مجلة دراسات دوليّة

تعزيز الامن السيبراني في العراق: التحديات والفرص

م.م. رعد خضير صليبي

جامعة بغداد/ مركز الدراسات الاستراتيجية والدولية/ قسم السياسات العامة

raad.k@cis.uobaghdad.edu.iq

تاريخ الاستلام 2024/3/6 تاريخ القبول 2024/5/12 تاريخ النشر 2024/10/30

الملخص:

تتزايد اهمية الامن السيبراني في العراق مع التقدم التكنولوجي السريع وكثرة استخدام التقنيات الرقمية في مختلف القطاعات، وهو يشمل جميع الإجراءات والتدابير التي تتخذها الحكومة والشركات لحماية الأنظمة الرقمية والمعلومات من التهديدات السيبرانية، وتعتبر التحديات في مجال الامن السيبراني في العراق ذات أهمية كبيرة، فمع التطور التكنولوجي، تتزايد أيضًا وسائل التهديد السيبراني، مما يتطلب إجراءات أمان أكثر تقدمًا، وتعاني الكثير من الكوادر البشرية في العراق من نقص في التحضير والوعي السيبراني، الامر الذي يزيد من تعرضهم، وقد يكون هناك تحدي في تحديث وتحسين البنية التحتية لتكنولوجيا المعلومات والاتصالات، وحاجة إلى تحسين التشريعات والسياسات المتعلقة بالأمن السيبراني لضمان فعالية الإجراءات الوقائية والتصدي، ومع ذلك، يتسع أيضًا الفضاء للفرص في مجال الامن السيبراني في العراق، اذ يمكن للتعاون مع دول وهيئات دولية تقديم فرص لتبادل الخبرات والدعم في مجال الامن السيبراني، وتطوير وتحسين المهارات والوعي السيبراني للكوادر العاملة مما يوفر فرصة لتعزيز التحضير والتصدي للتهديدات، ويمكن أن يوفر الاستثمار في تكنولوجيا الامن السيبراني فرصة لتعزيز القدرة على مواجهة التحديات، ويظهر الامن السيبراني في العراق كمجال مهم يتطلب اهتماماً وجهوداً مستدامة لتعزيز الحماية الرقمية وضمان استمرار التنمية التكنولوجية.

الكلمات المفتاحية : الأمن السيبراني، الفضاء السيبراني ، الحرب الافتراضية، الارهاب السيبراني

Abstract:

The importance of cybersecurity in Iraq is increasing with rapid technological advancements and the widespread use of digital technologies across various sectors. It encompasses all measures taken by the government and companies to protect digital systems and information from cyber threats. The challenges in the field of cybersecurity in Iraq are significant. With technological advancement, cyber threats are also increasing, necessitating more advanced security measures. Many human resources in Iraq suffer from a lack of preparation and cyber awareness, increasing their vulnerability. There may be challenges in updating and improving the infrastructure of information technology and telecommunications, as well as the need to improve legislation and policies related to cybersecurity to ensure the effectiveness of preventive and response measures. However, there is also room for opportunities in cybersecurity in Iraq. Collaboration with international countries and organizations can provide opportunities for exchanging experiences and support in the field of cybersecurity, developing and enhancing skills and cyber awareness for the workforce, thereby enhancing preparedness and resilience

against threats. Investing in cybersecurity technology can provide an opportunity to enhance the ability to face challenges. Cybersecurity in Iraq appears as an important field that requires sustained attention and efforts to enhance digital protection and ensure the continuity of technological development.

المقدمة:

اصبح تحقيق امن سيبراني فعال في العراق أمرًا ذا أهمية بالغة في ظل الثورة التكنولوجية المتسارعة واعتماد القطاعات الحيوية على البنية الرقمية، اذ يشكل الامن السيبراني اليوم ركيزة أساسية للحفاظ على استقرار النظم الحيوية وضمان استمرار تطور التكنولوجيا بشكل مستدام، ففي سياق التقدم التكنولوجي السريع، تصبح البنية السيبرانية للدولة أكثر عرضة للهجمات والتهديدات الإلكترونية المتطورة، ويتطلب الامن السيبراني في العراق تحليلًا دقيقًا للتحديات المحتملة، مثل التهديدات السيبرانية الدولية والجرائم الإلكترونية، وضرورة تبني سياسات وإجراءات فعالة لمكافحتها، والفرص الفعّالة التي يمكن أن تخلقها التكنولوجية لتعزيز الامن السيبراني، وتعتبر التحديات البنوية والتشريعات في العراق عاملين أساسيين يجب معالجتهما بجدية، فمن خلال تحسين البنية التحتية لتكنولوجيا المعلومات وتعزيز التشريعات ذات الصلة، يمكن تعزيز فعالية إجراءات الامن السيبراني، وإن فهم التحديات واستغلال الفرص في مجال الامن السيبراني يشكلان خطوة حيوية نحو بناء مجتمع رقمي آمن في العراق، من خلال تكامل الحماية والابتكار التكنولوجي، يمكن للعراق أن يحقق تقدمًا مستدامًا في ميدان الامن السيبراني ويضمن استمرار تطوره التكنولوجي.

اهمية البحث:

تأتي اهمية البحث من الدور الكبير الذي يؤديه الامن السيبراني وعدم الاهتمام به سيؤدي الى عدم التوازن في كافة مؤسسات الدولة وهذا سيؤثر بطبيعة

الحال على العراق بصورة كبيرة جداً، لذلك سنبين في بحثنا اهم التحديات التي تواجه الامن السيبراني في العراق وفرص نجاحه.

مشكلة البحث:

تكمن مشـــكلة البحث في التحديات الكثيرة التي تواجه الامن الســـيبراني في العراق وفي مقدمتها البنية التحتية الضـعيفة وعدم وجود تشـريعات حقيقية لمعالجة المشاكل التي تطرأ

وهناك تســـــاؤلات فرعية مفادها: كيف يمكن للعراق ان يعمل على تفادي تلك التحديات؟ وما هي اسباب تخلف العراق في هذا المجال؟

فرضية البحث:

تنطلق فرضية البحث من أن: تحسين مستوى التحضر والتوعية السيبرانية في العراق يمكن أن يكون له تأثير إيجابي على تعزيز الامن السيبراني والتصدي للتحديات المتزايدة في ظل التقدم التكنولوجي السريع.

منهجية البحث:

نظراً لتعدد القضايا المرتبطة بالأمن السيبراني اعتمدت الدراسة على عدة مناهج مثل المنهج الوصفي لمتابعة اهتمام الحكومة العراقية بهذا المجال، وكذلك اعتمدنا المنهج التحليلي للوقوف على تأثير الامن السيبراني في العراق ومدى تطبيقها وابراز التحديات والفرص التي من شأنها أن تحد من المخاطر .

المطلب الاول: الاطار المفاهيمي للأمن السيبراني

في ظل ظهور الإنترنت واستخدامه بشكل متزايد منذ أواخر القرن العشرين، توسع المجال العام ليشمل المساحات التقليدية والإلكترونية، مع تكامل وسائل التواصل الاجتماعي والمواقع الإلكترونية، وأصبحت هذه المنصات مساحات ممتدة للحوار والنقاش، تجاوزت حدود الزمان والمكان، ونشأت في سياق مجتمعات افتراضية تلعب أدواراً مؤثرة في القضايا العامة، سواء داخل الدول أو خارجها، وقد شهد العالم تطوراً مطرداً في مجال التكنولوجيا الرقمية وتطبيقاتها، وأدى هذا التقدم

إلى ارتباط أعمق لحياة الإنسان بالأجهزة الإلكترونية والعالم الافتراضي، وتأثرت الأنظمة السياسية والعلاقات الدولية بتلك التكنولوجيا، حيث أصبحت الحدود الجغرافية للدول تتأثر باندماج الفضاء السيبراني مع مفاهيم السيادة والأمان القومي.

اولاً: المفهوم اللغوي للأمن السيبراني

لقد وردت كلمة "الأمن" في القرآن الكريم في مواضع كثيرة، وهو ضد الخوف مثل قوله تعالى "الذي اطعمهم من جوع وامنهم من خوف[1]، وايضاً في قوله تعالى "ادخلوها بسلام امنين[2] ، ولقد وردت ذكر كلمة "الامن" كذلك في مصادر اللغة العربية بمعنى كونه نقيض الخوف أي بمعنى السلامة، والأمن مصدر الفعل أمن أمناً وأماناً وأمنة، أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه ونقول: أمن منه أي سلم منه، وأمن على ماله عند فلان أي جعله في ضمانته، والأمان والأمانة بمعنى واحد فالأمن ضد الخوف، والأمانة ضد الخيانة، والمأمن الموضع الأمن[3]، وقد ذكر في المعجم الوسيط بمعنى "أمن" امناً وامانا وامانة اطمأن ولم يخف، فهو امن البلد الذي اطمأن فيه إهله[4]، أما مصطلح السيبرانية فقد اشتقت من لفظة سيبر cyber اليونانية الأصل، وقد اشتقت من كلمة kybernetes، بمعنى (الشخص الذي يدير دفة السفينة)، وقد تستخدم مجازاً لتعبر عن المتحكم[5]، فهناك ايضاً من يرجع أصلها إلى منتصف القرن العشرين لعالم الرياضيات الأمريكيNorbert Wiener، حيث استخدمها للتعبير عن التحكم الآلي[6] 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[7].

ثانياً: المفهوم الاصطلاحي للأمن السيبراني

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"[8]، 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[9] ، 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[10] ، ويعرفه ريتشارد " Richard " كمرر بأنه " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة[11] ،أما من الناحية الاجرائية يمكن القول إن الأمن السيبراني " هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات واجهزة الكمبيوتر في الفضاء السيبراني ومن مختلف التهديدات والهجمات والاختراقات التي تهدد الامن القومي للدولة نفسها[12].

وعليه يمكن تعريف الأمن السيبراني بأنه "الجهود المبذولة لضمان حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، أذ يشمل ذلك تحديد وتقييم المخاطر والتهديدات المحتملة، واتخاذ الإجراءات

الوقائيـة والتصـحيحية لتقليـل الفـرص لحـدوث خسـائر أو أضـرار، والهـدف منـه هـو تحقيـق تـوازن بـين الأمـان والتشـغيل الفعّـال، مـع الحـرص علـى تقـديم استجابة فعّالة في حالة وقوع هجمات أو انتهاكات.

ثالثاَ: المفاهيم المقاربة للأمن السيبراني

نتيجـة أتسـاع مفهـوم الأمـن السـيبراني وذلـك بسـبب التقـدم الكبيـر فـي التكنلوجيـا والتقنيـات الحديثـة وبعـد انتهـاء الحـرب البـاردة فـي مطلـع تسـعينيات القـرن العشـرين ظهـرت عـدة مفـاهيم أخـرى مقاربـة منهـا علـى سـبيل المثـال كالآتي:

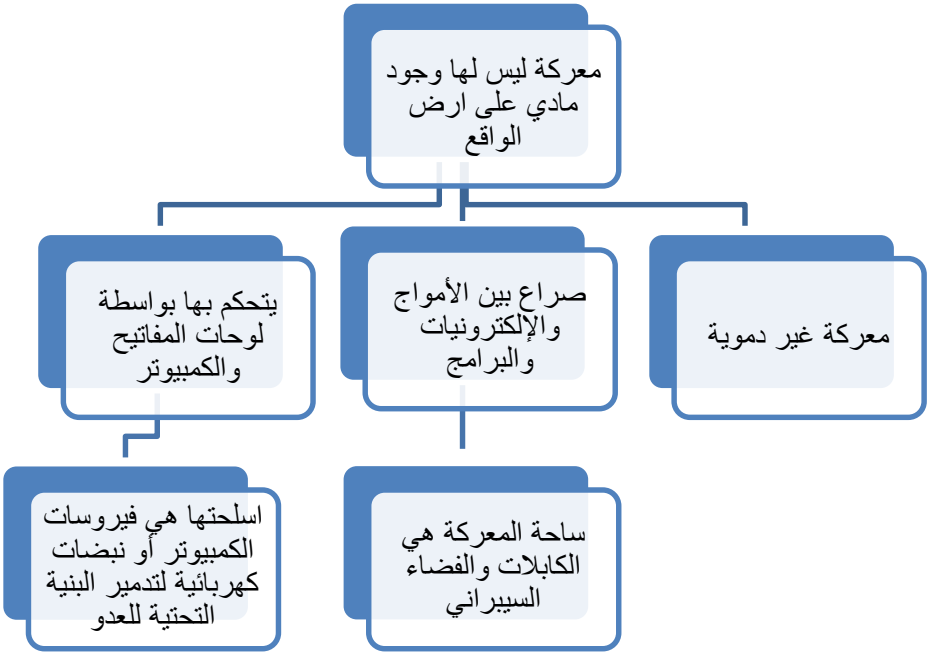
1- **الفضاء السيبراني:**

أي فضـاء التواصـل المشـكل مـن خـلال الـربط البينـي العـالمي لمعـدات المعالجـة الآليـة للمعطيـات الرقميـة، وهـو بيئـة تفاعليـة حديثـة ماديـة ومعنويـة، تتكـون مـن الأجهـزة الرقميـة وأنظمـة الشـبكات والبرمجيـات ويطلـق عليهـا "الـذراع الرابعـة للجيـوش الحديثـة"، وقـد أصـبح سـاحة لنقـل الصـراعات وتصـفية الخلافـات بكـل أنواعهـا بـين أطـراف الصـراع كافـة، وزادت التقنيـات الرقميـة ومـدى التقـدم العلمـي بهـا مـن إضـفاء درجـة الفاعليـة علـى ذلـك النـوع مـن الحـروب عبـر الفضـاء الالكترونـي فـي الصـراع الـدولي وقـد لا تـؤدي هـذه الحـرب الـى مأسـاة الكترونيـة بالضـرورة بـل الـى فـرض نـوع مـن السـيطرة علـى مجرى الاحداث في العالم[13].

2- الحرب الافتراضية:

يشير إلى نوع من أنواع النزاعات يدور أساسًا في المجال الرقمي والإلكتروني، ويشمل استخدام الحواسيب والشبكات ووسائل الاتصال الإلكتروني لتنفيذ هجمات وتكتيكات لتحقيق أهداف سياسية أو استراتيجية. يمكن أن تشمل هذه الهجمات السيبرانية الهجمات على الأنظمة الحاسوبية، والتجسس الإلكتروني، والتلاعب في البيانات، وانتشار البرامج الضارة، والحملات الإعلامية الإلكترونية[14]، كما هو موضح بالشكل رقم (1)

الشكل رقم (1) ما هي الحرب الافتراضية



الشكل من اعداد الباحث بالاعتماد على: رزق سعد علي، انعكاسات التحول الرقمي على الجرائم الجنائية، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، مدينة السادات الجامعية، القاهرة ، العدد 2، 2021، ص 242 .

وتشير الحرب السيبرانية الى الوسائل والاساليب القتال التي تدور في الفضاء الالكتروني وفي بعض الاحيان ترتقي الى مستوى النزاع المسلح أو ما هيتها، فهي حرب ذكية أقوى من أي هجوم بري أو جوي وأقل تكلفة وهي تطور طبيعي في مفهوم الحروب، كما ان مضمون الحرب السيبرانية يتعلق بالتطبيقات العسكرية للفضاء السيبراني[15].

3- الجريمة السيبرانية:

تعرف الجريمة السيبرانية على أنها" فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف الى الاعتداء على الاموال المادية أو المعنوية أو الاعتداء على خصوصية الافراد"[16]، أو 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، و قد ترتكب الجريمة السيبرانية لعدة أغراض كتحقيق مكاسب مادية معينة أو لإثبات الفاعل لمهاراته الفنية وقدرته على اختراق أجهزة الحاسب أو بهدف التسلية و الترفيه أو لمجرد الرغبة في الإضرار بالغير، وإن الجرائم السيبرانية تختلف عن الهجمات السيبرانية في البيئة التي تحدث فيها أي الفضاء السيبراني، من حيث الأشخاص والأهداف، فغالباً ما يكون مرتكبي الجرائم السيبرانية هم الأفراد و توجه ضد مؤسسات مالية أو شركات وحتى أفراد داخل أو خارج إقليم الدولة بخلاف الهجمات التي تتم من قبل دول أو مجموعات حكومية أو غير حكومية ضد دولة أخرى، وإن الجرائم السيبرانية غالباً ما يكون الهدف منها تحقيق مكاسب شخصية كسرقة الملكية الفكرية عن طريق شبكات الحاسب الآلي أو التسلل الى أنظمة المصارف و التلاعب بأرقام الحسابات و تحويل الأموال، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي و السياسي للدولة أو يقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية[17].

4- الإرهاب السيبراني:

كانت بداية استخدام هذا المصطلح في الثمانينات من القرن العشرين على يد "باري كولين" " Barry Cullen " والتي خلص فيها إلى صعوبة وضع تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفاً للإرهاب الإلكتروني بأنه : "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب ويعرفه جيمس لويس"James Lewis بأنه 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 ،ووفقاً لوزارة الدفاع الأمريكية البنتاغون فإنها تعرف الإرهاب الألكتروني بأنه: عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة[18] .

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، واتخذ الإرهاب السيبراني داخل العراق أشكال عدة منها عمليات الاحتيال المالي والاختلاس المصرفي التي تعرض لها العديد من الأفراد بصورة يصعب السيطرة عليها والابتزاز والتشهير الإلكتروني بحسابات وهمية على مواقع التواصل الاجتماعي لأغراض ودوافع مادية مما تسبب بمشاكل اجتماعية كبيرة وخصوصاً النساء[19]، وقد تعددت مخاطر الإرهاب السيبراني على الاقتصاد القومي ولكون الوجود الاقتصادي الرقمي للبلد

يعتمد على الأداء الفعال للبنية التحتية الرقمية في الفضاء السيبراني فإن البلد يكون مترابط مع بلدان أخرى وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية المعلوماتية، وبالتالي فإن البلد معرض لمخاطر 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[20].

5- الفضاء السيبراني:

الفضاء السيبراني يرتبط بالواقع الافتراضي وبشبكات الاتصال الالكترونية وانظمة الحاسوب، ولهذا تعددت تعاريفه، منها تعريف ادارة السلامة العامة الكندية بأنه: " العالم الالكتروني الذي تم إنشاؤه بواسطة شبكات مترابطة لتكنولوجيا المعلومات، والمعلومات متاحة على تلك الشبكات؛ أي انها مشاعة عالميًا حيث يرتبط الناس معًا بتبادل الأفكار والخدمات والصداقة، علماً ان الفضاء السيبراني ليس ثابتًا، بل هو نظام بيئي ديناميكي ومتطور ومتعدد المستويات للبنية التحتية المادية والبرمجيات واللوائح والأفكار والابتكارات والتأثيرات التي يتأثر بها عدد متزايد من المساهمين، وقد عرَف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الفضاء السيبراني 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[21].

ويعتبر العراق واحدًا من البلدان التي تواجه تحديات كبيرة في مجال الفضاء السيبراني، خاصة في الجوانب الأمنية، فالضعف العام وعدم الاستقرار يجعلان المسألة أكثر تعقيدًا، حيث يفتقد العراق إلى القدرات الضرورية للتكيف مع تلك التحديات الناجمة عن الفضاء السيبراني، ومع التحول السريع للمجتمعات من الواقع

الفعلي إلى الفضاء الافتراضي، يجد العراق نفسه يدخل هذا الفضاء الديناميكي بشكل سريع دون مروره بمرحلة انتقالية، فأن البنى التحتية والموارد البشرية في العراق لا تزال غير قادرة على التفاعل بشكل فعال مع التحديات الكثيرة التي يفرضها الفضاء السيبراني، وعند فحص الإمكانيات الأمنية السيبرانية في العراق، يظهر أن هناك حاجة ملحة لجهود معرفية وإدارية وقانونية وتقنية كبيرة، لذلك يتعين على العراق بذل جهد كبير لتعزيز التأثير في مجال الأمان السيبراني وفي الوقت نفسه ضمان حماية أمنه السيبراني من التهديدات السيبرانية[22] .

المطلب الثاني: التحديات التي تواجه الامن السيبراني في العراق

الأمن السيبراني في العراق يواجه تحديات هائلة نتيجة للتقدم التكنولوجي السريع والتحولات الكبيرة في مجال الاتصالات والمعلومات، فيعد هدفًا استراتيجيًا للهجمات السيبرانية لضعف الأمان الإلكتروني في البنية التحتية الوطنية، تلك التحديات تتفاقم بسبب استخدام المؤسسات العراقية لخدمات خارجية تتيح للمعلومات المهمة تداولها في خوادم خارج الحدود الوطنية، مما يفتح بابًا لاختراقات واستخدامات غير مشروعة، مما ينتج عنها اعمال تجسسية، أو حتى للمساس بأمان الدول الأخرى ويمكن أيجاز عددًا من تلك التحديات:

اولاً: **ضعف البنية التحتية التكنولوجية:**

أن تهديدات الأمن السيبراني يمكن اعتبارها "تحديات غير مرئية" تؤثر على منظومة الأمن الوطني العراقي ، فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات والذي تزامن مع ضعف البنية الأمنية الإلكترونية التحتية الوطنية سواء أكانت (أمنية، مصرفية، شخصية)، مما أدى إلى أن يصبح العراق منكشفاً إستراتيجياً لكثير من دول العالم، لإختراقه والتجسس على المعلومات الخاصة بالمؤسسات كافة، واستخدامه كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات أي دولة كانت واختراقه ، فضلاً عن سرقة أي معلومة واستخدامها لأغراض المساومة، وتنفيذ العمليات الإرهابية، وأن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من

أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية مما يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق ، إذ يشكل هذا الإجراء خرقاً لأمن المعلومات، أذ يجب تشكيل مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والتقنية والتكنلوجية حيث تمثل جهود مشتركة للقطاع العام والخاص محلياً وخارجياً وذلك لحماية الفضاء السيبراني العراقي والتركيز على ضمان توافر أنظمة للمعلومات وحماية سرية للمعلومات الخصوصية واتخاذ جميع الاجراءات اللازمة لحماية المواطن من مخاطر الفضاء السيبراني[23].

ويشهد العراق بين الحين والآخر هجمات سيبرانية من قبل مجموعات متطرفة وهاكرز غير معروفين، تستهدف البنية التحتية الحكومية والقطاع الخاص، مما يؤثر سلبًا على الخدمات الحكومية ويعرض الأفراد والمؤسسات لمخاطر جرائم الاحتيال وسرقة الهوية، لذلك فأن ضعف الأمان السيبراني يؤثر على استقرار العراق، حيث يعيق الأعمال الحكومية والتجارية ويثني المستثمرين عن الاستثمار، مما يؤدي إلى تباطؤ النمو الاقتصادي وزيادة معدلات البطالة، ويحتاج العراق إلى تطوير بنيته التحتية لتعزيز الأمن السيبراني وتعزيز القدرة على مواجهة التحديات الحديثة، مع التشديد على أهمية تحسين القدرات الفنية والقانونية والإدارية لتحقيق أهداف الأمان السيبراني، كذلك يُسلط الضوء على حاجة البلاد إلى منظومة تعليمية تركز على دراسة الأمن السيبراني لتأهيل الكوادر البشرية وتقديم التدريب الملائم، اذ شهد العراق في الآونة الاخيرة استحداث 3 أقسام متخصصة في دراسة الأمن السيبراني في جامعات رئيسية منها جامعة المستنصرية، والجامعة التقنية الشمالية، وجامعة الموصل" وكذلك في جامعة المستقبل، وافتتاح فروع لأكاديميات دولية لتدريس الأمن السيبراني والحوسبة السحابية[*] في العراق، وهو تطور إيجابي يسهم في تعزيز الكفاءات في هذا المجال.

ثانياً: ضعف تشريعات الأمن السيبراني:

أن استخدام التقنيات المستحدثة للتحكم في المعلومات واساليب تجميعها ومعالجتها واختزانها وتحسين الانتفاع منها من خلال الحاسبات وثورة الاتصالات[24]، والسرعة والتطور التكنولوجي في العراق والعالم، مع وجود فجوات قانونية في مجال الإنترنت تشكل تحديًا كبيرًا، ففي ظل غياب معايير موحدة لقوانين الإنترنت، يصبح التنظيم أمرًا حيويًا، خاصةً عندما تتعلق المسألة بأفراد أو كيانات من دول مختلفة، ويظهر الخلل بشكل واضح عندما يتورط الهجوم السيبراني في قضايا تجاوز الحدود، أذ قد يقوم المهاجمون بتنفيذ هجمات إرهابية في بلد لا تكون فيه قوانين صارمة، مما يثير تحديات في مجال تنازع القوانين، وتكمن المشكلة الحقيقية في عدم وجود سلطة مركزية على مستوى دولي تعمل على تطبيق قوانين تحمي الخصوصية وتضمن الأمان الرقمي، إذاً، يصبح الحل لهذه التحديات هو التعاون الدولي الفعّال، وفي ظل غياب سلطة دولية مركزية، يزيد نشوء ظاهرة الإرهاب الإلكتروني فهي التحديات التي تواجه الأمان الوطني، ولحماية الخصوصية وضمان الأمان السيبراني، يجب وضع معايير وسياسات تنظيمية دولية تحدد التزامات يجب اتباعها في البيئة السيبرانية، لذلك أن الفجوات القانونية تجعل من الصعب إثبات الدليل المادي للاعتداءات السيبرانية، مما يجعل التحقيق والمساءلة أمورًا معقدة، ولكن يمكن أن تؤثر الهجمات السيبرانية على مستويات مختلفة، مما يبرز أهمية تنسيق الجهود الدولية لمواجهة هذه التحديات، ولتحقيق ذلك، يجب أن تلتزم الدول بالتعاون الدولي وتطوير إطار قانوني دولي ينظم الهجمات السيبرانية ويحدد العقوبات للمتورطين، وإن إقامة هياكل دولية تعمل على توحيد الجهود وتعزيز التعاون ستكون أساسية لتحقيق أمان الإنترنت ومواجهة التهديدات السيبرانية بفعالية[25].

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 و50) 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[26].

ثالثاً: **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 مُترابط

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[27].

المطلب الثالث: فرص تحسين الامن السيبراني في العراق

تسعى الحكومة العراقية إلى تحسين فعاليتها وخدماتها من خلال تبني التقنيات الرقمية، ويعكس تحليل نموذج "نضوج الحكومة الرقمية" مدى تكامل هذه التقنيات في أنظمة الحكومة،" ويعرض هذا السياق تحديات تبني التحول الرقمي والفرص المتاحة، ويسلط الضوء على استراتيجيات العراق في تطوير حكومة رقمية تعزز التقدم والفعالية في إطار نظمها السياسية ويمكن ايجازها بالآتي[28]:

اولاً: حماية البنية التحتية للمعلومات الحيوية الوطنية لذلك ينبغي العمل على تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية التي تتضمن وضع اطار زمني لإدارة المخاطر على البنية التحتية وتقييم التهديدات ونقاط الضعف والعواقب واجراء تقييمات منتظمة للمخاطر التي تواجه وزارات الدولة ومؤسسات القطاعات الحيوية، واجراء تقييمات حول مدى الترابط والاعتماد المتبادل بين مؤسسات الدولة لتحديد المخاطر التي تواجهها.

ثانياً: الاستجابة للحوادث والهجمات الالكترونية وحلها والتعافي منها من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الاجراءات اللازمة.

ثالثاً: وضع الاطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الالكتروني.

رابعاً: تعزيز ثقافة الامن السيبراني التي من شأنها دعم الاستخدام الامن والمناسب للفضاء الالكتروني.

خامساً: تطوير قوى وصقل الامكانيات الوطنية للأمن السيبراني.

سادساً: تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة، وتعزيز استخدام المنتجات والخدمات التكنلوجية الموثوق بها، ووضع استراتيجية وطنية للتصدي للأخطار ومواطن الضعف في البنية التحتية السيبرانية من قبل صانع القرار العراقي.

سابعاً: اتخاذ اجراءات دولية ومشتركة للتصدي للجرائم المعلوماتية عن طريق ابرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرام والعمل على محاربتها [29]، لكن من المستحيل معرفة الحراكات في الفضاء السيبراني دون رؤية استراتيجية، والمصالح هي المحفز للحراك الدولي الرقمي وأن جميع الدول يجمعها هدف واحد هو تحقيق التكامل الأمني [30].

وقد عمل العراق بالتنسيق مع حلف شمال الاطلسي "الناتو" على تدريب "16" موظفاً من فريق الاستجابة السيبرانية في عام 2016، اذ تضمن البرنامج التدريبي دورات نظرية ومختبرية عملية عن اساسيات الدفاع السيبراني وحماية البيانات من التسرب وتحليل الشفرات والادلة الاكترونية ورفع مستوى الخبرة التقنية لحماية الشبكة الوطنية وزيادة الوعي بالأمن السيبراني حيث ستعمل هذه الدورات على تعزيز القدرات الدفاعية للعراق لمواجهة أي تحديات سيبرانية [31].

الخاتمة:

في ظل التطورات السريعة للتكنولوجيا والتحولات الرقمية، يظل الامن السيبراني في العراق أمرًا حاسمًا لضمان استدامة التقدم والازدهار، ويتطلب هذا التحدي تبني استراتيجيات شاملة لتعزيز القدرات السيبرانية وحماية المعلومات والبنية التحتية

الرقمية، ومن المهم تعزيز التعاون الدولي وتبادل المعلومات لمكافحة التهديدات السيبرانية العابرة للحدود، وتعزيز القدرة على التصدي للهجمات المتقدمة، ويجب تعزيز الوعي والتدريب للمواطنين والكوادر العاملة لتكون قوة فاعلة في حماية الأمان السيبراني، مع استمرار التحديات، يتعين على العراق أن ينظر إلى مجالات الفرص المتاحة، مثل تطوير صناعة الأمان السيبراني واستثمار الشباب في مجالات الابتكار وتطوير التقنيات السيبرانية المتقدمة، ويكمن مستقبل الامن السيبراني في تحقيق توازن بين التحديات الحالية واستغلال الفرص المستقبلية، مما يمكن العراق من أن يكون لاعبًا فاعلًا ومبتكرًا في عالم الامن السيبراني المتطور.

التوصيات:

هنالك عدة توصيات لتعزيز الامن السيبراني في العراق:

1. **تطوير البنية التحتية السيبرانية** :يجب على الحكومة العراقية الاستثمار في تحديث وتعزيز البنية التحتية السيبرانية لتكون قوية ومتقدمة، تحسين أمان الشبكات وتعزيز الحماية من هجمات القرصنة والاختراق.
2. **تعزيز التشريعات والسياسات:** ينبغي تطوير وتعزيز التشريعات والسياسات ذات الصلة لتكون أكثر فعالية في مكافحة الجرائم السيبرانية، بما في ذلك فرض عقوبات صارمة على المتسللين والمخترقين.
3. **تعزيز التعاون الدولي:** دعم التعاون الدولي لمواجهة التهديدات السيبرانية، من خلال مشاركة المعلومات والخبرات مع دول أخرى والانضمام إلى مبادرات دولية لتحسين الامن السيبراني.
4. **تعزيز الوعي والتثقيف** : يجب تعزيز الوعي بأمن الإنترنت ومخاطر الهجمات السيبرانية بين المواطنين والكوادر العاملة من خلال حملات توعية وبرامج تثقيفية.
5. **تطوير قدرات الموارد البشرية** : يتعين تعزيز تدريب وتطوير قدرات الكوادر البشرية لفهم التهديدات السيبرانية والاستجابة الفعالة لها.

6. **تعزيز الابتكار وريادة الأعمال** : العمل على دعم الابتكار في مجال الامن السيبراني وتشجيع ريادة الأعمال لتطوير حلول فعّالة لمكافحة التحديات السيبرانية.

7. **تعزيز الشراكات مع القطاع الخاص** :يجب تعزيز التعاون مع الشركات والقطاع الخاص لضمان أمان أنظمتهم ومشاركتهم في جهود مكافحة الجرائم السيبرانية.

8. **تكنولوجيا الذكاء الصناعي والتحليل الضوئي** :يمكن استخدام التكنولوجيا المتقدمة مثل الذكاء الصناعي والتحليل الضوئي لتحسين قدرات رصد واكتشاف التهديدات السيبرانية بشكل أكثر فاعلية.

وتحقيق هذه التوصيات يسهم في بناء مجتمع سيبراني آمن وقوي في العراق، الامر الذي يحقق التوازن بين التطور التكنولوجي والحفاظ على أمان الأفراد والمؤسسات.

الهوامش:

(1) القرآن الكريم، سورة قريش، آية (4).

(2) القرآن الكريم، سورة الحجر، آية (46).

(3) ابن منظور محمد بن مكرم، لسان العرب ، ط1، دار صادر ،ج1، بيروت، لبنان، 2000، ص163.

(4) شعبان عبد العاطي عطية واخرون، المعجم الوسيط، ط4، مكتب الشروق الدولية" مجمع اللغة العربية" ، مصر، 2004، ص28.

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

(6) Joanna F. DeFranco, What Every Engineer Should Know about Cyber Security and Digital Forensics.Boka Raton: CRC press, 2014, P40.

(7) ج. رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية ،الجزائر ، العدد 603، جانفي، 234، ص14.

(8)منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، لبنان، 2017، ص25.

[9] الاتحاد الدولي للاتصالات: دليل الأمن السيبراني للبلدان النامية 2007،الموجز التنفيذي المعلومات "، ص 44.

[10] منى الاشقر جبور ، الامن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2012، ص3.

[11] Richard Akemmerer , Cyber Security, University of California Santa Barbara, Department Computer Science, 2003, P.3.,

[12] 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.

[13] يسرى خالد ابراهيم، حرب المعلومات ماهيتها وانواعها ومستوياتها، مجلة الباحث الاعلامي، كلية الاعلام – جامعة بغداد، المجلد 3، العدد 13، 2011، ص 3-5.

[14] عادل عبد الصادق ، الإرهاب الالكتروني ، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة ، مركز الدراسات السياسات الاستراتيجية، القاهرة، مصر، 2009، ص 201.

[15] علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة "الامن السيبراني والحروب المعززة والهجينة" ، دار العربي للنشر والتوزيع، القاهرة ، مصر ،2023، ص 143.

[16] فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع ، عمان ، الاردن ، 2022، ص 74.

[17]زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية ، 2020, المجلد 1، العدد 1/44، 2020 ، ص52.

[18] 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، 2020، ص 281.

[19] 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.

[20] باسم علي خريسان، الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020 ، مركز البيان للدراسات والتخطيط، بغداد، 2021، ص 9-10.

[21]مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية_ جامعة ديالى ، المجلد 10 ، العدد1، 2021، ص 152.

[22] باسم علي خريسان، الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد، المجلد 1، العدد 36 ، 2023، ص 23.

[23] ظفر عبد مطر التميمي، العراق والأمن السيبراني .. الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط، العراق، المجلد 18 ، العدد 51 ، 2022 ، ص11-12.

(*) الحوسبة السحابية: هي مجموعة من الخوادم التقنية المتصلة معاً والتي تدار بشكل مركزي عن طريق شبكة اتصال محلية أو الأنترنت فيما يعرف بالسحابة لتوفير خدمات حاسوبية حديثة الى جمهور العملاء من المستخدمين وهذه السحابة يمكن أن تكون في مكان محدد أو موزعة في أماكن عدة، ويمكن أن نؤطر مفهوم الحوسبة السحابية بشكل مهني وأكثر رسمية وكما حددها المعهد الوطني للمعايير والتكنولوجيا (NIST) نموذج لتمكين الوصول إلى الشبكة في كل مكان ، والمريح ، عند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للاستعمال مثلاً الشبكات والخوادم والتخزين والتطبيقات والخدمات التي يمكن توفيرها وإصدارها بسرعة بأقل جهد إداري أو تفاعل مزود الخدمة، ويجري توفيرها عبر شبكة مما يتطلب التفاعل بين المستخدمين ومقدمي الخدمات، إذ أن الفكرة الرئيسة للحوسبة السحابية هي الاستعانة بمصادر خارجية لإدارة وتسليم موارد البرامج والأجهزة لشركات الطرف الثالث موفري أو مزودي السحابة ، والتي تتخصص في تلك الخدمة المعينة ويمكن أن توفر جودة خدمة افضل بكثير بتكاليف اقل بطريقة مريحة. للمزيد ينظر الى : Arjun , U. , & Vinay S. A Review on Remote Data Auditing in Cloud Computing International Journal of Engineering Research in Computer Science & Engineering 2018 ,p5

[24] أيمن عبدالله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية، معهد الادارة العامة، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014، ص20.

[25] علي ابراهيم المعموري ، الامن السيبراني واثره في الامن الوطني العراقي بعد العام 2003، رسالة ماجستير (غير منشورة) ، كلية العلوم السياسية ، جامعة بغداد، 2019، ص 74-75.

[26] عمر العجلوني، لماذا يجب تعديل مشروع قانون الجرائم المعلوماتية في العراق؟ على الموقع الالكتروني الاتي :
/5498https://euromedmonitor.org/index.php/ar/article/

[27] مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق، المجلد2، العدد20، 2020، ص57.

[28]صلاح مهدي هادي الشمري، زيد محمد علي اسماعيل، مصدر سبق ذكره، ص 287.

[29] شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، كلية القانون ، جامعة الشارقة ، الامارات العربية المتحدة، المجلد17 ، العدد1، 2019، ص 740.

[30] حازم حمد موسى، الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني "مقاربة بين المعضلة الامنية والمكنة الادائية" ، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد 57، العدد 5، 2020، ص 557.

[31] مصطفى ابراهيم سلمان الشمري، مصدر سبق ذكره ، ص 173.

قائمة المصادر:

القرآن الكريم

اولا: المصادر العربية

(1) ابن منظور محمد بن مكرم، لسان العرب ، ط1، دار صادر ،ج1، بيروت، لبنان، 2000، ص163.

(2) شعبان عبد العاطي عطية واخرون، المعجم الوسيط، ط4، مكتب الشروق الدولية" مجمع اللغة العربية" ، مصر، 2004.

(3) ج. رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية ،الجزائر ، العدد 603، جانفي.

(4) منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، لبنان، 2017.

(5) الاتحاد الدولي للاتصالات: دليل الأمن السيبراني للبلدان النامية 2007،الموجز التنفيذي المعلومات "،

(6) منى الاشقر جبور ، الامن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2012.

(7) 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.

(8) يسرى خالد ابراهيم، حرب المعلومات ماهيتها وانواعها ومستوياتها، مجلة الباحث الاعلامي، كلية الاعلام – جامعة بغداد، المجلد 3، العدد 13، 2011.

(9) عادل عبد الصادق ، الإرهاب الالكتروني ، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة ، مركز الدراسات السياسات الاستراتيجية، القاهرة، مصر، 2009.

(10) علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة "الامن السيبراني والحروب المعززة والهجينة" ، دار العربي للنشر والتوزيع، القاهرة ، مصر ،2023.

(11) فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع ، عمان ، الاردن ، 2022.

(12)زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية ، 2020, المجلد 1، العدد 1/44، 2020 .

(13) 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، 2020.

(14) قمر ثامر صبري، الارهاب السيبراني واثره على الامن القومي "العراق انموذجاً"، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، بغداد، العدد 71، 2022.

(15) باسم علي خريسان، الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020 ، مركز البيان للدراسات والتخطيط، بغداد، 2021.

(16)مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية_ جامعة ديالى ، المجلد 10 ، العدد1، 2021.

(17) باسم علي خريسان، الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة ، مجلة كلية التراث الجامعة ، بغداد، المجلد 1، العدد 36 ، 2023.

(18) ظفر عبد مطر التميمي، العراق والأمن السيبراني .. الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط، العراق، المجلد 18 ، العدد 51 ، 2022 .

(19) أيمن عبدالله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية، معهد الادارة العامة، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2014.

(20) علي ابراهيم المعموري ، الامن السيبراني واثره في الامن الوطني العراقي بعد العام 2003، رسالة ماجستير (غير منشورة) ، كلية العلوم السياسية ، جامعة بغداد، 2019.

(21) عمر العجلوني، لماذا يجب تعديل مشروع قانون الجرائم المعلوماتية في العراق؟، على الموقع الالكتروني الاتي: https://euromedmonitor.org/index.php/ar/article/

(22) مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق، المجلد2، العدد20، 2020.

(23) شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، كلية القانون ، جامعة الشارقة ، الامارات العربية المتحدة، المجلد17 ، العدد1، 2019.

(24) حازم حمد موسى، الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني "مقاربة بين المعضلة الامنية والمكنة الادائية" ، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد 57، العدد 5، 2020.

(25) رزق سعد علي ،انعكاسات التحول الرقمي على الجرائم الجنائية، مجلة الدراسات القانونية والاقتصادية ، كلية الحقوق ، مدينه السادات الجامعية، القاهرة ، العدد 2، 2021.

ثانيا: المصادر الانكليزية:

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

(2) Joanna F. DeFranco, What Every Engineer Should Know about Cyber Security and Digital Forensics.Boka Raton: CRC press, 2014.

(3)Richard Akemmerer , Cyber Security, University of California Santa Barbara, Department Computer , Science, 2003.

(4)Arjun , U. , & Vinay S. , A Review on Remote Data Auditing in Cloud Computing , International Journal of Engineering Research in Computer Science & Engineering, 2018