مجلة الحكمة للدراسات والأبحاث المجلد 06 العدد 04 (32) 2026/06/30
ISSN print/ 2769-1926 ISSN online/ 2769-1934

Cyberattacks and the challenges of legal adaptation under the rules of international law

Ali Adel Hamza[1]
Al-Qasim Green University
Alia8108@gmail.com

Falah Mahdi Abdulsada[2]
General Directorate of Education in Babylon
Falahmahdi19801980@gmail.com

Received:20/04/2026 **Accepted : 22/06/2026**

Abstract:

While the international community strives to implement the rules of international law aimed at preserving human rights and mitigating the effects and risks of armed conflicts, new forms of these conflicts are emerging. Their danger lies in the lack of a legal framework governing their status under an international instrument, thus increasing their risk. Humans have always sought to develop methods and means of warfare to weaken the enemy's capabilities. For this reason, innovation and development in the military and security sectors have never ceased. This technological advancement has led to the emergence of numerous threats to international peace and security, including a new concept of conflict: cyberattacks and their ongoing repercussions.

The main problem lies in the absence of a legal system addressing this new concept. This has made it difficult to identify attacks, determine their perpetrators, and establish the resulting international responsibility. The danger lies not only in these issues but also in the potential for an increase in such conflicts and a corresponding impunity for perpetrators. Therefore, this study seeks to establish a universally agreed-upon definition and legal

ISSN print/ 2769-1926 ISSN online/ 2769-1934

framework for such attacks, adapting them to international law. It also aims to develop an international charter that defines these concepts and establishes their legal framework, thereby ensuring the international community's objectives of protecting international peace and security. The research employs a descriptive-analytical approach to examine the position of international jurisprudence and law in addressing the research problem, culminating in key findings and recommendations.
Keywords: Cyberattacks, Dimensions of Cyberattacks, International Law.

مجلة الحكمة للدراسات والأبحاث المجلد 06 العدد 04 (32) 2026/06/30
ISSN print/ 2769-1926 ISSN online/ 2769-1934

الهجمات السيبرانية وتحديات التكييف القانوني في ظل قواعد القانون الدولي

م.م علي عادل حمزة[1]
جامعة القاسم الخضراء
Alia8108@gmail.com

م. د فلاح مهدي عبد السادة[2]
المديرية العامة لتربية بابل
Falahmahdi19801980@gmail.com

الملخص :

في الوقت الذي يسعى المجتمع الدولي لتطبيق قواعد القانون الدولي الرامية الى الحفاظ على حقوق الانسان و التقليل من آثار ومخاطر النزاعات المسلحة، تظهر وسائل جديدة لتلك النزاعات، تكمن خطورتها الى عدم تنظيم وضعها القانوني بموجب وثيقة دولية؛ مما يجعل خطرها في تزايد و لطالما سعى الإنسان إلى تطوير أساليب ووسائل حرب لإضعاف قدرات الخصم ولهذا السبب، لم تتوقف عملية الابتكار والتطوير في القطاعين العسكري والأمني، ادى هذا التطور في المجالات التكنولوجية والتقنية الى ظهور العديد من المخاطر التي تهدد الامن والسلم الدوليين وظهور مفهوم جديد لتلك النزاعات وهو الهجمات السيبرانية وآثارها المستمرة .

تكمن المشكلة الرئيسة في عدم وجود نظام قانوني يعالج هذا المفهوم الجديد مما ادى الى صعوبة تحديد الهجوم وتحديد فاعليه والمسؤولية الدولية المترتبة على ذلك، ان خطورة ذلك لا تكمن في تلك المواضيع فقط وانما لزيادة مثل تلك النزاعات من باب والافلات من المسؤولية من باب آخر .

لذلك تسعى الدراسة الى ايجاد مفهوم متفق عليه و الموقف القانوني لمثل تلك الهجمات وتكيفيها القانوني في ظل قواعد القانون الدولي، والسعي لأبرام ميثاق دولي يحدد هذه المفاهيم وتحديد اطارها القانوني بما يضمن تحقيق اهداف المجتمع الدولي بحماية الامن والسلم الدوليين، وانتهج البحث اسلوب الوصف التحليلي لدراسة موقف الفقه والقانون الدولي لمعالجة مشكلة الدراسة التي خلصت في نهايتها الى اهم النتائج والمقترحات.

الكلمات المفتاحية : الهجمات السيبرانية، ابعاد الهجمات السيبرانية، القانون الدولي .

مقدمة:

اهميه موضوع البحث:

تثير الهجمات السيبرانية العديد من التساؤلات حول مدى امكانية تطبيق قواعد القانون الدولي الانساني على مثل تلك النوع من الهجمات، في ضوء الاتفاق على بعض المفاهيم الاساسية والاختلاف في اخرى، وما يوحد المجتمع الدولي هو محاولة الحد من مخاطر تلك الهجمات في ظل غياب التنظيم القانوني من باب وتزايد تلك الهجمات وازدياد آثارها من باب آخر .

لذلك تحاول الدراسة الاجابة عن تلك التساؤلات اولا بتحديد مفهوم تلك الهجمات وابعادها و موقف القانون الدولي منها من حيث مدى امكانية تطبيق قواعد القانون الدولي وامكانية التعامل معها في المستقبل من خلال الاتفاق على ميثاق دولي يحاول الحد من مخاطر تلك الهجمات والتعامل معها قانونا .

إشكالية البحث

تكمن صعوبة البحث في تحديد تعريف دقيق (للهجمات السيبرانية) لأسباب مختلفة؛ قد تكون بسبب نشأة تلك الهجمات وصعوبة تحديد فاعليها، بخلاف النزاعات التقليدية التي تقع من دول لها حدود ثابتة جغرافيا عند التعرض لموضوع النزاع المسلح ذو الاتجاه التقليدي ، وهنا تبدو بداية المشكلة التي تطرح العديد من التساؤلات على امل الاجابة عنها :

ما هي الهجمات السيبرانية ؟

ما هو التكييف القانوني لها

هل تنطبق قواعد القانون الدولي الإنساني على هذه الهجمات ؟

ما السبيل لحل هذه الفجوة القانونية؟

هل هناك ضرورة لعقد معاهدات جديدة تنسجم مع التطور التكنولوجي؟

فرضيات البحث

١-يفترض البحث وجود تكييف قانوني للهجمات السيبراني جاء بعد عدة محاولات دولية.

٢-امكانية تكييف الهجمات السيبرانية وفقا لقواعد القانون الدولي

ISSN print/ 2769-1926 ISSN online/ 2769-1934

منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي من خلال دراسة التطورات السياسية والأمنية والاقتصادية المرتبطة بطوفان الأقصى وتحليل انعكاساتها على العراق. كما يستفيد من منهج تحليل النظم لفهم التفاعلات بين المتغيرات الداخلية والخارجية المؤثرة في البيئة العراقية .

هيكلية البحث: سيتم دراسة هذا البحث في مبحثين، يدرس الاول (الهجمات السيبرانية تعريفها وتطورها) من خلال مطلبين يتناول الاول مفهوم (الهجمات السيبرانية) والثاني تطور وابعاد (الهجمات السيبرانية) اما المبحث الثاني حيث يتناول تكييف الهجمات السيبرانية ايضا في مطلبين الاول يتحدث عن التكييف في ظل مبدا السيادة والثاني يتحدث عن التكييف في ظل مبدا القانون الدولي العام.

اهمية البحث :

تنطلق الاهمية في أن (الهجمات السيبرانية) شغلت اهتمام المجتمع الدولي في العديد من المحافل الأكاديمية والدولية معا، فضلا عن ازدياد التعامل بها ولآثارها المدمرة ولصعوبة تحديد فاعليها تحاول الدول معالجة الثغرات القانونية في نظامها القانوني للحد من مخاطرها .

المبحث الاول

الهجمات السيبرانية تعريفها وتطورها

سندرس في هذا المبحث مفهوم الهجمات السيبرانية بشكل خاص وكذلك نتطرق في المطلب الاول الى ما قالة الفقهاء في القانون الدولي بخصوص هذه الهجمات . وفي المطلب الثاني يبتدأ بدراسة تطور الهجمات السيبرانية ونشأتها ..

المطلب الاول

مفهوم الهجمات السيبرانية

تزيد الهجمات السيبرانية من تعقيد الوضع القانوني من خلال تهديد سيادة الدول، مما يعقد الوضع هو اختلاف تلك الهجمات عن الحروب التقليدية التي تسبب اضرار مادية ومعنوية ملموسة؛ نتيجة التطورات التكنولوجي قد لا نجد انطباق قواعد القانون الدولي على الفعل السيبراني، مما يعقد المسألة (Esther In ,

(Modern Cyber Warfare and International Law, 2026, p. 1031)، ومن هنا فان التعريفات تختلف حول الفضاء السيبراني وفق النظام القانوني لكل دولة وكذلك وفق رؤية الفقه وبحسب الزاوية التي ينظر لها كل فقيه فهناك من عرف الهجمات السيبرانية على انها : (عالم افتراض يتشابك مع عالمنا المادي يتأثر به ويوثر فيه بشكل معقد حيث تقوم العلاقة بين العالمين على نظرة متكاملة تحمل بين طياتها مزايا ومخاطر لا تتوقف) (شلوش، 2018، صفحة 110)

هذا التعريف يحمل بعض معاني الغموض والذهاب الى مصطلحات الخيال اقرب منه الى الفكر القانوني الذي هو محور دراستنا في هذا البحث، ومن ثم فهو وصف لحالة وليس معنى لظاهرة او نزاع في الوقت الحاضر يراد فهم معناه.

وهناك من عرفها على انها : (الاجراءات التي يتم اتخاذها من قبل الاطراف المتنازعة لتحقيق تفوق على الخصم بواسطة الفضاء السيبراني باستخدام تكنلوجية وتقنيات تعتمد على الافراد، تؤدي الى اتلاف او تدمير او تعطيل او الاستيلاء على انظمة او اجهزة الكترونية للخصم) (Herbert Lin, 2012, p. 515)

في التعريف الذي اطلقه هربرت لين يتبين ان السلوك المادي او الفعل الذي تقوم به الدول في الهجمة السيبرانية يعتمد على استخدام تكنولوجيا متعددة ومتطورة في آن واحد وهذا التعريف يبين السلوك والادوات ونتيجة الفعل او السلوك وهذا التعريف اكثر دقة من التعريف الاول لشموله على الاطراف المتنازعة والفعل الذي تقوم به والنتيجة المطلوبة او الناتجة عن سلوك الاطراف المتنازعة، لكن ما يؤخذ عليه استعماله عبارة الاجراءات الواردة في بداية التعريف .

لذلك يتوسع جانب من الفقه في معنى الهجمة السيبرانية وتعرف على انها : (عمل عدائي يتم تنفيذه عبر الفضاء الالكتروني باستخدام ادوات تقنية او برامج ضارة ومثالها تعطيل او حجب خدمة او اختراق، بهدف الحاق ضرر مادي او معنوي او تقني بأنظمة المعلومات او الشبكات او البنى التحتية او المؤسسات الحكومية وحتى الخاصة) (معمر، 2025، صفحة 563)

هذا التعريف يركز على نتائج الهجمات السيبرانية ويعددها على سبيل المثال ولعل تلك النماذج هي ابرز صور الهجمات السيبرانية، الا ان التركيز عليها يؤدي الى الابتعاد عن جوهر معنى الهجمة السيبرانية المراد اعطاء معناها او بيان تعريفها .

ويؤيد الدكتور احمد عبيس في كتابه الهجمات السيبرانية ما ذهب اليه شميت (schmit)؛ كونه الاقرب لمفهوم الهجمات السيبرانية التي عرضها دليل تولين، اذا يعرفها بالقول : (هو اي تصرف دفاعيا كان ام هجوميا, يتوقع منه وعلى نحو معقول في الشي بجرح او قتل اشخاص او الحاق اضرار ماديه او دمار بالهدف المهاجم) (الفتلاوي، 2018، صفحة 17) وقد ادركت الدول اهمية تعريف الهجمات السيبرانية واعطاء معنى لها في التشريعات الوطنية التابعة لها في مصر فقد عرفت احدى صور الهجمة الالكترونية الا و هي الاختراق على انها : " الدخول غير المرخص به او المخالف لإحكام الترخيص او الدخول بطريقة غير مشروعة الى نظام معلوماتي او حاسب آلي او شبكة معلوماتية وما في حكمها " (المادة (1) من قانون مكافحة جرائم تقنية المعلومات ، 2018)

المطلب الثاني

تطور الهجمات السيبرانية وابعادها

يتصف كل عصر بصفات وسمات خاصة تميزه عن العصور الاخرى، فقد مر الانسان بفترات مختلفة استخدم فيها الحجر كعنصر اساسي في متطلبات حياته، فسميت تلك الحقبة بإسم (العصر الحجري)، و مع اكتشاف المعادن تغيرت الظروف و ظهرت العصور الحديدية، ومع تعاظم التطور الانساني بشكل مستمر ووصول الانسان الى معترك الحياة العلمية بدأ تاريخ الصراع الحديث، فاندلعت بذلك الثورة الصناعية واستعمال الالة في مختلف انحاء العالم، ونتيجة لرغبه الانسان في التطور والتجديد والابتكار جاءت الثورة الفكرية لتضاف للثورة الصناعية لتغيير معالم البشرية، حتى وصلت الى ما عليه اليوم من ثورة تكنولوجية في ظل عالم متطور يستعمل شبكات الاتصال، فالحاسوب اصبح جزء لا يتجزأ عن حياة الانسان اليومية، ثم ظهر الانترنيت لتتضاعف قدرة المستخدمين في البحث والاتصال وربط معظم سكان الارض بعضهم ببعض بشكل لم يشهد له التاريخ مثيل من قبل ولم يقتصر الاستخدام البشري لهذه الوسائل والتطورات في المجالات الصناعية والاقتصادية والاجتماعية فحسب (كلنتر، 2016، صفحة 21) بل دخلت البشرية ثورة

معلوماتية ضخمه في القطاعات الامنية والعسكرية والسياسية ومختلف القطاعات اثر ذلك حتى على النزاعات المسلحة، فبعد ما كانت المعارك تحسم بقوة الخصم من الناحية البشرية والاقتصادية والعسكرية، وكانت المعركة على الارض وقد يتم استخدام القوة في البحر والجو الى ان دخلت وسائل الاتصال الالكترونية ساحة الصدام البشري لتضيف بعدا جديدا على مستوى النزاعات والصراعات البشرية (سعيد، 2013، صفحة 3) فاصبح النزاع بواسطة تقنيات حديثة تختصر الجهد والوقت والمال، و هكذا ظهرت الحرب السيبرانية واول هجوم نفذته الولايات المتحدة الامريكية على الاتحاد السوفيتي السابق عام 1982 من خلال تعطيل خطوط انابيب نقل الطاقة وتسبب بحريق هائل، كما قامت الولايات المتحدة بهجمات سيبرانية اثناء عدوانها على العراق عام 1991 عندما قامت بالتحكم بمرافق النقل والاتصالات وتعطيل شبكات المياه والطاقة فضلا عن حملات التتبع عبر الاقمار الصناعية لدعم عملياتها العسكرية، ولعل حرب كوسوفو تعد اول حرب سيبرانية بمعنى تلك الحرب، اذ تم استخدام الهجمات السيبرانية على مستوى واسع النطاق، اذ تم استخدام تقنيات متطورة ومهاجمة البنى التحتية وتعطيل اغلب محطات الانترنيت واستخدام القرصنة والتهكير ، ثم امتد الامر الى ان وصل لاستخدام الكيان الصهيوني لهجمات سيبرانة ضد العراق وايران ومعاقل المقاومة الفلسطينية، حتى ردت الاخيرة بهجمات تم استخدام وسائل تقنية ضد مواقع البنوك والاتصالات الصهيونية، واستمرت تلك النزاعات لتنتقل بين روسيا والدول التي استقلت عنها كاستونيا وجورجيا بين عامي (2002-2007) ، وانتقلت تلك الهجمات لتشمل قطاع مهم وخطير الا وهو قطاع الطاقة النووية وتبادلت ايران والكيان الصهيوني هجمات من هذا النوع لتصل ذروة الهجمات اثر العدوان الامريكي الصهيوني على الجمهورية الاسلامية عام 2024 وما بعدها (جنديل، 2025، صفحة 288) اما فيما يخص ابعاد الهجمات السيبرانية فلها ابعاد عسكرية واجتماعية وسياسية ولها ابعاد اقتصادية وقانونية (كلنتر، 2016، صفحة 20) .

فيما يخص البعد القانوني : يبقى غياب النص القانوني او عدم كفايته مشكلة ازلية لمثل هذا النوع من الهجمات اذ ان ابرز اشكالية قانونية تتمثل بغياب التنظيم القانوني الخاص بالهجمات السيبرانية بالرغم من بعض المحاولات القانونية سواء على المستوى الدولي او المستوى الاقليمي وحتى الوطني لمعالجة هذه الهجمات والحد منها وفق اطار قانوني، حتى وان غاب النص الاتفاقي الدولي، وكانت اتفاقية اوروبا التي وقعت عام

2001 وضمت فضلا عن عدد من الدول الاوروبية امريكا وكندا وجنوب افريقيا، بشأن الانترنيت واستخدامه وتخزين المعلومات والخوادم وغيرها، كذلك دليل تالين عام 2013 الذي تم برعاية حاف شمال الاطلسي ودراسة امكانية انطباق قواعد القانون الدولي الانساني على الهجمات السيبرانية (ربيع، 2021، صفحة 209) .

البعد التقني : في ظل التطور الهائل في تكنولوجيا المعلومات والاحداث المتسارعة وما رافق ذلك من اهتمام كبير من قبل الدول في تعزيز تلك التكنلوجيا في اطار ثورة المعلومات ومدى عطاء المجتمعات البشرية، لذلك سارعت الدول في زيادة استعمال الاجهزة الالكترونية من اجل تطوير الانظمة المعلوماتية في كل المجالات ومنها المجال العسكري، وهذا ما بدا واضحا مطلع تسعينيات القرن الماضي ولا يزال مستمرا حتى وصلت تلك التقنيات الى تطور كبير لا حدود له في عالم التقنيات حتى اختصرت هذه القدرات سنوات طويلة من تطوير الاسلحة التقليدية لتكون هناك ثورة في المجال الالكتروني لتظهر مجالات جديدة في الجوانب المالية والفنية والتقنية والامن السيبراني ونظام الفايروسات والاجهزة الحديثة وغيرها، وبهذا دخل الفضاء السيبراني في انماط جديدة لتحديد القدرات التقنية لتلك الاليات واتساع دائرة الهجمات بطريقة تكنولوجية في ظل فضاء سيبراني واسع النطاق (مهدي و محمود، 2024، صفحة 1025) .

البعد العسكري : يكاد يجمع المختصون في عالم تكنلوجيا المعلومات على ان الابعاد العسكرية للهجمات السيبرانية باتت الشغل الشاغل للدول والكيانات والمنظمات الدولية في ظل التطور السريع، على ان العالم يترقب مآل النزاعات الالكترونية ومصير (الهجمات السيبرانية) خاصة مع التطورات الحاصلة في المجتمع البشري، مما جعل الدول لاسيما المتقدمة منها، بزيادة الانشطة الالكترونية وتكثيف الجهود في المجالات العلمية المتعلقة بالامن السيبراني، كما تعمل على الاهتمام بضمان المؤسسات التي تحمي الفعاليات الالكترونية مما يجعل تلك المؤسسات هدفا للدول في حال حدوث نزاع مسلح وخاصة بواسطة التقنيات الإلكترونية وتوجد عدة امثله تبين ذلك الهجوم منها الهجوم على شركة سوني حيث ساهم الهجوم على شركة (Sony) في امريكا عام 2014 ، الذي جاء على خلفية إنتاج هذه الشركة فيلم (The Interview) الذي تدور أحداثه الخيالية حول عملية اغتيال الرئيس الكوري الشمالي (كيم جونغ اون) في إحداث أزمة جديدة بين امريكا وكوريا الشمالية، إذ قامت مجموعة تطلق على نفسها إسم (GOP :

فرسان السلام) بتخريب النظام المعلوماتي لشركة سوني للأفلام وسرقة آلاف الملفات السرية، وبثها من على الإنترنيت، ما ألحقت أضراراً مادية بالغة بالشركة (الفتلاوي، 2018، صفحة 28)

المبحث الثاني

تكييف الهجمات السيبرانية

انتقل استخدام الانترنيت من عمل المؤسسات الرسمية وشبه الرسمي ليكون حاضرا بشكل يومي بين يدي جميع افراد المجتمع تقريبا، ومع توسع عمل الانترنيت كان اعتماد كافة الدول عليه واجهزتها المختلفة ومنها العسكرية؛ ونتيجة للتطورات التكنولوجية التي ادت الى ظهور نزاعات من شكل جديد ما يعرف بالنزاع السيبراني الذي تمثل الهجمات السيبرانية احدى صوره، و للخطورة الحاصلة جراء استخدام الهجمات السيبرانية اصبحت هناك تحديات على جميع المستويات من ضمنها التحديات القانونية التي تواجه القانون الدولي في تكييف تلك الهجمات التي تخلو من تنظيم قانوني ينظم وجودها واساليبها ووسائل العمل بها، فبات بحكم المؤكد الحاجة الى تنظيم قانوني يعالج الثغرات القانونية، فوجود نصوص متفرقة او نصوص عامة تشير الى الهجمات السيبرانية ربما لا تكفي للحد من خطورتها التي انتشرت بشكل واسع .

لذلك سيتم مناقشة هذا المبحث وفق المطلبين الآتيين :

كل ذلك يكون الجواب علية من خلال دراسة المطلبين :

الاول :- تكييف الهجمات السيبرانية في ظل مبادئ القانون الدولي الثابتة :

الثاني :- تكييف الهجمات السيبرانية في ظل القانون الدولي الانساني

المطلب الاول

تكييف الهجمات السيبرانية في ضل مبدأ السيادة

تشكل الهجمات السيبرانية تهديدا كبيرا لأبرز مبادئ القانون الدولي التي اقرتها منظمة الامم المتحدة مبدأ احترام سيادة الدول، ان مبدا السيادة هو من المبادئ المهمة التي ترتبط ارتباطا وثيقا بمفهوم الدولة التي يجب ان يكون لها نظام قانوني يحميها من الداخل والخارج اي ان تكون لها سيادة داخلية على اراضيها مقابل سيادة خارجية قادرة على ردع الاعتداءات من جانب واشاعة الهيبة من جانب آخر، وكلما كانت السيادة كاملة كلما كانت الدول محط احترام المجتمع الدولي، الا ان هذا المبدأ الذي اكدت عليه الامم

ISSN print/ 2769-1926 ISSN online/ 2769-1934

المتحدة من خلال النص عليه في ميثاقها وتم التعامل مع الدول على هذا الاساس (الفقرة (1) من المادة (2) من ميثاق الامم المتحدة، 1945)

الا ان هذا المفهوم اصبح في حكم القانون الدولي التقليدي، بعد ان اصبحت هناك حاجة لتغيير هذا الجمود في المفهوم وخاصة مع ظهور النزاعات السيبرانية التي باتت تستغل الفراغ القانوني في تنظيمها الا ان ذلك لا يعني وجود مبررات لشرعية الهجمات السيبرانية او انتهاك اصل مبدأ السيادة في الوقت الذي تمتد فيه سيادة الدول فضلا عن مجالها البري والبحري الى المجال الجوي الذي يعنيه الفضاء السيبراني، مع ذلك اصبح بحكم المؤكد مع انتشار الجرائم السيبراني الى عدم قدرة السيادة الوطنية السيطرة على ذلك الفضاء، خاصة مع انتشار الجرائم السيبرانية، اذ تشكل عمليات الاختراق وصعوبة تحديد مصدره ثغرة قانونية في هذا المجال وتصدع في مبدأ السيادة الذي لا يمكن تجزئته، وفي الوقت الذي يخلو فيه النظام القانوني الدولي من ميثاق دولي ينظم هذا الامر سعت الدول عبر قوانينها الوطنية لسد هذه الثغرة طالما الامر متعلق بالسيادة الوطنية، ان الهجمات السيبرانية تشكل تهديدا للمبادئ الاساسية الرئيسية في القانون الدولي كاحترام مبدا السيادة في الدول لما فيها من اختراق لمعلومات امنيه وعسكريه تصنف بالسرية . كما تفوض واجبا اساسيا وهو الامتناع عن استخدام او التهديد باستخدام القوه نضرا الى اضراراها البالغة على سير عمل الحكومة والخدمات في الدولة والتي ستتعرض لمثل هكذا هجمات (Esther In، Modern Cyber Warfare and International Law، 2026)

ان السيادة بمعناها التقليدي تعني استقلال القرار الداخلي والخارجي وتمتع الدول باستقلال تام يمكنها من اتخاذ قرارتها بمعزل عن اي تأثير خارجي، هنا السيادة بمظهرها الخارجي اذا مرتبطة باستقلال الدولة. فالسيادة قد تكون كامله وقد تكون ناقصه ، الا انه وفي كل الاحوال فان ذلك (الاستقلال والتبعية) لا يؤثران كما يذهب اليه اغلب الفقه على وجود الدولة القانوني والفعلي .وتنطوي سيادة الدولة الخارجية بسمات منها الاستقلال والمساواة، فيعني الاستقلال هي ان تكون الدولة حره في بناء علاقاتها الخارجي، اما المساواة فتعني ان جميع الدول متساوية امام القانون الدولي من الحقوق والالتزامات وبهذا فان التحديات الراهنة امام سيادة الدولة ونطاقها، ظهور الهجمات السيبرانية .فالتغييرات التكنلوجية الهائلة وتطورات استخدام الحاسوب وشبكات الاتصال التي تعيشها في الوقت الحاضر والتي لا تعترف بالدود الجغرافية خلق فضاء جديد الى جانب البر والبحر والجو وهو الفضاء السيبراني (فرج الله، 2018، صفحة 346)

ان الفضاء السيبراني يختلف عن العالم المادي من عدة جهات اهمها :-

انعدام جغرافية المكان الطبيعي وهو بمثابة فرصه جديده هرعت اليها الحركة العلمية والثقافية المعاصرة .وصولا الى اتخاذ صورتان هما: الجريمة والهجمات التي تمس سيادة الدولة المستهدفة. واصبح هذا الفضاء هو المسرح الحقيقي للهجمات السيبرانية التي باتت الا طراف الدولية تتنازع وتتسابق على استغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من اشكال السباق التسلح (نعوس، 2012، صفحة 128) ان مستخدمي شبكات الكمبيوتر والانترنيت اي الافراد الذين يكونون الفضاء السيبراني ينتمون الى مجتمعات سياسيه متعددة او في حالة ارتكاب جريمة ما ضن هذا الفضاء وقيام الدولة بتتبع مصدر الجريمة, فقد تنتهك في سبل ذلك مفهوم السيادة الوطنية او قد يكون مصدر الجريمة ينتمي الى واقع ضمن نطاق السيادة لدولة اخرى (كناكي، 2011، صفحة 113) .

وبناء على ذلك يمكن القول بان سيادة الدولة التقليدية ومقوماتها بدأت تتقلص بوجود وسائل الاتصال الإلكترونية التي تجعل الحدود الإقليمية للدول والانتماءات الوطنية تتضاءل شيئا فشيئا مما يثير التساؤل بشان نطاق سيادة الدولة في الفضاء السيبراني فضلا عن ان تسريب معلومات امنية تخص الدول قد يتجاوز الاضرار بحماية المدنيين اذ ان هؤلاء يعتمدون على الامن من جهة وتوفير الخدمات من جهة اخرى، فاذا كان الامن مخترق وخدمات الطاقة والمياه بل ابسط الخدمات مفقودة فان سيادة الدول تم اختراقها، وتكمن الخطورة في امكانية تعدد ردة فعل الدولة المعتدى عليها ففي الوقت الذي يصعب اثبات الهجمة السيبرانية ونسبتها الى طرف محدد فان ردة فعل الطرف الاخر قد تتعدى مفهوم الدفاع عن النفس الذي اقرته الامم المتحدة، ويكون هذا الرد بمثابة خرق لمبدأ السيادة كذلك، ومن ثم فان على القائمين على حفظ الامن والسلم الدولي ان يكونوا اكثر حرصا في هذا الجانب، بدل ان يكون هناك انفلات وافراط في الهجمات السيبرانية .

المطلب الثاني

تكييف الهجمات السيبرانية في ظل القانون الدولي الانساني

في الحروب التقليدية كانت القوة والنفوذ من نصيب من يمتلك القدرات العسكرية اما اليوم فقد غيرت وسائل التكنولوجيا جذريا من هذا التوازن في القوة فأصبحت تمثل واحده من اكثر التحديات الهامة التي تواجه اصحاب الشأن، واصبح الاهتمام ينصب على كيفية ايجاد الصيغ القانونية المناسبة للحد من الهجمات السيبرانية التي باتت تظهر حتى في النزاعات التقليدية، فالأطراف المتنازعة اخذت تميل لاستخدام التقنيات

الذكية، فاصبح بموجب هذا التطور بإمكان اي طرف تنفيذ الهجمات السيبرانية التي قد تؤدي الى تدمير البنى التحتية بأكملها او جزء كبير منها او تعطيل الاتصالات واحداث اضرار جسيمة في الارواح والممتلكات، واصبح بإمكان الدول الاقل خبرة في المجالات التقنية ان تمثل تهديدا لأي دولة كانت وفي هذا الشأن ولما كانت تلك الهجمات غير منظمة قانونا فهل يمكن الاعتماد على القواعد العامة في انطباقها على قواعد القانون الدولي الانساني؟

اتجه جانب من الفقه الى عدم امكانية انطباق القانون الدولي الانساني على الهجمات السيبرانية؛ لصعوبة التعامل مع تلك الهجمات؛ لكون تكنولوجيا الانترنيت بلا قانون، وهذا الاتجاه مثله جانب من الفقه القانوني في امريكا واوروبا على اعتبار ان منطقة الفضاء السيبراني منطقة خالية من القانون، ومن ثم تكون هذه المنطقة متاحة امام الجميع للقيام بأي نشاط سواء سلمي او غير سلمي، واشار الفقه انه من هذا الجانب لا يمكن انطباق قواعد القانون الدولي التقليدي، كما ان عالم الانترنيت خال من الواقع المادي الملموس، ثم قالوا : انه ان سلمنا جدلا بخضوع الانترنيت لقواعد القانون الدولي فأي سلطة يمكن فرضها على تلك الهجمات واي سلطة يمكنها ملاحقة مرتكبي تلك الهجمات، ثم ان الطبعة المفتوحة لمثل تلك الهجمات واتساعها تشكل عائق امام تطبيق القوانين، كما انهم اعترضوا على انطباق قواعد القانون الدولي الانساني على تلك الهجمات؛ لعدم وجود مادة قانونية في قواعد القانون تنطبق على تلك الهجمات يمكنها معالجة الهجمات الحاسوبية والالكترونية، فضلا عن ان تلك المواثيق الدولية الخاصة بالقانون الدولي الانساني سبقت ظهور الهجمات السيبرانية بشكلها المتطور الحالي ومن ثم فان تلك الهجمات غير معروفة قانونيا ولا يمكن التعامل معها كما انها غير محددة، فضلا عن كونها هجمات استباقية من دون سابق انذار وتكون في الغالب غير معروفة المصدر وهذا ما تم التعامل معه في النزاع الجورجي الاستوني لعدم وجود قواعد قانونية دولية يمكن اعتمادها لتنطبق على ذلك النزاع (علي، 2022، صفحة 274)

في حين اتجه جانب ثاني من الفقه الى امكانية انطباق قواعد القانون الدولي الانساني بصفة عامة على اي نزاع مسلح بما في ذلك الهجمات التي تعتمد تقنيات متطورة كالهجمات السيبرانية، وذلك من خلال عدم الاعتراف بموضوع الفراغ القانوني وعليه يمكن ان تنطق قواعد القانون الدولي الانساني على تلك الهجمات وذلك من خلال اعتماد شرط مارتنيز الذي يعد من المبادئ الهامة والاساسية الراسخة في القانون الدولي الانساني ويمثل هذا الشرط الحد الادنى الذي يتم اعتماده مع قواعد الضمير العام (البصيصي، 2017، صفحة 71)

وقد تجسد هذا الشرط وفق قواعد القانون الدولي العرفي ويرى هذا الشرط : انه " في الحالات غير المشمولة بإحكام القانون يبقى المدنيون والمتحاربون في حماية وسلطان مبادئ الامم التي استقر عليها الحال بين الشعوب وقوانين الانسانية ومقتضيات الضمير العام "، وقد تجسد هذا المبدأ فيما بعد ليصبح ضمن قواعد القانون الدولي الانساني اذ جاء في البروتوكول الاضافي الاول الملحق باتفاقيات جنيف لعام 1977 يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في هذا الملحق البروتوكول او اي اتفاق دولي اخر تحت حماية وسلطان مبادىء القانون الدولي كما استقر بها العرف ومبادىء الانسانية وما يمليه الضمير العام " (الفقرة (2) من المادة (1) من البروتوكول الاضافي الاول الملحق باتفاقيات جنيف، 1977)

مما تقدم يمكن القول : امكانية انطباق هذا الشرط على الهجمات السيبرانية طالما لا يوجد قانون دولي ينظم تلك الهجمات، وخاصة انها طرق حديثة بل تتطور بين الحين والاخر، فمسألة اعتماد هذا الشرط نجدها اقرب من عدم انطباق اي نص قانوني على تلك الهجمات .

كما ان اللجنة الدولية للصليب الاحمر في مؤتمرها الـ(28) بإمكانية خضوع الاسلحة الحديثة واساليب القتال الجديدة لمراجعة دقيقة وانطباق قواعد القانون الدولي عليها، طبقا لنص المادة (36) من البروتوكول الاضافي الاول الملحق باتفاقيات جنيف لعام 1977 التي اشارت الى " يلتزم اي طرف سام متعاقد عند دراسة او تطوير او اقتناء سلاح جديد او اداه للحرب او اتباع اسلوب للحرب بان يتحقق مما اذا كان ذلك محظورا في جميع الاحوال او في بعضها بمقتضى هذا الملحق البروتوكول او اية قاعدة اخرى من قواعد القانون الدولي التييلتزم بها هذا الطرف السامي المتعاقد " .

وهذا ما اكده تقرير اللجنة الدولية للصليب الاحمر في عام 2019 عندما اشار الى ذلك بالقول : (ليس لدى اللجنة الدولية اي شك في ان القانون الدولي الانساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة وبالتالي يحد من استخدامها تماما مثلما ينظم الاسلحة والوسائل والاساليب الاخرى للقتال في اي نزاع مسلح ... سواء كان الفضاء السيبراني يعتبر مجالا جديدا للحرب يشبه الفضاء الجوي والبري والبحري والفضاء الخارجي او اذا كان مجالا مختلفا؛ لأنه مجال من صنع الانسان ...) (https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_ared_conflict_ar.pdf، 2019)

السؤال الذي يطرح نفسه ما مدى مشروعية اللجوء الى الهجمات السيبرانية ؟

ان الاجابة عن هذا السؤال تقتضي اللجوء الى القواعد الناظمة لأساليب وقواعد الحرب، فضلا عن ميثاق الامم المتحدة الذي يؤكد على عدم جواز استخدام القوة

في ذات الوقت فان بعض الفقه يشير الى امكانية استخدام القوة وفق مبدأ الدفاع عن النفس الذي نص عليه ميثاق الامم المتحدة تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية: الفقرة (4) منه على " يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة " (المادة (2) من ميثاق الامم المتحدة، 1945)

الا ان حق الدفاع الشرعي له شروط وفق قواعد القانون الدولي، وهناك شرطين مهمين الاول منهما ان يكون الرد على مصدر الاعتداء والشرط الثاني ان تكون قوة الردع متناسبة مع العدوان اي ان يكون الرد ضروري ومناسب (عساف و جعفر، مشروعية استخدام الهجمات السيبرانية في النزاعات الدولية والمسؤولية الدولية عنها،، 2021، صفحة 685)

الا ان هناك رأي يعارض العودة الى المادة (51) من الميثاق كونها تتعلق باستخدام القوة وان الامر لا ينطبق على الهجوم السيبراني؛ لكونه لا يخضع لقواعد القتال التقليدية، كما ان الامر يتعلق بالعلاقات بين الدول وربما يكون الهجوم ناشئ عن جماعات او افراد (هاشم، 2013، صفحة 17)

لذلك نرى انه لا يمكن اعطاء صفة الدفاع الشرعي على مرتكبي الهجمات السيبرانية؛ لاختلاف الوسائل والظروف وتطور قواعد ووسائل الاشتباك، كما ان الهجمات السيبرانية خضعت اخيرا لاتفاقية دولية عام 2024 حددت لمفاهيم الاساسية والقواعد القانونية الناظمة لها ووسائلها واساليبها وكيفية التعامل معها والاجراءات التي تتخللها وما الى ذلك من المواضيع المهمة لمعالجة تلك الجرائم، مع صدور اتفاقية الامم المتحدة لمكافحة استخدام تكنلوجيا المعلومات والاتصالات للأغراض الاجرامية عام 2024 التي جاء في اهدافها تعزيز التعاون الدولي لمكافحة الجريمة السيبرانية (المادة (2) اتفاقية الامم المتحدة لمكافحة استخدام تكنلوجيا المعلومات والاتصالات للأغراض الاجرامية عام 2024 ، 2024) وقد اكدت الاتفاقية التعاون في مجالات عدة منها التجريم وصون السيادة وهذا كله يعتمد على التعاون من خلال القوانين الوطنية للدولة الطرف على سبيل المثال المواد (4 ،5، 7، 8، 9....)، من الاتفاقية .

وفي ظل عدم وجود اتفاقية دولية تنظم الهجمات السيبرانية وصعوبة اثبات مسؤولية طرف عن هجوم سيبراني وغياب قواعد المسؤولية الدولية في هذا الجانب؛ ولانتشار تلك الهجمات بصورة كبيرة جدا تكاد تخرج عن

السيطرة، لذلك ندعوا المجتمع الدولي الى عقد مؤتمر دولي يتم الاتفاق من اجل التعاون في هذا المجال والاتفاق على النقاط الاساسية لعقد ميثاق دولي يشمل تحديد مفهوم الهجوم السيبراني وعناصره والقانون الذي يسري عليه والتدابير اللازمة من الطرف المعتدى عليه والمسؤولية المترتبة على الطرف المعتدي وانشاء محكمة مختصة او اللجوء الى المحاكم الدولية التي تتواجد في النظام العالمي حتى يتم على اقل تقدير الحفاظ على ما تبقى من جهود الامم المتحدة في حظ الامن والسلم الدوليين والحد من انتشار هذه الهجمات التي تكاد تفتك بالمجتمع الدولي (كلنتر، 2016، صفحة 59) .

الخاتمة

خلصنا في هذه البحث الى إن الهجمات السيبرانية هي واحدة من أهم التحديات المعاصرة التي تواجه المجتمع الدولي، لما لها من تداعيات على الأمن القومي للدول و تهديدا للسلم و الأمن الدوليين، وتم التوصل الى عدة نتائج و توصيات و على النحو الاتي:

اولا : النتائج :

1- إن الهجمات السيبرانية لازالت من المفاهيم الحديثة التي لا يوجد اتفاق دولي بشأن تحديد مفهومها مما القى بظلاله على المعنى والتكييف القانوني لها فضلا عن المسؤولية الدولية عنها.

2- إن تحديد مسؤولية الدولة عن الهجمات السيبرانية يتسم بصعوبات بالغة جدا تشكل تحديات كبيرة امام امكانية وضع حل قانوني لمثل تلك الهجمات و ذلك لصعوبة إسناد الهجوم الى الدولة او الكيانات خارج نطاق الدولي وهذه الاخيرة تزيد من صعوبة الاسناد من جهة وتحديد الفاعل من جهة وامكانية الافلات من العقاب وزيادة التأثير .

3- زاد من حجم التحديات عدم وجود تنظيم قانوني لتلك الهجمات مما جعل الحد من مخاطرها امر في غاية الصعوبة ومن ثم ضعف امكانية الحد من تلك المخاطر وعرقلة جهود المجتمع الدولي الرامية الى حفظ الامن والسلم الدوليين .

4- إن عملية وضع تنظيم قانوني لهذه الظاهرة الخطيرة يتسم بصعوبات شتى وذلك لأن المصالح الدولية تقف حجر عثرة أمامها، مما يزيد من صعوبة معالجتها بشكل قانوني سليم .

ثانيا :التوصيات

1- يتوجب على الدول اتخاذ خطوات جدية للحد من مخاطر الهجمات السيبرانية وتفعيل الجانب الاكاديمي من خلال الدعوة الى عقد مؤتمرات دولية لتعريف المجتمع الدولي بمخاطرها من جهة والسعي لعقد ميثاق دولي لبيان الموقف القانوني منها .

2- ضرورة زيادة التعاون الدولي في المجالات الامنية والتكنلوجية وضرورة اخذ منظمة الامم المتحدة والوكالات التابعة لها زمام المبادرة للحفاظ على الامن والسلم الدوليين والحد من مخاطر تلك الهجمات التي باتت تشكل خطرا يهدد مبادئ السيادة والامن والاستقرار .

3- ضرورة عقد اتفاقية دولية تتضمن تحديد مفهوم الهجمات السيبرانية والنظام القانوني الذي يعالج مضامينها، وتحديد قواعد المسؤولية واركانها، وفرض مزيد من القيود على استخدامها لتجنب اثارها المدمرة .

المراجع:

(1945). *الفقرة (1) من المادة (2) من ميثاق الامم المتحدة*. الامم المتحدة.

(1945). *المادة (2) من ميثاق الامم المتحدة*. الامم المتحدة.

(1977). *الفقرة (2) من المادة (1) من البروتوكول الاضافي الاول الملحق باتفاقيات جنيف*. الامم المتحدة.

المادة (1) من قانون مكافحة جرائم تقنية المعلومات . (2018). *قانون مكافحة جرائم تقنية المعلومات، 175*، المادة 1. العراق.

https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_ared_conflict_ar.pdf. (2019).

ISSN print/ 2769-1926 ISSN online/ 2769-1934

تاريخ الاسترداد 1 6, 2026، من اللجنة الدولية للصليب الاحمر: https://www.icrc.org

(2024). *المادة (2) اتفاقية الامم المتحدة لمكافحة استخدام تكنلوجيا المعلومات والاتصالات للأغراض الاجرامية عام 2024* . الامم المتحدة.

Esther In . (2026). Modern Cyber Warfare and International Law. *Cornell Law Review*, p. 1031.

.Modern Cyber Warfare and International Law .(2026) .Esther In *Cornell Law Review*، صفحة 1031.

Herbert Lin. (2012). Cyber conflict and international humanitarian law. *Icrc*(94), p. 515.

احمد عبيس الفتلاوي. (2018). *الهجمات السيبرانية دراسة مقارنة* (المجلد 1). بيروت، لبنان: نشورات زين الحقوقية.

حامد محمد علي. (2022). مواجهة الحرب السيبرانية في قواعد القانون الدولي الانساني. *مجلة الجامعة العراقية*(57)، صفحة 274.

روبرت كناكي. (2011). *حكومة الانترنيت في عصر انعدام الامن الالكتروني , سلسلة دراسات عالميه* (الإصدار 95). ابو ضبي: مركز الامارات للدراسات والبحوث الاستراتيجية.

زهراء عماد كلنتر. (2016). *المسؤولية الدولية الناشئة عن الهجمات السيبرانية*. النجف: كلية القانون، جامعة الكوفة.

سلوان جبار هاشم. (2013). *حالة الضرورة العسكرية في القانون الدولي الانساني*، (المجلد 1). بيروت، لبنان: المؤسسة الحديثة للكتاب.

صلاح جبر البصيصي. (2017). *دور محكمة العدل الدولية في تطوير مبادئ القانون الدولي الانساني*، (المجلد 1). عمان: دار المنهل للنشر والتوزيع.

عمر محمود مهدي، و محمد نوح محمود. (2024). الهجمات السيبرانية واثرها على تغيير مفهوم السيادة لحدود الدولة من وجهة نظر جيوسياسية. *مجلة مداد الاداب*، صفحة 1025.

فيصل اياد فرج الله. (2018). مبدا السيادة في القانون الدولي العام. *مجلة كلية القانون ، جامعة الكوفة*(12)، صفحة 346.

قيس معمر. (2025). الهجمات الالكترونية بموجب القانون الدولي. *مجلة الميار*، صفحة 563.

محمد دهام عساف، و محمود خليل جعفر. (2021). مشروعية استخدام الهجمات السيبرانية في النزاعات الدولية والمسؤولية الدولية عنها. *مجلة كلية القانون، جامعة بغداد*(عدد خاص)، صفحة 685محمد صلاح ربيع. (2021). الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع. *مجلة الدراسات القانونية والاقتصادية*، صفحة 209.

مصطفى عصام نعوس. (2012). سيادة الدولة في الفضاء السيبراني ,. *مجلة الشريعة والقانون ,جامعة الامارات العربية المتحدة*(51)، صفحة 128.

مهند عجب جنديل. (2025). لهجمات السيبرانية والاسلحة الذاتية في ظل مبدأ التناسب. *مجلة جامعة واسط للدراسات الانسانية*(21)، صفحة 288.

ISSN print/ 2769-1926 ISSN online/ 2769-1934
نورة شلوش. (2018). القرصنة الالكترونية في الفضاء السيبران. *مجلة بابل للدراسات الانسانية*(2)، صفحة 110.

وليد غسان سعيد. (2013). *دور الحرب الالكترونية في الصراع العربي – الاسرائيلي*. نابلس، فلسطين: جامعة النجاح الوطنية، كلية التحقيق والتنمية السياسية.