدول من حيث الوعي، والفهم والمعرفة والقدرة، أخيرًا على نشر الاستراتيجيات والقدرات والبرامج المناسبة لضمان الاستخدام الأمن، والملائم لتكنولوجيا المعلومات والاتصالات كعوامل تضمن الأمن وتحقق التنمية الاقتصادية[49]

ومن الجدير بالذكر ان الدول المعتمدة على البنية التحتية للمعلومات والاتصالات يمكن لأي هجوم سيبراني ان يؤثر في طبيعة عمل مجتمعاتها، ولهذا يوصف الأمن السيبراني بأنه "حجر الزاوية لمجتمع المعلومات"، وعليه فانه يتطلب تخطيطا استراتيجياً متماسكاً ومفصلاً وتنظيماً قانونياً مناسباً، وقد أخذت الدول تتبنى استراتيجيات وطنية للأمن السيبراني خاصة بها اعتباراً من العام 2011، وتختلف الاستراتيجيات الوطنية للأمن السيبراني في كل دولة على حدة من حيث المحتوى والشكل والتنفيذ وغيرها، فلا يوجد حالياً إطار وطني موحد لحماية الأمن السيبراني، ومع ذلك فإن وجود مثل هذه الاستراتيجيات وتنفيذها بشكل صحيح يمكن أن يساعد في حماية الأمن الوطني لأية دولة كما يضمن التطور السليم للمجتمع، ويمكن أن تساعد الاستراتيجية الوطنية الفعالة للأمن السيبراني في حل النزاعات بين الدول وضمان السلام، وفي هذا الخصوص صرح (ينس ستولتنبرغ الأمين العام لحلف الناتو بان الانترنت أصبح الآن جزءًا أساسيًا من جميع الأزمات والصراعات تقريباً[50]

وتتباين الهجمات السيبرانية من حيث التأثير والحجم، إذ يستطيع أي هجوم ناجح على بعض مكونات البنية التحتية الحيوية أن يكون له تأثيرات كبيرة على الأمن الوطني والاقتصاد ومعيشة وسلامة المواطنين، إلا أنه من الصعب قياس التأثيرات الاقتصادية، إذ تختلف تقديرات تلك التأثيرات على نطاق واسع، ويرى بعض المختصين ان التكاليف تزداد بشكل كبير لا سيما مع التوسع المستمر في البنية التحتية لتكنولوجيا المعلومات والاتصالات، ولكن عمومًا تُعد باهظة[51] وتشير بعض التقارير ان الخسائر العالمية المقدرة من جرائم الإنترنت تتجاوز (400) مليار دولار أمريكي في السنة هذا الواقع دفع بالرئيس الامريكي حينها (باراك اوباما) إلى وصف الأمن السيبراني بأنه واحد من أخطر تحديات الأمن الاقتصادي والوطني التي نواجهها وتزداد تكلفة الجريمة السيبرانية بالارتفاع مع زيادة عدد الهجمات السيبرانية، وتقسم جرائم الهجمات السيبرانية إلى أربعة اقسام رئيسة هي تعطيل الأعمال، وفقدان المعلومات، وخسارة الإيرادات، وتلف المعدات[52]

ان الإنفاق العالمي على أمن المعلومات بلغ أكثر من (114) مليار دولار في العام 2018 بزيادة قدرها (4,12 % عن العام 2017، وارتفع إلى (124) مليار دولار في العام 2019 أي بزيادة تقدر بـ(7,8)[53]

وبناءً على المؤشرات السابقة صنف تقرير المخاطر العالمية للعام 2020 حرب الجيل الخامس بانها أعلى الحروب خطرًا في العام 2020، بعد ان أثرت الهجمات السيبرانية على مدن بأكملها وشملت القطاعين العام والخاص على حدٍ سواء، وما زاد من خطورتها صعوبة كشفها وملاحقتها[54]

مما تقدم يتضح بان الأمن السيبراني أصبح وثيق الصلة بالأمن الوطني لأية دولة، وتزداد الخطورة كلما زاد اعتماد الدولة على تقنية المعلومات وارتباطها بالفضاء السيبراني، ذلك ان الهجمات السيبرانية يمكن لها ان تقوض الأمن الوطني، فأية فجوة تقنية ستؤدي إلى خسائر كبيرة للدولة في مؤسساتها الرسمية ولمواطنيها، بل انه يعرض هيبة الدولة وسمعتها الدولية إلى الخطر، إذ لا تقف هذه الخسائر عند الجانب المادي فحسب بل ستؤثر مباشرة ايضا على الجانب المعنوي إذ ستلحق ضررا في نفسية المواطنين وقادتهم، كونه يولد قناعة عامة بضعف قدرة الدولة على حماية المواطنين ومؤسساتها، وعليه يمكن القول ان الأمن السيبراني يعد قضية أمنية وطنية ضرورية يجب فهمها بعناية وشمولية.

## المبحث الثالث: الأمن الوطني العراقي في ظل تحديات الأمن السبراني

أصبح الأمن الوطني العراقي مرتبطًا بشكل متزايد بمستوى الحماية في الفضاء السيبراني، في ظل تصاعد الهجمات

الإلكترونية وتطور أساليبها. الأمر الذي يفرض ضرورة تعزيز القدرات الوطنية لمواجهة هذه التهديدات وحماية استقرار الدولة ومؤسساتها، وهو ما سيتم بحثه في ثنايا هذا المبحث.

## المطلب الأول: تحديات الامن السيبراني في العراق

إن ثورة المعلومات، والتكنولوجيا في العالم، تفرض علينا أن نتحرك بسرعة وفاعلية، لنلحق بركب هذه الثورة، لأن من يفقد في هذا السباق العلمي والمعلوماتي مكانته، لن يفقد فحسب صدارته، ولكنه يفقد قبل ذلك إرادته[55].

وتساعد المعلومات الأمنية المختلفة على تهيئة القيادة السياسية العليا في أي دولة لاتخاذ القرارات السليمة لإدارة نظامها السياسي، وحماية مصالحها الوطنية والقومية، وهذا يعني بالضرورة العمل على إيجاد مؤسسات تعتمد على المعلومات وتقنياتها المتطورة في رفد المؤسسة الحاكمة بالخطط والقرارات الأكثر حكمة.

إن وجود تقنية متقدمة لدى الدولة تتطلب فريقا متخصصًا لاستغلالها، إن تقنية الأمن السيبراني تشكل وبقدر كبير جداً مفاتيح الحل للنجاح والتصدي لجميع مشاكل الدولة ولان الأجهزة الأمنية تعتمد وبشكل كبير على المعلومات الواردة لها وعلى دقتها فان ذلك يقتضي تفعيل دور نظم المعلومات واستغلال التكنولوجيا بشكل كامل يتجاوب مع المتغيرات التي أفرزتها أشكال متنوعة من الأزمات والتي أصبحت تمثل تحديا لزعزعة الاستقرار في منطقة الشرق الأوسط[56]. ويحاجج الكثيرون من المحللين بأن الحروب في العقد الثالث من القرن الحادي والعشرين، لن تكون حروبا بالمفهوم الكلاسيكي، إذ تتقاتل الجيوش على الأرض وفي البحر أو الجو، وإن كانت هذه واردة وبقوة، إلا أن أحد أوجه الحروب المعاصرة الشديدة الوقع، هي الحروب الاقتصادية، ومن هنا تتأتى قضية الاختراقات السيبرانية من أجل الحصول على المعلومات الاقتصادية، سواء تلك التي تتعلق بالشركات أو الأفراد، وحتى المؤسسات الاقتصادية الكبرى في الدول ، فالعالم يشهد زيادة في أنواع المنصات التي قد تستخدم للاعتداء الإلكتروني ومنها السيارات، وطائرات الدرون، والأقمار الصناعية ، ومكونات الأجهزة الإلكترونية، وسيكون أمام تشويش متزايد يعتمده لاعبون محنكون من خلال إعادة استخدام رموز البرامج الخبيثة.[57]

ويمكن القول إن منظومة الأمن الوطني (الاستراتيجي للعراق، تواجه جملة من التحديات التي يمكن تصنيفها بالتحديات المرئية وغير المرئية ، وتتجلى أخطرها بتلك التي تتمظهر بالصورة غير المرئية، فلا يمكن التماسها بصورة مباشرة إلا من خلال البحث والاستقراء التحليلي ، وتشكل هذه التحديات تهديداً استراتيجياً من شأنها أن تؤثر على الأمن الاستراتيجي للفرد والدولة)، بمعنى: أن هذه التحديات تشمل معظم القطاعات والمؤسسات الحكومية وغير الحكومية ، التي تتمحور حول البنية التحتية الارتكازية للدولة لتصل إلى الأمن الإدراكي للمواطن، وتتراوح هذه التحديات ما بين التهديدات السيبراني لمنظومة الرقمي للدولة ، وزيادة عدد السكان من دون أن يصيب هذه الزيادة تخطيط استراتيجي يواكب التطورات والتحديات المحدقة بمؤسسات الدولة الرسمية وغير الرسمية، فتشكل تحدياً كبيراً لمنظومة الأمن الاستراتيجي للعراق، وبالتالي باتت الضرورة الملحة تركز الجهود البحثية والاستشرافية في هذا المجال ، ولاسيما في ظل زيادة الملحوظة للتحديات المحدقة بمنظومة الأمن الاستراتيجي للعراق. [58]

أن التهديدات الإلكترونية (السيبرانية) تنتشر عبر تحديات غير مرئية تؤثر على منظومة الأمن الوطني العراقي ومن المظاهر التي أشرتها الأجهزة الأمنية أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق ، إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي،

ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات؛ مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني. (59)

تمثل التحديات غير المنظمة للأمن الوطني عموماً مجمل العوامل التي تشكل تهديداً مباشراً على الثوابت القيمية والتحتية لأي مجتمع، فالأمن الوطني العراقي يوجه جملة من التحديات المرئية التي تشكل خطراً مباشراً على منظومة الأمن الاستراتيجي، وهذه التحديات يمكن التماس حيثياتها وتأثيراتها بنحو عيني مباشر، لكن التحديات التي تشكل تهديداً أكبر على المنظومة الإستراتيجية للأمن الوطني هي التي لا يمكن التماس تأثيراتها مباشرةً على وحدات الأمن الوطني ، لذا فإن التحديات غير المرئية للأمن الوطني العراقي تتجلى بجملة من العوامل والمؤثرات التي تخص قطاعات إستراتيجية مهمة في الدولة، كقطاع البنى التحتية، التي تمس تأثيراتها حياة المواطنين، فضلاً عن تحديات أخرى محدقة بالمنظومة الرقمية للعراق والمتمثلة بالتهديدات السيبرانية الإلكترونية، فضلاً عن تحديات زيادة السكان وضعف التخطيط الاستراتيجي ، ويمكن التطرق إلى هذه التحديات بنحو أوسع كالآتي:-(60)

1- ضعف البنى التحتية: البنى التحتية ضرورة لا غنى عنها لعملية النمو والتنمية الاقتصادية في العراق، إذ إن وجودها يعد من أهم عناصر جذب الاستثمار وتنمية الاقتصاد الوطني وتطوره، وبالتالي أن عملية التنمية الشاملة في العراق يجب أنه ترافقها خدمات للبنى التحتية موازية لها، تهدف إلى تحسين الظروف المعيشية للأفراد من خلال تزويدهم بالخدمات المادية والاجتماعية، ولكن دخول البلد بحروب طويلة عقوبات اقتصادية دولية على العراق، وكل ذلك أدّى إلى دمار تلك البنى التحتية وخرابها

2- ضعف التخطيط التنموي: نتيجة التداعيات والانعكاسات السلبية التي تمس مسار عمل المؤسسات الدولة العراقية الإستراتيجية، يعاني العراق اليوم من حالة ضعف في منظومة التخطيط الاستراتيجي، وهو ما انعكس سلباً على عمل معظم مؤسسات الدولة العراقية ونتاجها التي باتت تعاني من ضعف في التخطيط الاستراتيجي الذي يمثل أحد السمات الرئيسة للعصر الحديث، وأساس عمل المؤسسات الحكومية لأجل تحقيق الأهداف الوطنية المنشودة، لذلك فإنه يتطلب قدرات خاصة على التوقع والتنبؤ فيما يخص المستقبل.

3- ضعف الأمن الالكتروني.

تتمثل التهديدات الإلكترونية (السيبرانية) بتحديات غير مرئية توثر على منظومة الأمن الوطني العراقي، ففي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر في صد أي هجوم إلكتروني ومنعه، وقد تتعرض له أنظمة الدولة المختلفة، وأيضاً حماية الأنظمة التشغيلية من أي محاولات للولوج بنحو غير مسموح به لأهداف غير سليمة، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات، لذا يتوجب على الأمن الإلكتروني العراقي أن يشكل مجموع الأطر القانونية والتنظيمية، والهياكل التنظيمية، فضلاً عن الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية و تهدف إلى حماية الفضاء

السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني.

4- ضعف تشريعات الأمن السيبراني:

أن استخدام التقنيات المستحدثة للتحكم في المعلومات واساليب تجميعها ومعالجتها واختزانها وتحسين الانتفاع منها من خلال الحاسبات وثورة الاتصالات[61] .والسرعة والتطور التكنولوجي في العراق والعالم، مع وجود فجوات قانونية في مجال الإنترنت تشكل تحديا كبيرًا، ففي ظل غياب معايير موحدة لقوانين الإنترنت، يصبح التنظيم أمرًا حيويًا، خاصةً عندما تتعلق المسألة بأفراد أو كيانات من دول مختلفة[62]

فعدم وجود تشريعات محددة في العراق لمكافحة الهجمات السيبرانية يتيح للمهاجمين والهاكرز فرصة لتنفيذ أنشطتهم دون مواجهة عواقب قانونية جادة، يمكن أن يؤدي هذا الوضع إلى عجز في تحقيق العدالة وتطبيق القانون على المخترقين مما يزيد من التهديدات ويقلل من فعالية الاستجابة، لتحسين الأمان السيبراني في العراق، يلزم إصدار وتعزيز تشريعات فعّالة وشاملة تغطي جوانب متنوعة من الأمان السيبراني، بما في ذلك الوقاية من الهجمات، وتحقيق العدالة في حال وقوع الاختراقات، وتحديد العقوبات المناسبة للمخترقين، وفي جلسته بتاريخ 21 نوفمبر/2023 طرح البرلمان العراقي مشروع قانون جرائم المعلوماتية، بعد فشل دورات المجلس السابقة في إقراره خلال العقد المنصرم، وعلى الرغم من التعديلات المتكررة على مشروع القانون، ومع التأكيد على أهمية تنظيم عملية التواصل الالكتروني خصوصاً وأنّ العراق تأخر كثيراً في سن تشريع، ذلك القانون الذي تضمن 31 مادة يعود إلى عام 2011، فقد نصت المادة السادسة من القانون على "يعاقب كل من حاول استخدام شبكة المعلومات لتكدير الأمن والنظام العام بالسجن المؤبد أو بغرامة تتراوح بين (25) و(50) مليون دينار عراقي"، أما المادة الثانية والعشرون تنص على "الحبس لمدة سنتين ودفع غرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين دينار، لمن نسب إلى الغير عبارات أو أصوات أو صوراً تنطوي على القذف والسب من خلال شبكة المعلومات"، وقد تم سحب ذلك المشروع من قبل الحكومة، لغرض إضافة بعض التعديلات عليه[63]

5- غياب الأمن الالكتروني:

غياب الأمن الالكتروني جعل العراق يعاني من انكشاف استراتيجي حيال أغلب بلدان العالم ومهد الطريق لهم لأختراقه والتجسس على البيانات والمعلومات بمنظومته الأمنية، بل والعمل على جعل العراق أداة لشن الهجمات الالكترونية على الأمن المعلوماتي لدول اخرى واختراقه وسرقة معلوماتها واستخدامها لأغراض المساومة وتنفيذ أفعال إرهابية، ويتضح تأثير المخاطر السيبرانية على الأمن الوطني والاقتصاد العراقي من خلال مؤشرات عديدة، ومنها؛ عدم فعالية البنية الرقمية التحتية كما أسلفنا، حيث يُعد العراق متخلفاً في مجال التبويب الرقمي وخصوصاً في المجال الاقتصادي، فالعراق في الفضاء المعلوماتي لا يعيش عصر العزلة بيد أنه مترابط مع دول أخرى في هذا الفضاء عبر شبكات ترابطية للبنى المعلوماتية التحتية، حتى بات بالإمكان عبر ذبذبات الاتصال الرقمي تنظيف خزينة العراق من أموالها بواسطة نظاماً حاسوبياً يتم إدارته من غرفة في قرية تبعد عنه آلاف الكيلومترات، فتلك الموجات الاثيرية تهاجم مركز الثقل في تطور الدولة وتسيطر على قدرات العراق وتتحكم بكافة مقدراته، وتستهدف المراسلات الحكومية لتقوم بعملية تدمير تلك الوسائط الالكترونية، وتستهدف الأسرار الأمنية والاقتصادية وأيضاً الاجتماعية للبلد، ليكتمل بذلك حلقات العملية التجسسية، وكذلك

احتواء الفضاء السيبراني على نقاط ضعف بالإمكان توظيفها لاستغلال المصالح الاقتصادية الوطنية وتمثل تحدياً للأمن الوطني العراقي، ومنها الإرهاب والتجسس الالكتروني والقرصنة الالكترونية وعملية غسيل الأموال، واستخدام شبكات الانترنت لممارسة أعمال العنف والنصب والاحتيال والاستغلال والجرائم المالية، ناهيك عن الاستخدام السلبي لمواقع التواصل الاجتماعي للقيام بإعمال مدمرة[64]

## المطلب الثاني: استراتيجيات مواجهة التحدي السيبراني

ان التهديدات السيبرانية تمثل تحديات غير مرئية تؤثر في منظومة الأمن الوطني العراقي، فمع الانفتاح على العالم والتطور التكنولوجي الذي شهده العراق لاسيما في مجال الاتصالات والمعلومات في الوقت الذي يعاني فيه العراق من ضعف في البنية التحتية الخاصة بالحماية الالكترونية من الهجمات السيبرانية الأمر الذي جعله مكشوفاً لدى الكثير من دول العالم لاختراقه والتجسس عليه لاسيما المتعلقة منها بالمؤسسات الامنية[65] ولأجل ذلك عمل العراق مع شركائه الدوليين في مجال تطوير الأمن السيبراني للإفادة من خبراتهم، وفي هذا الخصوص قامت الحكومة العراقية بالتنسيق مع حلف شمال الاطلسي (الناتو) على تدريب (16) موظفاً من فريق الاستجابة للأحداث السيبرانية للمدة من 21 تشرين الثاني ولغاية 2 كانون الأول 2016 [66]وتضمن البرنامج التدريبي جلسات نظرية ومختبرية عملية عن أساسيات الدفاع السيبراني، وحماية البيانات من التسرب، وتحليل الشفرات، والادلة الالكترونية، ورفع مستوى الخبرة التقنية لحماية الشبكة الوطنية، وزيادة الوعي بالأمن السيبراني، وستعمل هذه الدورات على تعزيز قدرات الدفاع السيبراني الوطنية العراقية[67]

وجدير بالذكر ان العراق احتل المرتبة (158) على الصعيد العالمي استناداً إلى مؤشر الصادر Global Cybersecurity Index – GCI 2017 الأمن من الاتحاد الدولي للاتصالات التابع إلى الأمم المتحدة كونه الوكالة المختصة في مجال تكنولوجيا المعلومات والاتصالات[68]وفي العام 2018 احتل العراق وفق مؤشر الأمن السيبراني العالمي للعام 2018 المرتبة (107) على الصعيد العالمي من أصل (175) دولة شملها التقرير، والمرتبة (13) على صعيد الدول العربية[69]وهذا يعني ان الأمن السيبراني في تطور ايجابي وهذه دلالة على نجاح القائمين عليه.

وبهدف تطوير استراتيجية العراق للأمن السيبراني انعقد في العاصمة العراقية بغداد في 5/اذار/2019 مؤتمر العراق الإلكتروني والأمن السيبراني بالتعاون مع المجلس الدولي للاستشارة الالكترونية (EC-Council) التابع لمفوضية الاتحاد الاوربي كونه المعني بمتابعة قضايا الأمن السيبراني وله دوره العالمي في هذا المجال، وكان الهدف منه تحديث وابتكار عمليات الأمن السيبراني الاستراتيجية والتكتيكية للحكومة العراقية، ومستقبل الحكومة الالكترونية، والتهديدات السيبرانية التي يتعرض لها العراق وسبل الدفاع السيبراني عنها، وزيادة الوعي لمنع الجريمة السيبرانية في العراق، فضلاً عن حماية البيانات والتعامل مع الحوادث السيبرانية، واستعادة القدرة السيبرانية على العمل بعد الحوادث، ودور (EC-Council) في تقديم الدعم للعراق، ويأتي هذا المؤتمر في سياق خطط الحكومة العراقية للاستثمار في الحكومة الالكترونية، وتعزيز الأمن السيبراني العراقي[70]

كما أعلنت مستشاريَّة الأمن الوطني عن (ستراتيجيَّة الأمن السيبراني العراقي)، لتوفير التدابير المتماسكة والإجراءات الستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتيَّة الحيويَّة للمعلومات، وبناء ورعاية مجتمع انترنت موثوق فيه، وحدد التهديدات

السيبرانيَّة الرئيسة في الجريمة الإلكترونية، والإرهاب الإلكتروني، والصراع السيبراني، والتجسس السيبراني، الى جانب إساءة معاملة الاطفال واستغلالهم الكترونياً، وشددت الستراتيجية على ضرورة تقييم مواطن الضعف الوطنية في المجال السيبراني وقياس الاثار والفرص، بهدف الاسهام في احداث تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني، وتطوير امكانات الامن السيبراني على جميع مستويات الدولة في العراق[71]

وقد وضعت الستراتيجية خريطة طريق تفصيليَّة من ثمانية محاور، متمثلة بالحكومة الفعالة، والإطار التشريعي والتنظيمي، وإطار تكنولوجيا الأمن السيبراني، وثقافة الامن السيبراني وبناء القدرات، والبحث والتطوير نحو الاعتماد على الذات، والامتثال والتنفيذ، والجاهزية لحوادث الأمن السيبراني، الى جانب التعاون الدولي.[72]

وجرى الإعلان عن فريق وطني مشترك مختص للاستجابة للحوادث السيبرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي.

حمل الفريق على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني، وتحقيق الرصانة والموثوقية للأنظمة الالكترونية، وتعزيز ثقة المواطن بالمؤسسات والارتقاء بمستوى العراق دولياً في مجال الامن السيبراني لتشجيع تطوير الخدمات الالكترونية ودعم مشروع أتمتة الخدمات والحكومة الالكترونية[73]

ويهدف الفريق الى الاستجابة للحوادث الأمنية والحد من آثارها وتوفير تدابير استباقية لتلافي هذه الحوادث، وبناء الأطر الوطنية للأمن السيبراني لتشجيع التعاون بين القطاعين العام والخاص وتبادل المعلومات، وزيادة الثقة في استخدام الخدمات الإلكترونية الحكومية، وتعزيز الوعي الأمني لمستخدمي انظمة تكنولوجيا المعلومات والإنترنت، وتطوير القدرات الأمنية لمدراء أنظمة تكنولوجيا المعلومات للتعامل مع الحوادث الأمنية، وتحليل التهديدات الأمنية وتأثيرها وتوفير معلومات عن آخر الحوادث وطرق تجنبها، وبناء مركز معتمد لتسلم البلاغات عن الحوادث السيبرانية، وتشجيع البحث والتطوير في مجال الأمن السيبراني، والتعاون المشترك مع فرق الاستجابة والمنظمات على الصعيدين الإقليمي والدولي[74]

كما قطعت وزارة الداخلية أشواطاً متقدمة في مجال إرساء قواعد الأمن السيبراني في العراق، لا سيّما ما يتعلق بمحوري الجريمة الإلكترونية، والإرهاب الإلكتروني، وتمكّنت من توفير عناصر متدربة على المهارات الرقميَّة المتقدمة لمواجهة تلك الجرائم، في مديرياتها بجميع المدن العراقية، ووفرت متطلبات الإبلا غ السريع عن تلك الجرائم، فضلاً عن قيامها بحملات توعية الشرائح العراقيَّة المختلفة بمخاطرها، ووسائل تجنبها من قبل الأفراد العاديين، عن طريق الحملات الإعلاميَّة والإلكترونيَّة والندوات الحواريَّة والتثقيفيَّة.

وهيأت جميع وزارات وتشكيلات الدولة العراقية ذات الطبيعة الحساسة فرقاً إلكترونية مختصة في مجال مواجهة الجرائم السيبرانيَّة، ومنها استهداف المواقع الإلكترونية واختراقها، والمواقع الإلكترونيَّة التي يجري توظيفها في جرائم أمنية وعسكريَّة وإرهابية وجنائيَّة متعددة، على الرغم من تحديات التشريعات العراقيَّة النافذة، التي ما زالت لا ترتقي إلى مستوى التحولات الرقميَّة التي تشهدها المجتمعات

المعاصرة، والمخاطر الحديثة التي تواجهها، ومنها ما يرتبط بالأمن السيبراني[75]

وعلى الرغم من الإجراءات المبذولة من الحكومة والجهات ذات العلاقة يبقى التحدي السيبراني تحدي الجيل الخامس والذي لا يزال مشاكله مستمرة ومفاجئاته متجددة واضعة الأمن القومي في تحدي مستمر ومما تقدم يمكن تحديد سبل معالجة هذا التحدي بالآتي:-[76]

1- تبني تشريعات قانونية فعالة يتم تطبيقها على القطاع الحكومي والخاص.

2-ان يكون للحكومة دور في تنفيذ اجراءات امنية محددة في الوزارات والمؤسسات والقطاع الخاص، تعزز الأمن المعلوماتي والسيبراني على حد سواء.

3- تدريب وتطوير كوادر مهنية محترفة في القطاع الحكومي والخاص تؤهلها على مواجهة التحديات السيبرانية.

4- تنمية الوعي بان التحديات الامنية المعاصرة تختلف عن المرحلة السابقة، مما يستلزم البحث عن حلول جديدة مناسبة للتطورات الامنية المعاصرة، والابتعاد عن وسائل المعالجة التقليدية بهدف انشاء تكنولوجيا معلوماتية متقدمة.

## الخاتمة

يعد العراق واحدًا من بلدان العالم التي واجهت ولا تزال تواجه تحديات كبيرة في مجال الأمن السيبراني وفضائه، سيّما في الجوانب الأمنية، والأمر الذي يجعل من هذا التحدي للأمن القومي مستمر وقائم هو الضعف العام وعدم الاستقرار، فالعراق يحتاج إلى القدرات القوية والضرورية للتكيف مع تلك التحديات الناجمة عن الفضاء السيبراني، خصوصاً وأنه أي العراق قد دخل الفضاء الديناميكي بشكل سريع دون مروره بمرحلة انتقالية، مع ضعف وعدم جاهزية البنى التحتية والموارد البشرية وقد اظهر فحص الإمكانيات الأمنية السيبرانية في العراق، هناك حاجة ملحة لجهود معرفية وإدارية وقانونية وتقنية كبيرة، على الرغم من المؤتمرات الكثيرة المنعقدة والاستراتيجيات الموضوعة من قبل الحكومة والجهات المختصة، إلا أن البلد بحاجة إلى بذل جهد كبير لتعزيز التأثير في مجال الأمن السيبراني وفي الوقت نفسه ضمان حمايته من التهديدات السيبرانية.

التي تمثل في الوقت ذاته أمراً مهمًا وحاسمًا لإستدامة التقدم والإزدهار، فالعلاقة عكسية ومتضادة مابين التقدم والإزدهار ومابين تحدي الفضاء السيبراني، الأمر الذي يتطلب من الحكومة السعي الدائم لوضع استراتيجيات شاملة للمجالات كافة وتعزيز واستمرارية ما وضعته من استراتيجيات من أجل:-

1- حماية البنية التحتية للمعلومات الحيوية الوطنية.

2- الاستجابة بصورة مباشرة للحوادث والهجمات الالكترونية.

3- سلامة وحماية حيوية الفضاء الإلكتروني.

4- صقل الإمكانيات الوطنية.

5- مواكبة التطورات القائمة.

## التوصيات

1- العمل على إصدار تشريع يواكب المستجدات التقنية والتطورات الحاصلة.

2- رفع كفاءة المؤسسات على صعيد القطاع الحكومي والخاص من خلال توجيه الاستثمارات إلى كل ما من شأنه ان يعزز ويرفع من كفاءة المؤسسات وبناءها.

3- إعداد وتدريب كوادر من أجل التثقيف بكل ما يتعلق بالأمن السيبراني.

4- العمل على إيجاد شراكات دولية مع الدول والمنظمات هدفها تبادل المعلومات والخبرات في كل ما يعزز ويدعم الأمن القومي وفضائه.

5- إعداد مراكز مشتركة مابين القطاع الحكومي والخاص هدفها تبادل المعلومات وتنسيق الجهود.

6- دعم مراكز الرصد والإنذار المبكر للهجمات الالكترونية.

7- وضع قاعدة بيانات وطنية للحوادث السسيبرانية وسبل معالجتها من اجل الاستفادة منها في تطوير السياسات، تكون بمثابة البنك المعلوماتي الوطني.

8- جعل مبدأ الأمن السيبراني كمبدأ سيادي يعامل كأحد عناصر حماية الدولة الأساسية.

9- ضرورة استقلالية البنية التحتية الرقمية الوطنية وفك الارتباط بالشبكات الخارجية غير المؤمنة.

## المصادر

(*)الأمن في اللغة ضد الخوف، إذ اشتقت كلمة الأمن من "الأمان" و "الأمانة"، بمعنى أمن من باب فهم وسلم، وأيضا من "آمن" و "آمنه". فيقال اطمئن ولم يخف فهو آمن، ويقال لك الأمان" أي قد أمنتك والبلد اطمأن فيه أهله والشر منه سلم. وهذا المعنى ما ورد ذكره في القرآن الكريم بقوله تعالى: " وهذا البلد الأمين" سورة التين الآية، انظر: مجد الدين محمد يعقوب الفيروز آبادي، القاموس المحيط، ج4، دار الجليل، بيروت، د.ت، ص200.

فالأمن يشير إلى حالة الشعور المتجانس من الثقة من جراء انتفاء الخطر، أو الشعور بالقدرة والكفاية على مواجهة ذلك الخطر بإجراءات وقائية سابقة من أجل تحقيق الأمن والأمان، انظر: سعد ياسين الناصري، محددات مفهوم الأمن القومي العربي، دراسات دولية، بيت الحكمة، بغداد، العدد5، 2000-2001، ص51.

(1) منذر سليمان، نحو إعادة صياغة مفهوم الأمن القومي ومرتكزاته، مجلة كنعان النشرة الالكترونية، السنة الثامنة، العدد 1544، 2008.

(2)محمد عوض الهزايمة، حاضر العالم الاسلامي، العلوم السياسية والدراسات الدبلوماسية تونس، 2003، ص8.

(3) حسام حمزة، الدوائر الجيوسياسية للأمن القومي الجزائري، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية، جامعة الحاج الخضر-باتنه، 2011، ص20.

(4) الاخضر عمر الدهيمي، القانون الدولي الإنساني من منظور الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية، الرياض،2010، ص26.

(5) انظر: ممدوح شوقي كامل، الأمن القومي والأمن الجماعي الدولي، دار النهضة العربية، القاهرة، 1985، ص28.

(6) انظر: قسوم سليم، دراسات الأمن البيئي المسألة البيئية ضمن حوار المناظرات في الدراسات الأمنية، المجلة العربية للعلوم السياسية، العدد39-40، 2013، ص ص94-95.

(8) انظر: عبد السلام ابراهيم البغدادي، مفهوم الكيان الصهيوني للأمن القومي، دار الحرية، بغداد، 1985، ص29.

(9) علي الدين هلال، الأمن القومي العربي دراسة في الأصول، مجلة شؤون عربية، العدد35، 1984، ص12.

(10) علي عباس مراد، مشكلات الأمن القومي أنموذج تحليل مقترح، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، 2005، ص35.

(11) عبد السلام ابراهيم البغدادي، المصدر السابق، ص26.

(13) عبدالله مسعود وعلي عباس مراد، الأمن والأمن القومي، المركز العالمي لدراسات وأبحاث الكتاب الأخضر، بنغازي، 2006، ص43-45.

(14) المصدر نفسه، ص45.

(15) عزيز نوري، الواقع الأمني في منطقة المتوسط دراسة الرؤى المتضاربة بين ضفتي المتوسط من منظور بنائي، رسالة ماجستير مقدمة إلى كلية الحقوق قسم العلوم السياسية، جامعة الحاج لخضر- باتنه، الجزائر، 2012، ص51.

(16) عبدالله مسعود وعلي عباس مراد، الأمن والأمن القومي، مصدر سبق ذكره، ص46.

(17) المصدر نفسه، ص12.

(18) علي الدين هلال، الأمن القومي العربي دراسة في الأصول، مصدر سبق ذكره، ص14.

(19) عبدالله مسعود وعلي عباس مراد، الأمن والأمن القومي، مصدر سبق ذكره، ص46.

(20) علي الدين هلال، الأمن القومي العربي دراسة في الأصول، مصدر سبق ذكره، ص14.

(21) عبدالله مسعود وعلي عباس مراد، الأمن والأمن القومي، مصدر سبق ذكره، ص71.

(22) عزيز نوري، الواقع الأمني في منطقة المتوسط دراسة الرؤى المتضاربة بين ضفتي المتوسط من منظور بنائي، مصدر سبق ذكره، ص53.

(23) عبدالله مسعود وعلي عباس مراد، المصدر السابق، ص76.

(24) علي الدين هلال، المصدر السابق، ص15.

(25) مستشارية الأمن القومي، استراتيجية الأمن الوطني العراقي (العراق أولاً) 2025-2030، المركز الوطني للتخطيط المشترك، العراق، ص19.

(26) Norbert Wiener, The Human Use of Human Beings: Cybernetics and Society. London: Free Association Books, 1989, P15

(27) Joanna F. DeFranco, What Every Engineer Should Know about Cyber Security and Digital Forensics.Boka Raton: CRC press, 2014, P40
(28) رضوان الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، الجزائر ، العدد 603 ، جانفي، 234، ص14.
(29) منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت،ص25.
(30) الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية 2007، الموجز التنفيذي المعلومات، ص 44.
(31) منى الاشقر جبور ، الأمن السيبراني : التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2012، ص3
32) Security, University of California Santa, Richard Akemmerer(11) Science, 2003, P.3., Barbara, Department Computer
(33) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8 ، العدد 4 ، كلية القانون ، جامعة بابل، العراق 2016، ص 616.
(34) المصدر يسرى خالد ابراهيم، حرب المعلومات ماهيتها وانواعها ومستوياتها، مجلة الباحث الاعلامي، كلية الاعلام - جامعة بغداد ، المجلد 3 ، العدد 13، 2011، ص 3-5
(35) عادل عبد الصادق ، الإرهاب الالكتروني ، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة ، مركز الدراسات السياسات الاستراتيجية، القاهرة، مصر ، 2009، ص 201.
(36) علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة "الأمن السيبراني والحروب المعززة والهجينة" ، دار العربي للنشر والتوزيع، القاهرة ، مصر ، 2023، ص 143.
(37) زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية ، 2020, المجلد 1 ، العدد 44/1، 2020 ، ص52
(38) صلاح مهدي هادي الشمري، زيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجة العراقية ، مجلة قضايا سياسية، كلية العلوم السياسية - جامعة النهرين، العدد 62 281 2020
(39) قمر ثامر صبري، الارهاب السيبراني واثره على الامن القومي العراق انموذجاً"، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، بغداد، العدد 71 ، 2022، ص 145
(40) باسم علي خريسان، الأمن السيبراني في العراق قراءة في مؤشر الأمن السيبراني العالمي 2020 ، مركز البيان للدراسات والتخطيط، بغداد، 2021، ص 9-10.
(41) مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية _ جامعة ديالى ، المجلد 10 ، العدد 1، 2021، 152
(42) باسم علي خريسان، الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد ، المجلد 1 ، العدد 36 ، 2023، ص 23.
(43) جبور منى الأشقر: السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية ، بيروت-لبنان،2016، ب ص.
(44) جوهر الجموسي الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي (الدوحة: المركز العربي للأبحاث ودراسة السياسات 2016، ص ص 87 – 89.
(45) Jerry Brito and Tate Watkins, Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, Harvard National Security Journal (United States: Cambridge, Harvard Law School, Vol. 3, 2011), p. 40.
(46) László KOVÁCS, National Cyber Security as the Cornerstone of National Security, Land Forces Academy Review (Romania: Sibiu, Nicolae Balcescu Land Forces Academy, Vol. 23, No. 2, 2018), p.p. 113-116.
(47) للمزيد انظر: الاتحاد الدولي للاتصالات تأمين شبكات المعلومات والاتصالات أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني: المسألة 1 - 22 جنيف،2014، ص ص 24 - 26 .
(48) للمزيد أنظر: الاتحاد الدولي للاتصالات، دليل لوضع استراتيجية وطنية للأمن السيبراني: التزام استراتيجي بالأمن السيبراني، جنيف، 2018، ص ص 36 – 50.
(49) )Kenneth Geers, Strategic Cyber Security (Estonia: Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2011), p. 9.
(50) Hans de Bruijn and Marijn Janssen, op. cit., p.p. 4 – 6.
5)Global Cybersecurity Index 2017 (Geneva: International Telecommunication Union, 2017), p1. (1.
(51) Darius Štitilis and others, A model for the national cyber security strategy The Lithuanian case, Journal of Security and Sustainability Issues (Lithuania: Vilnius, Entrepreneurship and Sustainability Center, Vol. 6, No. 3, 2017 March), p.p. 357 – 358.
(52) Eric A. Fischer, Cybersecurity Issues and Challenges: In Brief, Report for Congress (Washington: Library of Congress, Congressional Research Service, No. R43831, August 2016), p. 3.
(53)Kelly Bissell and Larry Ponemon, The Cost of Cyber Crime (United States: Michigan, Ponemon Institute, 2019), p.p. 10, 19.

(54) Cybercrime Magazine, Global Cybercrime Damages Predicted To Reach Trillion Annually By 2021, 2019.
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by- 2021/
(55) Cybercrime Magazine, Global Cybercrime Damages Predicted To Reach 6 Trillion Annually By 2021, op. cit.
(57) إبراهيم عبد الله الهجري : التعليم في الوطن العربي أمام التحديات التكنولوجية، كلية العلوم،قسم الفيزياء، جامعة صنعاء، الجمهورية اليمنية ، ص1.
(58) محمود محمد غنام: دور تكنولوجيا المعلومات في إدارة الأزمات لدى العاملين في غرف عمليات الأجهزة الأمنية التابعة لوزارة الداخلية الفلسطينية ، جامعة الخليل ، فلسطين ، 2011،ص2.
(59) إميل أمين الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية، مقال منشور، المكتبة الالكترونية، 93586https://www.independentarabia.com/node/
(60) علي زياد العلي : التحديات غير المرئية للأمن الوطني العراقي ، 2018/6/26 ، المكتبة الالكترونية - : /4565/06/2018https://www.bayancenter.org/
(61) حامد شهاب : مخاطر المواقع الالكترونية على الأمن الوطني، مقال منشور ، صحيفة ميدل :- المكتبة الالكترونية، ايست أون لاين ، 20/10/2020 .
(62) علي زياد العلي : التحديات غير المرئية للأمن الوطني العراقي، مصدر سبق ذكره.
(63) أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية، معهد الادارة العامة، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية 2014 ، ص20.
(64) علي ابراهيم المعموري ، الأمن السيبراني واثره في الامن الوطني العراقي بعد العام 2003،رسالة ماجستير غير منشورة، مقدمة إلى كلية العلوم السياسية ، جامعة بغداد ، 2019، ص 74-75.
(65) عمر العجلوني، لماذا يجب تعديل مشروع قانون الجرائم المعلوماتية في العراق؟ على الموقع الالكتروني الاتي : https://euromedmonitor.org/index.php/ar/article5498/
(66) مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق ، المجلد 2 ، العدد 20، 2020، ص 57.
(67) علي زياد العلي التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، http://www.bayancenter.org/2018/06/45652018.
(68) فريق الإستجابة للأحداث السبرانية، حلف الناتو يدرب خبراء عراقيين في مجال الدفاع السبراني، https://cert.gov.iq/library/events/62016
(69) raq Business News, NATO trains Iraqi Experts in Cyber Defence, United Kingdom, 12th December 2016.
https://www.iraq-businessnews.com/2016/12/12/nato-trains-iraqi- experts-in-cyber-defence.(/
(70) Global Cybersecurity Index 2017, op. cit., p. 64
(71) Global Cybersecurity Index 2018 (Geneva: International Telecommunication Union, 2018), p. 58.
(72) EC-Council, EC-Council Sponsors e-Iraq and Cybersecurity Event, 2019. https://blog.eccouncil.org/ec-council-sponsors-e-iraq-and-cybersecurity-event/).
(73) الدكتور صفد الشمري، ما واقع الأمن اليبراني في العراق ، جريدة الصباح.
(74) المصدر نفسه.
(75) الدكتور صفد الشمري، ما واقع الأمن اليبراني في العراق ، مصدر سبق ذكره.
(76) الدكتور صفد الشمري، ما واقع الأمن اليبراني في العراق ، مصدر سبق ذكره.
(77) المصدر نفسه.
(78) Farook Al-Jibouri, Iraq Cyber Security Overview, and announcing our Cyber Security Framework, LinkedIn Corporation, 2016.