Problems Of The Actual Application Of International Humanitarian Law To Cyber Attacks In Contemporary Armed Conflicts

Dr. Maya Shawkat Safatly*

(Received 9 / 4 / 2024. Accepted 5 / 6 / 2024)

□ ABSTRACT □

In recent years, the dilemma of using the Internet or computers as a tool of modern warfare has emerged, and it has become common to raid and destroy websites remotely to detonate their contents. For example, it is possible to close the centrifuges of nuclear facilities, disable air defense systems, air traffic control systems, and oil and gas pipeline flow system, open damgates, or control electrical networks, water facilities, communication, transportation, and other facilities that affect national security or the national economy or the supreme interest of the state. Thus, it represent and disruption at the international level accordingly, disagreement arises and the international legal and jurisprudential debate is currently escalating regarding cyber attacks launched during contemporary international or non- international armed conflicts. Especially regarding the actual and real application of the most important rules and principles applicable in international humanitarian law to these attacks, because the targets in any cyber conflicts will be civilians, not military, and will effect the civilians population and civilians objects and will not be limited to military forces and targets only .

Key words: Cyber attacks, Fifth generation warfar, International humanitarian law, Contemporary armed conflicts, International organizations, International jurisprudence.

*Assistant Professor, Section Of International, Law Faculty Of Law, Tishreen University, Lattakia, Syria. dr.safatly@gmail.com

إشكالية التطبيق الفعلي لقواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية أثناء النزاعات المسلحة المعاصرة

الدكتورة مايا شوكت صفطلي*

(تاريخ الإيداع 9 / 4 / 2024. قُبِل للنشر في 5 / 6 / 2024)

□ ملخّص □

برزت في السنوات الأخيرة معضلة استخدام "الإنترنت" أو"الكومبيوتر" كأداة من أدوات الحرب الحديثة، وأصبح سائدا اقتحام المواقع وتدميرها عن بعد لتفجير محتوياتها، فعلى سبيل المثال يمكن عبرها إغلاق أجهزة الطرد المركزي الخاصة بالمنشآت النووية أو تعطيل أنظمة الدفاع الجوي وأنظمة التحكم في الحركة الجوية وأنظمة تدفق خطوط وأنابيب النفط والغاز أو فتح بوابات السدود أو التحكم في الشبكات الكهربائية ومرافق المياه والاتصالات والمواصلات وغيرها من المرافق التي تؤثر على الأمن القومي او الاقتصاد القومي أو المصلحة العليا للدولة. لتمثل بذلك جزءا من الوسائل الحربية الشائعة حديثا للتدمير والتعطيل على المستوى الدولي. وعليه يثور الخلاف والجدل القانوني والفقهي حاليا حول "الهجمات السيبرانية" التي تشن أثناء النزاعات المسلحة الدولية أو غير الدولية، وخاصة بشأن إشكالية التطبيق الفعلي والحقيقي لأهم القواعد والمبادئ المعمول بها في القانون الدولي الإنساني على تلك الهجمات. لأن الأهداف في أي نزاع سيبراني ستكون مدنية لا عسكرية وستؤثر على السكان المدنيين والأعيان المدنية ولن تقتصر على القوات والأهداف العسكرية فقط .

الكلمات المفتاحية: الهجمات السيبرانية، حروب الجيل الخامس، القانون الدولي الانساني، النزاعات المسلحة المعاصرة، المنظمات الدولية، الفقه الدولي.

* مدرس – قسم القانون الدولي – كلية الحقوق – جامعة تشرين– اللاذقية – سورية.dr.safatly@gmail.com

مقدمة:

شهد العقدان الماضيان تطورا ملحوظا في اللجوء الى الهجمات السيبرانية أثناء النزاعات المسلحة حتى أضحى استخدام تلك الهجمات سمة واقعية من سمات النزعات المسلحة المعاصرة، فقد أقرت بعض الدول علنا بأنها قامت بعمليات سيبرانية أثناء نزاعات مسلحة جارية وتزايد عدد الدول التي أصبح لديها قدرات عسكرية سيبرانية هجومية أو دفاعية أوبصدد تطوير تلك القدرات ومنها الدول الخمس دائمة العضوية في مجلس الأمن الدولي التابع للأمم المتحدة. وأمام هذا الواقع انقسمت آراء ومواقف الفقهاء والمختصون في القانون الدولي الإنساني فمنهم من يرى أن القواعد والمبادئ التي أرساها قانون النزاعات المسلحة تنطبق فعليا على الهجمات السيبرانية ويجب تفعيلها والعمل بها مباشرة عند شن عملية سيبرانية عدائية من قبل أحد أطراف النزاع المسلح .وعلى العكس يرى آخرون أن المدة التي جرى فيها تقنين القواعد القانونية والمبادئ الدولية ذات الصلة لم يكن لاستخدام الهجمات السيبرانية للأغراض العسكرية وجود يذكر، الأمر الذي يفهم منه أنها خارج التنظيم القانوني الدولي، وأن القانون الدولي الإنساني عاجزعن اللحاق بهذه التكنولوجيا العسكرية الحديثة.

لذلك سيتم البحث في هذا الموضوع من خلال مطلبين:

- يتناول المطلب الاول: مدى إمكانية تطبيق القانون الدولي الإنساني على الهجمات السيبرانية.
- اما المطلب الثاني: مواءمة المبادئ الناظمة للعمليات القتالية مع الهجمات السيبرانية والموقف الدولي منها.

مشكلة البحث:

تتمحور النقطة الاساسية في البحث حول التساؤل الآتي:

ما مدى إمكانية تطبيق القانون الدولي الإنساني فعليا على تكنولوجيا عسكرية حديثة في ضوء عدم وجود قواعد قانونية خاصة تنظم استخدامها ؟

ويتفرع عن هذا التساؤل الرئيس التساؤلات الفرعية الآتية:

1- هل ينطبق قانون النزاعات المسلحة على الهجمات السيبرانية باعتبارها أداة من أدوات الحرب الحديثة؟

2- كيف يمكن مواءمة المبادئ الأساسية التي تحكم سير العمليات القتالية مع شن الهجمات السيبرانية؟

3- هل يمكن لأطراف النزاعات المسلحة أن يتقيدوا فعليا بقواعد ومبادئ القانون الدولي الانساني عند وقوع هجمة سيبرانية عدائية؟

4- ما هو موقف الدول والمنظمات الدولية الحكومية وغير الحكومية من إشكالية التقيد الفعلي بأحكام القانون الدولي الإنساني أثناء الهجمات السيبرانية؟

5- ما هو موقف الفقه الدولي الحديث من إمكانية تطبيق القانون الدولي الإنساني خلال العمليات السيبرانية العدائية وتفعيل دوره من أجل حماية المدنيين؟

6- هل سيستطيع القانون الدولي الإنساني القيام بدوره الجوهري المتمثل بحماية المدنيين أثناء النزاعات المسلحة على أرض الواقع عند وقوع هجمة سيبرانية عدائية؟

أهمية البحث واهدافه:

تظهر اهمية البحث انطلاقا من اعتباره محاولة بحثية قانونية تخوض في موضوع معاصر على مستوى الدراسات القانونية في مجال القانون الدولي لكون الهجمات السيبرانية العدائية أداة من أدوات حروب الجيل الخامس وأحدثت ثورة في الحرب الحديثة لما لها من المزايا ما يكفي لدفع بعض الدول وخاصة المتطورة منها الى استخدامها في عملياتها القتالية وأثناء النزاعات المسلحة الدولية وغير الدولية، وإنطلاقا مما سبق فإن البحث يهدف إلى حل المشكلات الرئيسية الناجمة عن استخدام الهجمات السيبرانية أثناء النزاعات المسلحة المعاصرة وتتلخص اهداف البحث بالآتي:

1-بيان موقف القانون الدولي الإنساني من استخدام التكنولوجيا العسكرية الحديثة المتمثلة بالهجمات السيبرانية الماسة بالبنية التحتية الحرجة للدول والمرتبطة بالإنسان بشكل مباشر.

2-دراسة إمكانية التطبيق الفعلي والحقيقي لقواعد ومبادئ القانون الدولي الإنساني أثناء شن الهجمات السيبرانية باعتباره القانون المعني بالمدنيين والأعيان المدنية أثناء النزاعات المسلحة.

3-دراسة إمكانية اتفاق استخدام الهجمات السيبرانية مع المبادئ القانونية الحاكمة لسير العمليات القتالية والمعمول بها أثناء النزاعات المسلحة.

4-الوقوف على أبرز المواقف الولية الحديثة بشأن الهجمات السيبرانية وعلى وجه الخصوص حول إمكانية إنطباق القانون الدولي اللإنساني عليها.

الدراسات السابقة:

1- **الدراسة الاولى: محمود حسين الشرقاوي: الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، 2021.**

وهدفت الدراسة الى تحديد الإطار القانوني الحاكم لاستخدام الهجمات السيبرانية أثناءالنزاعات المسلحة الدولية وغير الدولية ورفضت الاتجاه القائل بعدم إمكانية خضوعها للقانون الدولي الإنساني وتوصلت الى نتيجة وجوهرها أن الأخير بوصفه الحالي ينطبق فعليا على الهجمات السيبرانية عندما تحدث في سياق نزاع مسلح دولي او غير دولي.

2- الدراسة الثانية: زينة عجيل: مدى شرعية الحرب في الفضاء الإلكتروني وفقا لقواعد القانون الدولي الإنساني والاتفاقيات الدولية، 2022.

وهدفت الدراسة الى بيان مدى شرعية اللجوء الى العمليات الإلكترونية العدائية عبر المجال الرقمي للفضاء الإلكتروني من وجهة نظر ميثاق الأمم المتحدة من جهة والقانون الدولي الإنساني من جهة أخرى وتوصلت الى نتيجة وقوامها ان الفراغ القانوني الذي يشهده موضوع الهجمات السيبرانية وعدم وجود اتفاقية دولية منظمة لها لا يمكن ان يضفي الشرعية عليها وسيبقى استخدامها غير شرعي من وجهة نظر القانون الدولي لإنساني.

3- الدراسة الثالثة: Lauran Jesel, Telman Rodnhouser, Knot Dorman: International humanitarian law and the protection of civilians in the effects of cyber opperations during armed conflicts ,2020.

هدفت الدراسة الى التأكيد على أن استخدام الهجمات السيبرانية أصبح سمة واقعية من سمات النزاعات المسلحة المعاصرة وركزت على كيفية تطبيق القانون الدولي الإنساني على تلك الهجمات بغية حماية المدنيين من آثارها وخلصت الى نتيجة ومضمونها أن القانون الدولي الإنساني يحكم وينظم الهجمات السيبرانية شأن أي سلاح او وسيلة او أسلوب للقتال يلجأ اليها أطراف النزاع.

وتهدف هذه الدراسة موضع البحث الى تسليط الضوء على الإشكاليات القانونية والصعوبات العملية التي تعترض تطبيق القانون الدولي الإنساني بشكل فعلي على الهجمات السيبرانية التي تشن أثناء النزاعات المسلحة المعاصرة

باعتبار أنها متمايزة ومختلفة عن الهجمات المسلحة التقليدية في ظل القصور التشريعي الذي يحيط بهذه المسألة ومن ثم مناقشة مدى انطباق القانون الدولي الإنساني عليها وكيفية انطباقه.

منهجية البحث :

تم إتباع المنهج الوصفي والمنهج التحليلي كمنهجين أساسيين في البحث من خلال تحليل القواعد القانونية ونصوص الاتفاقيات الدولية الخاصة بالقانون الدولي الإنساني وتوصيف إمكانية وكيفية تطبيقها على التكنولوجيا العسكرية الحديثة المتمثلة بالهجمات السيبرانية أثناء النزاعات المسلحة المعاصرة.

خطة البحث:

1- المطلب الاول: مدى أمكانية تطبيق القانون الدولي الإنساني على الهجمات السيبرانية.

1- الفرع الاول: صعوبات تطبيق القانون الدولي الإنساني على الهجمات السيبرانية.

2- الفرع الثاني: إنطباق القانون الدولي الإنساني على الهجمات السيبرانية العدائية.

2- المطلب الثاني: مواءمة المبادئ الناظمة للعمليات القتالية مع الهجمات السيبرانية والموقف الدولي منها.

1- الفرع الاول: مدى مواءمة المبادئ الأساسية الناظمة للعمليات القتالية مع الهجمات السيبرانية.

2- الفرع الثاني: موقف الفقه الدولي والمنظمات الدولية بشأن الهجمات السيبرانية.

الجانب النظري للبحث:

المطلب الاول: مدى إمكانية تطبيق القانون الدولي الإنساني على الهجمات السيبرانية:

شكل الفضاء السيبراني أو الإلكتروني[1] بعدا جديدا ومؤثرا في إطار العلاقات الدولية والتفاعلات العالمية وبرز كمجالا حيويا وجيو استراتيجيا لخوض حروب الجيل الخامس من قبل الفاعلين الدوليين أو غير الدوليين، وأصبحت الهجمات السيبرانية العدائية[2] التي يتم شنها من خلاله وعبر مجاله الرقمي عنصرا مهما وفعالا في النزاعات المسلحة الدولية أو غير الدولية المعاصرة[3].

أثارت تلك الهجمات مخاوف دولية وإنسانية شديدة بسبب عدم معرفة مدى قدرتها على الامتثال لما يتطلبه القانون الدولي الإنساني من قواعد ومبادئ خلال النزاعات المسلحة، وعلى الرغم من أن الاتفاقيات الدولية والنصوص القانونية الأخرى للقانون الدولي الإنساني لم تتطرق بشكل صريح وواضح لتلك الهجمات إلا أن هذا الفراغ القانوني لا يعني جواز انتهاك القانون الدولي الإنساني[4].

---

[1] الفضاء السيبراني او المجال الخامس: مجال افتراضي رقمي او تفاعلي جديد أفضت إليه ثورة المعلومات والاتصالات وساهم بخلقه التطور التكنولوجي المتسارع، يختلف عن المجالات الدولية الأخرى كالإقليم البري والبحري والجوي والفضاء الخارجي، كونه من صنع الإنسان، يشمل الشبكات العنكبوتية المحوسبة ومنظومات الاتصالات والمعلومات وأنظمة التحكم عن بعد ، يتفاعل فيه المواطنون عن طريق الشبكات.

[2] الهجمات السيبرانية: سلسلة هجمات إلكترونية عدائية نقوم بها دولة ضد دولة أخرى باستهداف او بالتسلل الى مواقع إلكترونية غير مرخص بالدخول إليها من خلال وسائل وأدوات إلكترونية وتتم عبر المجال الرقمي للفضاء السيبراني لتحقيق أهداف تتراوح بين التصعيد المادي، السياسي، العسكري، الاقتصادي والاستراتيجي، ويختلف الدمار والضرر فيها بحسب طبيعة وحجم ونوع الهجوم.

[3] زينة عجيل، مدى شرعية الحرب في الفضاء الإلكتروني وفقا لقواعد القانون الدولي الإنساني والاتفاقيات الدولية. رسالة ماجستير: سورية، جامعة تشرين، كلية الحقوق، قسم القانون الدولي، 2022، ص 1+4.

[4] محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني ، أطروحة دكتوراه: مصر، جامعة بني سويف، كلية الحقوق، قسم القانون الدولي، 2021، ص 195.

الفرع الاول: صعوبات تطبيق القانون الدولي الإنساني على الهجمات السيبرانية:

يواجه المجتمع الدولي في طريقة تعامله مع الهجمات السيبرانية العديد من الإشكاليات القانونية والعملية يأتي في مقدمتها الجدل الذي ما يزال مستمرا ومتصاعدا حول القواعد القانونية واجبة التطبيق على هذه التقنيات الحديثة والمتطورة وتمثل مدار الخلاف بصورة أساسية في مدى قدرة قواعد ومبادئ القانون الدولي الإنساني التعاهدية أو العرفية على تنظيم وحكم هذه الوسيلة القتالة الجديدة وفيما اذا كان استخدامها متوافقا من عدمه مع تلك الأحكام والنصوص القانونية الدولية المرعية[5].

ومع تزايد اللجوء الى استخدام الهمات السيبرانية في السنوات الأخيرة لأغراض عسكرية واستخباراتية وعدائية في النزاعات المسلحة انقسم الفقهاء والمختصون في آرائهم بشأن واقع وتكييف تلك الهجمات وتركزت تلك الآراء حول فرضيتين اثنتين:

الأولى: في عدم القدرة على إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية وهي العائق الأكبر الذي يواجهه المختصون في القانون الدولي، على عكس وسائل وطرائق القتال الأخرى والتي تترك أثرا ماديا ملموسا ومباشرا أو غير مباشر بعد الهجوم كالدمار او التعطيل الجزئي او الكلي الذي تتعرض له الأهداف العسكرية أو الأعيان المدنية او القتل او الجرح الذي يصيب المقاتلين والمدنيين

أما الفرضية الثانية فعلى العكس اذ تثبت بأن الهجمات السيبرانية تؤدي فعلا الى آثار مادية ملموسة ومباشرة بل وخطرة على المستويات الاقتصادية والأمنية والعسكرية كافة[6].

وفي ذات السياق تظهر صعوبة التفرقة بين الأعيان المدنية والأهداف العسكرية لارتباطهما ببعضهما البعض في الفضاء السيبراني ففي العصر الحالي يتم استخدام أجهزة الإنترنت والاتصالات بالإضافة الى استخدام نظام تحديد المواقع العالمي(GPS) والمرتبط بالأقمار الصناعية من قبل المدنيين والعسكريين على السواء ومن الممكن ان تتحول الاهداف المدنية في الفضاء السيبراني الى اهداف عسكرية[7].

وبالعودة الى اتفاقيات القانون الدولي الانساني والى تعريف النزاع المسلح الوارد في المادة (2) المشتركة من اتفاقيات جنيف الأربع لعام 1949والتي نصت على أنه:

تنطبق هذه الاتفاقية في حالة الحرب المعلنة او اي اشتباك مسلح آخر ينشب بين طرفين او اكثر من الاطراف السامية المتعاقدة حتى ولو لم يعترف احدهم بحالة الحرب8. وعند تحليل نص المادة (2) يتضح ان الاتفاقية ستنطبق بأي حالة اشتباك مسلح اي انها استلزمت وجود اشتباك مسلح تقليدي كي تنطبق وذلك مبدئيا غير متوفر في حالة الهجمات السيبرانية. نظرا لعدم استخدام الأسلحة الحركية او القوة المسلحة التقليدية اضافة الى ان المادة ذكرت بانها تشمل وتغطي مجالات الحرب التقليدية فقط[9]. أما بالنسبة لتعريف الهجوم المسلح الوارد في الفقرة الاولى من المادة 49 من

---

[5] **Lauran Jesel, Telman Rodnhouser, Knoth Dorman. International humanitarian law and the protection ofcivilians in the effects of cyber operations during armed conflicts. International Journal of the Red Cross, Geneva, 2020,Vol 102, No 913, page 290.**

[6] **عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الاربعة لسنة تسع وأربعين (الهجمات السيبرانية). القاهرة: المركز العربي للنشر والتوزيع ، 2022، ص 179.**

[7] **زينة عجيل، مدى شرعية الحرب في الفضاء الإلكتروني، مرجع سابق، ص 106.**

[8] **المادة (2) المشتركة من اتفاقيات جنيف الأربعة لحماية المدنيين أثناء النزاعات المسلحة لعام 1949.**

[9] **محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، مرجع سابق، ص 209.**

5 المادة (49) من البروتوكول الإضافي الأول الملحف باتفاقيات جنيف الأربعة لعام 1977 والخاص بحماية ضحايا النزاعات المسلحة الدولية.

البروتوكول الاضافي الملحق باتفاقيات جنيف الاربعة لعام 1977 والخاص بحماية ضحايا النزاعات المسلحة الدولية والتي نصت : تعني الهجمات أعمال العنف الهجومية والدفاعية ضد الخصم[10].

وبقراءة وتحليل نص المادة يتبين ان مهاجمة الخصم باستخدام اجهزة الحاسوب والشبكات في اطار عمليات سيبرانية عدائية لا يعد هجوما وفقا للمفهوم الذي حدده القانون الدولي الانساني وذلك للأسباب التالية:

لغياب الأعمال العدائية التقليدية ففي العمليات السيبرانية لا وجود لأي احتكاك مباشر او التحام جسدي او مادي بين أطراف النزاع.

لغياب اعمال العنف المسلح الملموسة والمباشرة لكون العمليات السيبرانية لا تصاحبها اعمال عنف او طاقة حركية تفجيرية او ضرر مادي[11].

وتأسيسا على جملة هذه الصعوبات والاشكاليات وفي ظل القصور التشريعي وفي حالة كون ميدان النزاع هو الفضاء السيبراني والادوات والوسائل المستخدمة فيه ذات خصائص حديثة ومتطورة هل سينطبق القانون الدولي الانساني؟

الفرع الثاني: انطباق القانون الدولي الانساني على الهجمات السيبرانية العدائية:

خلا القانون الدولي الإنساني من أية قواعد صريحة وواضحة بشأن العمليات العدائية التي تتم عبر الفضاء السيبراني ولم تشر قواعد ومبادئ ذلك القانون الى الهجمات السيبرانية اثناء النزاعات المسلحة بوصفها النطاق المادي لتطبيقها.

إلا أن عدم تنظيم استخدامها قانونيا لا يعني بأي حال من الأحوال تركها لمشيئة أطراف النزاع. فلا يمكن التسليم بإخراج الهجمات السيبرانية من إطار القانون الدولي الإنساني وذلك من خلال قواعده العامة المتصفة بالشمولية والوضوح والمرونة والاتساع بما يكفي لتنظيم وسائل الحرب وأساليبها بما في ذلك المستحدثة منها كالهجمات السيبرانية. حيث جاءت تلك القواعد لتشتمل على كافة التطورات ذات الصلة وتستوعب التقنيات التكنولوجية الحديثة وتتبنى التحديثات الت يقد تصيب وسائل واساليب القتال في المستقبل كما هو الحال بالنسبة للهجمات السيبرانية[12].

من هذه القواعد المادة (36) من البروتوكول الإضافي الأول لعام 1977 والتي تنص على أنه: يلتزم أي طرف سام متعاقد بعد دراسة او تطوير او اقتناء سلاح جديد او اداة للحرب او اتباع اسلوب للحرب بان يتحقق مما اذا كان محظورا في جميع الاحوال او بعضها بمقتضى هذا الملحق او البروتوكول او اي قاعدة اخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[13].

وبتحليل نص هذه المادة نجد بأنها أقرت حقيقة أن أي نشاط عسكري معين يرتبط بوسائل واساليب الحرب ولو لم يتم تنظيمه بشكل دقيق وصريح لا يعني ذلك انه مباح ويمكن استخدامه بدون أي قواعد أو ضوابط . وعليه فإن الهجمات السيبرانية رغم أنه لم يتم تضمينها في استخدامات الأسلحة التقليدية في الاتفاقيات التقليدية ينطبق عليها القانون الدولي الإنساني وتخضع له كأي سلاح جديد يتم استخدامه في النزاع المسلح[14]. وفي الإطار نفسه يمكن الاسترشاد بالمادة (35) من البروتوكول الإضافي الأول والتي تعد إحدى القواعد الأساسية في القانون الدولي الإنساني وتنص على أن : إن حق أطراف أي نزاع في اختيار أساليب وسائل القتال ليس حقا لا تقيده قيود[15].

---

[11] **محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، مرجع سابق، ص 210.**

[12] **Lauran Jesel, International humanitarian law , OP.sit, page 295.**

[13] **المادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1977.**

[14] **Lauran Jesel, International humanitarian law , OP.sit, page 299.**

[15] **المادة 35 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1977.**

وبتحليل نص المادة يتبين أن الوسائل والأساليب القتالية الحديثة ستخضع لنفس قواعد الأسلحة التقليدية وسينطبق عليها القانون الدولي الإنساني على اعتباره قانون واسع ومرن بما فيه الكفاية للحاق بالتقدم الحاصل في التكنولوجيا والتقنيات العسكرية الحديثة. ومن زاوية أخرى يمكن الاستناد الى المبادئ الأساسية للقانون الدولي الإنساني لمعرفة مدى انطباقها على الهجمات السيبرانية وأهم تلك المبادئ "شرط مارتنز" والذي ينص على:

في حالة عدم وجود قاعدة معينة في القانون التعاهدي يظل المتحاربون في حمى وتحت سلطان القانون العرفي ومبادئ الانسانية وما يمليه الضمير العام[16]. وتأسيسا على شرط مارتنز فإن كل ما يقع أثناء النزاعات المسلحة سيخضع لقواعد ومبادئ القانون الدولي الانساني الامر الذي يفهم منه عدم خلو الهجوم على شبكات الحاسوب من القانون أثناء النزاع المسلح[17].

وأخيرا وحول هذا الخصوص يمكن الاستعانة أيضا بفتوى محكمة العدل الدولية بشأن، مشروعية التهديد باستخدام الأسلحة النووية او استخدامها ، فقد أكدت المحكمة في رأيها الاستشاري الصادر عام 1996 أن:

مبادئ وقواعد القانون الدولي الإنساني المنطبقة في النزاعات المسلحة والمستقرة تنطبق على جميع أشكال الحروب وعلى جميع انواع الأسلحة بما في ذلك المستقبلية[18].

وتأسيسا على فتوى المحكمة فإنه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو للتمييز بين الأسلحة النووية والهجمات السيبرانية على الأقل من حيث الزمن الذي استحدثت فيه ومن حيث الآثار الناجمة عن استخدامها مما يعني معه القول بانطباق القانون الدولي الإنساني عليها قياسا[19].

ووفقا لهذه المقاييس فان استخدام العمليات السيرانية العدائية اثناء النزاعات المسلحة للتسبب بمعاناة انسانية غير ضرورية وأضرارا وآلاما مفرطة لا داعي لها او لاستهداف السكان المدنيين والفئات المحمية والاعيان المدنية هو أمر غير جائز بموجب القانون الدولي الإنساني ويب أن يخضع له وأن يتقيد بقيوده وقواعده.

المطلب الثاني: مواءمة المبادئ الناظمة للعمليات القتالية مع الهجمات السيبرانية والموقف الدولي منها.

يقوم القانون الدولي الإنساني على مجموعة من المبادئ العامة والمتعلقة بالنزاعات المسلحة والتي تتميز بالطبيعة العرفية العامة والآمرة وتسري في مواجهة جميع أطراف النزاع مصادقين على الاتفاقيات الدولية المتضمنة لهذه المبادئ أم لا، كمبدأ الإنسانية، الضرورة العسكرية، التمييز، التناسب، والاحتياط. وتتجلى الغاية الجوهرية لهذه المبادئ بحماية المدنيين والأعيان المدنية والثقافية وتفادي المعاناة المفرطة وتحييد الأشخاص غير المنخرطين في العمليات العسكرية البرية والبحرية والجوية ومعاملة الجرحى والمرضى والأسرى معاملة إنسانية ومنع المساس بالبيئة[20].ولأن طبيعة الهجمات السيبرانية تختلف عن الهجمات التقليدية فإن ذلك طرح إشكالية قانونية تتمثل بمدى إمكانية مواءمة المبادئ الأساسية المنظمة لسير العمليات القتالية مع تلك الهجمات التي تشن أثناء النزاعات المسلحة المعاصرة.

الفرع الأول: مدى مواءمة المبادئ الأساسية الناظمة لسير العمليات القتالية مع الهجمات السيبرانية:

---

[16] المادة 2 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1977.

[17] موسى بن تغري، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، المجلد 12، العدد22، ص 203.

[18] الرأي الاستشاري لمحكمة العدل الدولية حول شرعية استخدام الأسلحة النووية او التهديد باستخدامها، 8 تموز /يوليو 1996، الفقرة 86.

[19] زينة عجيل، مدى شرعية الحرب في الفضاء الإلكتروني، مرجع سابق، ص 108.

[20] اللجنة الدولية للصليب الأحمر، ما هو القانون الدولي الإنساني؟ الخدمات الاستشارية في مجال القانون الدولي الإنساني، منشورات اللجنة الدولية للصليب الأحمر، سويسرا، جنيف، 2014، ص1.

هناك ضرورة ملحة للقيام بمواءمة الهجمات السيبرانية مع مبادئ القانون الدولي الإنساني خاصة تلك المتعلقة بتنظيم سير العمليات العدائية منعا من خرقها وفرضا لاحترامها[21].

أولا: مبدأ الضرورة العسكرية:

يعد مبدأ الضرورة العسكرية من أهم المبادئ التي قام عليها القانون الدولي الإنساني ويقصد به التزام أطراف النزاع المسلح باستخدام القوة الضرورية لتحقيق هدف القتال الذي يتمثل في إخضاع العدو وتحقيق النصر عليه وكسب الحرب وفقا للقوانين المنظمة لها. ومن ثم فإن كل استخدام للقوة المسلحة يتجاوز تحقيق الهدف من القتالي يصبح دون مسوغ من مسوغات الضرورة العسكرية ويدخل في خانة العمل غير المشروع[22].

تظهر إشكاليات تطبيق هذا المبدأ على الهجمات السيبرانية في صعوبة التمييز بين الأهداف العسكرية والأعيان المدنية واذا كان بالإمكان التمييز بينهما أثناء النزاعات المسلحة التقليدية فان الأمر ليس كذلك في حالة الهجمات السيبرانية التي يمكن أن تستهدف منشآت تقدم خدمة للجهد العسكري وللمدنيين في الوقت نفسه[23].

كما أن الضرورات العملية في تطبيق مبدأ الضرورة العسكرية يصعب تطبيقها على الهجمات السيبرانية فعلى سبيل المثال يمكن تحقيق الاهداف بأسر المقاتلين فقط دون قتلهم فوجود المقاتلين في ساحة القتال افضل دائما لجهة اتخاذ هكذا قرار وفي القدرة على التمييز بين من يدعي الإصابة وبين الذي لا يزال يمثل تهديدا وبالتالي يمكن استهدافه وقتله وفقا لمبدأ الضرورة العسكرية وهذا الأمر المفتقد حقيقة في سياق الهجمات السيبرانية[24].

وبناء عليه يتبين بأن تلك الهجمات تنشئ تحديا واضحا أمام مبدأ الضرورة العسكرية ، لأن عدم تحديد معايير قانونية منظمة لاستخدام تكنولوجيا المعلومات للأغراض العسكرية الهجومية سيعني إمكانية اللجوء إلى استخدامها بداعي الضرورة العسكرية. ولحل هذه المعضلة لا بد من تضافر الجهود بين خبراء القانون الدوليين ومهندسي الصناعات الإلكترونية لتحديد ما يمكن أن يوصف بهدف عسكري أو مدني وذلك حسب رأي **الأستاذ ركس هوجيس**[25].

ثانيا: مبدأ التمييز:

يعد مبدأ التمييز حجر الزاوية لأحكام القانون الدولي الإنساني الرامية لحماية السكان المدنيين من آثار العمليات العدائية ويتضمن تطبيقين أساسيين:

ضرورة التمييز بين المقاتلين وغير المقاتلين في جميع الأوقات وأن يتمتع المدنيون بالحصانة ضد الهجمات التي توجه ضد الأهداف العسكرية.

وضرورة التمييز بين الأعيان المدنية والأهداف العسكرية وأنه لا يجوز مهاجمة الأعيان المدنية بأي حال[26].

Lauran Jesel, International humanitarian law, OpSit, page 310.2

[22] نيلس ميلزر، القانون الدولي الإنساني ، مقدمة شاملة، منشورات اللجنة الدولية للصليب الأحمر، جنيف ، سويسرا، 2016، ص 70.

4 نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، المجلد 16 العدد 4 2021 ص 230.

[24] يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، العدد 4، مصر جامعة القاهرة كلية الحقوق فرع الخرطوم ، 2018، ص 96.

[25] عدنان النقيب، الحرب الإلكترونية، مرجع سابق، ص 189.

[26] نيلس ميلزر، القانون الدولي الإنساني، مرجع سابق، ص 78.

إن تطبيق مبدأ التمييز بين المقاتلين والمدنيين في سياق الهجمات السيبرانية أمر غاية في الصعوبة والتعقيد على عكس الهجمات المسلحة التقليدية اذ سيكون المهاجم على الأغلب بعيدا عن المكان المستهدف بالهجوم مما يعني معه ان التمييز بين المقاتلين والمدنيين هو أمر صعب إن لم يكن مستحيلا[27]. كما تعد مسألة التمييز في الاهداف العسكرية والاعيان المدنية في سياق الهجمات السيبرانية عسيرة خاصة وان نظم الحواسيب العسكرية غالبا ما تتصل بالنظم المدنية والتجارية بل وقد يكون هناك تداخل بين الاستخدامات المدنية والاستخدامات العسكرية بارتباطهما بشبكة واخدة وبمجال واحد هو الفضاء السيبراني ومن ثم سيكون من المستحيل شن هجوم سيبراني تقتصر آثاره على هدف عسكري وحسب دون الإضرار بالمدنيين والمنشآت المدنية[28].

وتبقى مسألة التمييز بين من يقاتل ومن لا يقاتل في سياق الهجمات السيبرانية غير ممكنة حيث لا يوجد أسرى او جرحى بل يوجد مرافق وأنظمة معطلة لا تعمل او دمار ذاتي من دون تدخل مباشر كالقصف والتدمير التقليدي[29].

وحول هذا الشأن دعا فقهاء كماركو روسيني الى ان يتحرك المحامون الدوليون لأجل البحث في مدى مواءمة الطابع السري للجهمات السيبرانية في ضوء أحكام القانون الدولي الإنساني وخاصة مبدأ سلوكيات الحرب خصوصا بعد تزايد ادعاءات الدول بتعرضها لهجمات سيبرانية غير معروفة المصدر[30].

ثالثا: مبدأ التناسب:

يعد مبدأ التناسب أحد المبادئ الجوهرية التي يجب تطبيقها اثناء النزاعات المسلحة لأنه يهدف الى الحد والتقليل من الخسائر واوجه المعاناة المترتبة على العمليات العسكرية سواء بالنسبة للأشخاص او للأشياء. ويعتمد على تحقيق التوازن بين أمرين جوهريين هما الميزة العسكرية المتوقعة من اعمال القتال من جانب والخسائر التي تلحقها هذه العمليات بالمدنيين والاعيان المدنية من جانب آخر[31].

تظهر إشكاليات تطبيق هذا المبدأ في سياق الهجمات السيبرانية في أن برمجة تلك العمليات لا يكون في مقدورها تطبيق مبدأ التناسب سيما وأن معادلة التناسب عد صعبة ودقيقة حتى اثناء إدارة العمليات الحربية التقليدية فتحقيق المنفعة القتالية وإحراز النصر هدف أساسي للقوات المسلحة وتنفيذ القوانين وضبط التدمير وعدم إلحاق أضرار مفرطة بالخصم التزام قانوني واجب النفاذ وبالتالي يحتاج الى قائد عسكري متمكن ليسوي هذه المعادلة والامر دون شك يزداد صعوبة وتعقيدا اذا ما تعلق بالهجمات السيبرانية[32].

وفي ضوء الآثار الناجمة عن الهجمات السيبرانية يذهب **شين** بالقول يمكن تطبيق مبدأ التناسب على الهجمات السيبرانية إلا أن ذلك المبدأ المذكور عند استخدام القوة السيبرانية لا يزال غامضا ويحتاج الى اجوبة وأهمها : كيف يمكن ضمان مبدأ التناسب بالرد على الهجمات السيبرانية ؟

---

[27] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية المجلد8 العدد 4 ص 636.

[28] نسيب نجيب، الحرب السيبرانية، مرجع سابق، ص 233.

[29] يحيى ياسين سعود الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مرجع سابق، ص 98.

[30] Marco Roscini, world wide warefare and the use of cyber force, Maxplan CK Year book of United Nation Law, pa:90.

[31] نيلس ميلزر، القانون الدوليالإنساني، مرجع سابق، ص 98.

[32] يحيى ياسين سعود، الحربالسيبرانية، مرجع سابق، ص 96-97.

ويتفق **ركس** مع ما ذهب اليه شين بالقول: اذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الاستعمال مدنية وعسكرية فلا يبدوان المنفعة العسكرية ستكون واضحة مما يجعل مبدأ التناسب في سياق الهجمات السيبرانية أمر غاية ي الصعوبة[33].

رابعا: مبدأ الاحتياط:

ويعني أن المتحاربين وجميع أطراف النزاع يجب أن يتخذوا جميع الاحتياطات الممكنة عند تبني وسائل واساليب الهجوم ويفرض التزاما على أطراف النزاع باختيار الوسئل الاقل ضررا بغية تحقيق الاهداف العسكرية وتجنب احداث الخسائر في ارواح المدنيين او الحاق الاصابات بهم او الاضرار بالممتلكات المدنية.

وأن يمتنع الطرف المحارب او يلغي او يعلق أي قرار يتعلق بشن هجوم قد يتم توقع نتائجه بصورة عرضية اوان يحدث خسائر في ارواح المدنيين والاعيان المدنية وان يتم توجيه انذار مسبق في حالة الهجوم وان يكون الهدف العسكري من بين عدة اهداف تلافيا لإصابات المدنيين[34].

إن قابلية الفضاء السيبراني للقيام بالأنشطة العدائية فرضت بعض الصعوبات والتعقيدات بخصوص الالتزام بمبدأ الاحتياط الواجب اتخاذه اثناء الهجوم وان تشابك شبكات الاتصالات والمعلومات تجعل من الصعوبة التمييز بين ما يعد انظمة مدنية واهداف عسكرية وبالتالي معرفة الاهداف العسكرية التي يكون استهدافها قانونيا والهداف المدنية التي يجب ان تبقى بعيدة عن الهجوم وباعتبار ان الاذى والضرر الناجمين عن تدمير او تعطيل نظم البنية التحتية الحيوية غير ضروريين ويتسببان في معاناة مفرطة للمدنيين لذلك صنفت من النوع الذي هدفت قوانين النزاع المسلح الى منعها لان هذه الشبكات تخدم اعداد ضخمة من السكان المدنيي فان الاذى والضرر المتأتيين من هذا الهجوم سيكونان على نطاق واسع وغير متناسبين مع المزايا العسكرية المحققة[35].

وعلى ضوء ما سبق تبقى مسألة مواءمة قواعد ومبادئ القانون الدولي الإنساني الحاكمة لسير العمليات القتالية والناظمة لها مع الهجمات السيبرانية غير ممكنة وغير عملية في الوقت الراهن وذلك بسبب الفوارق الجوهرية بين الهجوم المسلح المادي والهجوم السيبراني وكذلك عدم إمكانية إسقاط بعض مبادئ القانون الدولي الإنساني على الهجمات السيبرانية خاصة عند تطبيق مبادئ سلوكيات الحرب المتمثلة أساسا بمبادئ الضرورة والتمييز والتناسب والاحتياط.

الفرع الثاني: موقف الفقه الدولي والمنظمات الدولية بشأن الهجمات السيبرانية:

يؤكد العديد من فقهاء القانون الدولي والمختصين في القانون الدولي الإنساني مسألة انطباق الأخير على الهجمات السيبرانية التي تشن أثناء النزاعات المسلحة المعاصرة ويدعمون موقفهم هذا بالقول أن تلك العمليات العدائية التي تطال المرافق الصحية وأفراد الرعاية الطبية وعمال الإغاثة الإنسانية أثناء النزاع المسلح وإن كانت أقل ضررا من العمليات الحركية التقليدية تبقى غير مشروعة بموجب القانون الدولي الإنساني نظرا للحماية القانونية الدولية المكفولة والتي تتمتع بها هذه الفئات وفقا لذلك القانون[36].

---

[33] عدنان النقيب، الحربالإلكترونية، مرجع سابق، ص 193.

[34] نيلس ميلزر، القانون الدولي الإنساني، مرجع سابق، ص 99.

[35]عدنان النقيب، الحرب الالكترونية،مرجع سابق، ص 195.

[36] اسحاق العشعاش، الهجمات السيبرانية ضد المنشآت الصحية الحرجة في زمن الأوبئة والجوائح، مجلة القانون الدولي للدراسات البحثية، العدد الخامس، 2020، ص 117+ 118.

ويؤكد هذا التوجه الفقيه البارز **مايكل شميث** بالقول: يجب أن ننظر الى نتائج وآثار هذا السلوك أكثر مما نأخذ بعين الاعتبار الوسيلة التي تم استخدامها والتي من الممكن أن تكون مشروعة لكنها تستخدم لتحقيق أغراض غير مشروعة كالتسبب معاناة إنسانية مفرطة او بتحميل المدنيين خسائر فادحة كخسائر الأسهم التجارية والقطاعات المالية والمصرفية التي يتعاملون معها والإضرار بحياة وسلامة المدنيين او بسلامة البنية التحتية المدنية والمنشآت المدنية كالجسور والسدود ومحطات توليد الطاقة الكهربائية[37]. وعبر الفقيه **ماركو روسيني** عن ذات الموقف بالقول : نظرا بأن العمليات السيبرانية يمكن أن تعطل الخدمات الأساسية وتعيق إمداداتها بشكل كبير دون التسبب بالضرورة في اضرار مادية او بشرية فانه من الممكن تفسير قواعد القانون الدولي الانساني مع مراعاة التطورات التكنولوجية الحديثة وتوسيع مفهوم العنف بحيث لا يشمل فقط الضرر المادي الذي يلحق بالأعيان فحسب بل يشمل ايضا تعطيل او اعاقة البنية التحتية دون تدمير[38]. أما الفقيه **دينيز هاريثون هايثر** فذهب الى القول : من غير المقنع الإصرار على ان مفهوم الهجمات يجب أن يقتصر على الأفعال التي تؤدي مباشرة الى وفيات او اصابات او اضرار مادية في وقتنا الحالي في ظل التقدم العلمي والتكنولوجي غير المسبوق وتوافر التقنيات العسكرية المتطورة39. وقد اعتبر الفقيه **هارولد هونجيو كوه** الأنشطة التي تؤدي الى الموت او الاصابة او التدمير او التعطيل أنشطة ينظر اليها على انها استخدام للقوة وبالتالي ينطبق عليها القانون الدولي الانساني[40].

فالفكرة الأساسية بالنسبة لهؤلاء الفقهاء تقوم على تبني معيار يعتمد على آثار وتداعيات العمل والنتائج المتوخاة منه كمعيار لتقرير انطباق القانون الدولي الانساني عليه من عدمه.

وبينت المستشارة القانونية للجنة الدولية للصليب الأحمر **كوردولا دروغيه** أن الإطار القانوني الدولي الإنساني القائم ينطبق على النزاعات السيبرانية ويجب احترامه والالتزام به وفندت مزاعم من يقولون بخلو الفضاء السيبراني من القوانين بقولها: ان هذه ليست المرة الاولى التي يحدث فيها تطور وتغير في التكنولوجيا المستخدمة وقد تعامل معها القانون الدولي الانساني واكدت ان القانون القائم قادر على التعامل مع هذه التطورات المستحدثة دون الحاجة الى وضع قواعد قانونية جديدة خاصة بالهجمات السيبرانية[41].

أما بالنسبة لموقف **اللجنة الدولية للصليب الأحمر** فيما يتعلق بمسألة انطباق القانون الدولي الإنساني على الهجمات السيبرنية فقد اعتبرت ان ذلك القانون هو الإطار الأساسي الذي يفرض قيودا على اللجوء للعمليات السيبرانية أثناء النزاع المسلح ويحمي السكان المدنيين من الأضرار المحتملة والارتدادية لتلك العمليات. وتؤكد اللجنة موقفها بالقول ليس ثمة شك بأن القانون الدولي الانساني ينظم العمليات السيبرانية شأنها شأن أي سلاح أو وسائل وأساليب القتال الاخرى سواء كانت قديمة او حديثة وان اعتماد العمليات السيبرانية على تقنية جديدة ومتطورة لا يحول دون انطباق

---

[37] **Michael N, Schmitt, Classification of cyber conflicts, Journal of conflicts andsecurity law,2012, Vol 17 No 3 P257.**

Marco Roscini , worldwide warfare, Opcit, p120. [38]

[39]. **Dinnes Harrison Heather Cyber warfare and the law of war Cambridge University press 2012 Cambradge p: 198**

[40] **Harold Hongiu Koh International law in cyber space Harvard International law Journal Vol 54 No 7 p8,2012.**

[41] **Cordula Drogeh Get of my cloud :cyber warfare , International humanitarian law and the protection of civilians International Review of the red Cross Vol 94 No 886 p 565.**

القانون الدولي الانساني عليها[42]. وأشار **دليل تالين** للقانون الدولي المطبق على العمليات السيبرانية لعام 2013 صراحة الى إمكانية انطباق القانون الدولي الانساني كما هو على العمليات . واعتبر الدليل أن الهجوم السيبراني بمثابة استخدام للقوة اذا كان أثر هذا الهجوم عند مقارنته بالاستخدام التقليدي للقوة مساويا له او قريبا منه. وعليه أكد الخبراء العاملون في دليل تالين على ضرورة تدخل القانون الدولي الانساني في الحرب السيبرانية كما حددوا معيار انطباقه عليها بالضرر المترتب أي أنه إذا ماكان الضرر يودي بحياة المدنيين ويؤثر عليهم تأثيرا مباشرا ام لا[43].

وفي تقريري عام 2013 و 2015 لفريق **الخبراء الحكوميين التابع للأمم المتحدة** خلص الخبراء الى ان احكام القانون الدولي الانساني وميثاق الامم المتحدة قابلين للتطبيق في بيئة تكنولوجيا الاتصالات والمعلومات[44] وهو استنتاج رحبت به الجمعية العامة للأمم المتحدة بداية الامر[45] ثم أكدته[46]. ودعم هذا التوجه العديد من الدول والمنظمات الدولية **كالاتحاد الأوروبي**[47] **والاتحاد الافريقي**[48] **وحلف شمال الاطلسي**[49] اللذين اكدوا علانية ان القانون الدولي الانساني ينطبق على الهجمات السيبرانية أثناء النزاع المسلح. وفي اجتماع الفريق العامل التابع للمنظمة **الاستشارية القانونية الآسيوية الإفريقية** عام 2019 المعني بالقانون الدولي للفضاء السيبراني تم التأكيد على أن نطاقي قانون الحرب وقانون مسوغات الحرب يجب ان ينطبقا مع مراعاة خصوصية الملايات السيبرانية[50] . وأعاد نداء **باريس للثقة والامن في الفضاء السيبراني** والذي أيدته 71 دولة في نيسان ابريل2020 التأكيد على انطباق القانون الدولي الانساني على الهجمات السيبرانية اثناء النزاعات المسلحة[51].

وبعد استعراض تلك الآراء ووجهات النظر بشأن مسألة انطباق القانون الدولي الانساني على الهجمات السيبرانية يتضح وبجلاء أنه وبرغم غياب أي إشارات صريحة واضحة في ذلك القانون حول الاستهداف المباشر للمدنيين والاعيان المدنية عبر العمليات السيبرانية يمكننا القول بانطباق القانون الدولي الانساني عليها فعليا.

وأساس هذه النتيجة يكمن في الغاية الجوهرية للقانون الدولي الانساني المتمثلة في حماية المدنيين والاعيان المدنية فعندما يكون الهدف من الاعتداءات السيبرانية هو تعريض المدنيين او الفئات المحمية او الاعيان المدنية والثقافية لخطر الاستهداف وعندما يكون اثر تلك الهجمات على حياة المدنيين يتمثل بقطع إمدادات الطاقة والمياه او اصابة

---

[42] القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر المقدمة الى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي ،والى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الامن الدولي تشرين الثني نوفمبر 2019 ص 10.

[43] Michael N, Schmitt, Tallinn Manual on the International law applicable to cyber warfare ed1 Cambridge University press New York 2013 p 125.

[44] الجمعية العامة للأمم المتحدة ، فريق الخبراء الحكوميين المعنيبالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية فيسياقالامن الدولي وثيقة الأمم المتحدة A/68/ 98 24 حزيران 2013 الفقرة 19 والوثيقة A/70 /174 12 تموز 2015 الفقرة 24.

[45] قرار الجمعية العامة للأمم الاحدة 237/70 المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي وثيقة الامم المتحدة A/RES/70/237 3 كانون الاول 2015 الفقرة 16.

[46] قرار الجمعية العامة للأمم المتحدة 73/27 القرة 17، والقرار266/73 الفقرة 12.

[47] European Union , European Union Cyber Security Strategy 2013.

[48] اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي اتفاقية مالابو 2014.

[49] Cyber Defence Strategy2016. North Atlantic Treaty Organization (NATO)

[50] AALCO, Summary report of the fourth meeting of the open ended working group on international law in cyber space 3 september 2019 p 10.

[51] France, Paris Call for Trust and Security in cyber space , France Diplomacy ,2018 12 November.

النظام الصحي او النظام المصرفي بخلل او التلاعب بالبنية التحتية الحيوية والحرجة للدولة يصبح القانون الدولي الانساني منطبقا حكما وفعليا على الرغم من إشكاليات تطبيقه.

الاستنتاجات والتوصيات:

1-الاستناجات:

1- لا يمكن وفقا لقواعد ومبادئ القانون الدولي الانساني القول بان مالم يحظر صراحة في المعاهدات او العرف يكون مباحا لان مبادئ الانسانية وما يمليه الضمير العام يمثلان عوامل تقييدية قانونية وذريعة استخدام الدول لسلاح جديد او اسلوب قتال جديد لم يتم تحريمه صراحة وبشكل مباشر بموجب القانون الدولي الانساني لم تعد مقبولة مطلقا.

2-تتسم القواعد العامة للقانون الدولي الانساني بالشمولية والاتساع والمرونة بما يكفي حيث جاءت هذه القواعد لتستوعب التقنيات التكنولوجية المستحدثة وتتبنى التطورات التي تطرأ على وسائل واساليب القتال في المستقبل.

3-تبقى مسألة مواءمة مبادئ القانون الدولي الانساني الحاكمة لسير العمليات القتالية والناظمة لها مع الهجمات السيبرانية غير عملية وغير ممكنة في الوقت الراهن وذلك بسبب الفوارق الجوهرية بين الهجوم المسلح التقليدي والهجوم السيبراني ولعدم امكانية إسقاط تلك المبادئ على الهجمات السيبرانية وتظهر الاشكاليات خاصة عند تطبيق مبادئ سلوكيات الحرب كالضرورة والتمييز والتناسب والاحتياط.

4-اعتمد الفقهاء والمختصون في القانون الدولي معيارا اساسا في تأييدهم لمسألة انطباق القانون الدولي الانساني على الهجمات السيبرانية وهو معيار يقوم على آثار وتداعيات الهجمة والنتائج والاضرار المتولدة عنها.

5-إن التوجه الدوليا لقائل بانطباق القانون الدولي الانساني على الهجمات السيبرانية وبامكانية خضوعها له وتقييدها بقواعده العامة اصناء النزاعات المسلحة المعاصرة يلقى مزيدا من التأييد على المستوى الفقهي والقانوني الدولي وقد تبنته صراحة معظم الدول والمنظمات الدولية والاقليمية الحكومية وغير الحكومية.

2- التوصيات:

1-ضرورة مراجعة وتطوير اتفاقيات ونصوص القانون الدولي الانساني الحالية التي تحكم النزاعات المسلحة بما يتناسب مع الطبيعة الخاصة للهجمات السيبرانية فعلى الرغم من انه يمكن استخدام القواعد الحالية لتنظم وتحكم وتقيد تلك الهجمات الا انه يبقى هناك حاجة ماسة لسد الثغرات والصعوبات النابعة من الطبيعة التقنية والفنية الخاصة بها.

2-ضرورة تضافر الجهود الدولية والاقليمية والوطنية لمواجهة هذه المشكلة والحد من آثارها بشكل فعال لان مواجهتها عن طريق الجهود الفردية والمحلية وحدها لن يكون كافيا لتحقيق استجابة قانونية عالمية فعالة ورادعة نظرا للخصائص التقنية الفريدة للهجمات السيبرانية وتميزها عن اي نوع اخرمن الاسلحة الحركية والتقليدية.

3-ضرورة العمل والتعاون الدوليين على ايجاد شبكة معلومات مدنية منفصلة تماما عن تلك المستخدمة لأغراض عسكرية وسياسية وامنية للحد من آثار وتداعيات الهجمات السيبرانية في المستقبل.

4-طلب رأي استشاري من محكمة العدل الدولية من قل الجمعية العامة للأمم المتحدة حول شرعية استخدام الهجمات السيبرانية شبيها بفتوى الاسلحة النووية 1996وتبنيقرار ملزم من مجلس الأمن الدولي ينظم وضع هذه الهجمات في ضوء رأي المحكمة.

5-تطوير النظام الجنائي الدولي ليشمل الجرائم الناشئة عن الهجوم السيبراني واحداث محاكم جنائية دولية متخصصة لإدانة ومحاكمة الدول القائمة بتلك الهمات والراعية لها.

6-ضرورة تشكيل لجان تحقيق دولية متخصصة بالهجمات السيبرانية وآثارها بهدف التحقيق واعداد التقارير الدولية اللازمة.

References:

Books:

1. Heather, H, D. Cyber Warfare and the law of war. Cambridge University Press, New York, USA, 2012, 360.

2. Schmitt, N, M. Talline Manual on the international law application to cyber warfare. (ed 1), Cambridge University Press, New York, USA, 2013, 304.

3. Melzer, N. International humanitarian law: a comprenesive introduction. Puplications of the International Committee of the Red Cross, Geneva, Switzerland, 2016, 326.

4. ALNakeeb, A. Electronic warfare in light of the seventy- seven protocols attached to the four Geneva conventions of the year forty-nine (Cyber Attacks). Arab center for puplishing and distribution, Egypt, Cairo, 2022, 392.

Scientific Theses:

1. ALSharkawy, H, M. Electronic attacks in light of the provisions of international humanitarian law. Doctoral thesis, Egypt, Beni suef University, faculty of law, dpartment of international law, 2021, 419.

2. Ojel, Z. The extent of the legitimacy of war in cyber space according to the rules of international humanitarian law and international conventions. Masters thesis . Syria ,Tishreen University , faculty of law , department of international law, 2022. 142.

Periodicals:

1. International Committee of the Red Cross. What is international humanitarian law? Advisory services in the field of international humanitarian law , Switzerland, Geneva, puplication of ICRC, 2014, 100.

Journals:

1. Roscini, M. World wide warfare and the use of cyber space. Max Planck Yearbook of United Nation law, Vol: 14, 2010, 85-130.

2.Drogen, C. Get off my cloud: cyber warfare, International humanitarian law and the protection of civilians. International Review of the Red Cross, Vol: 94, No: 886, 2012, 533- 578.

3.Koh, H H. International law in cyber space. Harvard International law Journal . Vol: 54, No: 25, 2012, 1-30.

4.Schmitt, N M. Classification of cyber conflicts. Journal of Conflicts and Security law , Vol: 17, No: 2, 2012, 245- 260.

5.ALFatlawy, A. Cyber attacks: their concept and the international responsibility arising from them in light of contemporary international regulation. ALmohaqeq Almhally Journal for legal and political sciences, Vol: 8, No: 4, 2016, 610- 687.

6.Saood, Y Y. Cyber warfare in light of the rules of international humanitarian law. Legal Journal , Vol: 4, 2018, 80-108.

7.Jesel, L. Rodnhouser, T, Dorman, K. International humanitarian law and the protection of cicilians in the effects of cyber operations during armed conflicts. International Journal of the Red Cross, Geneva, Vol: 102, No: 913, 2020, 287- 334.

8.ELEshaash, I. Cyber attacks against critical health facilities in times of epiedemics and pandemics. Journal of International law for research studies, Issue: 5, Germany, Berlin, 2020, 106- 135.

9.BenTaghry, M. cyber warfare and international humanitarian law. Journal of Judical jurisprudence, Vol: 12, No: 22, 2020, 199- 218.
10.Najeeb, N. Cyber warfare from the perspective of international humanitarian law. Critical Journal of law and political scienes, Vol: 66, No: 4, 2021, 218- 236.

International Documents and Reports:

1.Advisory opinion of the International Court of Justice, in 8 July 1996, relating to the legality of the use or threat of use of nuclear weapons.
United Nation, Document : 2.
A\68\98 in 24 June 2013, A\70\ 174 in 15 July 2015.
United Nation, General Assembly Resolutions: 3.
A\RES\ 70\237 in 3Janeuary 2015, A\RES\73\27, A\RES\73\266 in 2015.
4. AALCO, Summary report of the fourth meeting of the open-ended working group on international law in cyber space, 3 September, 2019.
5. Report of the international committee of the Red Cross to the open-ended working group on Developments in the field of information and telecommunication in the context of international security and to the group of governmentel experts on promoting responsible state behavior in cyber space in the context of international security.
United Nation, General Assembly, New York, November, 2019.

International Conventions:

1.The four Geneva Conventions for the protection of civilian persons during armed conflicts 1949.
2.The First additional protocol annexed to the four Geneva Conventions of 1977 relating to the protection of victim of international armed conflicts 1977.
Tallinne Manual on international law applicable to cyber warfare 2013. 3.
European Union cyber security strategy 2013. 4.
5. African Union Convention on cyber security and protection of personal data , Malabo Agreement 2014.
6. North Atlantic Treaty Orgnization (NATO) cyber defence strategy 2016.
Paris Call for Trust and Security in cyber space 2018