مجـــلـة الحـــق للعلوم الشرعية والقانونية
Al-haq Journal for Sharia and Legal Sciences
تصدر عن كلية القانون – جامعة بني وليد – ليبيا
Website: https://www.al-haqjournal.ly/index.php/alhaq/index
العدد الرابع عشر ـ ديسمبر 2024 ـ الصفحات (196-210)
ISSN 3005-3919

الحروب السيبرانية (الواقع – التحديات)
في ضوء القانون الدولي الإنساني (I.H.L)

د. رمضان عبد الله العموري *
قسم القانون الدولي، كلية القانون ،جامعة خليج السدرة، خليج السدرة ،ليبيا .
Dr.ramdan@gsu.edu.ly

Cyber Wars (Reality – Challenges)
In light of international humanitarian law (I.H.L.)

Ramadan Abdullah Al-Amouri*
Department of International Law, Faculty of Law, Gulf of Sidra University, Gulf of Sidra, Libya

تاريخ الاستلام: 27-10-2024 تاريخ القبول: 24-11-2024 تاريخ النشر: 09-12-2024

الملخص
تناول البحث موضوع بالغ الأهمية حيث ناقش خطورة الحرب السيبرانية والاشكاليات المترتبة عليها، وتناولت الإشكالية مدى خضوع الحروب السيبرانية للقواعد الإنسانية الدولية (I.H.L) والآثار المترتبة عليه، واستخدم في هذا البحث المنهج الوصفي والمنهج التحليلي، وقد توصل البحث إلى عدة نتائج أهمها: أن الحروب السيبرانية تؤدي الى أضرار كبيرة تؤثر سلباً على البُنى التحتية للدول ، وكذلك بعد أن أصبحت الحروب السيبرانية عامل مهم في أمن الدول وقوتها، ومن ثم أصبحت الحروب السيبرانية في تزايد مستمر، وتوصل البحث إلى عدة توصيات أهمها السعي إلى مراجعة القواعد الإنسانية الدولية، بهدف ضمان سلامة المدنيين، والسعي إلى إبرام اتفاقيات دولية تهتم بتطبيق القانون الانساني على الحروب السيبرانية، والتعاون في ما بين الدول في التعرف على مرتكبي الهجمات الالكترونية.
الكلمات المفتاحية: الحروب السيبرانية ، الواقع ، التحديات ،الاتفاقيات الدولية، القانون الدولي الإنساني.

Abstract
The research dealt with a very important topic, as it discussed the danger of cyber warfare and the problems resulting from it. The problem dealt with the extent to which cyber warfare is subject to international humanitarian rules (I.H.L) and the consequences thereof. The descriptive and analytical approaches were used in this research. The research reached several results, the most important of which are: that cyber warfare leads to significant damage that negatively affects the infrastructure of countries. Also, after cyber warfare has become an important factor in the security and strength of countries, cyber warfare has become increasingly common. The research reached several recommendations, the most important of which is seeking to review international humanitarian rules, with the aim of ensuring the safety of civilians, seeking to conclude international agreements concerned with applying humanitarian law to cyber warfare, and cooperation between countries in identifying perpetrators of cyber attacks.
Keywords: Cyber wars, reality, challenges, international agreements, international humanitarian law.

المُقَدّمَةُ:

يعتبر ظهور الإنترنت قفزة نوعية في مسيرة التطور التقني، وذلك من خلال ما أوجدته من سهولة الاتصالات وسرعة تبادل المعلومات، إلا أنه رغم هذا التطور له مردود سلبي ، حيث أضحت اليوم أحد الوسائل التي تستخدمها الدول في الحرب في ما بينها، وعليه تكون تقنية المعلومات قد أوجدت حرب جديدة يطلق عليها الحرب السيبرانية(**CYBER WAR**) أي الحرب الالكترونية، وفى أغلب الأحيان تكون نتائجها ضارة بالمدنيين، ومن ذلك الهجوم الإلكتروني الذى قامت به الدولة الروسية ضد أوستوانيا عام 2007، حيث آلت هذه الحرب إلى دمار وشلل كبير للدولة ومرافقها العسكرية وغير العسكرية، ثم توالت الهجمات الالكترونية تزامناً مع ما قامت به روسيا ضد جوريا عام 2008، وكل تلك الهجمات قد تضر بالمدنيين والتي تُشكل تعدي كبير على قواعد الإنسانية الدولية الذى يحكم حالات الحروب ، وهدفه التقليل من الآثار السلبية خاصة ضد المدنيين والأهداف المدنية.

إشكالية البحث:

تتمثل في الإجابة على التساؤلات الآتية:

ما مدى خضوع الحروب السيبرانية للقانون الدولي الإنساني؟

ماهي الحروب السيبرانية وما هي خصائصها وأدواتها؟

ما الطبيعة القانونية للحروب السيبرانية؟

ما مدى تطبيق القانون الدولي الإنساني على الحروب السيبرانية؟

ما مدى تنظيم القانون الدولي الإنساني للقواعد التي تحكم الحروب الالكترونية؟

ما مدى اعتبار الهجمات ضد الأهداف المدنية انتهاك وتعدى على القانون الدولي الإنساني؟

هل يمكن تطبيق القانون الدولي الإنساني على الحروب السيبرانية وماهي الآثار الناتجة على التطبيق؟

أهداف البحث:

يمكن أن يسهم هذا البحث في بيان وتوضيح مفهوم الحروب الالكترونية، وبيان ما ينتج من اشكاليات عنها وتثيرها في نطاق القانون الدولي الإنساني، وتوضيح مدى احتواء أحكام القانون الدولي الإنساني للحروب الالكترونية وإيضاح الآثار القانونية المترتبة على خضوعها إلى أحكام القانون الدولي الإنساني.

أهمية البحث:

الأهمية العملية: يمكن أن يسهم هذا البحث في إثراء المحتوى العلمي فيما يتعلق بحروب الذكاء الاصطناعي والعوامل المرتبطة بها.

الأهمية التطبيقية: نظرا لاستخدام العمليات السيبرانية من قبل بعض الدول خلال شنها الحرب فإن هذا الخطر قد أصبح حقيقة واقعية، فإذا كان هناك عدد قليل من الدول قد أقرت بإجراء مثل تلك الهجمات فمن الأرجح أن يزداد عدد مستخدميها من طرف الدول، الأمر الذي يؤدي إلى زيادة خطورتها، حيث تكمن أهمية الموضوع في حداثته وقلة الأبحاث التي تعالجه.

حدود البحث: يتمحور البحث في نطاقه وحدوده حول الهجمات السيبرانية أثناء النزاعات المسلحة ومدى انطباق القانون الدولي الإنساني عليها، وبهذا تخرج الهجمات السيبرانية في حالة السلم من نطاق البحث الهجمات.

منهجية البحث: يستخدم الأسلوب الوصفي، لوصف الهجمات السيبرانية، والمنهج التحليلي لتحليل القواعد العامة في القانون الدولي الإنساني؛ ومعرفة مدى إمكانية تطبيقها على الهجمات السيبرانية أثناء النزاعات المسلحة.

خطة البحث:

المبحث الأول: الإطار النظري والقانوني للحروب السيبرانية

المطلب الأول: تعريف الحروب السيبرانية وخصائصها

المطلب الثاني: أهداف الحروب السيبرانية وطبيعتها القانونية

المبحث الثاني: القانون الدولي الإنساني كإطار قانوني منظم للحروب السيبرانية

المطلب الأول: القدرة على تطبيق قواعد القانون الدولي الإنساني على حروب الذكاء الاصطناعي
المطلب الثاني: الجهود الدولية لتنظيم القانوني للهجمات في الفضاء الالكتروني

المبحث الأول

الإطار النظري والقانوني للحروب السيبرانية

الحروب السيبرانية تشير الى الهجمات الموجهة نحو الدول عبر أنظمتها الالكترونية، حيث أصبحت الدول اليوم تعتمد على حروب الذكاء الاصطناعي في الأزمات تكون بينها، فأضحت هذه الحرب الإلكترونية خياراً وبديلاً لاستخدام القوة العسكرية للدول في أغلب الأحيان، وخاصة كونها أقل تكلفة وتميزها بعنصر السرية وبهذا أصبحت الخيار الأفضل للدول..[1]

المطلب الأول

تعريف الحروب السيبرانية وخصائصها

يعتبر نوربرت أول المستخدمين لمصطلح السيبرانية وذلك عام 1948، واستخدم مصطلح القوة الإلكترونية كمرادفاً للحرب السيبرانية على المستوى العربي.

وبهذا أصبحت الحروب السيبرانية مصطلحاً يدل على أي نزاع يحدث في الفضاء الالكتروني؛ كونها تعد عامل فعال في النظام الدولي الجديد، حيث يؤسس لوجود ميدان جديد للحرب والصراع بين الدول[2]، فكانت محط اهتمام أكثر الدول في العالم، وبهذا وبهذا فإن ضعف النية التكنلوجية يعرض الدول لخطر الهجمات الالكترونية قد تفوق الأضرار المرتبة عليها الحرب التقليدية .[3]

يعرفها نيلز ميلزر بأنها " تلك التي تجرى في الفضاء السيبرانى من خلال الوسائل والأساليب السيبرانية).وأشار إلى أن الفضاء السيبرانى يتجه إلى بعد آخر" .[4]

وعرفها عبد السلام بدران بأنها " هي معارك حديثه ترتكز على استهداف البنية التحتية الرقمية والأنظمة المعلوماتية للأطراف المعنية وتستخدم هذه العمليات أدوات متطورة للتجسس ومراقبة الاتصالات والاشارات الالكترونية، بهدف اضعاف القدرات السياسية والعسكرية والأمنية للخصم من خلال تعطيل الشبكات وارباك أنظمة الاتصالات".[5]

وعرف البنتاغون العمليات في الفضاء الالكتروني بانها " هي استخدام القدرات التقنية لتحقيق أهداف عسكرية أو تأثيرات معينة ضمن هذا المجال" .[6]

وتم تقسيم هذه العمليات الى ثلاثة أنواع رئيسية:

1/ الهجمات الالكترونية الهجومية التي تهدف الى اختراق أنظمة الخصوم وتعطيلها

2/الدفاع الالكتروني الذي يركز على حماية الأنظمة والشبكات من الاختراق

3/الأنشطة الاستخباراتية الالكترونية التي تشمل جمع وتحليل للبيانات لدعم القرارات العسكرية.[7]

وعرفها مجلس الأمن الدولي بأنها " هي أفعال تنفذها او توافق عليها الحكومات، تستهدف جهات أخرى بغرض الوصول الى البيانات واعتراضها أو اتلافها مع تضمين انتاج وتوزيع أدوات تستخدم لإضعاف الأنشطة الداخلية للجهة المستهدفة" .[8]

---

[1] حسين حسن الفتلاوي، عماد محمد ربيع، موسوعة القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع، الأردن، 2020، ص101

[2] Edl,amK R.D. Rethinking cyber warfare the international Relations of Digital Disruption . Oxford University press. 2024

[3] صابر بلقاسم، وحيد محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الانسان والحريات، جامعة عبدالحميد بن باديس، الجزائر، العدد4،2020، ص186

شريف عبد الحميد حسن، الحروب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مجلة الشريعة والقانون، الدقيلية – مصر، العدد23، الجزء الرابع، سنة 2021، ص3069

[4] نبيل عودة، العمليات السيبرانية في الحرب الروسية الاكرانية، الشروق للأبحاث الاسترتجية،2022، ص7

[5] عباس بدران، الحروب الالكترونية في عالم المعلومات، ط1، لبنان بيروت، مركز دراسات الحكومة الاكترونية،2010، ص30

[6] Schreier.fred. on cyber ware. Edition. DCAF.switzerland.Geneva.2015.p16

[7] محمد عادل عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، مجلة البحوث القانونية والاقتصادية،2021، المجلد33، العدد1، ص24

[8] صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، دراسة في مفهومها، جامعة الشرق الأوسط، الأردن، 2021، ص22

ويعرفها الاتحاد الدولي للاتصالات بأنها "هي تلك الاعتداءات التي تشمل المجال المادي وغيره والذي يحتوي على العناصر الآتية: الحاسوب، الشبكات، البرامج، والتحكم، وكل مستعملي هذه المكونات" .[1]
وقام العديد من الباحثين بمحاولة لتعريف الحروب السيبرانية، حيث عرفها، ريتشارد كلارك، وروبرت، على انها " التدابير التي تتخذها الدولة لاستهداف أنظمة الكمبيوتر والاتصالات لدولة ما ".[2]
كما تتميز الحروب السيبرانية بنوعية الأسلحة التي يمكن استخدامها في القتال الإلكتروني، وفى هذا الصدد عرف دليل تالين في القاعدة 41 الأسلحة الالكترونية، إذ صنف وسائل وطرق الحرب.[3]
وهذا يدل إلى أن الحروب السيبرانية أصبحت مصطلحاً يشير إلي أي نزاع يحدث في الفضاء الالكتروني ويأخذ الطابع الدولي، واذا ما تم النظر في هذا التعريف يعتبر غير شديد الدقة ، اذا ما أخذ هذا التعريف بعين الاعتبار فانه قد يعتبر غير دقيق بما يكفي لتمثيل جوهر الحروب في الفضاء الالكتروني وفحواها بشكل عام، فقد أشار بعض الباحثين الى أهمية التركيز على اشكال النزاعات المختلفة التي تحدث في الفضاء الالكتروني مثل التجسس الالكتروني، أما الحروب السيبرانية فتعد أخطر من بين كل ذلك، حيث تعتبر جزء من حروب المعلومات بشكل واسع؛ حيث تؤثر على الإرادة السياسية للطرف المستهدف.[4]
وفى الواقع أن الحروب السيبرانية ماهي إلا استخدام لتكنولوجيا المعلومات ضمن استراتيجية عسكرية (ما بين الدفاع والهجوم) يكون الهدف منها شلل البنية التحية للدولة المنافسة.[5]
واتفق مع تعريف طارق المجدوب الذي عرف الحروب السيبرانية بأنها: "هي مجموعة من الأعمال العدائية الموجهة ضد معطيات الدولة الالكترونية المخزنة أو المعالجة أو المتبادلة من حاسوب إلى أخر؛ بهدف كشفها أو نسخها أو تعديلها أو إتلافها أو عرقلة تدفقها كالهجوم على أنظمة المراقبة وانابيب نقل الغاز والبترول".[6]
ومن هذا المنطلق نرى أن الفضاء السيبراني أصبح يشكل اليوم ميداناً جديداً لأوجه الصراع العسكري، إذ يمكن عن طريقه أن تشن الهجمات الإلكترونية، تهدف الى إلحاق الأذى والضرر بالبنى الرقمية للخصم، ومن هنا يمكن الاستنتاج إن الحروب السيبرانية هي تلك العمليات الإلكترونية التي تتخذها أطراف النزاع من أجل الهجوم على نظام المعلومات لعدو والتي تتسبب في أضرار غير محدودة.[7]
وهنا نود أن نبين الاختلاف بين النزاعات الالكترونية عن الإجراءات الالكترونية "" التي تهتم اهتماماً خاصاً باستخدام القدرات المتعلقة بالمعلومات في أثناء الهجوم المسلح؛ للتأثير في عملية صنع القرار لدى الدولة الخصم، وقد تستخدم العمليات المعلوماتية الفضاء الإلكتروني كوسيط، ولكنها قد تستخدم ايضاً إمكانات من المجالات المادية"" .[8]
حيث تعتبر حروب افتراضية وهلامية، ومتطورة بألياتها ووسائلها التي لها علاقة بأكبر المجالات التكنولوجية وهذه البرامج هي البرمجيات الضارة.[9]
هذا النوع الجديد من الحرب وآليات الصراع أدت إلى أن تكون الدول الكبرى مع الدول الصغرى، في سياق متكافئ في تطوير الأسلحة السيبرانية.[10]

---

[1] إسماعيل زروقة، الفضاء السيبرانى وأثره في الامن الوطني العربي، مجلة العلوم القانونية والسياسية، المجلد1، العدد1،2019، ص1018
[2] مركز الجزيرة للدراسات، الحروب الالكترونية في القرن 21، المجلد الخامس على الرابط التالي https//studies.aljazeera.com تاريخ الزيارة 2023/2/5
[3] عمرو رضا بيومي، مخاطر أسلحة الدمار الشامل الإسرائيلية على الامن القومي العربي، ط1، دار النهضة العربية، 202، ص25
[4] فيصل محمد عبد الغفار، الحرب الالكترونية، ط1، الجنادرية، للنشر والتوزيع، ط1، الأردن،2015، ص10-11
[5] مهند جبار عباس، هيثم كريم صوان، الحروب السيبرانية بين التحديات واستراتيجيات المواجهة، العراق أنموذجا، مجلة قضايا سياسية، العدد70، كلية العلوم، جامعة النهرين، العراق،2022، ص146
[6] طارق المجدوب، السايبر ساحة خفيفة لحرب ناعمة قادمة، منشورات مجلة الدفاع الوطني، العدد49،2014،
[7] محمد عبد الرحمن، الهجمات السيبرانية في سياق النزاع المسلح، المجلة الليبية العالمية، كلية التربية، المرج، جامعة بنغازي، ليبيا،2022، ص9
[8] نبيل عودة، مرجع سابق، ص7
[9] ليلي بشلالق، تأثير الحروب الالكترونية على العلاقات الأمريكية الروسية، رسالة ماجستير غير منشورة، جامعة محمد بوضياف، الجزائر،2018، ص14
[10] عادل عبد الصادق، اسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، العدد23، مصر،2016، ص137

نـرى أن للحـروب السـيبرانية وسـائل عـدة، منهـا اختـراق الشـبكات والحـروب النفسـية والفكريـة وسـرقة المعلومات، والتنافس بين أجهزة المخابرات الدولية وكذلك البرامج الضارة ومنها الفيروسات.[1]
ومن ناحية أخرى تعد شبكات الانترنت هي إحدى الأدوات الفعالة في حروب أنظمة الذكاء الاصطناعي التي تشنها الجماعات المتشددة.[2]
ومن خلال عرض تعريفات الحروب السيبرانية ووسائلها يمكن أن نجمل خصائصها بأنها: تتمتع بالشمولية وذلك لتعدد الموارد السيبرانية، وانعدام البعد المكاني للفضاء السيبراني، مما يصعب التحكم بمسارات التهديدات السيبرانية، وسرعة تنفيذ الهجمات السيبرانية عبر شبكات المعلومات بدون أي إنذار، مما يؤدى إلى تسارع المخاطر، وكما انها تقع في ميدان افتراضي غير محدد النطاق وعليه تكون قد أزاحت حدود الجغرافيا، وتعتبر طريق آمن للهجوم، كما أن تكلفة الحروب في الفضاء الالكتروني أقل بكثير مقارنة بالحرب التقليدية.[3]
وايضاً تعتبر ذات آثار مدمرة وغير محدودة، وذلك باعتبار أن الحروب السيبرانية ذات أثر مدمر؛ لأنها توجه ضد المنشأة الحيوية والبنية التحية المدنية، والخدمات الحيوية للسكان المدنيين، ما قد يترتب عليها آثار بالغة أو واسعة النطاق أو طويلة الأمد بالمدنيين، وقد تكون آثارها كبيرة جداً مثل تفجير المنشآت النووية، وتعطيل الملاحة الجوية والبحرية، وما يزيد من حدة الاثار في العصر الحالي تزايد اعتماد المنشآت الحيوية المدنية كالمستشفيات ومحطات التوليد للطاقة والمياه على الرقمنة والانترنت.[4]
تعود صعوبة تحديد مرتكبي هذه الحروب الى أنها لا تترك اثاراً مادية بالإضافة الى الحاجة الماسة الى الخبرة الفنية التي تقتصر اليها الدول المتضررة بالإضافة الى الاعتماد على الذكاء في تنفيذ العمليات.[5]
وهذا ما يجعلها تتسبب في خسائر كبيرة في أوقات محدودة وبأقل التكاليف، فنجد لجوء الدول إليها في الفترة الأخيرة سواء واكبت العمليات العسكرية أو بمفردها.[6]

المطلب الثاني

أهداف الحروب السيبرانية ووضعها القانوني

إن الهدف من الحروب الالكترونية هو الإضرار بالبنى الأساسية والحيوية لأي دولة وتشمل أغلب المجالات الاقتصادية منها أو العسكرية أو الثقافية.[7]
ومصطلح البنى التحتية كما بينتها السياسة الرئاسية للولايات المتحدة الامريكية وتشمل ستة عشر قطاع تم إدخالها إلى ضمن مجالات الأمن القومي وهي: المرافق التجارية، الاتصالات، التصنيع الحربي، مشاريع السدود، الطاقة، مزارع الغذاء والزراعة، تقنية المعلومات، أنظمة النقل، أنظمة المياه.[8]
وتسعى الحرب السيبرانية إلى احداث توقف المواقع الالكترونية الحساسة، وهجمات ضد البنية التحتية المدنية، وأخرى ضد المواقع العسكرية، وتسعى إلى تشتيت قدرات الخصم والتجسس وسرقة البيانات وضرب مراكز السيطرة والتحكم، وإحداث حالة من الذعر بين المدنيين، وهذا ما حصل في الهجمات الالكترونية على

---

[1] محمود شاكر، الحرب السيبرانية وتداعياتها على الامن العالمي، الموسوعة الجزائرية للدراسات السياسية والاستراتجية،2019، ص 35
[2] مهند جبار عباس ومن معه، الحروب السيبرانية بين التحديات والمواجهة، العراف أنموذجا، مجلة قضايا سياسية، العراق، كلية العلوم السياسية، جامعة النهرين، العدد70، 2022 ص153
[3] مهند جبار عباس ومن معه، مرج سابق، ص154
[4] نور امين الموصلي، المجلة الالكترونية الشاملة متعددة التخصصات، العدد24، 2020، ص12
[5] صالح عمر خليل، الاطار النظري للأمن الإلكتروني السيبراني، ط1،القاهرة، منشورات الدار للنشر، 1993، ص14
[6] صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها، رسالة ماجستير، كلية الآداب والعلوم، جامعة الشرق الأوسط، الأردن،2020، ص29
[7] هبه عبدالفتاح، الحروب السيبرانية الأكثر دماراً اخبار اليوم 2019/9/14، متاح على الرابط www.akhbaralyom.com ، تاريخ الزيارة 2023/2/15
[8] مهند جبار عباس، ومن معه، الحروب السيبرانية بين التحديات واستراتيجيات المواجهة العراق نموذجا ، مجلة قضايا سياسية، العدد70، ص146-148

أوكرانيا من قبل الدولة الروسية[1]، وهذا ما أكده أحد المسؤولين بأوكرانيا فيقول : أن بلاده تعرضت إلى هجوم سيبرأني ويعتبر من أقوى الهجمات التي تتعرض لها بلاده، ونظراً لكون الهجوم السيبراني لا يحمل أي إشارات عسكرية فلا يمكن نسبته إلى فاعل على وجه التحديد.[2]

وقد تسعى الدولة المهاجمة إلى استخدام الهجوم السيبراني؛ لغرض تعطيل الدفاعات حتى تتمكن من قصف موقع معين، كما حصل في سوريا سنة 2012 عندما تم الهجوم على الدفاعات السورية بهجوم سيبراني حتى تتمكن الطائرات المعادية ضرب مواقع، وهنا يمكن أن نقول أن الهجوم السيبراني موازي للحرب التقليدية.[3]

وقد يكون الهجوم السيبراني لا يتواكب مع الحرب التقليدية وهذا ما حصل ونلاحظه في سنة 2021 بعد قيام إيران بإسقاط طائرات أمريكية في مضيق هرمز، حيث قامت الولايات المتحدة الأمريكية بهجمات سيبرانية استهدفت أنظمة الدفاع الإيرانية.[4]

الطبيعة القانونية للحروب السيبرانية:

نتيجةً للقصور الذي شاب اتفاقيه (بودابست) حول الهجمات الالكترونية، الواقعة ما بين الدول يجعلنا هذا الأمر نبحث عن أساس قانوني آخر يمكننا الاعتماد عليه في تطبيقه على تلك الهجمات أو ينظم سير العملية العدائية[5].

ووفقاً لمجال اللجنة الدولية للصليب الأحمر في مجال القانون الدولي الإنساني، وسعيها واهتمامها أيضا بالمجال المسلح وتخوفها من المخاطر التي أفرزتها التكنولوجية العسكرية، تم إبرام صك قانوني في عام 2013 يدعى (دليل تالين) يهدف إلى دراسة مدي استطاعة تطبيق اسس القانون الدولي على الهجمات الالكترونية وذلك في أثر الهجوم الذي قامت به روسيا على استونيا عام 2007، حيث نص الدليل على مبدأ حظر استعمال القوة المحرم دوليا[6] في القانون الدولي.

وقد وصف (دليل تالين) الهجومات التي تقوم بها الدول ضد بعضها البعض بواسطة التكنولوجيا بالحرب الالكترونية كما يقر بأن العمليات في الفضاء الالكتروني بمفردها إمكانية اعتبارها حروب مسلحة وفقاً للأحداث لاسيما النتائج المدمرة الناشئة عن تلك العمليات ويقدم دليل تالين بهذا الصدد تعريفا للهجوم السيبراني بأنه: عملية إلكترونية سواء هجومية أو دفاعية تتسبب في أصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها.

ولعل العيب الثاني الذي يشوب هذا الدليل يتمثل في عدم الإلزام، أي كونه ليس ملزما لدول الأطراف التي شاركت في إعداده إذ لا يرتقي هذا الدليل إلي مستوى الاتفاقية الدولية فضلا عن معارضة بعض الدول لإحكامه كروسيا والصين على اعتبار أنهما لم تشاركا في إعداده وكما لم يتم مراعاة التمثيل العالمي للدول في اختيار الخبراء الذين أعدوه [7]

و بالتالي لا يمكننا تكييف الهجوم السيبرانى على أنه حرب إلكترونية تخضع لإحكام (دليل تالين) من حيث اعتبارها حرب ، حيث لا توجد بها السمات المتمثلة في الحرب التقليدية ، والتي نجدها في المحاولة للحد من قدرات الخصم العسكرية خلال معركة مفتوحة و هي حرب معلنة بين الدول ، و لا يرى سوى انتشار جنود م

---

[1] Topor. L. Cyber Warfer :Global Trends and proxy Wars. In Cyber Sovereiginy international. And the Future of the internt.2024.cham : Springer nature switzerland. Pp 75-110

[2] نبيل عودة، العمليات السيبرانية في الحرب الروسية الاكرانية، مرجع سابق، ص11

-كبارا طه محمد، نطاق فعالية الحرب في تنفيذ أهداف السياسة الروسية، دراسة حالة الحرب السيبرانية، مجلة البيئة الاقتصادية، العدد23/ سنة2024، ص216-217

[3] يحي ياسين سعود، الحروب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، المجلد4، العدد4،2018، ص88

[4] صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2021، ص29

[5] حسين إبراهيم حسن، الحرب السيبرانية في ضوء قواعد القانون الدولي، مجلة البحوث القانونية والاقتصادية، المنوفية، مصر، سنة 2024، ص204-205

[6] سعيد درويش، الحروب السيبرانية وارها على حقوق الانسان دراسة على ضوء احكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، ص139

[7] منذر رابح، و سعيد درويش، الطبيعة القانونية للهجمات السيبرانية التي تقع على الدول، مجلة صوت القانون، المجلد8، العدد1، 2021، ص548

لدعم الأهداف العسكرية و المناورات العسكرية التقليدية أما الحروب السيبرانية فهي حروب تتم بالخفاء و دون إعلان و تصريح بهويه المرتكب كما أنها لا تتطلب عدد من جنود حيث تمتاز بسمات خاصة و مختلفة تماما عن الحروب الأخرى و بالتالي فإن الهجمات الالكترونية نوع من الحروب الالكترونية، فإنه يطبق عليها ما ذكرناه سابقا بشأن الحرب السيبرانية .[1]

المبحث الثاني

القانون الدولي الإنساني كإطار قانوني منظم للحروب السيبرانية

إن اللجوء المتزايد من قبل بعض الدول لاستخدام الهجمات السيبرانية في النزاعات المسلحة يجعل هذا الأمر التشريعات الدولية الانسانية أمام اختبار ضعيف ومتشابك، ويدور حول يتركز حول قدرة انطباق تلك الأسس التي وضعت من فترات زمنية حول الهجمات السيبرانية، وعلى ذلك سوف نقوم في هذا المبحث بدراسة مدى القدرة على تطبيق قواعد القانون الدولي الإنساني على الهجمات الالكترونية والأثار التي تترتب عليها في حالة تطبيق تلك القواعد.

المطلب الأول:

مدى القدرة على تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية

إن العمليات السيبرانية تشمل حروب الفضاء الالكتروني، بشكل عام و الاعتداءات في الفضاء الالكتروني بشكل خاص، و كلها ترمي إلى إحداث أثر قانوني في العالم الحقيقي، يتعلق بالدول و شعوبها و بالرغم أن من يرى أنه يمكن تطبيق القانون الإنساني علي هذه الهجمات باعتبارها أسلوب مستحدث من أساليب الحروب إلا أن هناك من يرى عدم جواز ذلك؛ نظرا لعدم وجود اتفاق دولي حول المعاني القانونية لمفهوم الاعتداء في الفضاء الالكتروني كما أنه ليست هناك قوانين دولية تنظم هذه الأمور و تحدد مسؤولية الدول عن تلك الهجمات و عليه: فإننا في هذا المبحث سوف نقوم بدراسة مدى القدرة على تنفيذ قواعد (**I.H.L**) علي الحرب الالكترونية و الأثار التي تترتب عليها في حالة تطبيق تلك القواعد .[2]

أولا: خضوع الحروب السيبرانية للقانون الدولي الإنساني:

يؤكد مؤيدي هذا الرأي إلى عدم التسليم بوجود فراغ قانوني في الفضاء السيبراني، و اعتبار مبادى (**I.H.L**) كافية لتنظيم النزاعات في الفضاء الالكتروني و أنه يمكن تطبيقه على الفضاء الالكتروني و الذي يشمل بدوره الهجمات السيبرانية التي تقوم ما بين الدول، و سمي هذا المذهب بالمذهب القانوني و الذين ذهبوا بالاعتراف إلى إمكانية التعامل مع الانترنت قانوناً لاسيما بعد أن سبق تنظيم وسائل الاتصال التي تشبهها مثل الهاتف النقال في فرنسا، و الفاكس و غيرها من الأساليب الحديثة، و ما علي فقهاء القانون سوى التعاون على تقنين قواعد خاصة تنظم هذه المسألة خصوصاً بعد وجود العديد من القواعد و المواد التي تنطبق عليها .[3]

و وفقا لأصحاب هذا المذهب يقرون بأن القانون الدولي الإنساني ينطبق بجميع مبادئه و قواعده بصفة عامة علي أي نزاع مسلح بما فيها الحروب السيبرانية فإن كنا نتفق بأن اتفاقيات القانون الدولي الإنساني لم تشير علي وجه التحديد للهجمات السيبرانية إلا أن الحجة لا توجد لها أهمية إلا أن شرط مارتينز والذي هو من المسلمات الراسخة في القانون الدولي الإنساني[4] يقرر صراحة أنه عند وجود وضع لا تشمله الاتفاقيات الدولية " يبقي المدنيون و المقاتلون تحت رعاية و سلطة مبادئ القانون الدولي الإنساني المستمدة من التقاليد الثابتة و من المبادئ الإنسانية.[5]

و معروف أن هناك اتجاه معادي لفكرة تطبيق قانون الحروب علي الحروب الالكترونية حيث يحتجون بأن ميثاق الامم المتحدة قد كان صريحاً و واضحاً، من اشتراطه لاستخدام القوه لكي يعد نزاع نزاعا مسلحا

---

[1] الموقع الإلكتروني لموسوعة المعرفة:www.marefa.com تاريخ الزيارة 2023/1/31 الساعة 8 10 صباحا
-شريف عبدالحميد، مرجع سابق، ص2093-2095

[2] محمد طلعت الغنيمي، الوجيز في قانون السلام، منشأة المعارف، الإسكندرية، 1973، ص399
احمد ابوالوفاء، الوسيط في القانون الدولي العام، دار النهضة العربية للنشر، القاهرة، ط5، 2010، ص63

[3] حامد محمد البداوي، مواجهة الحرب السيبرانية في القانون الدولي الإنساني، مجلة الجامعة العراقية، كلية الامام، العدد257، ص385

[4] احمد ابوالوفاء، النظرية العامة للقانون الدولي الإنساني، دار النهضة العربية، القاهرة، ط3، 2013، ص74

[5] سهيل حسين الفتلاوي، الطبيعة القانونية العرفية لقواعد القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع، الأردن،2012،ص 45

يخضع لقانون الدولي الإنساني و وفقاً لما ذكر يرون أن الاعتداء في الفضاء الالكتروني اعتداء مسلح لأنه لا يتضمن استعمال القوة و يرد عليه أصحاب هذا الاتجاه بأنه: إذا كان معاهدة المنظمة الدولية في م 2 ف 4 حظر علي دول التلويح بالقوة أو استخدام ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة أو علي وجه آخر لا يتفق مع المقاصد ميثاق الأمم المتحدة لكن الوثيقة تركت مهمة تحديد المعنى لهذه القاعدة بين مجلس الامن وفق ما يحيط به من مستجدات، و هذا واضح من نص المادة 39 من الميثاق التي تعطى مجلس الأمن صلاحيات تقرير الإجراءات القهرية حيث أن هذا النص ورد بصورة غير ملزمة و ذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن و السلم الدوليين أو الإخلال بهما أو كان وقع عملاً من أعمال العدوان، و قد يقوم مجلس الأمن إلى القيان بالإجراءات دون نص المادة 2 فقره 4 في حال رأي مجلس الأمن في موقف معين تهديداً للسلم و ذلك لعدم مخالفة الإجراء لأحكام الميثاق أو قواعد و أسس التشريع الدولي كل ذلك يفيد أن الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة و المواد ذات صلة من بالمعاهدة التي تنطبق علي الهجمات السيبرانية دون الامعان في صنف السلاح المستعمل و استعمال القوة كما نوه اليه في م الثانية فقره الرابعة في الميثاق.[1]

و في نفس الصدد تُشير م (36) من البرتوكول الإضافي الأول المرفق باتفاقيات جنيف لعام 1939 م المتعلقة بحماية ضحايا النزاعات المسلحة الدولية لعام 1988 على ما يلي{ يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب بأن يتحقق مما إذا كان محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق البرتوكول أو اية قاعدة أخري من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد بناء على ذلك ينطبق هذا النص على الاعتداءات في الفضاء الالكتروني بأنها سلاح أو أسلوب من أساليب الحرب فعلى الدول التأكد من مدى مشروعية استخدامها وفقا لقواعد هذه الاتفاقية أو أي قاعدة أخري من قواعد قانون المنازعات القتالية، و هو ما يحتم انطباق أحكام التشريع الدولي لحقوق الانسان على الحرب السيبرانية و عليه فإن مبادئ (**I.H.L**) تنطبق أينما كان هجوم سيبرأني على دولة ما بشكل مكثف فلا يمكن بقبول فرضية أن كل تصرف ينشأ عنه قرصنة أو اختراق للبيانات الكترونية هو بمثابة أعمال عنف كما يشترط في ذلك أن ينتج من تلك الهجمات إلحاق الضرر بالمدنيين أو إحداث أضرار بالبنى التحتية للدولة المستهدفة و عليه قد أجمع الفقهاء الدوليون علي أن الهجمات الإلكترونية تعد حرباً صحيحة عندما تنتج أثرها على العالم المادي، و يشترط أن يكون هذا الأثر مدمراً و عليه يطبق القانون الدولي الإنساني .[2]

بناء لما سبق يتضح لنا أن أصحاب هذا الاتجاه قد اتفقوا علي اخضاع الهجمات الالكترونية للقانون الدولي الإنساني استنادا إلى أن ميثاق الأمم المتحدة قد ترك أمر تحديد معنى نص المادة 4 الفقرة 2 إلى مجلس الأمن و ذلك تبعاً للظروف المحيطة فإذا رأي مجلس الأمن بأنه ظاهرة مخالفة لأحكام القانون الدولي اعتبرها نزاعا مسلحا يخضع لقواعد القانون الدولي بغض النظر عن طبيعة السلاح المستخدم طالما نتج عن هذا التصرف ضرر للأفراد أو للبنى التحتية لدول و عليه: فإن الهجمات لا تخضع للقانون الدولي الإنساني إلا إذا استهدف إحداث أضرار للأفراد و البنى التحتية للدول و بالتالي يمكن اعتبارها حرب صحيحة طالما نتج أثرها على العالم المادي و أن يكون هذا الأثر مدمراً[3].

ووفقاً لأصحاب هذا الاتجاه فقد أشاروا إلى المبادئ التي تحكم استخدام الهجمات السيبرانية أثناء العمليات العدائية، فمن المعروف أن أطراف أي نزاع مسلح يعتمدون عند استخدامهم للقوة أو الهجمات السيبرانية على وجه الخصوص إلى إنهاء أو على الأقل إضعاف القدرة العسكرية للطرف الآخر لأقصى حد ممكن إلا أن القانون الدولي الإنساني بوصفه القانون الذي وجد لترشيد استعمال القوة وليس لمنع استخدامها وضبط هذا الاستخدام بمبدأين من المبادئ الرئيسية التي يجب أن تبقي محل احترام من كافة أطراف النزاع وهما:

1-التوفيق بين الضرر والفوائد العسكرية:

---

[1] عمر محمود اعمر، الحرب الالكترونية في القانون الدولي الإنساني، الحرب الالكترونية في القانون الدولي الانساني، مجلة دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد46،العدد4 ص، 140-141

[2] حامد محمد على البلداوي، مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني، مرجع سابق، ص385

[3] نورية الساعدي، مرجع سابق، ص14-18

يقصد بهذا المبدأ أن الميزة العسكرية تحصل عليها عمليات معينة يجب أن تفوق الضرر الذي يلحق بالمدنيين و الأعيان المدنيين من جراء ذلك الإجراء، و قد تم التعبير عنه في متن المادة 57 البند الثاني الفقرة الثالثة و البند الثالث)[1] و المادة 25 من البرتوكول الإضافي الأول لعام 1977 إلى جانب الطابع التعاهدي البارز لهذا المبدأ يبرز طابعه العرفي الذي يؤكد وجوده كقاعدة أصلية من نصوص التشريع الدولي للصراعات العسكرية العرفي بتالي انطباقه علي النزاعات المسلحة و غيرها ذات الطابع الدولي على حد سواء و كما هو الحال مع جميع أنواع الأسلحة الأخرى المستخدمة في هذه النزاعات و يجب أن تمتثل الهجمات الالكترونية لمبدأ التوازن .[2]

يهدف مبدأ التوازن إلى التوفيق بين الحاجة العسكرية والمبادئ الانسانية المعاملة الإنسانية ويهدف إلى التقليل من الخسائر الإنسانية المترتبة على العمليات العسكرية.[3]

2-مبدأ الضرورة العسكرية:

هي الظروف الطارئة التي تظهر أثناء الحروب والتي تتطلب اتخاذ إجراءات سريعة نتيجة لمواقف أو ظروف استثنائية في اللحظة نفسها، وهذا ما تضمنته اتفاقية (لاهاي) الخاصة باحترام قوانين الحرب لسنة1907، والبرتوكول الإضافي الأول لاتفاقيات جنيف لسنة 1949[4]، وبالتالي يكون الاعتداء في الفضاء الالكتروني وسائل الحروب في حالة إذا كان هناك ضرورة ملحة للقيام بالهجوم [5]، ويعتبر انتهاك مبدأ الحاجة العسكرية جريمة حرب لدى المحكمة الجنائية الدولية والنظام المنظم لها[6]

ومما تقدم يمكن القول إن المبادئ والقواعد المشار إليها لا تقتصر علي وسائل و أساليب القتال وفقا للمفهوم التقني لبعض الأسلحة أو طريقة استخدامها، و إنما تقتضي تلك القواعد علي وجه التحديد مفهوما مستقبليا ينطبق علي تطوير أو اقتناء أو الاعتماد علي سلاح جديد أو وسائل و أساليب جديده للحرب .[7]

ثانيا: عدم اخضاع الهجمات الالكترونية للقانون الدولي الإنساني:

يري مؤيدو هذا الاتجاه أنه: الا يوجد نص قانوني بأي اتفاقية أو وثيقة من مواثيق القانون الدولي الإنساني ينص على تطبيق نصوص القانون الدولي الإنساني على الهجمات السيبرانية، وأن اتفاقيات جنيف الأربع عندما حددت مجال انطباقها قيدت ذلك في حالة وحيدة لا يمكن أن تشمل الهجمات السيبرانية، وهي حالة الاشتباك المسلح، فالمادة2 من اتفاقية جنيف الأولى نصت على أنها تنطبق فقط على حالة الحرب المعلنة أو أي اشتباك مسلح ينشب بين طرفين أو أكثر .[8]

كما قد رأى أصحاب هذا الاتجاه أن خصوصية الفضاء الإلكتروني تمكن في عدم وجود دولة بإمكانها فرض سيطرتها و سيادتها الأحادية عليها، و بهذا يكون استخدامه بشكل يسبب أضرار إنسانية و على هذا الأساس ظهر اتجاه فقهي سمى بالاتجاه (الحر) يرفض التعامل القانوني مع الإنترنت و يقضي بأن الانترنت منطقة بلا قانون و لذلك اتجه جانب من الفقهاء القانونيين الأوروبي و الأمريكي إلي اعتبار الفضاء الالكترونية لا تخضع للقانون حيث كل شيء متاح و يمكن لأي شخص العمل بأنشطة معادية بدون الخضوع إلي قوانين أو ضبط للنفس فقد قيل بأن كلمات المرور و ألواح المفاتيح و أجهزه الحواسيب تعد حدوداً بين العالمين ولا بد من دخول إلي هذا العالم من خلال هذه الأدوات ، فهذا العالم لا يمكن أن تختص به دولة معينة و عليه لا يمكن توافق القانون الدولي العام التقليدي، فهو لم يثبت نجاحه حتي اللحظة في مجال البحر والجو الالكتروني و

---

[1] جون ماري، القانون الدولي الإنساني العرفي المجلد الأول، القواعد، القاعدة رقم 14، ص41-43

[2] نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، الجامعة الافتراضية السورية، 2021، مرجع سابق، ص51

[3] احمد ابوالوفاء، النظرية العامة للقانون الدولي، مرجع سابق، ص82

[4] حيث تمت الإشارة الى مبدأ الضرورة العسكرية في المواد 2/54 و 1/62 و 3/79 و 4/67 من البرتوكول الإضافي الأول الملحق باتفاقيات جنيف بتاريخ 1949/8/12

-حنان دربول محمد، محددات مبدأ التناسب في القانون الدولي الإنساني، مجلة الجامعة العراقية، المجلد68، العدد1، سنة 2024، ص327-330

[5] عبدالسلام هماش، مفهوم الضرورة العسكرية في القانون الدولي الإنساني، جامعة الشرق الأوسط، 2014، ص19

[6] نظام روما الأساسي للمحكمة الجنائية الدولية القاعدة 8(2/أ/4)

[7] يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية، مصر،2018، ص93

[8] المادة 2 من اتفاقية جنيف الأولى

الجوي الخارجيين، لذلك فإن أنصار الاتجاه الحر الذي يقر بأن الانترنت لا يخضع إلى القانون و الحجة في ذلك أن الإنترنت عالم حديث لا يتوافق مع واقع المادي التقليدي .[1]

وإذ كان قد تطرقنا فيما سبق إلي شمولية مبادئ و قواعد القانون الدولي الإنساني من حيث جواز تطبيقها في النزاعات في الفضاء الالكتروني إلا أنه لا نستطيع تجاهل واقع خلل الذى وجد في الحروب منذ اعتماد اتفاقيه جنيف الأصلية قبل ما يقارب مائة و خمسون سنة حيث أصحبت الوسائل و الأساليب للحروب متطورة إلي درجة لم يكن يتصورها واضعي تلك الاتفاقية و لعل الاستخدام المتزايد للفضاء السيبرانى للأغراض العسكرية أحد أهم الأسباب التي تدعو إلي إعادة تقييم النصوص التي تنظم سير العمليات الحربية المسلحة و صياغتها بالشكل الذي يتلاءم مع طبيعة هذه الاستخدام[2]، بمعنى أوضح أنه لا يجوز تطبيق ذات القواعد أو الركائز المقننة في التشريع الدولي الانساني و انما لابد للمجتمع الدولي أن يجتمع و أن يقنن قواعد و مبادئ خاصة ينظم فيها الوضع القانوني لتلك الهجمات نظرا لما تمتاز به تلك الهجمات من خصائص و طبيعة مغايرة عن طبيعة الحروب التقليدية التي تحدث بدورها علي أرض الواقع بينما الحرب السيبرانية تحدث في نطاق افتراضي ليس له وجود مادي .[3]

و وفقا لما تقدم فإن امكان الاخذ بنصوص قانون الحروب المسلحة ا قد تتمايز أحياناً بشأن الحروب السيبرانية عنها في الحروب التقليدية[4] على أنه من وجهة نظرنا أن معايير هذا التباين أو الاختلاف لا تتعلق بتطبيق أو عدم تطبيق تلك المبادئ والأحكام فحسب و إنما هناك العديد من الامور الأخرى التي تطرح اشكاليات الاعتداءات الشبكية في إطار الصراع العسكري منها ما يخص بتحمل مسؤولية الأفعال التي تتجاوز القانون ، تلك المسؤولية التي يمكن أن تتضمن خيارات القائد العسكري و المبرمج و المصنع بالإضافة إلي تحديد مفهوم واضح للفضاء السيبراني و بيان معالمه و تحديد طبيعة الأثر الذي يلحقه الهجوم و بيان الوضع القانوني في حالة لو وقع ضرر علي بنية افتراضية خاصة لبيانات دولة ما و غيرها من المسائل الأخرى التي تدخل في إطار الهجمات و عليه نجد من الضروري تحديد وضع قواعد تتفق مع طبيعة الهجمات الالكترونية وقت الاعتداءات خصوصا بعد ذلك ظهور بعض الجهود الدولية التي تنظم هذه المسائل بصوره مباشرة أو غيره مباشرة[5].

المطلب الثاني

الجهود الدولية لتنظيم القانوني للهجمات السيبرانية

من المعروف أن الهجمات الالكترونية من المواضيع الحديثة لم تتطرق لها بصورة واضحة إلا أنه بعد التعمق في الدراسة نرى أن هناك بعض المواثيق والاتفاقيات التي تناولت هذا الموضوع بصورة مباشرة أي بالإشارة إليه بشكل واضح او غير واضح عن طريق استخلاص قاعدة من مفهوم ضمني غير واضح وبما أن تلك المواثيق والاتفاقيات كثيره فإننا سوف نتناول أهما وهي ميثاق الأمم المتحدة ودليل تالين.

أولاً: ميثاق الأمم المتحدة ودوره في تطبيق القانون على الحروب الالكترونية:

لم ينظم الميثاق الحروب السيبرانية بصوره مباشرة أي بمعنى أنه لم يتناول الموضوع بصورة خاصة وشاركت الجمعية العامة[6] ومجلس الأمن[7] في المفاوضات من أجل وضع معايير تعزيز أمان الهياكل الشبكية الشبكية الدولية و قد اتضح لنا من المادة الثانية الفقرة الرابعة من ميثاق الأمم المتحدة[8] التي تمنع من استعمال القوة او التلويح بها داخل العلاقات الدولية و قد جرى العرف على أن المقصود بالقوة هنا هي (القوة

---

[1] حامد محمد البداوي، مرجع سابق، ص73

[2] سلافة طارق الشعلان، تكييف استخدام الحروب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة جامعة الكوفة للعلوم السياسية والقانونية، العراق، المجلد9، العدد26، 2016، ص137-140

[3] حامد محمد البداوي، مرجع سابق، ص93

[4] نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، 2021، ص53

[5] حنان دربول، مرجع سابق، ص332-334

[6] قرارات الجمعية العامة للأمم المتحدة ذات الأرقام 55/63- 56/121 – 75/239 – 58/199 – 73/187 – 173/74

[7] قرارات مجلس الامن ذات الأرقام 72/284 – 2017/2341 – 2017/2370

[8] تنص المادة 2 الفقرة 4 من ميثاق الأمم المتحدة على انه (يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة او استخدامها ضد ضد سلامة الأراضي او الاستقلال السياسي لأية دولة او على أي وجه اخر لا يتفق ومقاصد الأمم المتحدة)

العسكرية) و هو حظر يستوجب تدخل المجتمع الدولي فيه ؛ للحفاظ علي السلم و الأمن الدوليين من أي تهديد و مع تطورات التكنولوجية غير المسبوقة ظهر مفهوم جديد و هو القوة السيبرانية أو ما يعرف بالقوة الإلكترونية فأصبح استخدمها أو التهديد بها يندرج تحت نطاق القوة العسكرية المحظورة بموجب المادة 2 فقره 4 و التي يتطلب الإخلال بها تطبيق التدابير التأديبية المقررة عليها وفقاً للمادة السابعة من وثيقة **un**[1] أم أنها خارج نطاق الحظر المقصود ؟ ولكي يتم الإجابة لابد من التفرقة بين الهجمات الالكترونية ذات الطبيعة العسكرية من عدمه.

*- الهجمات الالكترونية ذات طبيعة عسكرية:

وهي هجمات لها نفس التبعيات الناجمة عن الاستعمال الملموس للإمكانيات الحربية ذات التأثير التدميري على الأرواح البنية التحتية للدولة ومنها:

*- السيطرة على الأنظمة العسكرية : و يقصد بها السيطرة علي نظم القيادة و السيطرة عن بعد بما يخرج من الأسلحة و الوحدات الكتائب العسكرية القيادة المركزية حيث تكمن الميزة النسبية لقوه الفضاء الالكتروني في قدرتها علي ربط الوحدات العسكرية بعضها ببعض بالأنظمة العسكرية، مما يسمح بسهولة تبادل المعلومات و تدفقها و سرعة إعطاء الأوامر العسكرية و القدرة علي إصابة الأهداف و التدمير عن بعد و قد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا منعا للتلاعب بالأنظمة العسكرية أو إعادة توجيه أسلحة الخصم ضد أهداف وهمية. [2]

*- استهداف البنية التحتية للدولة: سواء كانت محطة الطاقة والبترول والوقود والأقمار الصناعية والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات والبث التليفزيوني والإذاعي والملاحة الجوية والبحرية واستهداف البرامج الحيوية مثل برنامج الفضاء والبرنامج النووي حيث أن استهداف هذه النظم يؤدي إلى آلاف الضحايا في دقائق معدودة[3]

*- سرقة المعلومات والبيانات العسكرية أو العبث بها، حيث يتم في هذه الحالة اختراق الشبكات الخاصة بالمؤسسات الأمنية والعسكرية بهدف سرقة استراتيجيات عسكرية أو خرائط انتشار أنظمة تسليح أو تصميمات لمعدات عسكرية وذلك من خلال اختراق قواعد البيانات العسكرية أو القومية وسرقتها أو تزييفها أو تدميرها إلكترونياً هو الذي يؤدي بدوره إلى إيقاع ضحايا مدنيين أو على الأقل إلى تهديد الأمن والسلم العالمي.[4]

وعليه فإن هذا نوع من الهجمات هي التي لها نفس التداعيات في استخدام القوة العسكرية التقليدية وهي التي ينطبق عليها الحظر لاستخدام القوة المفروض من قبل **UN** ومن ثم يتم التعامل مع هذه الهجمات من منطلق المادة الثانية الفقرة الرابعة من نصوص ميثاق الأمم المتحدة والذي تستوجب تدخل المجتمع الدولي للمحافظة على الأمن والسلم وتطبيق العقوبات اوردها نص عليها ميثاق الامم المتحدة ضد من يخترق مبدا استخدام القوة.

وفي حالة الحرب في الفضاء الالكتروني يمكن للأمم المتحدة اعمال مبادئها الخاصة بممارسة حفظ السلام في الفضاء السيبراني حيث رأت الأمم المتحدة أنه من المفيد للغاية حفظ الأمن السيبراني خصوصاً فيما يتعلق بالمستقبل ولكون التطور الدائم الذي يشهده العالم في الوقت الحالي، وحيث بدأت التكنولوجية تأخذ حيز كبير على الصعيد الدولي فيما يتعلق بأنظمة الدول، نظرا لكون المبدأ قد أتى بصياغة عامة وغير محددة تجعل منه يشمل كل ما يؤدي بدوره إلى الإخلال بالأمن والسلم الدولي حتى ولو كان ذو وجود افتراضي[5].

---

[1] طارق المجدوب، السايبر ساحة خفية لحرب ناعمة، مرجع سابق، ص44

[2] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (6) on Rule (38).

[3] ياسر كلزى، النظرية العامة في القانون الدولي الإنساني، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق، سوريا، 2020، ص10

[4] ايمان حمدان، التكنولوجيا الجديدة والقانون الدولي الإنساني، الحرب السيبرانية، دراسات معمقة في القانون الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية، السورية، 2020، ص9

[5] هبه جمال الدين،مجلة كلية الاقتصاد والعلوم السياسية، مصر، المجلد24،العدد1،سنة2023، ص 195-199

كذلك يحظر ميثاق الأمم المتحدة والقانون الدولي الإنساني مهاجمة المنشأة التي ينتج من استهدافها عسكرياً ضرراً كبيراً بالمدنيين كمحطات توريد الكهرباء ويترتب عن هذا الحظر استخدام الأنظمة الالكترونية على البيانات الخاصة بتلك المنشأة إلا أنه في بقية بنوده الأخرى تجد أن المسائل التي ينظمها فيما يتعلق بأساليب الحروب تتنافي وفكرة الحرب السيبرانية بوجه عام و الهجوم السيبراني بوجه خاص مثل فكرة اشتراط حدوث الهجوم داخل إقليم الدولة المعادية فمن المعروف أن الهجوم السيبراني يحدث في نطاق خاص به و هو ما يمسى بالفضاء السيبراني الذي لا يحده حدود جغرافية و وبالتالي تجعل من مسألة تطبيق الميثاق أمر صعب نظرا للفروقات الواضحة فيه [1].

الخاتمة

ومن خلال هذا البحث تم التوصل الى الاتي

أولاً – الاستنتاجات:

. إن الحروب الحديثة في العصر الحالي أضحت حروب إلكترونية تدار في فضاء إلكتروني وبشكل إلكتروني وهي بذلك تستهدف البنى التحتية للدول مما يحدث أضرار كبيرة جداً.

2. القدرات الرقمية تشمل الأنظمة الأساسية للدولة والنظام المالي والاقتصادي والطيران والكهرباء، وأصبحت القوة الالكترونية في عصرنا الحالي عامل مهم في أمن الدولة وقوتها؛ لأن اللجوء إليها أصبح في ازدياد مستمر

3.صعوبة تحديد الهجوم في الفضاء الالكتروني بسبب الطبيعة المتغيرة وغير الملموسة.

4. في الواقع الفعلي تنطبق الأليات العقابية المقررة في القانون الدولي الإنساني على الحروب الالكترونية إلا أن الكشف عن هوية مرتكبها صعبة

5.نقص التغطية القانونية في الاتفاقيات الدولية مما يؤدى الى فراغات قانونية في تنظيم هذا النوع من الحروب.

6.صعوبة تطبيق مبدأ التناسب الذي ينظم استخدام القوة في الحروب التقليدية وفى الحروب في الفضاء الالكتروني بسبب الطبيعة المعقدة للهجمات في الفضاء الالكتروني

ثانياً – التوصيات:

1. تحديث القانون الدولي الإنساني وتطوير الاتفاقيات المتعلقة بالحروب لتشمل تنظيمات خاصة بالهجمات في الفضاء الالكتروني.

2. السعي إلى إبرام اتفاقيات دولية تقنن تطبيق القانون الدولي الإنساني الحالي على الحروب السيبرانية

3. التعاون الكبير بين الدول في كشف هوية منفذي العمليات السيبرانية وخاصة عندما تكون انتهاك صارخ للقانون الدولي الإنساني.

4.الترويج للوعي العام حول المخاطر الالكترونية والتأكيد على أهمية الامن الشخصي والحكومي في الفضاء الالكتروني

قائمة المصادر والمراجع:

أولا: الكتب :

1/ أحمد أبوالوفا، النظرية العامة للقانون الدولي الإنساني، دار النهضة العربية، القاهرة، ط3، 2013

2/أحمد أبوالوفا، الوسيط في القانون الدولي العام دار النهضة العربية للنشر، القاهرة، ط5، 2010

3/ جون ماري، القانون الدولي الإنساني العرفي المجلد الأول، القواعد، القاعدة رقم 14.

4/سهيل حسين الفتلاوي، عماد محمد ربيع، موسوعة القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع، الأردن، 2020.

5/ سهيل حسين الفتلاوي، الطبيعة القانونية العرفية لقواعد القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع،2012.

[1] حسين إبراهيم حسين، مرجع سابق، ص206-207

6/ صالح عمر خليل، الإطار النظري للأمن الإلكتروني السيبراني، ط1، القاهرة، منشورات الدار للنشر، 1993
7/صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، دراسة في مفهومها، جامعة الشرق الأوسط، الأردن، 2021
8/ عبدالسلام هماش، مفهوم الضرورة العسكرية في القانون الدولي الإنساني، جامعة الشرق الأوسط، 2014.
9/عباس بدران، الحروب الالكترونية في عالم المعلومات، ط1، لبنان مركز دراسات الحكومة الالكترونية،2010
10/عمرو رضا بيومي، مخاطر أسلحة الدمار الشامل الإسرائيلية على الامن القومي العربي، ط1، الأردن،2022
11/فيصل محمد عبد الغفار، الحرب الالكترونية، ط1، الجنادرية للنشر والتوزيع، ط1، الأردن، 2015
12/محمد شاكر، الحرب السيبرانية على الأمن العالمي، الموسوعة الجزائرية للدراسات السياسية والاستراتجية،2019
13/ محمد طلعت الغنيمي، الوجيز في قانون السلام، منشأة المعارف، الإسكندرية،1973
14/ نبيل عودة العمليات السيبرانية في الحرب الروسية الأوكرانية، الشرق الأوسط للأبحاث الاستراتيجية، 2022

ثانيا: الرسائل العلمية والمقالات.

أ.الرسائل العلمية.

1/ إيمان حمدان، التكنولوجيا الجديدة والقانون الدولي الإنساني، الحرب السيبرانية، دراسات معمقة في القانون الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية، السورية، 2020.
2/ صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها، رسالة ماجستير، كلية الآداب والعلوم، جامعة الشرق الأوسط، الأردن،2020.
3/ صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2021.
4/ نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، 2021.
5/ليلي بشلالق، تأثير الحروب الالكترونية على العلاقات الأمريكية الروسية، رسالة ماجستير غير منشورة، جامعة محمد بوضياف، الجزائر،2018.
6/ ياسر كلزى، النظرية العامة في القانون الدولي الإنساني، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق، سوريا، 2020.

ب. المجلات العلمية:

1/ إسماعيل زروقه، الفضاء السيبراني وأثره على الامن الوطني العربي، مجلة العلوم القانونية والسياسية، المجلد10، العدد1، 2019.
2/ حامد محمد البلداوي، مواجهة الحرب السيبرانية في القانون الدولي الإنساني، مجلة الجامعة العراقية، كلية الامام، العدد257.
3/ حنان دربول محمد، محددات مبدأ التناسب في القانون الدولي الإنساني، مجلة الجامعة العراقية، المجلد68، العدد1، سنة 2024.
4/ حسين إبراهيم حسن، الحرب السيبرانية في ضوء قواعد القانون الدولي، مجلة البحوث القانونية والاقتصادية، المنوفية ، مصر، سنة 2024.
5/ سعيد درويش، الحروب السيبرانية وارها على حقوق الانسان دراسة على ضوء احكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية.

6/ سلافة طارق الشعلان، تكييف استخدام الحروب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة جامعة الكوفة للعلوم السياسية والقانونية، العراق، المجلد9، العدد26، 2016.
7/ شريف عبد الحميد حسن، الحروب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مجلة الشريعة والقانون، الدقيلية – مصر، العدد23، الجزء الرابع، سنة 2021.
8/صابر بلقاسم، وحيد محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الانسان والحريات، جامعة عبدالحميد بن باديس، الجزائر، العدد4، 2020.
9/ طارق المجدوب، السايبر ساحة خفيفة لحرب ناعمة قادمة، منشورات مجلة الدفاع الوطني، العدد49، 2014
10/ عمر محمود اعمر، الحرب الالكترونية في القانون الدولي الإنساني، الحرب الالكترونية في القانون الدولي الانساني، مجلة دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد46، العدد4.
11/كبارا طه محمد، نطاق فعالية الحرب في تنفيذ أهداف السياسة الروسية، دراسة حالة الحرب السيبرانية، مجلة البيئة الاقتصادية، العدد23، سنة2024.
12/ محمد عبد الرحمن، الهجمات الالكترونية في اطار النزاع المسلح، المجلة الليبية العالمية، كلية التربية، المرج، جامعة بنغازي، ليبيا،2022.
13/محمد عادل عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، مجلة البحوث القانونية والاقتصادية، المجلد33، العدد1، 2021..
14/ مهند جبار عباس، هيثم كريم صوان، الحروب السيبرانية بين التحديات واستراتيجيات المواجهة، العراق أنموذجا، مجلة قضايا سياسية، العدد70، كلية العلوم، جامعة النهرين، العراق،2022.
15/ ناجي محمد أسامة، الجوانب القانونية للحرب السيبرانية، دراسة في القانون الدولي الإنساني، مجلة روح القوانين، العدد103، سنة 2023.
16/ نور امين الموصلي، المجلة الالكترونية الشاملة متعددة التخصصات، العدد24، 2020.
17/-نورية الساعدي، الحرب السيبرانية في ضوء احكام القانون الدولي العام، مجلة أبحاث قانونية، العدد2، المجلد السابع، سنة2022.
18/ منذر رابح، وسعيد درويش، الطبيعة القانونية للهجمات السيبرانية التي تقع على الدول، مجلة صوت القانون، المجلد8، العدد1، 2021.
19/يحي ياسين سعود، الحروب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، المجلد4، العدد4، 2018.
20/ هبه جمال الدين، مجلة كلية الاقتصاد والعلوم السياسية، مصر، المجلد24، العدد1، سنة2023.

ج/الاتفاقيات الدولية:

1/ اتفاقيات جنيف الخاصة بضحايا النزاعات المسلحة لسنة 1449
2/ميثاق الأمم المتحدة
3/البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة 1977
4/النظام الأساسي للمحكمة الجنائية الدولية

د.المقالات.

1/ مركز الجزيرة للدراسات، الحروب الالكترونية في القرن 21، المجلد الخامس على الرابط التالي **https//studies.aljazeera.com** تاريخ الزيارة 2023/2/5
2/ هبه عبدالفتاح، الحروب السيبرانية الأكثر دماراً اخبار اليوم 2019/9/14، متاح على الرابط **www.akhbaralyom.com**، تاريخ الزيارة 2023/2/15

هـ. المواقع الالكترونية

1 موسوعة المعرفة:**www.marefa.com** تاريخ الزيارة 2023/1/31 .

و. المراجع الأجنبية:

1/Edl,amK R.D. Rethinking cyber warfare the international Relations of Digital Disruption . Oxford Universty press. 2024
Nils melzer. Cyberwar fareand international.law.2011 /1
Schreier.fred. on cyber ware. Edition. DCAF.switzerland.Geneva.2015
2/ Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicableto Cyber
3/ Topor. L. Cyber Warfer :Global Trends and proxy Wars. In Cyber Sovereiginy international. And the Future of the internt.2024.cham : Springer nature switzerland.
Warfare, op.cit, comment (6) on Rule (38)./ 4

ز. قرارات الجمعية العامة:

GA. Res. 55/63, UN. Doc. No, A/RES/55/63 (Jan, 22, 2001), Available At:/1
https://undocs.org/ar/A/RES/55/63
GA. Res. 56/121, UN. Doc. No, A/RES/56/121 (Jan, 23, 2002), Available At:/2
https://undocs.org/ar/A/RES/56/121
GA. Res. 57/239, UN. Doc. No, A/RES/57/239 (Jan, 31, 2003), Available At/3
https://undocs.org/ar/A/RES/57/239
GA. Res. 58/199, UN. Doc. No, A/RES/58/199 (Jan, 30, 2004), Available At/4
https://undocs.org/ar/A/RES/58/199

ح / قرارات مجلس الامن:

SC. Res. 2341, U. N. Doc. No, S/RES/2341(2017) (February, 13, 2017)/1
Available At: https://undocs.org/ar/S/RES/2341)2017
SC. Res. 2370, U. N. Doc. No, S/RES/2370(2017) (August, 2, 2017)/2
Avalibale At: https://digitallibrary.un.org/record/1298189?ln