IRAQI Academic Scientific Journals

Sumer Journal of Legal Science
مجلة سومر للعلوم القانونية

P.ISSN: -3081-1082
https://sjls.edu.iq/index.php/su/ar/index

Vol. (1), No. (2) June 2026
Pages 733-750

المجلد (١) العدد (٢) حزيران ٢٠٢٦
الصفحة ٧٣٣-٧٥٠

The Theoretical and Legal Framework of Cyber Warfare

Dr. Nabil Obeid Khalaf Al-Dulaimi
General Directorate of Education in Anbar

Abstract:

This research addresses a highly important topic in the field of public international law, highlighting cyberattacks that target national infrastructure, damaging internet and communication networks, vital facilities, and paralyzing security, economic, and military systems. These attacks pose a significant threat to national security. The difficulty in identifying the source of these attacks or attributing them to a specific state or entity exacerbates this problem.

It has become essential to understand this new form of warfare, which now operates in cyberspace. It utilizes tools and methods representing a new generation of warfare, entirely different from conventional or nuclear weapons. The research also examines whether the provisions of international agreements and customary rules governing the conduct of hostilities apply to these attacks.

Keywords: Cyber warfare, cyberspace, international agreements, public international law, United Nations Charter.

1: Email **hwhwcw4@gmail.com**
2 : Email:

Submitted: 16-2-2026
Accepted: 24-2-2026
Published:2-6-2026

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

الإطار النظري والقانوني لحروب الفضاء الالكتروني

م.د. نبيل عبيد خلف الدليمي
المديرية العامة لتربية الانبار

الملخص

يتناول هذا البحث موضوع غاية في الاهمية على صعيد القانون الدولي العام اذ يسلط الضوء على الهجمات السيبرانية التي تصيب البنى التحتية للدول وتحدث اضرار بشبكات الانترنت والاتصالات والمنشآت الحيوية وتشل الانظمة الامنية والاقتصادية والعسكرية، والتي تعد مصدر خطر لأمن الدول، ومما زاد من تفاقم هذه المشكلة هو صعوبة معرفة مصدر هذه الهجمات او نسبة هذا الفعل لدولة او جهة معينة.

وأصبح من الضروري التعرّف على هذا النمط المستحدث من الحروب، الذي بات مجالُه الفضاءَ الإلكتروني، حيث تُستخدم فيه أدوات ووسائل تمثل جيلاً جديداً يختلف كلياً عن الأسلحة التقليدية أو النووية، وهل تطبق عليها احكام الاتفاقيات الدولية والقواعد العرفية المتعلقة بسير العمليات القتالية.

الكلمات المفتاحية: الحرب السيبرانية، الفضاء الالكتروني، الاتفاقيات الدولية، القانون الدولي العام، ميثاق الامم المتحدة.

مقدمة

أولا/ التعريف بموضوع البحث:-

يشهد المجتمع البشري تطورا مطردا في مجال التكنولوجيا الرقمية وتطبيقاتها بشكل خاص، مما جعل حياة الانسان والدول ومصالحها اكثر ارتباطا بالفضاء الافتراضي والاجهزة الإلكترونية، إذ اثرت تلك التكنولوجيا على الانظمة السياسية والعلاقات الدولية للدول وامنها القومي وسيادتها ومصالحها، فهو يسهل عمل الدول وقيامها بمهامها، إلا ان الدول تواجه مخاطر كبيرة في هذا الفضاء بسبب ما تتعرض له من هجمات تهدد سيادتها وتعرض مصالحها للخطر على مختلف المستويات فكان لا بد من مواجهة تلك التهديدات لان استمرارها سيؤدي الى تهديد السلم والامن الدوليين.

ثانيا/ اهمية البحث: -

تكتسب دراسة الحروب السيبرانية وفهمها أهمية متزايدة، في ظل تنامي المؤشرات التي تدل على تسارع توجه الدول نحو اعتماد الهجمات الإلكترونية كجزء أساسي من استراتيجياتها وتكتيكاتها، واستراتيجياتها فيما يخص علاقاتها بالدول الأخرى، ونزاعاتها معها، وبالتالي فإن الفهم الأفضل والأعمق لها يفرض على الباحثين وصناع القرار العمل من أجل تطوير استراتيجيات تتبنى وتوظف هذه الأساليب المستحدثة على أفضل وجه، من أجل التصدي لأي هجمات متوقعة من هذا النوع في المستقبل.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

ثالثاً/اشكالية البحث:-

ومن اهم الاشكاليات التي تثار لدى البحث والتحليل في موضوع هذه الدراسة هو تحديد مفهوم الحرب السيبرانية، وعدم وجود الاساس القانوني الذي ينظمها، ومدى انطباق قواعد القانون الدولي الانساني عليها، ومع تطور هذا النمط الجديد من الحروب الذي يدور في الفضاء الإلكتروني بأسلحة تختلف عن التقليدية والنووية، تبرز الحاجة إلى توضيح :-هل تشكل الهجمات السيبرانية استخداماً للقوة وفق ميثاق الامم المتحدة؟

رابعاً/منهج البحث:-

للإجابة عن التساؤلات السابقة تم اتباع المنهج الوصفي ومنهج التحليل القانوني باعتبارهما الانسب لمعالجة هذا الموضوع، من خلال بيان ماهية الحروب الالكترونية وتميزها عن الحروب التقليدية، ومن ثم التطرق للتكيف القانوني للحروب الالكترونية ومدى شرعيتها ومتى يتم اللجوء اليها .

خامساً/ هيكلية البحث:-

سوف نقسم خطة البحث على مبحثين، سنتناول في المبحث الاول تعريف حروب الفضاء الالكتروني وبيان خصائص هذه الحروب، بينما سنبحث في المبحث الثاني تكيف حروب الفضاء الالكتروني وفقاً للمبادئ الرئيسة في القانون الدولي العام وكذلك تكيفها وفقاً لمبادئ القانون الدول الإنساني. وسنختم البحث بعرض اهم النتائج والتوصيات المتعلقة بحروب الفضاء الالكتروني.

المبحث الاول

ماهية حروب الفضاء الالكتروني

ان الثورة التكنولوجيا التي حدثت في المجال المعلوماتية، أصبح الفضاء الإلكتروني اهمية بالغة على صعيد الحروب والصراعات والتي تستخدم أدوات مختلفة تماما، عن الاسلحة المستخدمة في الحروب التقليدية، ومن وهنا برزت ما يسمى بحروب الفضاء الإلكتروني، أو" الحروب السيبرانية"، والتي قد غيرت من قواعد وطبيعة الحرب ذاتها؛ فالحرب السيبرانية لا تستهدف تدمير المعدات والاليات العسكرية للعدو، ولا يكون هدفها احتلال ارض لدولة ما، وانما يكون هدفها إلحاق الضرر البالغ بالبنية التحتية الالكترونية.

شكلت الثورة الرقمية في المجال التكنلوجي قفزة نوعية على صعيد الفضاء الالكتروني وعنصرا مهما على صعيد النظام الدولي المعاصر، واضافت المزيد من التعقيد للعمليات العسكرية، واصبحت التكنولوجيا اكبر تأثيرا في المعادلات الاستراتيجية للدول، والدولة التي لا تملك التكنلوجيا المتطورة لا تكون محصنة امنيا، ولا تكون بمنأى عن الهجمات السيبرانية التي ممكن تلحق اضرار جسيمة بالبنى التحتية الحيوية بما في ذلك الامنية والعسكرية، ومن اجل بيان ماهية هذه الحروب بشكل دقيق سوف نتناول هذا الموضوع من خلال مطلبين،

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

نبحث في الاول تعريف حروب الفضاء الالكتروني، ونتناول في الثاني افردته لخصائص حروب الفضاء الالكتروني.

المطلب الاول

تعريف حروب الفضاء الالكتروني

لم يتفق فقهاء القانون الدولي العام على تعريف محدد للهجمات السيبرانية كون هذا المصطلح يكتنفه الغموض واللبس، فمنهم من اعتمد مصطلح الفضاء السيبراني (cyber space) بالاعتماد على المكان الذي تتم فيه الاعتداءات السيبرانية، ومنهم من اخذ بمصطلح الحرب السيبرانية (cyber warfare) استنادا الى معطيات عسكرية او امنية ضد العدو المفترض، بينما تبنى البعض منهم مصطلح الهجمات السيبرانية (cyber attacks) كون مصطلح الحرب غير مرغوب على صعيد التنظيم القانوني الدولي في الوقت الراهن، كما ان استخدام مصطلح الهجمات السيبرانية يكون اكثر دلالة ومعنى يتلائم مع القانون الدولي المعاصر.[١] وان الهجمات السيبرانية دائما ما تكون اوسع نطاقا من الحرب السيبرانية، وعليه سوف نتناول تعريف الهجمات السيبرانية من خلال بيان معناها لغة في الفرع الاول: ومن ثم بيان معناها اصطلاحاً في الفرع الثاني:

الفرع الاول

تعريف الهجمات السيبرانية لغة

السيبرانية لغة: تعد كلمة سيبرانية او سيبراني هي ترجمة حرفية لكلمة (cyber) والمشتقة من كلمة (cybernetics)، وقد تم استخدام هذا المصطلح الاخير أكاديميا للمرة الاولى من قبل العالم الامريكي المختص بالرياضيات "نوربرت وينز" عام ١٩٤٨، في كتابه الشهير:

(علم التحكم الالي: او التحكم والاتصال في الحيوان والالة اي اليات التحكم الذاتي).[٢]

اما معاجم اللغة العربية فلم نجد فيها مصطلح يدل على كلمة السايبر (cyber) وانما جاء معنى مقارب لهذا المصطلح :

أ. في قاموس المورد الحديث ب "الكمبيوتري" او "عصري جداً" كما ورد معنى مصطلح (cybernetics) بانه "علم الضبط" او "علم التحكم الاوتوماتيكي".[٣]

ب. وفي قاموس المعاني جاء بمعنى " تخيلي".[٤]

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

الفرع الثاني

تعريف الهجمات السيبرانية اصطلاحاً

الهجمات السيبرانية مصطلح حديث النشأة نسبياً، لذلك عكف فقهاء القانون على وضع تعريف مناسب لهذا المصطلح، ومن اهم التعاريف التي تبنت تعريف هذا المصطلح هي:

تعريف فيورتس(Fuertes) الذي وصفه بانه "هو هجوم إلكتروني يتم عبر الإنترنت من خلال التسلل إلى مواقع غير مصرح بالدخول إليها، بقصد تعطيل البيانات أو إتلافها أو الاستحواذ عليها، ويُعد سلسلة من العمليات السيبرانية التي تنفذها دولة ضد أخرى". بينما عرفه شمت (Schmitt) بانه "مجموعة من الاجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والاضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة".(٥)

واذا نتج عن الهجمات السيبرانية نزاعاً مسلحاً، فنكون امام ما يطلق عليه الحرب السيبرانية، وبالتالي فان الهجمات السيبرانية تكون اوسع نطاقاً من الحرب الالكترونية ومن الممكن حدوثها خارج اطار الحرب وقد تكون سبب رئيسي لنشوب الحرب.(٦)

واهم ما يميز الحرب السيبرانية عن الحرب التقليدية، هو أن مفهوم الحرب التقليدي يقتصر على استخدام الجيوش النظامية والتي عادتا ما يسبقها الاعلان عن الحرب، ويكون لها ميدان قتال محدد، بينما الهجمات الالكترونية ليس لها مجال محدد واهدافها غامضة، وتتحرك من خلال شبكات الاتصالات العابرة للحدود الدولية.(٧)

وتعرف الاسلحة غير التقليدية وفقاً لما تضمنته لجنة الاسلحة التقليدية التابعة للأمم المتحدة والصادر عام 1968 بأنهاالأسلحة التي تعتمد على الانفجارات الذرية، أو المصنعة من مواد ذات نشاط إشعاعي، إضافة إلى أسلحة التدمير الكيميائي والبيولوجي، وأي أنواع أخرى قد تُنتج مستقبلاً وتتماثل في آثارها التدميرية مع القنبلة الذرية أو غيرها من الأسلحة المشابهة).(٨)

وعرفت اللجنة الدولية للصليب الاحمر الهجوم السيبراني بانه : "كل استخدام متعمد لأنشطة بقصد تغير او افساد او خداع او اضعاف او تدمير انظمة الحاسوب او شبكات الحاسوب للخصم او المعلومات او البرامج المدرجة في هذه الانظمة والشبكات او التي ترسل من خلالها، وقد تؤثر هذه الانشطة ايضا في الكيانات المرتبطة بهذه الانظمة والشبكات". والهجوم السيبراني قد يستخدم في منع وصول المستخدمين الى حواسيب او خدمات معينة (هجوم الحرمان من الخدمة) او اتلاف وتدمير بيانات حيوية.(٩)

وقد عرف بعض الخبراء القانونيين مصطلح الهجمات السيبرانية بأنها (هي عمليات سيبرانية، هجومية كانت أم دفاعية، يُقصد بها إحداث إصابات أو التسبب بالوفاة لأشخاص، أو إلحاق الضرر بال أهداف وتدميرها).(١٠)

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

فيما عرفت وزارة الدفاع الامريكية الهجمات السيبرانية بأنه(توظيف القدرات السيبرانية، وذلك بهدف تحقيق غرض أساسي، يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء السيبرانية أو من خلاله)[١١]

اما مجلس الامن الدولي فقد عرف الهجمات السيبرانية بانها (استخدام اجهزة الحاسوب أو الوسائل الرقمية من قبل حكومة ما، أو بعلمها أو بموافقتها الصريحة، ضد دولة أخرى أو ممتلكات خاصة داخلها، ويشمل ذلك الوصول المتعمد إلى البيانات أو اعتراضها، وتدمير البنية التحتية الرقمية، وكذلك تصنيع وتوزيع أدوات يمكن توظيفها في الإخلال بالنشاط الداخلي)[١٢]

حيث يجمع الخبراء أن اول هجوم الكتروني قد استهدف دولة استونيا عام2007 ، لهذا يعد الهجوم الالكتروني الاول الذي ادى الى تعطيل المواقع الالكترونية الحكومية والمصرفية والتجارية والإعلامية مسببا قي ذلك خسائر بمئات الملايين من الدولارات إضافة إلى شلل كبير في مفاصل البلاد، وكان المتهم الرئيسي في هذا الهجوم روسيا وذلك باعتبار أن الهجوم تم بعد فترة وجيزة من الخلاف الكبير الحاصل بين إستونيا وموسكو بالرغم من عدم تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي حدث، وهذه تعد من المصاعب والمشاكل التي ترتبط بحروب الانترنت إلى الآن .[١٣]

وفي دراسة بعنوان(لقد بدأ سباق التسلح السيبراني) قام بها كيفين كولمان(Kevin Coleman الباحث في معهد Technolytics) يقول فيها "أن الصراع بين استونيا وروسيا كان مجرد قمة جبل الجليد في الحرب السيبرانية " واصفا الصراع الذي حدث عام 2007 بـ (حرب إلكترونية في ذروتها تم إطلاق أكثر من 4 ملايين معاملة وهمية في الثانية ضربت الأهداف المرجوة منها).[١٤]

وتعد الضربة الإلكترونية الأمريكية التي استهدفت اجهزة الطرد النووية الايرانية عام ٢٠١١ بواسطة جرثومة افتراضية وسميت هذه العملية (Stuxnet) . واما العمليات التي استهدفت دولة جورجيا اثناء الحرب ضد روسيا تعد من اكثر الحروب الالكترونية تعقيداً. .واما الرد الإيراني ما لبث ان اتى الرد سريعًا من خلال استهداف المصالح الأمريكية والصهيونية بالمنطقة كاستهداف شركة أرامكو في السعودية. [١٥]

وفي عام 2014 شنت كوريا الشمالية هجومًا إلكترونيًا ضد شركةSony Pictures" Entertainment "، مما ادى الى تعطل الاف من أجهزة الكمبيوتر(سوني)، وتم سرقة المعلومات السرية الخاصة بالشركة ومن اهمها (مستندات تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي شركة Sony رافقت كوريا الشمالية هجماتها الإلكترونية بالإكراه والتخويف والتهديد)، اذ يعد هجوم كوريا الشمالية على شركة سوني واحدًا من أكثر الهجمات الإلكترونية تدميرا مما دفع الهجوم الى تزايد النقاش حول طبيعة الهجوم السيبراني ومدى الحاجة إلى تحسين الأمن السيبراني. [١٦]

وان عام2017 ، شكل تنبيها مروعا لحقيقة الصراع السيبراني، وكذلك جاء كصافرة انذار مبكرة تكشف حجم التهديدات السيبرانية خصوصا ان الحكومات والمجرمين قد اظهروا معا مستوى غير مسبوق من الاستعداد

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

للتحرك بسلاسة لشن هجماتهم وتنفيذ جرائمهم الالكترونية دون عوائق على شبكة الإنترنت، ولهذا يعد الفضاء السيبراني في العصر الحديث ساحة للصراع بين الدول للتحشيد والدعاية والتنظيم. (١٧)

ومن هذه التعاريف السابقة نستخلص، أن الهجمات السيبرانية ميدانها هو الفضاء الإلكتروني والذي يعد المجال الخامس للحرب، اضافة الى المجالات التقليدية السابقة (البحر، اليابسة، الجو، الفضاء)، والذي يمثل نقطة اتصال الشبكات العنكبوتية لأجهزة الحاسوب، وربطها مع بعضها من خلال أجهزة ومعدات يتم التحكم بها من خلالها.

المطلب الثاني

خصائص حروب الفضاء الالكتروني

بعد الثورة المعلوماتية وانتشار الانترنت بشكل واسع، ظهر فضاء جديد تجري فيه الحروب وهو الفضاء الالكتروني، مما ادى الى حدوث تطورات كبيرة في اساليب القتال في الهجوم والدفاع، واحدث تغيرات في طبيعة الاسلحة المستخدمة، والاستراتيجيات العسكرية وقواعد الاشتباك المتبعة في القتال، اذ تعد حروب الفضاء الالكتروني انعكاس للثورة الرقمية والالكترونية في الميدان العسكري، والتي تهدف بالأساس الى شن هجمات تستهدف تكنولوجيا المعلومات للخصم، وشل قدراته العسكرية ويكون الحاق الضرر بها مواز للقصف العسكري المباشر.(١٨)

وقد اتجهت الدول إلى تبني خيار المواجهة في الفضاء الإلكتروني بشكل متزايد، لما يمتاز به هذا النوع من الصراعات من خصائص عديدة، أبرزها انخفاض تكلفته مقارنة بالحروب التقليدية، فهي لا تحتاج جيوش ومعدات، كما أن نسبة وقوع خسائر بشرية في صفوف القوة المهاجمة تكون منعدمة، وبالتالي، تؤدي الى تحمل الدولة كلفة اقل، مع إلحاق أكبر ضرر بالعدو.

ولا يقتصر تدني التكلفة على النواحي المادية والبشرية، وانما تمتد الى المسؤولية عن الهجمات، اذ يكون من الصعوبة بمكان معرفة جهة مصدر الهجوم، إضافة إلى امكانية شن هجوم بواسطة وكلاء يعملون لصالح هذه مما يصعب معه تتبع الدولة التي قامت بشن الهجوم.(١٩)

وقد ادى التحول نحو حروب الفضاء الإلكتروني الى حدوث تغيرات في نوع الأهداف المراد استهدافها، لذلك فإن هذه الحروب تستهدف البنى التحتية المدنية التي تكون مرتبطة بشبكات المعلومات، بحيث اصبحت التعاملات التجارية تعتمد بشكل اساسي على الفضاء الإلكتروني، وكذلك بقية المجالات والمؤسسات الحكومية.(٢٠)

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

كما ان حروب الفضاء الالكتروني لم تعد قاصرة على الجانب المدني بل تعدتها الى استهداف مواقع عسكرية وبنى تحتية حساسة ومنشآت صناعية بواسطة فايروس يمكنه احداث اضرار مادية هائلة تؤدي الى وقوع انفجارات ودمار شامل، وكمثال على ذلك استهداف انظمة التحكم بالمنشآت النووية الايرانية في الفترة الاخيرة.

ومن خصائص حروب الفضاء الالكتروني الاخرى انها لم تعد تقتصر على الدول، اذ قد يكون هناك اطراف اخرى فاعلة من غير الدول لان الاسلحة المستخدمة في الهجمات السيبرانية لم تعد حكرا بيد الدولة، نظرا للتكلفة المادية المتدنية نسبيا مقارنتا بالأدوات والمعدات المستخدمة في الحروب التقليدية، اذ يكفي في لشن هجوم الكتروني امتلاك حاسبة وتطوير البرمجيات اللازمة لاختراق اي هدف، كما تعد من اهم خصائص حرب الفضاء الالكتروني، هو عدم امكانية تطبيق مبدأ الردع في هذا النوع من الحروب، وذلك يعود الى اسباب عديدة منها صعوبة تحديد الدولة او الجهة التي شنت الهجوم.[٢١]

وعليه فان الردع والانتقام لا ينطبق على هذه الحروب، اذ يتعذر اظهار القوة الالكترونية المهاجمة، على عكس الحروب التقليدية فان الاسلحة والصواريخ يمكن رصدها وتحديد الدولة التي انطلقت منها، وحتى في حالة تم تتبع مصدر الهجمات السيبرانية فليس هناك قواعد مادية لكي يتم الرد عليها، كما ان معظم هذه الهجمات لا يتم كشف مصدرها الا بعد مضي عدة اشهر وهو ما يستبعد فكرة الردع بالانتقام بتوجيه ضربة تالية للطرف الذي بدأ الهجوم.[٢٢]

تختلف حروب الفضاء الإلكتروني عن الحروب التقليدية بغياب الحدود الجغرافية الواضحة، إذ لا تُمارس السيادة فيها بمعناها المتعارف عليه، ولا يمكن مطالبة الأطراف الأخرى بالامتناع عن اختراق المجال السيادي لدولة ما كما يحدث في العالم الواقعي، لان الحدود تتداخل مع بعضها في العالم الافتراضي وتشترك معظم الدول في نفس الشبكات المستخدمة، كما ان خوادم الشبكات (Network Servers) تكون في الغالب موجودة في دول اخرى غير الدول المستخدمة لها، وهذا يؤكد أن مفهوم السيادة في الفضاء الإلكتروني يعد مفهوماً مرناً وغير ثابت، تفرضه طبيعة البيئة الافتراضية نفسها.[٢٣]

ونستنتج مما سبق ان حروب الفضاء الالكتروني تتمتع بخصائص ومميزات تختلف كثيرا عن المواجهات في الحروب التقليدية، فأصبحت المواجهات الإلكترونية بلا حدود واضحة، ويصعب تحديد مصدر الهجمات، مما منحها طابعاً مختلفاً أثّر في الخطط العسكرية وقواعد الاشتباك.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المبحث الثاني

التكيف القانوني لحروب الفضاء الالكتروني وفقاً لمبادئ القانون الدولي

ان حروب الفضاء الالكتروني ما هي الا انعكاس للتطور التكنلوجي التي تميزت بسرعة وسهولة تنفيذها، والتي تؤثر بشكل مباشر بالبنية التحتية للدول فتصيب انظمتها الامنية والاقتصادية والعسكرية.

ونظراً لتزايد الهجمات الالكترونية بشكل كبير في الآونة الاخيرة، وصعوبة معرفة الجهة التي تقف خلف هذه الهجمات، وعدم وجود الاساس القانوني الذي ينظمها تكمن اهمية هذه الدراسة في كونها تتناول موضوعاً حديثاً لا يزال في مرحلة التطور، يسلط الضوء على تحديد مفهوم الهجمات السيبرانية وخصائصها بشكل دقيق، بالإضافة الى بحث مدى انطباق قواعد القانون الدولي الانساني على الهجمات الالكترونية سنتناول في هذا المبحث التكييف القانوني للهجمات الالكترونية في مطلبين تناولنا في المطلب الاول التكييف القانوني لحروب الفضاء الالكتروني وفق المبادئ الرئيسة في القانون الدولي العام. وافردنا المطلب الثاني للتكيف القانوني لتلك الحرب وفقا للقانون الدولي الانساني.

المطلب الأول

تكيف حروب الفضاء الالكتروني وفقاً للمبادئ الرئيسة في القانون الدولي العام

ان تكييف الهجمات الالكترونية وفقاً لمبادئ القانون الدولي والتي تضمنها ميثاق الامم المتحدة وهي مبدأ سيادة الدول ومبدأ حظر استخدام القوة او التهديد باستخدامها، اذ ان التطورات التكنلوجية اظهرت مجالات جديدة مثل السيادة السيبرانية وما يهدد هذه السيادة من هجمات الكترونية، وهذا يقودنا الى التساؤل عن مدى امكانية عد الهجمات الالكترونية استخدام للقوة ضد سيادة الدولة؟ وما مدى انطباق هذه المبادئ على الهجمات الالكترونية؟ وهذا ما سوف نتناوله في الفروع الاتية:

الفرع الأول

مبدأ السيادة

ظهر هذا المبدأ لأول مرة في معاهدة (وستفاليا) لعام ١٦٤٨ ويقصد به (ان تقوم الدولة بإدارة شؤونها دون تدخل من أي دولة اخرى).[٢٤]

ويعد مبدأ السيادة والاعتراف به من المبادئ التي تضمنها ميثاق الامم المتحدة اذ نص فيه على (تقوم الهيئة على مبدأ المساواة في السيادة بين جميع اعضائها)[٢٥]

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

وفي ظل التطور التكنولوجي وما رافقه من ظهور الفضاء الافتراضي بدا مفهوم السيادة التقليدي بالتراجع وبرز ما يطلق عليه بالسيادة السيبرانية[٢٦] وهي اشتقاق لمصطلح الامن السيبراني الذي يتضمن حماية شبكات الاتصال والبنى التحتية الالكترونية وشبكات الحواسيب ومجالات الطاقة والنقل والتقنيات المتعلقة بالفضاء السيبراني[٢٧] وهذا ادى ازدياد الهجمات الالكترونية بواسطة الحواسيب وشبكات الانترنت في الفضاء الالكتروني والتي تصدر من داخل احدى الدول وتنتهك السيادة الوطنية لدولة اخرى والتي يصعب معها تحديد الحدود الاقليمية في الفضاء الافتراضي،والذي نتج عنه الكثير من المخاطر ، مما استوجب على الدول تحديث تشريعاتها وقوانينها الداخلية لتضمينها الجرائم التي تحدث في الفضاء الافتراضي لتلك الدول.[٢٨]

نستنتج مما تقدم ان مبدأ سيادة الدولة في الفضاء الالكتروني يتحقق عندما تبدأ احدى الدول بشن الهجمات الالكترونية ضد دولة اخرى، وتشكل هذه الهجمات خرقاً لسيادة تلك الدولة.

الفرع الثاني

مبدأ حظر استخدام القوة والتهديد باستخدامها

نص ميثاق الامم المتحدة في المادة (٢/الفقرة ٤) على (يمتنع اعضاء الهيئة في علاقاتهم الدولية عن التهديد باستخدام القوة او استخدامها ضد سلامة الاراضي او الاستقلال السياسي لاي دولة....) كما ان القانون الدولي العرفي تضمن قاعدة تعزز الحظر الذي نص عليه الميثاق وهي قاعدة عدم التدخل في الشؤون الداخلية للدول، وهذا ما ايدته محكمة العدل الدولية من ان القاعدة اعلاه جاءت متوافقة مع ميثاق الامم المتحدة، وعلى الرغم من اهمية هذا المبدأ في حفظ السلم والامن الدوليين الا ان هناك استثنائين يردن عليه، الاول هو ما تضمنته المادة (٣٩) من ميثاق الامم المتحدة (يختصّ مجلس الأمن بتحديد ما إذا كان هناك تهديد للسلم أو إخلال به، أو وقوع عمل من أعمال العدوان، وله أن يقدّم في هذا الشأن توصياته، أو يقرر التدابير اللازمة وفقًا للمادتين (٤١ و٤٢) بهدف حفظ السلم والأمن الدولي أو إعادتهما إلى وضعهما الطبيعي)، والثاني ما تضمنته المادة (٥١) من ميثاق الامم المتحدة والتي تتعلق بحق الدولي في الدفاع عن نفسها اذا ما تعرضت لأي اعتداء من دولة اخرى والتي جاء فيها (لا يحدّ هذا الميثاق من الحق الطبيعي للدول، فرداً أو جماعة، في الدفاع عن نفسها عند تعرّض أي عضو لاعتداء مسلح، وذلك إلى حين اتخاذ مجلس الأمن الإجراءات اللازمة لحفظ السلم والأمن الدوليين. ويجب إبلاغ المجلس فوراً بأي تدابير تُتخذ استناداً إلى هذا الحق، دون أن يمسّ ذلك بصلاحياته المستمرة في اتخاذ ما يراه مناسباً من إجراءات لحفظ السلم والأمن الدولي أو إعادتهما إلى وضعهما الطبيعي).

من خلال الاطلاع على نص المادتين اعلاه نستنتج انها تنطبق على الهجمات التقليدية التي تتم على ارض الواقع، لكن مدى انطباق تلك النصوص على الهجمات الالكترونية التي تتم في الفضاء الافتراضي؟ وهل من حق الدولة التي تتعرض للهجمات السيبرانية الدفاع عن نفسها؟

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

هذا التساؤلات سوف يتم الاجابة عليها من خلال نظريات ثلاثة تتعلق بالهجمات الالكترونية:

١. نظرية النهج القائم على الوسيلة:-

تعتمد هذه النظرية على "الوسيلة" التي تستخدم في الهجوم، اذ ان الهجمات السيبرانية وحدها لا تعد هجوم مسلح، ومن ثم لا يكون للدول حق الدفاع عن نفسها طبقاً للمادة (٥١) من ميثاق الامم المتحدة، كون هذا الهجوم خالي من الخصائص الفيزيائية المرتبطة بالإكراه العسكري، وما يعزز من هذه النظرية هو قرار الجمعية العامة للأمم المتحدة في تعريفها للعدوان (هو قيام القوات المسلحة لدولة ما بمهاجمة القوات البرية والبحرية والجوية او الاسطولين البحري والجوي لدولة ما)، كما وتضمنت المادة الثالثة منه اعمال العدوان والتي جاءت على سبيل المثال لا الحصر، وعلى الرغم من ان هذه النظرية سهلة التطبيق الا انها لا تأخذ بالاعتبار الهجمات الالكترونية في الفضاء الخارجي التي تسبب اضرار بالغة. [٢٩]

٢. نظرية النهج القائم على الاهداف: – ملخص هذه النظرية عندما تتعرض احدى الدول الى هجوم سيبراني يمكن ان يصنف كهجوم مسلح، يكون لها الحق في الدفاع عن نفسها، مثال ذلك الهجوم السيبراني الذي يستهدف البنى التحتية للدولة يعد هجوما مسلحاً وفقا لهذه النظرية، ومن الانتقادات التي وجهت لهذه النظرية انها تجاهلت مفهوم البنى التحتية الحرجة وجسامة الهجوم السيبراني واثاره.[٣٠]

٣. نظرية النهج القائم على الاثار: تقوم هذه النظرية على خطورة اثار الهجوم، فيعد الهجوم السيبراني مسلحا متى ما كانت اثاره خطيره، مثال ذلك الهجوم الالكتروني الذي يستهدف انظمة مراقبة الملاحة الجوية والتسبب بحوادث الطائرات، فهذا الهجوم يعد مسلحا لأنه من المتوقع ان يتسبب بخسائر كبيرة في الاموال والارواح، فالهجوم السيبراني الذي تتعرض له انظمة الكمبيوتر او شبكة الانترنت لا يعد هجوم مسلح مالم ينتج عنه اضرار جسيمة مادية وجسدية، وتعد هذه النظرية اكثر مقبولية من النظريات السابقة.[٣١]

المطلب الثاني

تكيف حروب الفضاء الالكتروني وفقاً لمبادئ القانون الدول الإنساني

سوف اتناول في هذا المطلب اهم مبادئ القانون الدولي الانسان ومدى تأثيرها على حروب الفضاء الالكتروني من خلال الفروع الاتية:

الفرع الأول

مبدأ الضرورة العسكرية

يقوم هذا المبدأ على الموازنة بين الضرورة العسكرية والاعتبارات الانسانية، اما الضرورة فتتطلب استخدام القوة العسكرية المتوفرة لإحداث تفوق او مكاسب عسكرية، بينما تقتضي الاعتبارات الانسانية تقييد استخدام

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

القوة لتحقيق التفوق العسكري باقل الخسائر المادية والجسدية وبأساليب قتالية انسانية، ولمكانة هذا المبدأ واهميته في القانون الدولي الانساني يمكن تعريفه بانه تشير الضرورة العسكرية إلى التدابير التي لا بدّ منها لتحقيق أهداف القتال، شريطة أن تكون مشروعة ومتوافقة مع أعراف وقوانين الحرب. وهي تُعدّ الملاذ الأخير الذي يبرّر اتخاذ ما يلزم لضمان التقدّم على العدو، بشرط عدم تعارض هذه التدابير مع قواعد القانون الدولي الإنساني.[٣٢]

وقد تم النص على هذا المبدأ في اتفاقيات عديدة منها اعلان سان بترسبورغ في عام ١٨٦٨ والذي جاء فيه (ضرورات الحرب يجب ان تخضع للمتطلبات الانسانية)، كذلك تضمنت اتفاقية لاهاي بشأن الحرب البرية لعام ١٩٠٧ ان (يمنع تدمير الممتلكات العائدة للعدو او حجزها الا اذا اقتضت ضرورات الحرب ذلك).[٣٣]

الفرع الثاني

مبدأ التناسب في استخدام القوة

يعد هذا المبدأ من اهم المبادئ الجوهرية التطبيقية في نطاق النزاعات العسكرية بمختلف انواعها الداخلية والدولية، فهدف هذا المبدأ هو التقليل من الخسائر المادية والجسدية التي تترتب على العمليات العسكرية، مثال ذلك الهجوم العسكري الذي من المحتمل ان يتسبب بخسائر كبيرة بالأرواح والممتلكات تفوق بكثير الميزة العسكرية المرجوة منها. [٣٤]

الفرع الثالث

مبدأ التميز

هدف مبدأ التميز لحماية السكان والاعيان من خلال لزام أطراف النزاع بضرورة التمييز بين المدنيين والمقاتلين، وكذلك بين الأعيان المدنية والأهداف العسكرية، ومن ثم تكون العمليات العسكرية موجهة نحو اهداف عسكرية وتجنب استهداف السكان المدنيين والممتلكات، وقد تضمن البروتوكول الاضافي الاول لاتفاقيات جنيف لعام ١٩٧٧ هذا المبدأ اذ تضمن ان (تلتزم أطراف النزاع بالتمييز بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، بحيث تُوجَّه العمليات العسكرية حصراً نحو الأهداف العسكرية دون غيرها، ضماناً لحماية المدنيين وصون الأعيان المدنية)[٣٥]

كما اكدت محكمة العدل الدولية على هذا المبدأ بقولها يجب ان تكون الاعمال العسكرية موجهة نحو المقاتلين والاهداف العسكرية فقط، وهذا يعني ان تستهدف الهجمات السيبرانية اهدافا عسكرية، كأجهزة الحاسوب والنظم الالكترونية التي تسهم بشكل فاعل في العمليات العسكرية، وعليه من غير الممكن توجيه الهجمات من خلال الفضاء الالكتروني نحو انظمة حاسوب تكون مستخدمة في المنشآت المدنية [٣٦]

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

ان تطبيق هذا المبدأ على الهجمات السيبرانية صعب من الناحية العملية على نقيض الهجمات التقليدية، لان المهاجم غالبا ما يكون بعيداً عن المكان المستهدف، وهذا يعني ان مسالة التمييز بين المدنيين والمقاتلين امر في غاية الصعوبة .[٣٧]

الفرع الرابع

مبدأ مارنتز

اول من وضع اسس هذا المبدأ هو الدبلوماسي الروسي (فيدور فيودفج مارتنز) في مؤتمر السلام الذي عقد في عام (١٨٩٩) وتضمن (في الحالات غير المشمولة بالأحكام يبقى السكان المتحاربون تحت سلطان وحماية مبادئ قانون الامم كما جاءت من تقاليد استقرت عليها الشعوب المتمدنة والقوانين الانسانية ومقتضيات الضمير العام)[٣٨]، وقد نصت الكثير من الاتفاقيات على هذا المبدأ منها (اتفاقية لاهاي لعام ١٨٩٩-١٩٠٧ الخاصة بقواعد واعراف الحرب البرية، واتفاقيات جنيف لعام ١٩٤٩، والبروتوكول الاضافي الاول لعام ١٩٧٧)، وبما ان هذا المبدأ له اهمية كبيرة في القانون الدولي كونه يطبق على النزاعات التقليدية التي لا يوجد نص ينظمها، فهل يمكن تطبيق هذا المبدأ على الهجمات الالكترونية التي لا يوجد تنظيم دولي متفق عليه ينظمها؟

بالرجوع الى رأي محكمة العدل الدولية والتي وضعت تفسيرات حديثة لمبادئ القانون الدولي الانساني وقواعده والتي يجب ان تطبق على جميع الاسلحة التي لم يتمكن المجتمع الدولي من تحريمها ووضع القيود على استخدامها، ولكي تمتنع الدول من استخدام الاسلحة ذات الطبيعة التدميرية الجديدة (الاسلحة النووية) بحجة عدم وجود نصوص قانونية تحرم استخدامها [٣٩] ، ونصت محكمة العدل الدولية على هذا المبدأ بقولها(اثبت انه وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية)[٤٠].

الخاتمة

في ختام هذه الدراسة نستخلص إلى أن ظهور الحرب السيبرانية كان نتيجة تطور المنظومة التكنولوجيا للدول لاسيما وسائل الاتصال وشبكات الانترنت، وكذلك لجوء معظم دول العالم لنمط « الحكومات الإلكترونية» وهذا ما يميز الحرب السيبرانية التي تتسم بطابع خاص مقارنة بالحروب التقليدية ذات النزاع المسلح.

الاستنتاجات

١. يعد اختيار مصطلح السيبرانية هو الادق في الاشارة الى مفهوم هذه الهجمات وتميزها عن وسائل الحرب الاخرى، وهذا المصطلح هو الاكثر مقبولية وتداول على الصعيد الدولي.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

٢. ان قواعد الامم المتحدة لم تضع لتنظيم النزاعات في الفضاء الالكتروني، مما يثير اشكاليات في تكييف الهجمات السيبرانية ضمن مفاهيم استخدام القوة او العدوان المسلح.

٣. تعد مسالة تحديد الدولة المسؤولة عن الهجمات الالكترونية من ابرز التحديات، وهو ما ينعكس على تطبيق قواعد المسؤولية الدولية التقليدية.

٤. تمتاز الهجمات السيبرانية بانها عابرة للحدود، مما يحد من فعالية مفاهيم السيادة الاقليمية التقليدية.

٥. اصبح الفضاء الالكتروني مجالاً حيوياً للصراع الاستراتيجي بين الدول، مما يعكس تحول في مفاهيم القوة والردع في العلاقات الدولية.

٦. تشكل الهجمات الالكترونية خرق لمبدأ عدم التدخل في الشؤون الداخلية لدول اخرى ويرتب مسؤولية تلك الدولة.

٧. ان الهجمات الالكترونية التي تحدث اثناء الحرب او النزاعات المسلحة تخضع للقانون الدولي الانساني.

المقترحات

١. عقد اتفاقية دولية لتنظيم استخدام القوة في الفضاء الالكتروني تحت مظلة الامم المتحدة.

٢. انشاء هيئة دولية تكون تابعة للأمم المتحدة تتولى التحقق من الهجمات السيبرانية وتحديد المسؤولية الدولية عنها، بما يسهم في الحد من ظاهرة الانكار وصعوبة الاسناد.

٣. النص صراحة على ابعاد الهجمات السيبرانية العسكرية عن المرافق الحيوية المدنية (كالمستشفيات ومحطات الطاقة) لحماية السكان المدنيين من خطر تلك الهجمات.

٤. انشاء هيئة وطنية مختصة بالأمن السيبراني تتولى تهيئة المستلزمات والبنى التحتية للأمن السيبراني، وتعمل مع الجهات العسكرية والمدنية.

الهوامش

(١) بالقاسم بن صابر، الهجمات السيبرانيةَ ومواجهتها في ضوء القانون الدولي المعاصر، مَجلة حقوق الأنسان والحريات العامة، العدد ٤، جامعة عبد الحميد باديس، الجزائر، ٢٠١٧، ص ١٧٩-١٩١.

(٢) نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير مقدمة الى الجامعة الافتراضية السورية، عام ٢٠٢١، ص ٨.

(٣) منير البعلبكي، ورمزي منير البعلبكي، المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩، ص٣٠٧.

(٤) موقع قاموس المعاني، معنى كلمة سايبر، تاريخ الزيارة ٢٠٢٤/١٢/٢٣:
/https://www.almaany.com/ar/dict/ar-en/cyber

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

(٥) احمد عبيس نعمه الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، الطبعة الاولى، منشورات زين الحقوقية، لبنان، ٢٠١٨، ص١٦.

(6) Philip Levitz، The law of cyber– Attack، 2012، Vol. 100، Issue 4، P833

(٧) عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الإسرائيلية على الأمن القومي العربي، دار النهضة العربية، ط١، ٢٠٠٢، ص25 .

(٨)عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، منشورات الحلبي الحقوقية، بيروت،2007 ، ص١٥.

(٩) لين هيربت، النزاع السيبراني والقانون الدولي الانساني، مجلة اللجنة الدولية للصليب الاحمر، مجلد ٩٤(٨٨٦)، ٢٠١٢، ص١١٨-١١٩، متاح على الرابط : https://cutt.ly/RkoansD

(١٠) نور امير الموصلي، مصدر سابق، ص١٠.

(11)Schreier، Fred (2015). **On Cyber Warfare**. 1st edition. DCAF. Switzerland: Geneva.

(12) The same source.p86.

(١٣) فيصل محمد عبد الغفار، الحروب الالكترونية، الجنادرية للنشر والتوزيع،2015 ، ص ١٠-١٤.

(14) Kevin Coleman، The Cyber Arms Race Has Begun، JAN 28.2008، available from https://goo.gl/xKcvK4 .

(١٥) د. علاء الدين فرحان، الفضاء السيبراني- تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المجلد١٠، العدد٣، سنة ٢٠١٩، ص٩٣.

(16) Department of Defense Cyber Stratigy، Department of Defense، April 2015، p 2. Book online، available from https://goo.gl/g4hpuA.

(١٧) شيرين فهمي، مراجعة كتاب الإرهاب الالكتروني :القوة في العلاقات الدولية، مجلة النهضة، المجلد١١،العدد٤،2010 ، ص:ص 195 - 204.

(١٨) كلارك، ريتشارد، وكنيك، روبرت (2012) حرب الفضاء الإلكتروني :الخطر القادم على الأمن القومي وسُبُل مواجهته، الطبعة الأولى، الإمارات العربية المتحدة - أبو ظبي :مركز الإمارات لدراسة السياسات، ص٢٨٦.

(١٩) المصدر نفسه، ص ٢٨٩.

(٢٠) عبدالقادر فهمي، المدخل إلى دارسة الاستراتيجية، الطبعة الثانية .الأردن، عمان، دار مجدلاوي للنشر والتوزيع، سنة ٢٠١٤، ص١٨.

(٢١) المصدر نفسه، ص٢٤.

(٢٢) صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير جامعة الشرق الاوسط، ٢٠٢١، ص ٤٣.

(٢٣) عباس بدران، الحرب الإلكترونية :الاشتباك في عالم المعلومات،الطبعة الأولى، لبنان -بيروت مركز دراسات الحكومة الإلكترونية، ص٣٢.

(٢٤) د. لمى عبد الباقي محمود، المسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية، مجلة كلية القانون جامعة بغداد، عدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني المجلد ٣٦، ٢٠٢١، ص٣٣٩.

(٢٥) المادة (٢) الفقرة (١) من ميثاق الامم المتحدة.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

(٢٦) حسام جاسم محمد الدليمي، التطور التكنولوجي وأثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية جامعة الانبار، ٢٠١١، ص١١٤.

(٢٧) فاطم بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية، الصين نموذجاً، المجلة الجزائرية للأمن الانساني، المجلد الخامس، العدد الاول، مخبر الامن الانسان جامعة باتنة، الجزائر، ٢٠٢٠، ص٧٩٨.

(٢٨)أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكيف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ٤٤، العدد ١، كلية القانون والعلوم السياسية، جامعة الكوفة، النجف، ٢٠٢٠، ص٥٧.

(٢٩) United Nations Audiovisual Library of International Law، General Assembly Resolution، 3314، Defining aggression، p5

(٣٠) احمد عبيس نعمه الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ٤٤، العدد١، كلية القانون والعلوم السياسية، جامعة الكوفة، ٢٠٢٠، ص٥٧.

(31)Oona A. Hathaway، The Law of Cyber-Attack، Yale Law School، United States of America، Vol. 100:817، 2012،p842

(٣٢) مروة ابراهيم محمد، مبدأ الضرورة العسكرية في القانون الدولي الانساني، رسالة ماجستير مقدمة الى مجلس كلية القانون، جامعة بغداد، ٢٠١٥، ص١٩.

(٣٣)) .المادة (٣) الفقرة (٢/ز) من اتفاقية لاهاي للحرب البرية لعام 1907 .

(٣٤) مروة ابراهيم محمد، مصدر سابق، ص٩٥.

(٣٥)) .المادة (٤٨) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام1977 .

(٣٦) بن تغري موسى، الحرب السيبرانية والقانون الدول الإنساني، مجلة الاجتهاد القضائي، المجلد (١٢)، العدد (٢٢)، مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، الجزائر، ٢٠٢٠، ص٢٠٩.

(٣٧) احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٦.

(38)Antonio Cassese، The Martens Clause: Half a Loaf or Simply Pie in the Sky Vol. 11،2000، p187.

(٣٩) سلافة طارق الشعلان، تكيف استخدام الحرب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد1 ، العدد26 ، كلية القانون جامعة .الكوفة،2016 ، ص25 .

(٤٠)) .أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، مصدر سابق، ص64 .

المصادر

اولاً: الكتب

١. احمد عبيس نعمه الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، الطبعة الاولى، منشورات زين الحقوقية، لبنان، ٢٠١٨.
٢. البعلبكي، منير. والبعلبكي، رمزي منير: المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩.
٣. عباس بدران، الحرب الإلكترونية :الاشتباك في عالم المعلومات،الطبعة الأولى، لبنان –بيروت مركز دراسات الحكومة الإلكترونية.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

٤. عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، منشورات الحلبي الحقوقية، بيروت، 2007 .
٥. عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الإسرائيلية على الأمن القومي العربي، دار النهضة العربية، ط١، ٢٠٠٢ .
٦. عبدالقادر فهمي، المدخل إلى دارسة الاستراتيجية، الطبعة الثانية، الأردن، عمان، دار مجدلاوي للنشر والتوزيع، سنة ٢٠١٤.
٧. فيصل محمد عبد الغفار، الحروب الالكترونية، الجنادرية للنشر والتوزيع، 2015 .
٨. كلارك ريتشارد، وكنيك روبرت، حرب الفضاء الإلكتروني :الخطر القادم على الأمن القومي وسُبُل مواجهته، الطبعة الأولى، الإمارات العربية المتحدة – أبو ظبي، مركز الإمارات لدراسة السياسات، ٢٠١٢.

ثانياً: الرسائل

١. حسام جاسم محمد أحمد الدليمي، التطور التكنولوجي واثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية جامعة الانبار، ٢٠١١ .
٢. صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير جامعة الشرق الاوسط، ٢٠٢١.
٣. مروة ابراهيم محمد، مبدأ الضرورة العسكرية في القانون الدولي الانساني، رسالة ماجستير مقدمة الى مجلس كلية القانون، جامعة بغداد، ٢٠١٥.
٤. نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير مقدمة الى الجامعة الافتراضية السورية، عام ٢٠٢١.

ثالثاً: البحوث

١. أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكيف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ٤٤، العدد ١، كلية القانون والعلوم السياسية، جامعة الكوفة، النجف، ٢٠٢٠.
٢. بالقاسم بن صابر، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الانسان والحريات العامة، العدد ٤، جامعة عبد الحميد باديس، الجزائر، ٢٠١٧.
٣. بن تغري موسى، الحرب السيبرانية والقانون الدول الإنساني، مجلة الاجتهاد القضائي، المجلد (١٢)،العدد مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، الجزائر، ٢٠٢٠.
٤. لمى عبد الباقي محمود، المسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية، مجلة كلية القانون جامعة بغداد، عدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني المجلد ٣٦، ٢٠٢١.
٥. سلافة طارق الشعلان، تكيف استخدام الحرب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد1 ، العدد26 ، كلية القانون جامعة .الكوفة،2016 .

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

٦. شيرين فهمي، مراجعة كتاب الإرهاب الالكتروني :القوة في العلاقات الدولية، مجلة النهضة، م11، 2010 .
٧. فاطم بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية، الصين نموذجاً، المجلة الجزائرية للأمن الانساني، المجلد الخامس، العدد الاول، مخبر الامن الانسان جامعة باتنة، الجزائر، ٢٠٢٠.
٨. علاء الدين فرحان، الفضاء السيبراني، تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المجلد١٠، العدد٣ .

رابعاً: الاتفاقيات والمواثيق

١. المادة (٢) الفقرة (١) من ميثاق الامم المتحدة.
٢. المادة (٣) الفقرة (٢/ز) من اتفاقية لاهاي للحرب البرية لعام 1907 .
٣. المادة (٤٨) من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام1977 .
٤. المادة (٥٢) الفقرة (٢) من البروتوكول الاضافي الاول لعام 1977 .

خامساً: المصادر الالكترونية

١. لين هيربت، النزاع السيبراني والقانون الدولي الانساني، مجلة اللجنة الدولية للصليب الاحمر، مجلد ٩٤(٨٨٦)، ٢٠١٢، ص١١٨-١١٩، متاح على الرابط : https://cutt.ly/RkoansD
٢. موقع قاموس المعاني، معنى كلمة سايبر، تاريخ الزيارة ٢٠٢٤/١٢/٢٣.
/https://www.almaany.com/ar/dict/ar-en/cyber

سادساً: المصادر الانكليزية

1. Schreier، Fred (2015). **On Cyber Warfare**. 1st edition. DCAF. Switzerland: Geneva.
2. Oona A. Hathaway، The Law of Cyber-Attack، Yale Law School، United States of America، Vol. 100:817، 2012 .
3. United Nations Audiovisual Library of International Law، General Assembly Resolution 3314، Defining aggression.
4. Antonio Cassese، The Martens Clause: Half a Loaf or Simply Pie in the Sky? available from https://goo.gl/xKcvK4 .
5. Department of Defense Cyber Stratigy، Department of Defense، April 2015،Book online، available from https://goo.gl/g4hpuA.
6. Kevin Coleman، The Cyber Arms Race Has Begun، JAN 28.2008، / https://www.almaany.com/ar/dict/ar-en/cyber.
7. Philip Levitz، The law of cyber– Attack، 2012، Vol. 100، Issue 4.، 2012.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م