Journal Of the Iraqia University (75-6) March (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

الحرب السيبرانية كتهديد لأمن المعلومات الوطني قراءة قانونية معاصرة

دعاء عبد الامير قاسم الذهبي
الاستاذ المشرف الدكتور مصطفى فضائلي
استاذ القانون الدولي في جامعة قم- كلية القانون ايران

Cyber Warfare as a Threat to National Information Security: A Contemporary Legal Perspective

Duaa Abdul-Amir Qasim Al-Dhahabi, PhD Candidate
Supervisor: Dr. Mustafa Fazaili
Professor of International Law, Qom University, Faculty of Law, Iran
m.fazayeli@qom.ac.ir

الملخص

تتناول هذه الدراسة موضوع الحرب السيبرانية باعتبارها أحد أخطر التهديدات الأمنية المعاصرة، التي تشكل تحديًا حقيقيًا لسيادة الدول واستقرارها الداخلي، دون الاعتماد على الأسلحة التقليدية. وتركز الدراسة على تحديد مفهوم الحرب السيبرانية وخصائصها، وتحليل آثارها على البنى الأمنية والاقتصادية والسياسية، مع إبراز خصوصية هذه الظاهرة في البيئة الرقمية. وتعتمد الدراسة المنهج الوصفي التحليلي من خلال استقراء الواقع وتحليل المؤشرات العامة، لإبراز الجوانب المفاهيمية والاستراتيجية المرتبطة بالحرب السيبرانية. وتوصلت الدراسة إلى أن غياب الإطار القانوني المتكامل، وضعف التنسيق المؤسسي، ونقص الكوادر المتخصصة تمثل أبرز المعوقات في التصدي الفعال للهجمات السيبرانية، في حين تبرز فرص واعدة تتمثل في توفر الطاقات الشبابية، والانفتاح على التعاون الدولي، وزيادة الوعي السياسي بأهمية الأمن السيبراني. وفي ضوء ذلك، قدمت الدراسة مجموعة من التوصيات التي تهدف إلى تطوير مقاربة وطنية شاملة تعزز من حماية الفضاء السيبراني العراقي.**الكلمات المفتاحية:** الحرب السيبرانية، تهديدات الأمن الوطني، التعاون الدولي، التشريع العراقي، الاستراتيجيات الوطنية، التحديات القانونية، التحديات التنظيمية.

Abstract:
This study addresses the topic of cyber warfare as one of the most serious contemporary security threats, posing a real challenge to the sovereignty of states and their internal stability, without relying on conventional weapons. The study focuses on defining the concept of cyber warfare and its characteristics, and analyzes its impacts on security, economic, and political structures, highlighting the uniqueness of this phenomenon in the digital environment. It adopts a descriptive-analytical approach by examining the reality and analyzing general indicators to highlight the conceptual and strategic aspects related to cyber warfare. The study concludes that the absence of a comprehensive legal framework, weak institutional coordination, and shortage of specialized personnel represent the main obstacles to effectively countering cyberattacks. At the same time, promising opportunities emerge in the form of available youth talents, openness to international cooperation, and increasing political awareness of the importance of cybersecurity. Accordingly, the study presents a set of recommendations aimed at developing a comprehensive national approach to strengthen the protection of Iraq's cyberspace.**Keywords:** Cyber warfare, national security threats, international cooperation, Iraqi legislation, national strategies, legal challenges, regulatory challenges.

المقدمة:

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين، وبعد:تعيش البشرية اليوم على وقع تحوّل حضاري واسع تقوده ثورة تكنولوجية غير مسبوقة، امتدت آثارها إلى أدق تفاصيل الحياة، واكتسحت بتطبيقاتها الذكية مختلف البنى الاقتصادية والاجتماعية والثقافية وحتى الأمنية، حيث لم يعد العالم كما عرفناه من قبل؛ فالعلاقات الإنسانية باتت تُدار رقمياً، والحدود الجغرافية انهارت أمام سطوة الفضاء السيبراني

الذي بات يمثل بُعدًا موازياً للواقع، بل أحيانًا بديلاً عنه.في هذا العالم الافتراضي، لم تعد شخصية الإنسان مقترنة بجسده وحده، بل أصبحت بياناته، صوره، وآراؤه المنتشرة عبر الفضاء الرقمي تشكّل امتدادًا افتراضيًا له، قد يبقى حيًّا حتى بعد وفاته بسنوات أو حتى قرون، من هنا، يبرز سؤال محوري: من يحمي هذا الامتداد؟ وكيف يمكن للدول أن تضمن أمن مواطنيها في هذا الفضاء المفتوح أمام كل الاحتمالات؟لقد فرضت الحرب السيبرانية نفسها كواحدة من أخطر أدوات الصراع المعاصر، حيث لم تعد الحروب تُخاض فقط بالأسلحة التقليدية، بل أصبحت تُدار عبر "كودات برمجية" تنفذ هجماتها الخفية على أنظمة الدولة الحيوية، من البنية التحتية للطاقة إلى الاتصالات والمؤسسات المصرفية والأمنية، ولم تعد تهديدات الأمن المعلوماتي تقتصر على القرصنة الفردية أو التسريبات العرضية، بل تحوّلت إلى استراتيجيات حرب منظمة، تنفذها أطراف دولية وجهات فاعلة غير تقليدية، بغرض زعزعة الأمن القومي واستهداف السيادة الرقمية للدول.وبما أن أمن المعلومات بات يُصنَّف ضمن أولويات الأمن الوطني، فإن المنظومة القانونية أصبحت مطالبة بتجاوز الأطر الكلاسيكية، من أجل تقديم مقاربة عصرية قادرة على استيعاب هذا النمط الجديد من التهديدات، فالحرب السيبرانية تطرح إشكاليات قانونية دقيقة ومعقّدة تتعلق بتحديد المسؤولية، وشرعية الرد، وحدود التدخل، ومدى كفاية التشريعات الوطنية في ردع أو احتواء هذا النوع من المخاطر.وانطلاقًا من هذا الواقع، تسعى هذه الدراسة إلى تقديم قراءة قانونية معاصرة لمفهوم الحرب السيبرانية، وتبيان أثرها في تهديد أمن المعلومات الوطني، من خلال تحليل الإطار القانوني الوطني والدولي، واستكشاف مدى قدرة أدوات القانون العام في مواجهة هذه التحديات الحديثة، لا سيما في الدول النامية التي تعاني من هشاشة رقمية وقصور تشريعي.

أهمية الدراسة

تنبع أهمية هذه الدراسة من طبيعة الموضوع الذي تتناوله، إذ تُعد الحرب السيبرانية من أخطر التحديات التي تواجه الأمن القومي في العصر الرقمي، نظرًا لما تفرزه من تهديدات غير تقليدية تمس صميم البنية التحتية للدولة، ولا سيما أنظمة المعلومات الحيوية والمؤسسات الحكومية والقطاعات الحساسة.وتبرز الأهمية العلمية للبحث في أنه يُقدّم قراءة قانونية معاصرة لهذا النوع من الحروب، من خلال تسليط الضوء على مدى كفاية الإطار التشريعي الحالي، وقدرة أدوات القانون العام على الاستجابة لمخاطر غير مادية، متغيرة، ولا مرئية، ما يجعل من المقاربة القانونية أمرًا حتميًا لضمان سيادة الدولة في الفضاء السيبراني، وحماية أمنها المعلوماتي.كما تكتسب هذه الدراسة أهمية عملية في ظل ما تشهده الدول من تصاعد الهجمات السيبرانية الموجهة، وخصوصًا الدول ذات البنية الرقمية الهشة أو غير المؤمنة بالكامل، مثل العراق، إذ تفتقر إلى منظومة قانونية متكاملة قادرة على المواجهة الوقائية والردعية الفعالة. ومن هنا، فإن هذه الدراسة لا تقدم توصيفًا للواقع فحسب، بل تسعى إلى بناء تصور قانوني عملي يُمكن أن يسهم في صياغة سياسات واستراتيجيات تشريعية ومؤسساتية تعزز من صلابة الأمن السيبراني الوطني، وتحافظ في الوقت ذاته على التوازن بين الأمن والحريات الرقمية.

إشكالية الدراسة:

شهدت السنوات الأخيرة تناميًا غير مسبوق في حجم الهجمات السيبرانية التي تستهدف البُنى المعلوماتية الحيوية للدول، مما أدى إلى تحول "الحرب" من مفهومها التقليدي المرتبط بالمواجهة المسلحة، إلى شكل جديد غير تقليدي وغير مرئي، يتم عبر الفضاء الإلكتروني، ويُعرف بـ"الحرب السيبرانية". هذه الحرب لا تستهدف الأفراد فحسب، بل تُهدد الأمن الوطني برمّته، من خلال ضرب قواعد البيانات، وتعطيل شبكات الاتصالات، والتلاعب بالبنى التحتية للمرافق العامة، بما يشمل الكهرباء، المياه، والقطاع المالي، وحتى المؤسسات السيادية للدولة.ورغم خطورة هذا النوع من الحروب، إلا أن التشريعات الوطنية في كثير من الدول، ومنها العراق، ما زالت متأخرة عن مواكبة هذه التهديدات، إذ تعاني من غياب قوانين سيبرانية شاملة، ومن ضعف في آليات الردع والمساءلة، فضلًا عن تداخل الصلاحيات بين الجهات الحكومية، وغياب الهيئات السيبرانية المستقلة ذات الطابع التنفيذي والرقابي.من هنا تبرز **مشكلة الدراسة** في التساؤل الجوهري الآتي:**إلى أي مدى تُشكل الحرب السيبرانية تهديدًا مباشرًا لأمن المعلومات الوطني؟ وهل تملك الدولة، من خلال أدوات القانون العام والتشريعات المعاصرة، القدرة الكافية على مواجهتها والحد من آثارها؟**

فرضيات الدراسة:

١. تُشكّل الحرب السيبرانية تهديدًا جوهريًا ومتعدد الأبعاد لأمن المعلومات الوطني، يتجاوز قدرة التشريعات التقليدية على الاستجابة الفاعلة.

٢. الإطار القانوني الحالي في العديد من الدول، ومنها العراق، لا يزال قاصرًا عن معالجة التحديات الناجمة عن الحرب السيبرانية بسبب غياب تشريعات سيبرانية متخصصة.

٣. تعزيز أدوات القانون العام وتحديث التشريعات الوطنية يساهم بشكل مباشر في بناء منظومة فعالة لحماية الأمن السيبراني الوطني.

٤. التكامل بين البعد القانوني والمؤسسي والبعد التقني يمثل السبيل الأنجع لمواجهة الحرب السيبرانية وضمان السيادة الرقمية.

المبحث الأول الإطار المفاهيمي للحرب السيبرانية وأمن المعلومات الوطني

أدى التحول الرقمي المتسارع إلى نشوء فضاء جديد للصراع لا يخضع للحدود التقليدية، يتمثل في الفضاء السيبراني، حيث باتت الهجمات المعلوماتية تشكل تهديدًا فعليًا لأمن الدول ومؤسساتها الحيوية، وقد أصبحت الحرب السيبرانية إحدى أبرز مظاهر هذا التهديد، بما تحمله من أدوات غير تقليدية وأهداف تمتد إلى البنى التحتية، والبيانات السيادية، والسيطرة على المعلومات، وفي ظل هذا التطور، برز مفهوم "أمن المعلومات الوطني" كمجال حيوي لحماية الكيان الرقمي للدولة وضمان استقرارها. ومن هنا، يهدف هذا المبحث إلى إيضاح المفهومين المتداخلين: الحرب السيبرانية من جهة، والأمن الوطني للمعلومات من جهة أخرى، عبر عرض تأصيلي لكل منهما في مطلبين مستقلين، كما يلي:

المطلب الأول مفهوم الحرب السيبرانية

تتكوَّن عبارة "الحرب السيبرانية" من كلمتين: "الحرب" و"السيبرانية"، ولكلٍّ منهما أصل لغوي يمكن الوقوف عليه قبل التوسّع في المدلول الاصطلاحي. حيث تُعرَّف الحرب في اللغة العربية بأنها "القتال بين جماعتين أو أكثر"، وتُستخدم للدلالة على النزاع المسلح بين الدول أو القبائل أو الفرق، وقد جاء في لسان العرب: «الحَرْب: نقيض السِّلم، والحرب تكون بين الناس إذا اقتتلوا» (ابن منظور، لسان العرب، مادة (حرب)، دار صادر، بيروت، ط.٣، مجلد ١، ص ٦٠٥)و الحرب: القتال، والمقاتلة، والنِّزاع بين الطوائف إذن، تدل "الحرب" لغةً على الصراع القائم بين طرفين أو أكثر، غالبًا ما يُستخدم فيه السلاح أو القوة لإلحاق الأذى أو فرض السيطرة.لكن التطور التكنولوجي الهائل الذي شهدته العقود الأخيرة أضفى بعدًا نوعيًا على مفهوم الأمن الوطني، تمثل في بروز الفضاء السيبراني باعتباره مجالًا استراتيجيًا جديدًا يستوجب الحماية والتنظيم. وقد أدى ذلك إلى بروز مصطلح "السيبرانية"، المشتق من الكلمة اليونانية"" (إن لفظ "السيبر" "Cyberمأخوذ من الكلمة اليونانية " ،"والتي تعني "قائد الدفّة" أو "الموجه مجمع اللغة العربية بالقاهرة، المعجم الموحد لمصطلحات الحاسبات والإنترنت والاتصالات، المنظمة العربية للتربية والثقافة والعلوم (ألكسو)، تونس، ٢٠٠٠م) التي تعني "القبطان" أو "من يقود السفينة ويوجهها بحكمة وسط الأمواج"، وهو تشبيه دقيق يعكس الدور الذي يؤديه من يتحكم في الأنظمة الرقمية الحديثة، ويسهر على حمايتها من الانزلاق نحو الفوضى أو الوقوع في قبضة التهديدات الرقمية لا سيما بما تكتسبه من مدلول خاص في الخطاب المعلوماتي والقانوني، وأصبحت تشير إلى الفضاء الرقمي اللامادي، أي ذلك الحيّز الإلكتروني غير الملموس الناتج عن التفاعل المعقّد بين الأجهزة الحاسوبية، وشبكات الاتصال، وقواعد البيانات(نوربرت فينر، السيبرنطيقا – علم التحكم والتواصل في الحيوان والآلة، ترجمة: الدكتور عبد السلام رضوان، سلسلة عالم المعرفة، الكويت، العدد ٢١٧، ١٩٩٧م)والمستخدمين، وأنظمة التحكم المؤتمتة. وهذا الفضاء، رغم لا مادّيته، أضحى يشكل جزءًا لا يتجزأ من البنية التحتية للدولة، ومسرحًا فعليًا لتهديدات تمس الأمن الوطني للمعلومات وتتطلب يقظة تشريعية وتقنية متقدمة.في المعاجم العربية الحديثة، مثل "المعجم الوسيط" و"معجم اللغة المعلوماتية"، يُقصد بـ"سيبراني" كل ما يتعلّق بالشبكات الإلكترونية أو الفضاء الرقمي، مثل: الأمن السيبراني، الهجوم السيبراني، الفضاء السيبراني. وعندما نجمع بين الكلمتين، تولّد لدينا تعبير "الحرب السيبرانية" الذي يشير إلى النزاع الإلكتروني أو الصراع الرقمي، وهو صراع تدور رحاه في فضاء الإنترنت والشبكات الإلكترونية،(نوربرت فينر، السيبرنطيقا – علم التحكم والتواصل في الحيوان والآلة، ترجمة: الدكتور عبد السلام رضوان، سلسلة عالم المعرفة، الكويت، العدد ٢١٧، ١٩٩٧م) يتضمن استخدام البرمجيات الخبيثة، الهجمات على البنى التحتية الرقمية، والتلاعب بالبيانات بهدف تشويش أو تدمير نظم دولية، دون الحاجة إلى القوة المادية المباشرة، وهذا الاستخدام اللغوي حديث ومتطوّر، لكنه قائم على جذور لغوية قديمة من خلال اشتقاق السيادة والتحكم من النظام والتحكم، والرابطة بين الحرب كأداة للصراع، والفضاء الإلكتروني كساحة للصراع غير التقليدي.وبالتالي، فإن "الحرب السيبرانية" لغةً تُشير إلى صراعٍ يدور في الفضاء الرقمي باستخدام أدوات إلكترونية، وهو نزاع لا يُمارس فيه العنف الجسدي المباشر، بل تُستخدم فيه وسائل تكنولوجية لاختراق أو تدمير نظم إلكترونية تخص طرفًا آخر. (أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التظيم الدولي المعاصر، المرجع السابق، ص ٦١٦)لقد أفرز التطور التكنولوجي المتسارع في العقود الأخيرة واقعًا جديدًا فرض على الدول مراجعة منظوماتها الأمنية والدفاعية بما ينسجم مع طبيعة التهديدات المستجدة في البيئة الرقمية. وفي هذا السياق، ظهر مصطلح "الحرب السيبرانية" بوصفه أحد المفاهيم الحديثة التي تنتمي إلى نمط الحروب غير التقليدية، والتي تُدار عبر الفضاء الإلكتروني باستخدام أدوات تقنية متقدمة، بعيدًا عن ميادين القتال المعروفة. وقد أثار هذا المصطلح منذ ظهوره اهتمام الباحثين وصانعي القرار على حد سواء، نظرًا لما ينطوي عليه من دلالات قانونية وسياسية وعسكرية جديدة، تقتضي إعادة النظر في مفاهيم السيادة، والدفاع، والأمن الوطني.من الناحية الاصطلاحية، يمكن تعريف الحرب السيبرانية بأنها: "استخدام الهجمات الإلكترونية الموجهة ضد أهداف رقمية تابعة لدولة ما، بقصد تعطيل بنيتها التحتية المعلوماتية أو شل مؤسساتها الحيوية أو التأثير في قرارها السياسي أو الاقتصادي، سواء كان ذلك ضمن نزاع دولي معلن، أو في سياق توترات غير معلنة بين الدول أو الجهات الفاعلة". وقد عرّفت وزارة الدفاع الأمريكية "الحرب

السيبرانية" بأنها "العمليات التي تستخدم قدرات الحوسبة والاتصالات بقصد تعطيل أو إتلاف أو السيطرة على أنظمة العدو المعلوماتية، سواء كانت مملوكة للقطاع العام أو الخاص"(محمد حسن الزعبي، الحرب السيبرانية، التهديد الجديد للأمن القومي، عمان: دار الحامد، ٢٠١٩، ص ٢١-٢٢) ولا تقتصر الحرب السيبرانية على مجرد عمليات التخريب أو إتلاف البيانات، بل تتضمن أنشطة تجسسية واستخباراتية معقدة، كاختراق شبكات المؤسسات الحكومية، أو سرقة الأسرار العسكرية والاقتصادية، أو التأثير في الرأي العام عبر التضليل الإعلامي الرقمي، كما حدث في الانتخابات الأميركية عام ٢٠١٦، أو في تعطيل خدمات حيوية كما في الهجوم السيبراني على منشآت النفط السعودية في "أرامكو" عام ٢٠١٢. إن هذا النوع من الحروب يتميّز بعدة خصائص تجعله مختلفًا عن الحروب التقليدية، من أبرزها: الخفاء والإنكار واللا مركزية، حيث يصعب تحديد الجهة المعتدية بدقة، كما يمكن تنفيذ الهجمات عن بُعد دون أن تكون هناك مواجهة مباشرة (حمد فوزي عبد العزيز، الحرب السيبرانية وأثرها في القانون الدولي الإنساني، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، ٢٠٢٠ ، ص١٧)ومن الناحية القانونية، يطرح مفهوم الحرب السيبرانية تحديات كبيرة على القانون الدولي الإنساني، خاصة فيما يتعلق بمسألة توصيف الفعل العدائي السيبراني وهل يرقى إلى مرتبة "العدوان" بموجب ميثاق الأمم المتحدة، أم أنه يظل دون العتبة القانونية التي تسمح برد فعل مسلح من الدولة المعتدى عليها. كما تثار إشكالية التمييز بين الفاعلين، إذ أن الهجمات السيبرانية قد تنفذها جهات غير حكومية مثل الجماعات الإرهابية أو القراصنة المدعومين من دول، وهو ما يربك مبدأ مسؤولية الدولة في القانون الدولي، ويضعف إمكانية الرد بالمثل وفقًا لقواعد القانون الدولي التقليدي.ويلاحظ أن الحرب السيبرانية لا تتقيد بأزمنة أو أماكن محددة، ولا تخضع للقواعد العسكرية المعروفة من هدنة أو إعلان حرب أو اتفاقيات جنيف، بل تحدث فجأة، وتُدار عن بعد، ولا يُعرف غالبًا من يقف خلفها. ويكفي أن يُستهدف نظام تشغيل أو خادم بيانات في إحدى المؤسسات الحكومية أو منشآت البنى التحتية (كالماء، الكهرباء، الطيران، الاتصالات) حتى تُشلّ حركة الدولة، أو يُصاب الاقتصاد بالجمود، أو تفقد المؤسسات قدرتها على اتخاذ القرار.(بشار خليل، ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي، مجلة الثقافة المعلوماتية، العدد ١٥٤ | آب (اغسطس)-٢٠٢٠، انظر الرابط Syrian Computer Society تاريخ الزيارة ٢٠٢٥/٧/١٨)ومن أبرز الأمثلة على الحروب السيبرانية الكلاسيكية ما يُعرف بفيروس Stuxnet الذي يُعتقد أنه استُخدم في العام ٢٠١٠ لتخريب منشآت نووية إيرانية، حيث استطاع هذا الفيروس إتلاف أجهزة الطرد المركزي في منشأة "نطنز"، دون الحاجة لأي تدخل عسكري تقليدي، مما أظهر حجم القوة التدميرية التي يمكن أن تُحدثها الحرب السيبرانية بصمت ودقة.وبالنتيجة، فإن الحرب السيبرانية لم تعد خيارًا نظريًا أو ساحة تنافس بين الدول العظمى فقط، بل أصبحت واقعًا يوميًا يشهده العالم في شكل صراعات خفية، تتخذ من الفضاء الرقمي ساحة لها، وتستهدف زعزعة استقرار الدول، وإضعاف سيادتها، وتهديد أمنها الوطني. وفي ظل هذا التطور المفاهيمي، أصبح من الضروري توسيع مفهوم أمن الدولة ليشمل إلى جانب الحدود الجغرافية والسيادة الترابية، السيادة الرقمية، بوصفها مجالًا مستحدثًا يجب أن يُصان، وأن تُبنى له قدرات دفاعية وتشريعات وطنية تُمكّن الدولة من مجابهة هذا النوع من التهديدات.(منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، ٢٠١٧، لبنان، ص٢٥)

المطلب الثاني مفهوم الأمن الوطني للمعلومات.

يُعدُّ الأمن الوطني للمعلومات أحد الأركان الحيوية في منظومة الأمن القومي للدول الحديثة، في ظل التحول الرقمي المتسارع، واعتماد الحكومات والقطاعات الحيوية على التكنولوجيا الرقمية في إدارة شؤونها السيادية والاقتصادية والعسكرية، وتتزايد أهمية هذا المفهوم مع تصاعد التهديدات السيبرانية التي تستهدف البنية المعلوماتية للدول، وتعرضها للاختراق، أو التلاعب، أو التدمير، مما يشكل تهديدًا مباشراً للسيادة الوطنية.يشكل الأمن الوطني للمعلومات أحد الأعمدة الأساسية في بنية الدولة الحديثة، لا سيما في ظل تنامي الاعتماد على الفضاء الرقمي في تسيير شؤون الحكم، وإدارة المرافق الحيوية، والتواصل الداخلي والخارجي. ومع تطور الوسائل التكنولوجية، لم تعد التهديدات الأمنية مقتصرة على العدوان التقليدي، بل أصبحت تمتد إلى المجال المعلوماتي، مما يجعل الحفاظ على أمن المعلومات مسألة تتعلق مباشرة بسيادة الدولة واستقرارها.(مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد ١٠، العدد ١، ٢٠٢١، ص ١٥٢)من الناحية اللغوية، فإن كلمة "أمن" تعني نقيض الخوف، وتدل على الطمأنينة وغياب التهديد، حيث يقال: "أمن من الشيء" أي شعر بالاطمئنان حياله، فكلمة "الأمن" في اللغة العربية ترتبط بالطمأنينة والسلام، وهي نقيض الخوف، وقد ورد هذا المعنى في القرآن الكريم في أكثر من موضع، من بينها قوله تعالى: {الذي أطعمهم من جوعٍ وآمنهم من خوف}[قريش: ٤]، كما يَرد الأمن كنعمة تُقابل الجوع والخوف، ويُمنّ الله بها على عباده، وكذلك قوله تعالى: {ادخلوها بسلام آمنين}[الحجر: ٤٦] والذي يبرز فيه الأمن كحالة من السلام النفسي والجسدي داخل الجنة وقد جاء في لسان العرب لابن منظور أن الأمن هو السكون والطمأنينة، وذهاب الخوف، أما "المعلومات" فهي جمع "معلومة"،

مأخوذة من "علم"، والمعلومة تعني ما يمكن إدراكه وفهمه وتخزينه واسترجاعه، وقد أصبحت الكلمة تُستخدم للدلالة على المحتوى المنظم من البيانات ذات الدلالة، خاصة في المجال الرقمي.(شعبان عبد العاطي عطية واخرون، المعجم الوسيط، المرجع السابق، ص٢٨)أما من حيث الاصطلاح، فإن الأمن الوطني للمعلومات يُقصد به الحالة التي تسعى الدولة إلى تحقيقها للحفاظ على سرية وسلامة واستمرارية الوصول إلى المعلومات المتعلقة بمؤسساتها وبناها التحتية الحيوية، ومنع التسلل إليها أو التلاعب بها أو تدميرها. وتُدرج ضمن هذا الإطار كافة التدابير الوقائية والتشريعية والتنظيمية التي تعكف الدولة على وضعها لحماية بيئتها المعلوماتية من المخاطر الداخلية والخارجية، وذلك باعتبار أن أي اختراق لمصادر المعلومات الحيوية قد يؤدي إلى شلل في القطاعات السيادية أو الاقتصادية أو الأمنية. ويُعتبر الأمن السيبراني أحد المرتكزات الأساسية لتحقيق هذا النوع من الأمن، إذ يمثل خط الدفاع الأول أمام التهديدات الرقمية والهجمات الموجهة إلى الأنظمة الحساسة.ويندرج تحت مظلة الأمن المعلوماتي الوطني مختلف المجالات التي تعتمد على البيانات الإلكترونية، ومنها أنظمة الطاقة، والاتصالات، والمصارف، والمجالات العسكرية، والمنشآت الاستراتيجية، ما يجعل أي تهديد موجه نحو تلك البنى لا يُعد مجرد جريمة تقنية، بل قد يرتقي إلى مصاف العدوان على أمن الدولة نفسه، ولهذا السبب، بات من الضروري أن تتبنى الدول منظومة قانونية وتشغيلية متكاملة لتعزيز أمنها المعلوماتي، بما يتلاءم مع التطورات المتسارعة في تكنولوجيا المعلومات وتكتيكات الحروب السيبرانية.(إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد ٦، العدد ٢، ٢٠٢٢، ص ١٤٦.)وفي هذا السياق، نشأت الحرب السيبرانية بوصفها شكلاً جديدًا من الحروب غير التقليدية، لا تُخاض بالأسلحة المادية التقليدية، بل تُدار عن بُعد، باستخدام أدوات رقمية معقدة تستهدف البنية التحتية المعلوماتية للدول، وتُحدث آثارًا تماثل في خطورتها آثار الحروب الكلاسيكية، وربما تفوقها في بعض الأحيان، لما تنطوي عليه من قدرة عالية على إرباك الأنظمة، وإفشاء الأسرار الوطنية، وتعطيل الخدمات الحيوية، وبث الفوضى والذعر داخل المجتمعات المستهدفة. فالهجمات السيبرانية قد لا تُحدث دمارًا ملموسًا في البنية التحتية المادية، لكنها تُصيب العصب الحساس للدولة الحديثة، والمتمثل في أنظمتها المعلوماتية، ما يجعلها من أخطر التهديدات في العصر الرقمي.لقد غيّرت الحرب السيبرانية من طبيعة المفاهيم الاستراتيجية المرتبطة بالأمن والدفاع، وأعادت تشكيل أولويات الدول في مجال الأمن القومي، إذ لم يعد الدفاع عن الوطن محصورًا في حماية حدوده البرية والبحرية والجوية، بل أصبح يشمل بعدًا رابعًا يتمثل في "الفضاء السيبراني" الذي بات يشكّل مسرحًا جديدًا للنزاعات والصراعات بين الدول، وبيئة خصبة لأعمال التجسس والتخريب والاستهداف المعلوماتي. وبذلك، لم يعد الأمن الوطني يُقاس فقط بمستوى التسليح العسكري أو الانتشار الاستخباراتي، بل أصبح مرتبطًا أيضًا بمدى قدرة الدولة على تأمين فضائها الرقمي، وحماية أنظمتها وشبكاتها المعلوماتية من التسلل والتلاعب.(زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، ٢٠٢٠ المجلد ١، العدد ٤٤/١، ٢٠٢٠، ص ٥٢)ومن هنا، برز مفهوم "أمن المعلومات الوطني" كمكون أساسي من مكونات السيادة الحديثة، وكمجال مستقل يتطلب سياسات وطنية واستراتيجيات شاملة لمواجهة التهديدات الرقمية المعقدة. فالحرب السيبرانية لا تعتمد على جيوش نظامية، بل على قراصنة محترفين، وكيانات غير حكومية، وجماعات متخفية تتبع أحيانًا لدول، وتعمل بأساليب غير تقليدية يصعب تتبعها أو إثبات مسؤوليتها المباشرة. وهذا ما يجعل التصدي لها أكثر صعوبة، ويستدعي تطوير قدرات دفاعية متقدمة، تشمل الإنذار المبكر، والتتبع الرقمي، والتحصين التكنولوجي، إضافة إلى تعزيز الوعي المجتمعي حول الأمن الرقمي.(مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق، المجلد ٢، العدد ٢٠، ٢٠٢٠، ص ٥٧)إن تهديدات الحرب السيبرانية لا تستهدف فقط المؤسسات العسكرية أو السياسية، بل قد تضرب في صميم الحياة اليومية للمواطنين، من خلال تعطيل شبكات الكهرباء، أو التحكم بشبكات النقل، أو اختراق الأنظمة الصحية، أو نشر الشائعات والمعلومات المضللة لزعزعة الثقة بالمؤسسات، وهو ما يجعل الفضاء السيبراني ميدانًا لا تقل فيه المعركة ضراوة عن ساحات الحرب المسلحة، بل قد تكون أكثر خطورة بسبب عنصر المباغتة وسرعة التنفيذ، والانخفاض النسبي لتكلفة الهجوم مقارنة بالهجمات التقليدية(رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ديسمبر ٢٠١٨، ص٣٤٦)

المبحث الثاني: الاستراتيجيات والتحديات في مواجهة الحرب السيبرانية

في ظل التصاعد المتزايد للهجمات السيبرانية عالميًا، تبرز الحاجة الملحة إلى تبني سياسات واستراتيجيات فعالة لتعزيز الأمن السيبراني، خاصة في الدول التي لا تزال في طور بناء بنيتها الرقمية، مثل العراق. وفي هذا السياق، يسلط هذا المبحث الضوء على ملامح الجهود المبذولة لمواجهة الحرب السيبرانية على المستويين الدولي والوطني، مع بيان التحديات والفرص التي تواجه العراق في هذا المجال، وسنتناول ذلك من خلال مطلبين كالآتي:

المطلب الأول :الإستراتيجيات الدولية والوطنية لمكافحة الحرب السيبرانية

بعد أن أصبحت الحرب السيبرانية من أخطر التهديدات التي تواجه الأمن القومي في العصر الحديث، لما تتسم به من سهولة في التنفيذ، وقلة في التكلفة، وصعوبة في تعقب الفاعلين، إلى جانب قدرتها على استهداف البنى التحتية الحيوية للدول، لم يكن ردّ الفعل الدولي تجاه هذا التهديد موحدًا، بل تباينت السياسات والإجراءات المتخذة من دولة لأخرى، وفقًا لمستوى التقدم التقني والإطار القانوني والمؤسساتي المتاح. وفي هذا السياق، سيتم عرض أبرز الاستراتيجيات التي اعتمدتها الدول في مواجهة هذا الخطر المتصاعد، ثم الانتقال إلى دراسة واقع التصدي له في العراق، وبيان مدى فعالية الإطار القانوني والمؤسساتي القائم في التعامل مع هذا النوع المعقّد من التهديدات.(بن عربية رياض التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا، دفاتر البحوث العلمية، المجلد ١٠، العدد ١، ٢٠٢٢، ص ٤٦٣)

أولًا: الاستراتيجيات الدولية في مكافحة الحرب السيبرانية مع تطور التكنولوجيا الرقمية وانتشار استخدام الإنترنت والأنظمة المعلوماتية على نطاق واسع، أصبحت الدول أكثر عرضة لمخاطر جديدة تهدد أمنها القومي، تتمثل في الهجمات السيبرانية التي باتت جزءًا لا يتجزأ من الصراعات المعاصرة. هذه الهجمات تتميز بقدرتها على تعطيل البنى التحتية الحيوية، وتعريض أنظمة الاتصالات والطاقة والمياه والنقل للخطر، مما يجعلها تهديدًا وجوديًا لأمن الدول. لذلك، تحولت الحرب السيبرانية إلى محور استراتيجي عالمي تتنافس فيه الدول لبناء قدرات ردع وحماية متقدمة تواكب هذا التحدي المعقد، وتلك المواجهة لم تكن عشوائية أو متفرقة، بل شهدت تطورًا منظّمًا عبر تبني استراتيجيات وطنية شاملة، وإنشاء مؤسسات متخصصة، وتطوير أطر قانونية، بالإضافة إلى تعزيز التعاون الدولي والإقليمي لتوحيد الجهود في مواجهة هذه المخاطر العابرة للحدود.

(شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٧ ، العدد ١ يونيو ٢٠٢٠، ص ٧٥٣-٧٥٥)في مقدمة هذه الاستراتيجيات تأتي وضع الخطط الوطنية للأمن السيبراني التي تعدّها دول عظمى مثل الولايات المتحدة الأميركية، وألمانيا، وفرنسا، وكوريا الجنوبية، وغيرها. هذه الاستراتيجيات الوطنية لا تقتصر على الجانب الدفاعي فقط، بل تشمل تطوير أنظمة متقدمة للإنذار المبكر، ومراكز للعمليات الأمنية السيبرانية، وأنظمة الرد السريع على الهجمات، بل وتمتد لبناء قدرات هجومية تتيح للدول فرض ردع فعّال على الجهات المهاجمة.فعلى سبيل المثال، تركز الاستراتيجية السيبرانية الوطنية الأميركية لعام ٢٠٢٣ على مبدأ "المسؤولية المشتركة"، الذي يحمّل كلًا من القطاعين العام والخاص مسؤولية تعزيز الأمن السيبراني، إذ إن أغلب البنى التحتية الرقمية مملوكة للقطاع الخاص أو تُدار من خلاله. وتُشدد الاستراتيجية أيضًا على مفهوم "التدخل الاستباقي"، وهو إجراء يسمح باتخاذ خطوات وقائية قبل وقوع الهجمات، وذلك عبر استخدام تكنولوجيا متقدمة للكشف عن التهديدات السيبرانية وتحليلها واستباقها.موازاة لذلك، أنشأت دول كثيرة هيئات متخصصة تُعنى بالأمن السيبراني، كمركز الأمن السيبراني الوطني في المملكة المتحدة(NCSC) ، ووكالة الأمن السيبراني الألمانية(BSI) ، إذ تقوم هذه المؤسسات بمراقبة النشاط السيبراني على نطاق الدولة، وتنسيق عمليات الاستجابة للحوادث، وتقديم المشورة الفنية، بالإضافة إلى إعداد الدراسات والبحوث التي تساعد في تطوير السياسات الوطنية. هذا الأمر يعكس إدراكًا عميقًا بأن الأمن السيبراني مسؤولية مؤسساتية مشتركة تتطلب تنسيقًا وتعاونًا داخليًا.(إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، ص ١٤٦)أما على الصعيد الدولي، فلا يمكن لأي دولة أن تواجه التهديد السيبراني بمعزل عن غيرها، نظرًا للطبيعة المتداخلة والمتشابكة للشبكة الرقمية. لذا، ظهرت أهمية التعاون الدولي والإقليمي، الذي تجسد في اتفاقيات متعددة الأطراف، أبرزها "اتفاقية بودابست لمكافحة الجرائم السيبرانية" (٢٠٠١)، والتي تعدّ حجر الزاوية في التعاون القانوني الدولي لمواجهة الجرائم الإلكترونية. هذه الاتفاقية تهدف إلى توحيد التعريفات القانونية للجرائم السيبرانية، وتيسير التعاون بين السلطات القضائية، وتشجيع تبادل المعلومات والتقنيات بين الدول، كما أن الاتحاد الأوروبي أسّس "المركز الأوروبي لمكافحة الجريمة السيبرانية"، الذي يعمل ضمن إطار وكالة الشرطة الأوروبية (يوروبول)، لتوفير الدعم الفني والتنسيق بين الدول الأعضاء في مجال التحقيق والرد على الحوادث السيبرانية. وتعد هذه المبادرات نموذجًا حيًا لكيفية ترجمة التعاون الدولي إلى آليات فعالة لمواجهة التهديدات الرقمية (باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد، المجلد ١ ، العدد ٣٦ ، ٢٠٢٣، ص ٢٣)من الناحية التشريعية، اتجهت الدول إلى تطوير أُطر قانونية متطورة لمجاراة التطورات التقنية، حيث تم إدخال تعديلات جوهرية على قوانين العقوبات لتشمل جرائم الاختراق، والاحتيال الإلكتروني، والتجسس السيبراني، والتدمير المادي عبر الهجمات الرقمية. ففي فرنسا، على سبيل المثال، يعتبر الأمن السيبراني جزءًا من قانون الدفاع الوطني، ويُنظر إلى الهجوم السيبراني على أنه شكل من أشكال العدوان يمكن الرد عليه عسكريًا. أما الاتحاد الأوروبي، فقد أنشأ إطارًا قانونيًا قويًا من خلال "اللائحة العامة لحماية البيانات(GDPR) "، التي تضع معايير صارمة لحماية خصوصية البيانات الشخصية، وتلزم المؤسسات باتخاذ إجراءات أمنية مشددة للحد من سرقة المعلومات.(مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، المرجع السابق، ص١٥٢)على

الصعيد الإقليمي، تعمل المنظمات الدولية والإقليمية مثل الأمم المتحدة والاتحاد الدولي للاتصالات على إقرار معايير وقواعد لتعزيز الاستخدام السلمي للفضاء السيبراني، وذلك من خلال تبني قرارات توعوية، وإطلاق مجموعات عمل فنية وقانونية، تهدف إلى تعزيز التعاون وبناء القدرات بين الدول. ورغم ذلك، تبقى هذه المبادرات غير ملزمة قانونيًا، مما يحد من فاعليتها، ويزيد من تحدي إقامة نظام رقابي دولي قادر على ضبط سلوك الدول والفاعلين غير الحكوميين في الفضاء السيبراني هذا إلى جانب وجود هوة رقمية عميقة بين الدول، حيث تمتلك دول العالم المتقدم القدرات التقنية والتنظيمية اللازمة لمجابهة الهجمات السيبرانية، بينما تفتقر الدول النامية، ومنها العراق، إلى البنى التحتية والتقنيات والخبرات الكافية، ما يخلق فجوة في الأمن السيبراني العالمي، ويزيد من عدم الاستقرار ويعمق مخاوف الأمن القومي.(باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة، المرجع السابق، ص ٢٣)

ثانيًا: الجهود الوطنية العراقية لمواجهة الحرب السيبرانية في ظل التطورات التقنية المتسارعة والتحولات العالمية في مجال الأمن السيبراني، أصبح العراق، كغيره من الدول، أمام تحديات حقيقية تتطلب تكثيف الجهود الوطنية لحماية بنيته التحتية المعلوماتية وتأمين بياناته الحيوية، لا سيما وأن الفضاء السيبراني لم يعد مجرد مجال تكنولوجي بحت، بل أصبح ميدانًا معقدًا للصراعات والتنافس الدولي والإقليمي. رغم الظروف الأمنية والسياسية والاقتصادية الصعبة التي شهدها العراق خلال العقود الماضية، لم تغفل الدولة الأهمية المتزايدة للحرب السيبرانية، وسعت إلى اتخاذ خطوات أولية في سبيل بناء إطار وطني للأمن السيبراني، يعكس إدراكًا متزايدًا لخطورة الهجمات الإلكترونية على استقرار الدولة وحماية سيادتها.(ظفر عبد مطر التميمي، العراق والأمن السيبراني ... الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط العراق، المجلد ١٨ ، العدد ٥١ ، ٢٠٢٢ ، ص ١١-١٢)

١ .البعد التشريعي والتنظيمي

يُعد التشريع هو الركيزة الأولى لأي استراتيجية أمنية ناجحة، ومن هنا كانت الحاجة ماسة إلى وضع إطار قانوني شامل يُنظم التعامل مع التهديدات السيبرانية، ويجرّم الأفعال المرتبطة بالاختراق الإلكتروني، والتجسس الرقمي، والتخريب المعلوماتي. إلا أن العراق حتى الآن لم يُصدر قانونًا خاصًا بالأمن السيبراني متكاملًا وفعّالاً، ما يمثل نقطة ضعف واضحة في القدرة الوطنية على مكافحة هذه التهديدات.وعلى الرغم من غياب قانون خاص، فقد تم اعتماد بعض المواد في قانون العقوبات رقم ١١١ لسنة ١٩٦٩، التي تنص على عقوبات ضد الاعتداء على الممتلكات، وبعض الأفعال التي يمكن أن تُفسر على أنها جرائم إلكترونية. إلا أن هذه النصوص كانت عامة، وغير مخصصة لتعقيدات الجرائم السيبرانية، وهو ما يجعل التعامل معها غير كافٍ في مواجهة الهجمات الحديثة التي تستهدف البنى التحتية الحساسة(باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة، المرجع السابق، ص ٢٥)في السنوات الأخيرة، بذلت جهات حكومية وجهود مدنية محاولات لإعداد مسودات قانونية متخصصة في الجرائم الإلكترونية، حيث تناول مشروع قانون الجرائم المعلوماتية قضايا مهمة مثل مكافحة الاحتيال الإلكتروني، وحماية البيانات الشخصية، ومكافحة الاختراقات، لكن تبقى هذه المشاريع قيد الدراسة أو المناقشة ولم تُقر رسميًا حتى الآن. كما أن بعض مواد هذه المشاريع أثارت جدلًا واسعًا فيما يتعلق بحرية التعبير وحماية الخصوصية.

٢ .الهيئات والمؤسسات المسؤولة

يمتد الفضاء السيبراني في العراق إلى عدة قطاعات حكومية، موزعة ما بين وزارات وأجهزة أمنية مختلفة، مما أدى إلى تشتيت الجهود وضعف التنسيق بين الجهات المعنية. لا يوجد حتى اليوم هيئة مركزية مستقلة تُشرف على الأمن السيبراني بشكل مباشر، بل تتقاسم وزارة الداخلية، عبر قسم مكافحة الجرائم الإلكترونية، وجهاز الأمن الوطني، بالإضافة إلى وزارة الاتصالات وتقنية المعلومات، المسؤوليات المتعلقة بحماية الفضاء الرقمي.(عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط١، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١، ص ٧)هذا التداخل في الاختصاصات يؤدي إلى ثغرات في متابعة الحوادث الأمنية، وتأخر الاستجابة، وصعوبة في وضع خطط وطنية موحدة، ويعيق بناء منظومة أمنية متكاملة تُحقق تكاملًا بين القدرات التقنية والقانونية. وهناك حاجة ملحة لإنشاء هيئة وطنية مركزية مستقلة تكون المرجع الأعلى في سياسات الأمن السيبراني، وتعمل على تنسيق الجهود بين الجهات المختلفة، وإعداد الاستراتيجية الوطنية.(مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، المرجع السابق، ص١٥٢)

٣ .**حماية البنى التحتية الحيوية** تُعتبر البنى التحتية الحيوية في العراق، مثل الكهرباء، والمياه، والنقل، والاتصالات، والقطاع المالي، من الأهداف الرئيسية للهجمات السيبرانية، نظرًا لأهميتها الاستراتيجية وحساسيتها الشديدة. ومع التحول الرقمي المتسارع في هذه القطاعات، ارتفعت المخاطر التي تواجهها بسبب ضعف أنظمة الحماية وغياب استراتيجيات متكاملة للدفاع السيبراني.تعاني العديد من القطاعات في العراق من نقص في البنى

التحتية التقنية الحديثة، وانعدام الخبرات المتخصصة في مجال الأمن السيبراني، فضلاً عن ضعف الاستثمارات الموجهة لهذا المجال، ما يجعلها عرضة لهجمات قد تؤدي إلى توقف الخدمات الحيوية أو تعطلها، وهو ما قد ينعكس سلبًا على استقرار الدولة وسلامة المواطنين.(شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، المرجع السابق، ص ٧٦١.)وقد قامت بعض الجهات بمحاولات محدودة لتطبيق حلول تقنية لحماية شبكاتها، مثل تركيب جدران نارية(Firewalls) ، وأنظمة كشف التسلل(IDS) ، وتدريب بعض الكوادر، لكن هذه الخطوات لا تزال غير كافية مقارنةً بحجم التهديدات، ولا تغطي كافة القطاعات الحيوية بشكل شامل.

٤ .**بناء القدرات والتدريب** واحدة من العقبات الرئيسية أمام تعزيز الأمن السيبراني في العراق هي نقص الكوادر المتخصصة، وضعف برامج التدريب والتأهيل في هذا المجال. تتطلب إدارة الأمن السيبراني وجود خبراء قادرين على مراقبة التهديدات، وتحليلها، والاستجابة السريعة، إلى جانب تطوير أنظمة دفاعية مستمرة التحديث(عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط١، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١، ص ٧)بدأت بعض الجامعات والمعاهد العراقية بإدخال برامج تدريبية وورش عمل تهدف إلى رفع مستوى الوعي الأمني والتقني لدى الطلاب والخبراء، كما تنشط بعض المنظمات المدنية في مجال التوعية، لكن هناك حاجة ماسّة إلى دعم حكومي شامل لتأسيس برامج تعليمية متقدمة، وتأهيل مراكز تدريبية وطنية متخصصة، وربطها بالجهات الأمنية والفنية.

٥ .**التعاون الدولي ودوره في تعزيز القدرات الوطنية**نظراً لعدم اكتفاء القدرات المحلية في العراق بمواجهة التهديدات السيبرانية المتطورة، تولي الحكومة العراقية أهمية كبيرة للتعاون مع المنظمات الدولية والإقليمية المختصة. فقد بدأ العراق خطوات في هذا الاتجاه عبر التعاون مع الإنتربول، واليونسيف، والاتحاد الدولي للاتصالات، وبعض المبادرات التي تهدف إلى بناء القدرات وتبادل الخبرات.على سبيل المثال، تسعى بعض المشاريع الدولية إلى دعم العراق في تطوير استراتيجيات للأمن السيبراني، وتقديم تدريبات متخصصة، وتعزيز البنية التحتية التقنية. كما يشكل الانخراط في منتديات الأمن السيبراني الإقليمية والدولية فرصة لتبادل المعلومات، ومواكبة أفضل الممارسات العالمية، والاستفادة من التجارب الناجحة للدول الأخرى.مع ذلك، يواجه العراق تحديات كبيرة في تطبيق هذه الشراكات بفعالية، بسبب عوامل إدارية وتنظيمية، ونقص الموارد المالية، وضعف التنسيق بين الجهات الحكومية المختلفة، مما يحد من الاستفادة القصوى من التعاون الدولي.(باسم علي خريسان الامن في الفضاء السيبراني، دراسة في التهديدات واستراتيجية المواجهة، المرجع السابق، ص٢٣)

٦ .**التوعية المجتمعية وأهمية الشراكة الوطنية**لا يمكن الحديث عن أمن سيبراني قوي دون إشراك المجتمع بشكل كامل، حيث يُعتبر المواطن هو الحلقة الأضعف والأكثر عرضة للاستهداف السيبراني، سواء عبر الاحتيال الإلكتروني، أو الهجمات على الهواتف الذكية، أو سرقة المعلومات الشخصية.يُلاحظ في العراق ضعفاً واضحًا في برامج التوعية والتثقيف السيبراني، على الرغم من المحاولات المتفرقة من قبل بعض المؤسسات التعليمية والمنظمات غير الحكومية. وتظل الحاجة قائمة لإطلاق حملات توعية وطنية واسعة النطاق، تستهدف مختلف فئات المجتمع، وتُعزز ثقافة الاستخدام الآمن للتكنولوجيا، وتعريف الجمهور بخطورة التهديدات وأساليب الحماية.

المطلب الثاني تحديات وفرص تطبيق الاستراتيجيات السيبرانية في العراق

يواجه العراق تحديات كبيرة ومعقدة في مجال الأمن السيبراني، تتجاوز الجوانب التقنية لتشمل أطرًا قانونية وتنظيمية غير مكتملة، حيث يفتقر البلد إلى قوانين شاملة تحكم الجرائم الإلكترونية وتحمي الفضاء الرقمي بشكل فعّال. هذا النقص في التشريعات يضعف من قدرة الجهات المعنية على التصدي للهجمات السيبرانية وملاحقة مرتكبيها، فضلاً عن التداخل والتشتت في الصلاحيات بين المؤسسات المختلفة، مما يعرقل وضع استراتيجية وطنية موحدة. إلى جانب ذلك، يعاني العراق من نقص حاد في الكوادر البشرية المتخصصة، إذ تفتقر العديد من المؤسسات التعليمية إلى برامج تدريبية متقدمة في هذا المجال، كما تندر فرص التدريب والتطوير المهني، ما يحد من قدرة الدولة على بناء فرق أمنية قادرة على مواجهة التهديدات الرقمية المتطورة. هذه التحديات القانونية والتنظيمية والإنسانية تشكل معًا عقبات رئيسية أمام تعزيز الأمن السيبراني وحماية المصالح الوطنية في ظل تصاعد التهديدات العالمية.(ظفر عبد مطر التميمي، العراق والأمن السيبراني، الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط العراق، المجلد ١٨ ، العدد ٥١ ، ٢٠٢٢ ، ص ١١-١٢)

أولاً: التحديات القانونية والتنظيمية في العراق يُعد الإطار القانوني والتنظيمي من الركائز الأساسية لأي نظام فعّال في مواجهة التهديدات السيبرانية التي تزايدت خطورتها وتعقيدها في السنوات الأخيرة. فقد باتت الدول المتقدمة تدرك أن مواجهة هذه التهديدات لا تقتصر على الجانب التقني فقط، بل تتطلب وجود تشريعات قانونية واضحة وشاملة تجرّم الهجمات الإلكترونية، وتضع ضوابط دقيقة لحماية البيانات والمعلومات، وتحدد بوضوح المسؤوليات والعقوبات المترتبة على ارتكاب الجرائم السيبرانية. إضافة إلى ذلك، فإن إنشاء هيئات وطنية متخصصة في الأمن السيبراني تُشرف

على تنفيذ السياسات والاستراتيجيات يشكل عاملاً جوهريًا في ضمان الاستجابة السريعة والمنسقة للتهديدات الرقمية.(باسم علي خريسان الامن في الفضاء السيبراني، دراسة في التهديدات واستراتيجية المواجهة، المرجع السابق، ص ٢٣)أما في العراق، فلا يزال الإطار القانوني والتنظيمي يعاني من ضعف كبير، إذ لم يتم بعد إصدار قانون شامل خاص بالأمن السيبراني يواكب التطورات الحديثة في هذا المجال. وتعتمد القوانين الحالية بشكل رئيسي على نصوص عامة ومجزأة في قانون العقوبات وبعض التشريعات المتعلقة بالجرائم الإلكترونية، وهو ما لا يكفي لمواجهة التعقيدات التقنية والمتنوعة للهجمات السيبرانية. إن هذا النقص التشريعي لا يتيح وضع معايير واضحة للحد من هذه الجرائم، كما يعوق إنشاء بيئة قانونية رادعة تردع المتسللين والمخربين الرقميين، علاوة على ذلك، يعاني العراق من تعدد الجهات التي تتولى مسؤوليات مرتبطة بالأمن السيبراني، حيث توجد جهات مختلفة مثل وزارة الداخلية، جهاز الأمن الوطني، وزارة الاتصالات، بالإضافة إلى بعض الوحدات الأمنية المتخصصة، دون وجود هيئة مركزية مستقلة تضع وتنظم وتنسق السياسات بشكل موحد. يؤدي هذا التداخل وتعدد الصلاحيات إلى تشتت الجهود وتضارب الإجراءات، مما يعيق تطبيق استراتيجية وطنية فعالة وشاملة لمكافحة التهديدات السيبرانية. وفي كثير من الأحيان، ينتج عن هذا التشتت تأخر في الاستجابة للحوادث السيبرانية، وصعوبة في جمع الأدلة اللازمة لإجراء التحقيقات القضائية الناجحة.(منى جبور الاشقر، السيبرانية هاجس العصرالمرجع السابق، ص٢٨)ولا يمكن تجاهل الأثر السلبي للظروف السياسية والاقتصادية التي يمر بها العراق، حيث تؤدي الأزمات المستمرة والتحديات المالية إلى تأجيل تحديث الأطر التشريعية والتنظيمية الخاصة بالأمن السيبراني. ضعف الموارد المالية المخصصة لهذه الملفات ينعكس بشكل مباشر على قدرة الأجهزة الأمنية والقضائية على مواجهة التهديدات الرقمية بكفاءة، سواء من حيث تأهيل الكوادر الفنية أو تحديث المعدات والبرمجيات المستخدمة في حماية الفضاء السيبراني. بالإضافة إلى ذلك، تؤثر هذه الضغوط في قدرة الدولة على توفير التدريب والتوعية اللازمة للكوادر العاملة، مما يزيد من هشاشة الوضع الأمني السيبراني في البلاد.مجمل هذه التحديات القانونية والتنظيمية تشكل حاجزًا كبيرًا أمام بناء منظومة أمنية متكاملة في العراق قادرة على حماية مصالح الدولة والمواطنين في الفضاء الرقمي. فغياب التشريعات الملائمة، والتشتت المؤسسي، والقيود الاقتصادية، تضع العراق في موقف ضعيف أمام المخاطر السيبرانية المتنامية، ما يستدعي إيلاء أولوية قصوى لتطوير الإطار القانوني والتنظيمي، وتوحيد الجهود الوطنية، وتوفير الموارد اللازمة لضمان بيئة رقمية آمنة ومستقرة.

التحديات التقنية والبشرية في الأمن السيبراني بالعراق

تُشكل القدرات التقنية والموارد البشرية ركيزتين أساسيتين لبناء منظومة أمن سيبراني متينة وفعالة، وعلى الرغم من الأهمية القصوى لهذين العنصرين، يواجه العراق العديد من التحديات التي تقف عائقًا أمام تطوير وتأهيل بيئة إلكترونية آمنة.

١. **النقص في البنية التحتية التقنية**على المستوى التقني، يُعاني العراق من قصور كبير في تحديث وتطوير بنيته التحتية الرقمية بما يتناسب مع التطورات الحديثة في مجال الأمن السيبراني. تستخدم أغلب القطاعات الحيوية، سواء كانت حكومية أو خاصة، أنظمة معلومات قديمة أو غير مؤمنة بالشكل الكافي، ما يجعلها هدفًا سهلًا للمتسللين والهجمات السيبرانية. هذه الأنظمة غالبًا ما تفتقر إلى أحدث برامج الحماية وأنظمة الكشف المبكر عن الاختراقات، كما أنها لا تخضع لصيانة مستمرة أو تحديث دوري يواكب تطور التهديدات الإلكترونية.(رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد تسعة وتسعون، ٢٠٢٤، ص ٥٠٩)إضافة إلى ذلك، يلاحظ ضعف الاستثمار في قطاع التكنولوجيا الأمنية، حيث لا تخصص ميزانيات كافية لتأمين الشبكات والأنظمة الرقمية ضد الهجمات المتطورة التي باتت تتسم بالتعقيد والسرعة، مثل البرمجيات الخبيثة المتطورة(Malware) ، وهجمات رفض الخدمة(DDoS) ، والاختراقات التي تستهدف سرقة البيانات أو تعطيل الخدمات الحيوية. ومن المؤسف أن ضعف البنية التحتية لا يقتصر فقط على نقص الأجهزة والبرمجيات، بل يتعداه إلى قلة وجود مراكز متخصصة لمراقبة وتحليل الهجمات السيبرانية، مما يُضعف من قدرة الدولة على رصد التهديدات والتصدي لها في الوقت المناسب.(عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط١، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١، ص ٧)

٢. **نقص الكوادر البشرية المتخصصة** أما من الناحية البشرية، فإن العراق يعاني من شحّ واضح في الكوادر المدربة والمتخصصة في مجال الأمن السيبراني. فقلة المؤسسات التعليمية التي توفر برامج أكاديمية متخصصة في هذا المجال تُعد من أبرز الأسباب التي أدت إلى نقص الخبرات الفنية القادرة على التعامل مع التهديدات السيبرانية الحديثة. كما أن فرص التدريب والتطوير المهني المستمر تعتبر محدودة للغاية، سواء على مستوى القطاع العام أو الخاص.(باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة، المرجع السابق، ص ٣٣)

عدم توفر الخبرات يؤدي إلى اعتماد كبير على خبرات خارجية أو على فرق محدودة العدد، وهذا بدوره يضعف القدرات الوطنية في رصد الهجمات وتحليلها، ووضع خطط الاستجابة السريعة والفعالة، كما يعرقل الابتكار في تطوير تقنيات جديدة للدفاع السيبراني. إضافة إلى ذلك، إن غياب برامج تدريبية منتظمة يترك العاملين في المؤسسات غير مهيئين للتعامل مع أساليب الهجوم الجديدة والمتغيرة باستمرار.

٣. **ضعف التوعية المجتمعية والثقافة الأمنية** جانب آخر مهم من التحديات التي تواجه العراق هو ضعف التوعية المجتمعية والافتقار إلى ثقافة الأمن الرقمي بين المستخدمين. فالعديد من موظفي المؤسسات الحكومية، والعاملين في القطاع الخاص، فضلاً عن الأفراد، يفتقرون إلى المعرفة الكافية بمخاطر الاستخدام غير الآمن للتكنولوجيا، كالبرمجيات غير الموثوقة، أو فتح روابط ورسائل إلكترونية مشبوهة، أو استخدام كلمات مرور ضعيفة، مما يجعلهم عرضة لعمليات الاحتيال الإلكتروني، والتصيد الإلكتروني، وسرقة المعلومات الشخصية.(رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، المرجع السابق، ص ٥١١)هذا النقص في الوعي يساهم بشكل مباشر في نجاح الهجمات السيبرانية، حيث يستغل المهاجمون هذا الجانب البشري كحلقة ضعيفة في سلسلة الحماية، ويستخدمون تقنيات هندسة اجتماعية لاستدراج الضحايا إلى تقديم معلومات حساسة أو تنفيذ إجراءات قد تضر بأنظمة المؤسسات أو أمن البيانات.إن هذه التحديات التقنية والبشرية مجتمعة تشكل حاجزًا حقيقيًا أمام قدرة العراق على بناء منظومة أمن سيبراني متكاملة وفعالة. فغياب البنية التحتية المؤمنة، إلى جانب نقص الخبرات وقلة التوعية، يجعل الفضاء السيبراني العراقي معرضًا لهجمات متزايدة سواء من قِبل جهات فاعلة حكومية أو مجموعات إلكترونية إجرامية أو حتى جهات إرهابية تسعى لتعطيل البنى التحتية الحيوية وإلحاق الضرر بالأمن الوطني.(مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، المرجع السابق، ص٥٧)ولا يمكن إغفال الأهمية الكبيرة للعنصر البشري، فالعراق يتميز بقاعدة شبابية ضخمة، تمتلك حماسة كبيرة للتكنولوجيا وميولًا متزايدة نحو مجالات التقنية الحديثة. هذه الفئة تعد المورد الأهم لبناء القدرات المستقبلية في الأمن السيبراني، وبإمكانها أن تتحول إلى قوة وطنية قادرة على مواجهة التحديات الرقمية إذا ما توفر لها التعليم والتدريب المناسبان. إن الاستثمار في برامج تعليمية متخصصة وتدريبات عملية مستمرة يسهم في تطوير مهاراتهم، ويفتح المجال أمامهم لتطوير حلول مبتكرة تعزز الدفاع السيبراني وترتقي بالمنظومة الوطنية إلى مستويات متقدمة. هذه الكفاءات الجديدة لا تعزز فقط القدرات التقنية، بل تسهم أيضًا في خلق ثقافة أمنية وطنية تستند إلى فهم عميق للمخاطر والحلول.

(مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، المرجع السابق، ص ٥٧)على الصعيد الدولي، تتسع الفرص من خلال التعاون مع منظمات عالمية وإقليمية تعمل في مجال الأمن الرقمي. العراق بدأ بالفعل خطوات مهمة لفتح قنوات التعاون مع جهات مثل الإنتربول والاتحاد الدولي للاتصالات، وغيرها من الهيئات التي توفر دعمًا فنيًا وتدريبيًا يمكن أن يعزز القدرات المحلية بشكل ملحوظ. هذا التعاون لا يقتصر على تبادل الخبرات، بل يمتد إلى الحصول على موارد تقنية متطورة، وأدوات حديثة لمراقبة وتحليل الهجمات السيبرانية، مما يتيح للعراق مواكبة أحدث التطورات العالمية في هذا المجال. كما يمكن أن يُفتح باب الشراكات الاستراتيجية مع دول متقدمة لبناء مشاريع مشتركة تستفيد من خبراتها وتكنولوجياها، علاوة على ذلك، توفر التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة فرصًا غير مسبوقة لتعزيز الدفاعات السيبرانية، و القدرة على استخدام هذه الأدوات المتطورة في مراقبة الفضاء السيبراني تمكن من رصد الهجمات قبل وقوعها، وتحليل سلوكها بدقة فائقة، ما يتيح استجابة أسرع وأكثر فاعلية. تطبيق هذه التقنيات يحتاج إلى رؤية استراتيجية وتخطيط مستدام لتوفير البنية التحتية والكوادر الفنية القادرة على تشغيلها واستثمارها بالشكل الأمثل، وهو ما يجعلها مجالًا واعدًا يستحق التركيز والاستثمار.(شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، المرجع السابق، ٧٥٣-٧٥٥)لتحويل هذه الإمكانيات إلى واقع ملموس، لا بد من اتخاذ خطوات استراتيجية متكاملة تشمل إصدار تشريعات متطورة تنظم الجرائم السيبرانية وتعزز الحماية القانونية للمواطنين والدولة. كما يستلزم الأمر إنشاء هيئة وطنية مستقلة تجمع بين الكفاءة التقنية والقانونية، تكون المرجع الأعلى في السياسات والتنسيق، وتعمل على دمج جهود جميع الجهات الحكومية والخاصة. بناء القدرات البشرية يجب أن يكون على رأس الأولويات، من خلال تطوير برامج تعليمية حديثة وتوفير فرص التدريب المستمر، مع تحديث البنية التحتية التقنية وتأمين التمويل الكافي لها. كذلك، لا يقل أهمية تعزيز التعاون الدولي والمشاركة الفاعلة في الاتفاقيات العالمية، والاستفادة من التجارب الدولية الناجحة. وفي الوقت ذاته، تبقى التوعية المجتمعية ضرورة قصوى لتعزيز ثقافة الاستخدام الآمن للتكنولوجيا، والحد من تأثير الهجمات السيبرانية، مما يخلق بيئة رقمية أكثر أمانًا واستقرارًا.(حازم حمد موسى الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني مقاربة بين المعضلة الأمنية والمكنة الأدائية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد ٥٧ العدد ٥ ٢٠٢٠، ص٥٥٧)

الخاتمة:

تُعد الحرب السيبرانية من أخطر التحديات التي تواجه الدول في العصر الرقمي، لما تنطوي عليه من قدرة على إلحاق أضرار واسعة من دون إطلاق رصاصة واحدة. وقد تبين من خلال هذه الدراسة أن العراق، بوصفه دولة في طور إعادة بناء مؤسساتها الأمنية والقانونية، يواجه مخاطر متزايدة على صعيد أمنه السيبراني، تتداخل فيها الأبعاد التقنية مع الإشكاليات القانونية والقصور في البنية البشرية المتخصصة. ورغم ذلك، لا يخلو المشهد من فرص حقيقية يمكن استثمارها لتعزيز الحصانة الرقمية الوطنية، إذا ما توفرت الإرادة السياسية والتخطيط الاستراتيجي المدروس.

أولاً: النتائج:

١. كشفت الدراسة أن مفهوم الحرب السيبرانية لا يزال يفتقر إلى تعريف قانوني موحد في السياقين الدولي والوطني، مما ينعكس سلبًا على جهود التصدي لها ويُربك آليات المحاسبة القانونية.

٢. الأمن الوطني للمعلومات في العراق يعاني من غياب إطار قانوني شامل، ما يجعل التعامل مع التهديدات السيبرانية يجري في أغلب الأحيان عبر استجابات آنية وغير ممنهجة.

٣. إنّ الاستراتيجيات الدولية، رغم ما تحمله من توجهات متقدمة، لا تتلاءم في كثير من الأحيان مع السياقات المحلية العراقية، سواء من حيث البنية المؤسسية أو من حيث البيئة التكنولوجية المتاحة.

٤. التحديات القانونية تتصدر قائمة المعوقات في العراق، وتشمل ضعف التشريعات السيبرانية، وتداخل الصلاحيات، وغياب التجانس بين الجهات المعنية.

٥. على المستوى البشري، تعاني البلاد من نقص في الكوادر المتخصصة، وغياب ثقافة أمن المعلومات على المستويين الفردي والمؤسسي، إلى جانب ضعف الوعي العام بمخاطر الفضاء الرقمي.

٦. مع ذلك، يمتلك العراق فرصًا واعدة تتمثل في: وجود بنى تحتية رقمية قيد التوسع، والإمكانات البشرية الشابة، والانفتاح المتزايد على التجارب الدولية، فضلًا عن إمكانية توظيف مبادئ الشريعة الإسلامية، خصوصًا في الفقه الإمامي، في بناء إطار أخلاقي وقيمي للحماية السيبرانية.

ثانياً: التوصيات:

١. إعداد قانون وطني شامل للأمن السيبراني، يتضمن تعريفًا واضحًا للحرب السيبرانية، ويحدد الجرائم والجزاءات وآليات الوقاية منها، على أن يستلهم في فلسفته مقاصد الشريعة، لاسيما في جانبها القيمي الذي يؤكد على حرمة التعدي والعبث بالحقوق العامة والخاصة.

٢. تعزيز التعاون بين المؤسسات الأمنية والقانونية والتقنية، عبر إنشاء مجلس أعلى للأمن السيبراني في العراق يضم ممثلين من وزارات العدل والدفاع والداخلية والاتصالات والتعليم العالي.

٣. إطلاق برامج وطنية لتأهيل الكوادر البشرية المتخصصة في مجال الأمن السيبراني، من خلال الجامعات ومراكز التدريب، وربط هذه البرامج بسوق العمل والحاجات الفعلية للمؤسسات العامة والخاصة.

٤. تبني استراتيجيات وقائية تستند إلى الذكاء الاصطناعي والرصد المبكر، بما يضمن التعامل مع التهديدات قبل وقوعها، مع ضمان التوازن بين الأمن الرقمي وحقوق الأفراد وحرياتهم.

٥. نشر الثقافة السيبرانية بين المواطنين من خلال حملات إعلامية وتربوية وتضمين مفاهيم أمن المعلومات في المناهج الدراسية منذ المراحل الأولى.

٦. إطلاق شراكات إقليمية ودولية مرنة مع الدول التي لديها خبرات في هذا المجال، دون التفريط في السيادة السيبرانية، وبما يضمن الاستفادة من أفضل الممارسات مع مراعاة خصوصية الواقع العراقي.

٧. الاستفادة من المبادئ الأخلاقية في الفكر الإسلامي الشيعي، لا سيما في ما يتعلق بمسؤولية الفرد والجماعة، لبناء وعي مجتمعي يجعل من أمن المعلومات واجبًا دينيًا ووطنيًا على حد سواء، ويُسهم في خلق مناعة ذاتية ضد التعدي والاختراق.

قائمة المصادر:

أولاً: القرآن الكريم.

ثانياً: المراجع اللغوية:

١.ابن منظور، لسان العرب، مادة (حرب)، دار صادر، بيروت، ط.٣، مجلد ١.

٢.شعبان عبد العاطي عطية واخرون، المعجم الوسيط، ط ٤، مكتب الشروق الدولية" مجمع اللغة العربية"، مصر، ٢٠٠٤.

٣.الزبيدي، مرتضى بن محمد. تاج العروس من جواهر القاموس، تحقيق مجموعة من العلماء، إشراف عبد الستار أحمد فراج، الكويت: وزارة الأوقاف والشؤون الإسلامية، ١٣٩٩هـ / ١٩٧٩م، ج٣٤.

٤.الفيروزآبادي، القاموس المحيط، مادة (حرب)، دار الفكر، بيروت، ٢٠٠٥.

٥.مجمع اللغة العربية بالقاهرة، المعجم الموحد لمصطلحات الحاسبات والإنترنت والاتصالات، المنظمة العربية للتربية والثقافة والعلوم (ألكسو)، تونس، ٢٠٠٠

ثالثاً: الكتب القانونية:

١.عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط١، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١.

٢.محمد السعيد خشبة، نظم المعلومات الإدارية، دار النشر للجامعات، القاهرة، ٢٠٠٨.

٣.محمد حسن الزعبي، الحرب السيبرانية، التهديد الجديد للأمن القومي، عمان: دار الحامد، ٢٠١٩.

٤.محمد فوزي عبد العزيز، الحرب السيبرانية وأثرها في القانون الدولي الإنساني، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، ٢٠٢٠.

٥.منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، ٢٠١٧، لبنان.

٦.نوربرت فينر، السيبرنطيقا – علم التحكم والتواصل في الحيوان والآلة، ترجمة: الدكتور عبد السلام رضوان، سلسلة عالم المعرفة، الكويت، العدد ٢١٧، ١٩٩٧م.

٧.يوسف حسن يوسف، الحرب السيبرانية: شكل جديد من الحروب في العصر الرقمي، المركز العربي للدراسات الاستراتيجية، القاهرة، ٢٠٢٠.

رابعاً: المجلات والدوريات:

١. إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد ٦، العدد ٢، ٢٠٢٢.

٢.أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد ٨، العدد ٤، كلية القانون، جامعة بابل، العراق ٢٠١٦.

٣.باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد، المجلد ١ ، العدد ٣٦ ، ٢٠٢٣.

٤.بن عربية رياض التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا، دفاتر البحوث العلمية، المجلد ١٠، العدد ١، ٢٠٢٢.

٥.حازم حمد موسى الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني مقاربة بين المعضلة الأمنية والمكنة الأدائية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد ٥٧ العدد ٥ ٢٠٢٠.

٦.رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، ، المجلد ١٥، العدد ٢، ديسمبر ٢٠١٨.

٧.رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد تسعة وتسعون، ٢٠٢٤.

٨.زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، ، ٢٠٢٠ المجلد ١، العدد ٤٤/١، ٢٠٢٠.

٩.شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٧ ، العدد ١ يونيو ٢٠٢٠.

١٠.ظفر عبد مطر التميمي، العراق والأمن السيبراني ... الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، المجلد ١٨ ، العدد ٥١ ، ٢٠٢٢.

١١.عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط١، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١.

١٢.مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، ، المجلد ٢، العدد ٢٠، ٢٠٢٠.

١٣.مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد ١٠، العدد ١، ٢٠٢١

خامساً: الروابط الالكترونية:

١.بشار خليل، ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي، مجلة الثقافة المعلوماتية، العدد ١٥٤ | آب (اغسطس)–٢٠٢٠، انظر الرابط Syrian Computer Society تاريخ الزيارة ٢٠٢٥/٧/١٨.

٢.الرابط الحرب السيبرانية: كيف أصبحت الهجمات الرقمية أداة للصراعات بين الدول؟ – فضاء رقمي آمن وحر || FreeTech ، تاريخ الزيارة ٢٠٢٥/٧/١٩.