***Dirasat*: Shari'a and Law Sciences, Volume 51, No. 1, 2024**

Deanship of Scientific Research

Cyber-Attacks in Accordance with International Humanitarian Law

Mohammad Hasan Daraji**, Omar Saleh AL- Okour

Department of Public Law, School of Law, The University of Jordan, Amman, Jordan.

Received: 11/5/2022
Revised: 17/7/2022
Accepted: 22/9/2023
Published: 1/3/2024

* *Corresponding author:*
dr.m.alsamarai@gmail.com

Citation: Daraji, M. H., & AL-Okour, O. S. . (2024). Cyber-Attacks in Accordance with International Humanitarian Law. *Dirasat: Shari'a and Law Sciences*, *51*(1), 1–12. https://doi.org/10.35516/law.v51i1.786

Abstract

Objectives: This study aims to demonstrate the applicability of the rules of international humanitarian law to cyber-attacks, as international humanitarian law aims to regulate the exceptional right to use force to resolve disputes, as such use of force is internationally prohibited under the UN Charter.

Methods: Two approaches were employed in this research. The first is a descriptive-analytical approach, which starts from the description of the phenomenon under question, the legal approach that is taught in political and international system institutions, and the relationship between them. The second is a historical approach, which traces the historical events surrounding the emergence of the term 'cyber-attacks'.

Results: There are two different approaches regarding the issue of the subordination or non-subordination of cyber-attacks to the provisions of international law, the most likely approach is that cyber-attacks are subject to the provisions of international law. This approach is encouraged so as to avoid falling into the problem of evasion of international responsibility which could then lead to committing more massacres against civilians as a result of the use of cyber-attacks as a weapon.

Conclusions: The study recommends the necessity of adapting the rules of international humanitarian law to align with the unique nature of cyber attacks and applying them as weapons and methods of warfare in armed conflicts. Efforts should continue to amend these legal rules to achieve explicit international legal regulation for cyber attacks.

Keywords: Cyber-attacks, International Humanitarian Law, armed conflicts.

الهجمات السيبرانيَّة وَفقًا لأحكام القانون الدولي الإنساني

محمد حسن سعيد دراجي* ، عمر صالح العكور

قسم القانون العام، كلية الحقوق، الجامعة الأردنية، عمان، الأردن.

ملخّص

الأهداف: تهدف هذه الدراسة، التي جاءت في مقدِّمة ومبحثَيْن، إلى بيان مدى إمكانيَّة انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانيَّة، وترمي إلى تنظيم مسألة الحق الاستثنائي في استخدام القوة لحلّ الخلافات بعد أن أصبحت محرَّمة دوليًّا بموجب ميثاق الأُمم المتحدة.

المنهجيَّة: استخدمت الدراسةُ عدَّة مناهج، تمثَّلت في المنهج الوصفي التحليلي الذي ينطلق من وصف الظاهرة موضع الدراسة، والمنهج القانوني الذي يهتمُّ بمؤسسات النظام السياسي والدولي، ويقفُ على العلاقة القائمة بينها، والمنهج التاريخي الذي يُعنى بتتبُّع الأحداث التاريخيَّة لبداية ظهور مصطلح الهجمات السيبرانيَّة.

النتائج: هنالك توجُّهان مختلفان في مسألة خُضوع الهجمات السيبرانيَّة، وعدم خضوعها لأحكام القانون الدولي، والرأي الراجح خضوعُها لتلافي الوقوع في إشكاليَّة التهرُّب من المسؤوليَّة الدوليَّة، ومن ثَمَّ ارتكاب المزيد من المجازر بحقِّ المدنيين نتيجة استخدام الهجمات السيبرانيَّة بِوَصفِها سلاحًا.

الخلاصة: توصي الدراسة بضرورة تطويع قواعد القانون الدولي الانساني لتنسجم مع الطبيعة الخاصة للهجمات السيبرانية وتطبيقها عليها باعتبارها سلاح وطريقة قتال في النزاعات المسلحة ، مع استمرار الجهود لتعديل تلك القواعد القانونية للوصل الى تنظيم قانوني دولي صريح للهجمات السيبرانية.

الكلمات الدالة: الهجمات السيبرانيَّة، القانون الدولي الإنساني، النِّزاعات المُسَلَّحة..

المقدمة

شهدت المجتمعات تطورا متسارعا في كافة مجالات الحياة، ودخلت التكنولوجيا، ومنها مايتعلق في الإطار الإلكتروني في المجالات المدنية والعسكرية والاقتصادية والصحية والاجتماعيه حتى أصبحت جزءًا لايتجزاء فيها، بحيث يترتب على عدم وجودها خلل كبير، وربما الشلل التام في عملها، حتى أصبح تطور المجتمعات يقاس بمدى استخدامها للتكنولوجيا الإلكترونيه في تسيير أمورها.

ومما لاشك فيه أن العمليات السيبرانية قد بدأت بشكل بسيط وفي إطار ضيق يتعلق بالأفعال الإجرامية ذات التاثير الأقل نسبيا من حيث الأضرار المترتبة عليها قياساً إلى ماوصلت إليه عملية استخدام التكنولوجيا الإلكترونيه إلى أبعد مدى؛ لتشمل مجالات خطيرة جدا عندما أصبحت تهدد أمن الفرد والمجتمعات ودول العالم أجمع لاسيما عندما أخذت تستخدم في إطار النزاعات المسلحة الدولية وغير الدولية، ومن قبل مجموعات وتنظيمات إجرامية وإرهابية أو ترتكتب في إطار الحروب الدولية سواء بشكل منفرد أو بالتزامن مع العمليات العسكرية التقليدية التي تخلف آثارا تدميرية هائلة، لاسيما وهي تعطي حافزا وعامل دعم للتفوق، والميزة العسكرية وإحداث نوع من الخلل في توازن القوى وغلبة وترجيح كفة الدول التي تمتلك وتستخدم الأسلحة السيبرانية على حساب الدول الأخرى التي تفتقر لتلك القدرات، كل ذلك دفع دول العالم وخبراء القانون والمختصين إلى التحذيرمن خطورة تلك العمليات السيبرانية، وبيان أهمية ايجاد إطار وتنظيم قانوني دولي يحكم ويضبط ايقاع هذا النوع الجديد والمستحدث من الخطر الذي تواجهه دول العالم باعتباره خطر متسارع بدرجة تفوق قدرات المواجهه القانونيه له سواء على المستوى القانون الوطني أو على مستوى القانون الدولي. وسوف تركز دراستنا على قاعدتين أساسيتين يقوم عليها القانون الدولي الإنساني، وهما: الحق في استخدام القوة أو حق اللجوء للحرب، وكذلك السلوكيات الواجب اتباعها أثناء النزاعات المسلحة ونقصد بها ما نصت عليه المبادئ التي يقوم عليها القانون الدولي الإنساني في حالة النزاعات المسلحة الدولية وغير الدولية ومراعاة خصوصية الهجمات السيبرانية عندما تستخدم في النزاعات المسلحة.

ولكوننا في إطار تناول مدى إمكانية تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية عندما تستخدم التكنولوجيا الرقمية كسلاح أو أداة في النزاعات المسلحة الدولية وغير الدولية؛ فيكون لزاما مناقشة ذلك من خلال بيان أهم قواعد القانون الدولي الإنساني المتعلقه بحق اللجوء إلى الحرب واستخدام القوة المسلحة ومدى إمكانية انطباقه على الهجمات السيبرانية في إطار العلاقات الدولية بين التحريم والاستثناءات الواردة عليه، وفقا لميثاق الأمم المتحدة بعد أن نبين ماهية الهجمات السيبرنيه وطبيعتها ومدى إمكانية خضوع الهجمات السيبرنية لأحكام القانون الدولي الإنساني كذلك ولغرض اكتمال الصورة أمام المتلقي، يجب بيان الجزء أو الأساس الثاني للقانون الدولي الإنساني، ونقصد أهم المبادئ التي يقوم عليها، ومدى انطباقها على الهجمات السيبرانية مع الأخذ بالنظر اعتبار شموليتها وعموميتها من جهة، وخصوصية الهجمات السيبرانية التي تتميز بها عن الأسلحة التقليدية المستخدمة في النزاعات المسلحة الدولية وغير الدولية من جهة أخرى.

مشكلة الدراسة وأسئلتها:

تتلخص مشكلة الدراسة أو إشكاليتها في حداثة الهجمهات السيبرانية ودخولها بقوة في إطار سباق التسلح باعتبارها سلاح أو أحد أدوات النزاعات المسلحة، بما يترتب على ذلك من آثار قانونيه وواقعية مهمه، لاسيما وأن هنالك افتقار وفراغ في المنظومة القانونيه للقانون الدولي الإنساني في تنظم الهجمات السيبرانية، وعليه، فإن مشكلة الدراسة تتمحور في مدى إمكانية اخضاع الهجمات السيبرانية إلى القانون الدولي الإنساني.

وقد تمخض عن مشكلة الدراسة الأسئلة الآتية:

1- هل عالجت الاتفاقيات الدولية الهجمات السيبرانية من ناحية إطار القانون الدولي الإنساني؟
2- هل ما موجود من قواعد قانونيه عرفيه واتفاقيه كافيه لمعالجة الهجمات السيبرانية في إطار القانون الدولي الإنساني؟
1- ما مدى انطباق حق اسخدام القوة والاستثناءات الواردة عليه على الهجمات السيبرانية؟
3- ما مدى توافق مبادئ القانون الدولي الإنساني مع خصوصية الهجمات السيبرانية ؟

أهمية الدراسة:

تنبع أهمية الدراسة من ضرورة تأمين المدنيين في حالة النزاعات المسلحة الدولية وغير الدولية في إطار تطبيق قواعد القانون الدولي بالإنساني، والتاكيد على وجود القصور في الأدوات القانونيه الدولية، كما تتضمن أهمية الدراسة بيان مدى إمكانية انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، ويضمن معاقبة مرتكبي تلك الهجمات السيبرانية المرتكبة في إطار النزاعات المسلحة، وتمثل هذه الدراسه إضافه بسيطة ومتواضعه؛ لايضاح جزء يسير من الصورة الضبابيه للتنظيم والتكييف القانوني للهجمات السيبرانية، وفقا لأحكام القانون الدولي الإنساني، وبما يمكن الباحثين والمختصين من الاستفادة مما تحتويه من أفكار متواضعه.

أهداف الدراسة:

تهدف الدراسة إلى بيان مدى إمكانية انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، الذي يرمي إلى تنظيم مسالة الحق الاستثنائي في استخدام القوة لحل الخلافات بعد أن اصبحت محرمة دوليا بموجب ميثاق الأمم المتحدة، كما تهدف الدراسة إلى تحديد نوع الأسلحة

المستخدمة، ومدى انطباق الجواز القانوني لاستخدام حق الرد دفاعا عن النفس في حالة ارتكاب الاعتداءات المسلحة باستخدام الأسلحة والأدوات السيبرانية، وتحديد الغطاء القانوني بموجب أحكام الفصل السابع من ميثاق الأمم المتحدة، وفق ما يسمى بتدابير الأمن الجماعي، لتوفير الحماية القانونية للمدنيين ولغير المشتركين والأعيان المدنيه وغير العسكرية في النزاعات المسلحة الدولية وغير الدولية. كما تهدف الدراسة إلى بيان مدى إمكانية التوافق بين شمولية وعموميه مبادئ القانون الدولي الإنساني وبين الخصوصية والطبيعة الخاصة التي تتميز بها الهجمات السيبرانية عندما تستخدم كسلاح في النزاعات المسلحة الدولية وغير الدولية.

حدود الدراسة ومحدداتها:

الحدود الزمانية: تتمثل الحدود الزمانية لهذه الدراسة منذ بداية استخدام مصطلح السيبرانية عام 1948 ولغاية 2022.

الحدود المكانية: تقتصر الدراسة على أحكام القانون الدولي الإنساني

الحدود الموضوعية: تتحدد الحدود الموضوعية في الهجمات السيبرانية وفقا لأحكام القانون الدولي الإنساني

أما محددات الدراسة فتتمثل في أنه لا يوجد هناك محددات تساهم في منع تعميم نتائج هذا البحث على المجتمع الأكاديمي والمجتمع القانوني بشكل عام.

منهج الدراسة:انطلقت هذه الدراسة بالاعتماد المناهج الآتية:

- **المنهج الوصفي التحليلي:** الذي ينطلق من توصيف الظاهرة موضع الدراسة من خلال عرض ما تتميز به من محددات وخصائص، ومن ثم يقرن الوصف بالبحث في الأسباب التي أدت لتشكيل الظاهرة(موضوع الدراسة) وتحديد خصائصها، وقد وظف هذا المنهج في هذه الدراسة من خلال استعراض ودراسة خصائص الهجمات السيبرانية، والبحث في أسباب هذه الخصائص.
- **المنهج القانوني** الذي يدرس في مؤسسات النظام السياسي والدولي والعلاقة بينها والصلاحيات والحدود التي تتمتع بها، وفق ما تنص عليه التشريعات والدساتير والقوانين الدولية، وقد تم توظيف هذا المنهج في هذه الدراسة من خلال معالجة موضوع الهجمات السيبرانية ومدى شرعيتها والمسؤولية القانونية المترتبة على الأطراف التي تلجأ إليها.
- **المنهج التاريخي:** وذلك من خلال تتبع بداية استخدام مصطلح الهجمات السيبرانية منذ عام 1948 والبحث في المدة الزمنية التي شرعت أو قننت فيها القواعد القانونية ذات الصلة باستخدام طرائق القتال ووسائله في النزاعات المسلحة والحروب وخصوصا اتفاقيات لاهاي لعام 1899-1907 واتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977.
-

المبحث الاول

الهجمات السيبرانية وحق استخدام القوة في النزاعات الدولية

ستتناول الدراسة في هذا المطلب بيان مفهوم الهجمات السيبرانية ومدى خضوعها لأحكام القانون الدولي الإنساني في حالة النزاعات المسلحة الدولية وغير الدولية، عندما تستخدم كأداة أو سلاح في الهجمات المسلحة من خلال تسخير التكنولوجيا الإلكترونية للأغراض العسكرية. وبذلك سوف يتم تناول هذا الموضوع في هذا المبحث من خلال المطالب الآتية:

المطلب الأول: مفهوم الهجمات السيبرانية

المطلب الثاني: مدى خضوع الهجمات السيبرانية لأحكام القانون الدولي الانساني

المطلب الثالث: حق استخدام القوة في حالة الهجمات السيبرانية.

المطلب: الرابع: نطاق ارتكاب الهجمات السيبرانية ووصفها القانوني.

المطلب الاول: مفهوم الهجمات السيبرانية

وردت عدة تعريفات فقهيه للهجمات السيبرانية، لكن وتلافيا للوقوع بالإسهاب غير المفضل في إطار هذه الدراسة البحثية المختصرة والأكثر تركيزا، فإننا نشير فقط إلى التعريف الوارد في دليل تالين حيث عرف الهجمات السيبرانية بقوله: "هي عملية سيبرانية هجومية أو دفاعية يتوقع أن تتسبب في ايقاع ضحايا في صفوف الأشخاص سواء إصابة أو قتلا أو إلحاق الأذى بالأعيان سواء إضرارا أو تدميرا". ودليل تالين هو دليل لدراسات تداعيات الحروب والهجمات السيبرانية والقواعد المعيارية المنظمة لها، أصدره مجموعة من الخبراء العسكريين والقانونيين بمشاركة اللجنة الدولية للصليب الأحمر(الحديثي، 2021، ص21).

وحصل نوع من التوافق في الفقه الدولي على أن المقصود بالأضرار التي تترتب على الهجمات السيبرانية لا تقتصر فقط على الأضرار المباشرة؛ بل يشمل الأضرار غير المباشرة المتمثلة بتوقف المنشآت والأعيان المدنية عن العمل نتيجة الهجمات السيبرانية، فإن ذلك يعد ضررا غير مباشر للهجمات

السيبرانية(الرشيدي، 2021، ص31).

ويشير مصطلح الهجمات السيبرانية (Cyber Attack)، إلى تصرف يدور في عالم افتراضي يقوم على استخدام بيانات رقمية ووسائل اتصال تعمل بشكل إلكتروني، ومن ثم تطور ليتضمن مفهوماً أوسع يعمل على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، نتيجة اختراق مواقع إلكترونية حساسة، وغالباً ما تقوم بوظائف تصنف بأنها ذات أولولية، مثل نظام حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل نقل أخرى..(Saalbach, 2014, p6)

وقد تعرض مصطلح الهجوم السيبراني لعدة تعاريف من عدة زوايا، وإن مضمون معناها مشترك ومتقارب، وهو استهداف مواقع إلكترونية من خلال وسائل اتصال إلكترونية أخرى(Jonathan, 2010, p 3). ومن تلك التعاريف ما ذهب إليه شين (Shin) إذ عرفها بأنها: "استخدام الطيف الإلكتروني أو الكهرومغناطيسي من أجل تخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية ترتبط بها"..(Shin, 2011, p105)

كما عرفه فيورتس (Fuertes) بأنه "هجوم من خلال الانترنت يقوم على التسلل لمواقع إلكترونية غير مرخص بالدخول إليها من أجل تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي سلسلة هجمات إلكترونية تقوم بها دولة ضد دولة أخرى(Micheal, 2013, p1) .

ويبقى أن نشير هنا إلى أن دليل تالين قد استند إلى نص المادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف والصادر في عام 1977 للقول بوجود الالتزام الدولي لأغراض تقييم مشروعية استخدام أي نوع من أنواع الأسلحة الجديدة وهو النص الذي يستند إلية مؤيدو إدراج الهجمات السيبرانية تحت مظلة أحكام القانون الدولي الإنساني متى ارتكبت ضمن النزاعات المسلحة..(Saalbach, 2014, p7)

كما أنه وفي إطار تطبيق مبدأ التميز على الهجمات السيبرانية أشار دليل تالين إلى أنه بالرغم من عدم إلزامية قواعده، إلا أنه لا يجوز اتخاذ الأعيان المدنية هدفاً للهجمات السيبرانية، فعلى سبيل المثال لا يجوز توجيه الهجمات السيبرانية التي قد تدمر الأنظمة المدنية والبنية التحتية ما لم تعتبر تلك الأنظمة من قبيل الأهداف العسكرية التي لا يجوز استخدامها وفق الظروف السائدة (الفتلاوي، 2016، ص638). كما تضمن دليل تالين فيما يتعلق بالقانون المطبق على الحروب السيبرانية، وجوب الالتزام بمبدأ التناسب، من حيث حظر الهجمات السيبرانية التي قد تسبب الخسارة في أرواح المدنيين أو إصابتهم أو الإضرار بالأعيان المدنية (شميت، 2002، ص121).

المطلب الثاني: مدى خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني

نتناول في هذا الإطار بيان التوجهات القانونية والفقهية حول خضوع أو عدم خضوع الهجمات والحروب السيبرانية لأحكام وقواعد القانون الدولي الإنساني الفرق بين مصطلح الهجمات السيبرانية والحروب بالسيبرانية ام الهجمات السيبرانية اوسع نطاقا من الحروب السيبرانية فقد تكون الهجمات جزءا من حرب سيبرانية أو جزء من حرب تستخدم أسلحة تقليدية أو تنفذ في أوقات أخرى غير الحروب أي في أوقات السلم وهذا مطبق كثيرا في الواقع العملي، والتي انقسم الفقه القانوني بين مؤيد ورافض ولكل فريق حججه وأسانيده ومبرراته القانونية بالإضافة إلى ماله مما يؤكده في التطبيقات القانونية العرفية والاتفاقية في إطار القانون الدولي. وسنبين ذلك وفقا لما يلي:

اولا: عدم خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني.

لعل أهم انصار هذا الاتجاه هم جانب من الفقه الأوربي كالفقيه ميشال ولزر (Michael Walzer)، والفقيه توماس فرانك ك (Thomas Franck.M)حيث يرون بأن الفضاء السيبراني الإلكتروني الافتراضي هو منطقة خالية من القانون، وهو عبارة عن عالم افتراضي ولا يمكن أن يتحدد بدولة أو بجهة معينة، وبالتالي لا يمكن اخضاعه لأحكام القانون الدولي العام من جهة، ولأحكام القانون الدولي الإنساني من جهة أخرى والمتعلق بالنزاعات الدولية وغير الدولية من حيث تنظيم حق استخدام القوة ونوعية الأسلحة المسموح باستخدامها ومن حيث مراعاة الجوانب والاعتبارات الإنسانية المتعلقة بحماية المدنيين وغير المشتركين بالعمليات المسلحة والأعيان المدنية المتمثلة بالمستشفيات، ودور العبادة والمنشآت المتعلقة بالبنى التحتية (ناي، 1997، ص12).

ويعللون رأيهم هذا إلى أن المدة الزمنية التي شرعت أو قننت فيها القواعد القانونية ذات الصلة باستخدام طرائق القتال ووسائله في النزاعات المسلحة والحروب، وخصوصا اتفاقيات لاهاي لعام 1899-1907 واتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977 وكذلك مارست وتواترت عليه القواعد العرفية في نفس الإطار والتي تمثل أساس وجوهر القانون الدولي الإنساني قبل تقنين البعض من أحكامه (الفتلاوي، 2016، ص123).

ثانيا: خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني.

ويذهب أنصار هذا الرأي، والذين يمثلون جزءا مهما من فقهاء القانون الدولي كالفقيه ماركو روسيني (Roscini Marco) والفقيه شين (Shin) إلى أنه لا يوجد فراغ قانوني في الفضاء السيبراني، وأن القواعد القانونية العرفية والاتفاقية الموجودة في إطار القانون الدولي الإنساني كافية لتطبيقها على الهجمات والحروب السيبرانية كإجراء مقبول، وإلى حين التوصل إلى مرحلة تشريع قانون دولي إنساني ذو نصوص قانونية واتفاقيه واضحة

وصريحة في إشارتها للهجمات والحروب والعمليات السيبرانية (ناي، 1997، ص12).

كما أن مبدأ شرط "مارتينز"*والذي يعتبر جزءا مهما من القانون الدولي الإنساني العرفي، والذي ينص على عدم وجود حالة لا تغطيها اتفاقية دولية في إطار القانون الدولي الإنساني، وهذا يعني أنه ليس هنالك خلو أو فراغ قانوني وأن كل ما يقع اثناء النزاعات المسلحة هو يخضع لمبادئ القانون الدولي الإنساني، وهذا ما يؤكد رأي وتوجه أنصار هذا الرأي المؤيد لخضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني. (سعود، 2018، ص3).

ويقضي شرط "مارتينز" بأنه عندما كانت المعاهدات الدولية المنظمة لقانون النزاعات المسلحة غير كاملة، فكل ما لا يكون محظور صراحة بموجب معاهدة ما، لا يكون مسموحا به، والتفسير الأوسع نطاقاً لشرط مارتينز فيقضي بأنه لا يحكم على سلوك الدول أثناء النزاعات المسلحة، وفقا للمعاهدات والأعراف الدولية فقط، إنما أيضاً وفق مبادئ القانون العامة التي يشير إليها شرط مارتينز (ناي، 1997، ص85).

وهذا التفسير الواسع لمبدأ مارتينز قد يكشف أن الغرض منه هو ليس تنظيم وضع السكان المدنيين أثناء النزاعات المسلحة فقط، إنما غرضه تغطية الحالات التي لا يغطيها القانون الدولي الإنساني الاتفاقي والعرفي، ويمكن إثبات ذلك بالرجوع الى حيثيات مؤتمر السلام المعقود في مدينة لاهاي الهولندية لسنة 1899 إذ لم يشر مارتينز في عبارته لحصر نطاق تطبيق مبدئه على موضوع السكان المدنيين في الأراضي التي يتم احتلالها، وإنما حاول أن يسد الثغرة التي اعترت القانون الدولي الإنساني في هذا المجال، وذلك من خلال تسليط الضوء على العادات الراسخة بين الشعوب والقوانين الإنسانية ومقتضيات الضمير العام، لذلك ذهب البعض(سعود، 2018، ص3) الى تسمية شرط مارتينز بالمبدأ "البديل أو الاحتياطي " كونه مبدأً احتياطياً يطبق عند عدم توفر نص قانوني صريح يحمي الاشخاص المعنيين بالحماية.(jallo.c,2010,181-213)

وقد تم إدراج شرط مارتينز في اتفاقيات لاهاي لعام 1899-1907 وفي اتفاقيات جنيف الأربع لعام 1949 وفي الفقرة 2 المادة1 من البروتوكول الإضافي لعام 1977. بالإضافة إلى شمولية وعمومية قواعد القانون الدولي الإنساني التي تتيح تطبيقها على الهجمات السيبرانية عندما تستخدم كأداة وسلاح في النزاعات المسلحة الدولية وغير الدولية (الحديثي، 2021، ص120).

المطلب الثالث: حق استخدام القوة في حالة الهجمات السيبرانية

إن تطور القانون الدولي قد أنتج أو فرض قاعدة مهمة، هي حظر استخدام القوة المسلحة في إطار العلاقات الدولية بعد أن كانت الحروب والنزاعات المسلحة، واستخدام القوة أمرا مباحا لكن الحظر جاء وفقا لأحكام القانون الدولي كحد فاصل بين الإباحة والتقنين وفقا لأحكام نص المادة 2 فقرة 4 من ميثاق الأمم المتحدة حيث نصت على " يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة" (الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة).(moreno,2020,p287)

وقد ذهب جانب من الفقه القانوني لاعتبار أن المفهوم الواسع لنص المادة 2 من ميثاق الأمم المتحدة يشمل الهجمات السيبرانية سواء اتخذت شكل هجمات عسكرية مباشرة أو كانت ذات تأثيرات على الجوانب الاقتصادية والبنى التحتية وبما يؤثر بشكل أو بآخر على حياة المدنيين والأعيان المدنية. ويكون المعيار هنا هو معيار الآثار المدمرة التي تترتب على الهجمات السيبرانية التي ربما تكون أكثر جسامة من الهجمات بالأسلحة التقليدية أو تعادلها في ذلك(الفتلاوي، 2013، ص127).

وبالرغم من اتفاق فقهاء القانون الدولي مثل ماركو روسيني(Marco Roscini) بأن التهديد باستخدام القوة المقصود به القوة المادية العسكرية الحركية إلا أن ذلك لا يعني إعطاء الشرعية القانونية للهجمات السيبرانية ولا يعفي الدول من المسؤولية الدولية المترتبة على خرق أحكام المادة 2 من ميثاق الأمم المتحدة في حالة أدت الهجمات السيبرانية إلى آثار مادية ملموسه في الأعيان المدنية أو العسكرية.(Tomar, 2014, p152)

ويكون من المهم أن نشير في هذا الإطار إلى الاستثناءات الواردة على قاعدة حظر استخدام القوة في العلاقات الدولية بموجب ميثاق الأمم المتحدة وكما يلي:

أولا: حق الدفاع الشرعي عن النفس.

يعتبر حق الدفاع الشرعي عن النفس استثناء جوهرياً على قاعدة حظر استخدام القوة في إطار القانون الدولي والمشار إليه في المادة 51 من ميثاق الأمم المتحدة عند تحقق شروط حالة الدفاع الشرعي الواردة فيها من حيث الشرط التعاهد والضرورة والتناسب والفورية (فورية الرد) وهذا ما أكدته محكمة العدل الدولية في قرارها الذي يؤكد على لزوم توفر تلك الشروط في قضية نيكارغوا لعام 1986، وهي قضية عرضت على محكمة

*ظهر شرط مارتينز لأول مرة من خلال الرأي الذي أدلى به فيورد فيورج مارتينز مندوب قيصر روسيا) نيكولاس الثاني (في مؤتمر السلام لسنة 1899 والذي عد وقتها أقوى الحيل الدبلوماسية التي استخدمت في المفاوضات الدولية حول الوضع القانوني للمدنيين)

العدل الدولية عام 1986، التي أقرت خرق الولايات المتحدة للقانون الدولي، وذلك بدعمها للمعارضة المسلحة في الحرب ضد حكومة نيكاراغوا، وتفخيخ الموانئ في نيكاراغوا. وقد حكمت المحكمة لصالح نيكاراغوا ضد الولايات المتحدة الأمريكية، الأمر الذي دفع أمريكا إلى رفض الحكم الذي صدر بحقها، وأقرت المحكمة بأن الولايات المتحدة قامت باستخدام القوة بشكل غير شرعي، «لقد أوقعت حرب ريغان ضد نيكاراغوا نحو 75 ألف ضحية، بينهم 29 ألف قتيل، ودمرت بلدا لا رجاء لقيامته» (سعودي، 2018، ص341).

وعليه فإن الهجمات السيبرانية التي تستهدف سيادة الدول تمثل انتهاكا لحظر استخدام القوة الوارد في المادة (2) من الميثاق، مما يسمح بتفعيل حق الدفاع الشرعي وفقا لاحكام المادة (51) من ميثاق الامم المتحدة من قبل الدول التي تقع ضحية الهجمات السيبرانية ويعطيها حق استخدام القوة ضد الدول المعتدية سيبرانيا.(العبيدي، 2021، ص117).

ثانيا: تدابير حماية الأمن والسلم الدوليين

وهنا نؤكد مسالة شرعية اتخاذ التدابير الجماعية استنادا لأحكام الفصل السابع من ميثاق الامم المتحدة في المواد من 39-51 حيث خول الميثاق لمجلس الأمن الدولي اتخاذ الإجراءات الكفيلة بالحفاظ على السلم والأمن الدولي، وهذه الإجراءات تبدأ بالإجراءات الدبلوماسية والاقتصادية والإجراءات العسكرية كحل أو إجراء أخير، وهذه الصلاحية تعطي لمجلس الأمن سلطة اتخاذ الإجراءات الكفيلة عندما يتعرض السلم والأمن الدولي للخطر، ولعل المفهوم الواسع لنص المادة 42 من الميثاق يعطي صلاحيات واسعه. وقد نصت المادة 42 من ميثاق الأمم المتحدة على (إذا رأى مجلس الأمن أن التدابير المنصوص عليها في المادة 41 لا تفي بالغرض أو ثبت أنها لم تف به، جاز له أن يتخذ بطريق القوات الجوية والبحرية والبرية من الأعمال ما يلزم لحفظ السلم والأمن الدولي أو لإعادته إلى نصابه. (المادة 42 من ميثاق الأمم المتحدة).(revdams,2012,p933)

المطلب الرابع: نطاق ارتكاب الهجمات السيبرانية ووصفها القانوني

إن الهجمات السيبرانية كأسلوب حديث في النزاعات والصراعات الدولية، قد يكون محلها هو الحروب والنزاعات المسلحة الدولية وغير الدولية؛ أي ترتكب في إطار مختلط أو بالتزامن أو بالتعاون بينها وبين الهجمات بالأسلحة التقليدية، ويكون نطاقها القانوني هنا هو القانون الدولي الإنساني عندما تعمد أطراف النزاعات المسلحة إلى تنفيذ أو القيام بأساليب ووسائل الحرب التي تعتمد على العمليات السيبرانية. أما الهجمات ذات الطبيعة غير العسكرية، وهي التي لا تكون جزءا من نزاع مسلح، وإنما ترتكب بشكل منفرد وليس لها صلة بنزاع مسلح، ولكن قد يترتب عليها آثار تدميرية أيضا في البنى التحتية، والمنشآت الصناعية والخدمية وشبكات الاتصالات مثلاً، فالهجمات السيبرانية غير العسكرية تخضع أيضا لحظر استخدام القوة في العلاقات بين الدول، وفقا لنص المادة 2 فقرة 4 من ميثاق الأمم المتحدة، وهذا ما استقر عليه الفقه القانوني الدولي، والتطبيقات العملية(الرشيدي، 2021، ص158).

ومن الجهود الدولية التي تهدف لتنظيم الهجمات السيبرانية، تطبيق نصوص وصكوك قانونية تنطبق بصورة مباشرة على الهجمات السيبرانية، وقد شكلت تلك النظم القانونية إلى حد كبير قبل ظهور الهجمات السيبرانية، بالتالي فهي لا تحظر أو تنظم الهجمات السيبرانية بصورة مباشرة وصريحة، إلا أن تلك الأطر تنطبق على الهجمات السيبرانية إذا ما استخدم الهجوم الوسائل المعينة التي تنظمها الاتفاقية المعينة بذلك، ومن تلك النصوص القانونية قانون الاتصالات، إذ أن تنظيم قانون الاتصالات الدولي الحديث من قبل الاتحاد الدولي للاتصالات، وهو وكالة تختص في مجال تكنولوجيا الاتصالات والمعلومات تابعة للأمم المتحدة. (الاتحاد الدولي للاتصالات ITU 2020، https://www.itu.int/ar/Pages/default.aspx).

وبالرغم من القيود المذكورة في دستور الاتحاد الدولي للاتصالات إلا أن تلك الاتفاقية لا تحظر على وجه التحديد استخدام الاتصالات للأغراض العسكرية، إذ تحتفظ الدول الأعضاء في الاتفاقية بحرية مطلقة في استخدام منشآتها الاتصالية العسكرية(المادة 34 من دستور الاتحاد الدولي للاتصالات)، طالما تتخذ كافة الخطوات اللازمة لمنع أي تدخل ضار(مادة 2/48 من دستور الاتحاد الدولي للاتصالات).وعليه، فإن عبارة "منع أي تدخل ضار" في نصوص تلك الاتفاقية، قد تشمل الهجمات السيبرانية. كما أن هناك قانون آخر في ذات الشأن ألا وهو قانون الطيران المدني، والذي يحتوي على صكوك رئيسية ثلاثة قد تنطبق على الهجمات السيبرانية، إذ تمثل الصك الأول باتفاقية شيكاغو لعام 1944 للطيران المدني، إذ تتعهد الدول الأعضاء في هذه الاتفاقية عند إصدار اللوائح التي تتعلق بطائراتها الحكومية مراعاة سلامة ملاحة الطائرات المدنية(مادة 3 من اتفاقية شيكاغو للطيران المدني لعام 1944). بالتالي، فالجهوم السيبراني الذي يستهدف الرحلات الجوية المدنية، إذا وجه من قبل دولة ما ضد طائرات مدنية تتبع دولة أخرى، قد يتعارض وضمانات تلك الاتفاقية بخصوص سلامة ملاحة الطائرات المدنية، أما الصك الثاني فيتمثل في اتفاقية مونتريال لعام 1971 التي حددت عددا من الأفعال غير المشروعة التي تهدد سلامة الطائرة، وترتكب عن قصد، بالتالي تعرض سلامة تلك الطائرة للخطر في حالة الطيران (مادة 1 من اتفاقية مونتريال لعام 1971)، على سبيل المثال، يتمثل ذلك الهجوم الذي يعرض أمن وسلامة تلك الطائرة للخطر في التخاذل بنظام تشغيل الطائرة، والتدخل في اتصالات مراقبة الحركة الجوية (الموصلي، 2021، ص29). والصك الثالث والأخير فيتمثل في بروتوكول مونتريال لعام 1988 الخاص بقمع أعمال العنف غير المشروعة في المطارات التي تخدم الطيران المدني الدولي، حيث وسع هذا البروتوكول الإطار القانوني لقمع

أعمال العنف غير المشروعة في المطارات التي تخدم الطيران المدني (مادة 1 من اتفاقية مونتريال لعام 1971).

كما تم وضع قانون آخر من شأنه تنظيم الهجمات السيبرانية كقانون الفضاء الخارجي، إذ يحتوي هذا القانون على نصوص وقواعد قانونية يمكن تطبيقها على الهجمات السيبرانية، وهذا الانطباق يعود في الأساس من حقيقة أن الشبكات العالمية والجوانب الرئيسة لتكنولوجيا المعلومات الحديثة معتمدة على منصات فضائية متعددة تدور حول الأرض لدعم المحطات الأرضية، كما أن تلك المنصات الفضائية لها أهمية كبيرة لمواجهة الهجمات السيبرانية وذلك باعتبار أن تلك المنصات الأكثر ضعفاً في نظام المعلومات كونه يستحيل صد أي هجوم قد يقع عليها. وعليه، فقد تندرج الهجمات السيبرانية في إطار قواعد قانونية تنظم الأنشطة في الفضاء التي تم صياغتها في معاهدة الفضاء الخارجي عام 1967 التي عرفت باسم "معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى". (نعوس، 2013، ص784).

أما القانون الأخير الذي نظم الهجمات السيبرانية قانون البحار، حيث تتضمن اتفاقية الأمم المتحدة لقانون البحار عام 1982 على قواعد قانونية عدة يمكن أن تطبق بصورة ثانوية على أنشطة الهجمات السيبرانية، حيث نصت تلك الاتفاقية على حق السفن بالمرور إذا كانت أنشطتها غير مضرة بالسلام، وحسن النظام، وأمن سواحل الدولة (المادة 19 من اتفاقية الأمم المتحدة لقانون البحار لعام 1982).

ويمكننا القول أن القوانين الدولية سواء التي تنظم الاتصالات أو الطيران أو الفضاء أو البحار، حتى وإن كانت تنطبق على الهجمات السيبرانية بصورة جزئية في نطاق اختصاص كل منها، إلا أنها غير كافية للتصدي لتلك الهجمات، كونها نصوص غير متماسكة ولا تقدم آلية كاملة لمواجهة الهجمات السيبرانية، إذ أنها تقدم فقط مجموعة أنظمة مختلطة، التي تترك كثير من الهجمات السيبرانية الضارة دون معالجة.

المبحث الثاني: انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية

إن النطاق المادي للقانون الدولي الإنساني هو في حالة قيام النزاعات المسلحة التي تستخدم فيها كافة الأنواع من الأسلحة التقليدية والسيبرانية، سواء كانت نزاعات مسلحة دولية أو غير دولية، ولغرض بيان مدى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية، فإننا بصدد تناولها من حيث شموليتها باعتبارها تنطبق على وصف النزاعات المسلحة عامة، وكذلك نبين الخصوصية التي تتمتع بها النزاعات المسلحة التي تستخدم فيها الأدوات والأساليب الإلكترونية، وتحت عنوان الهجمات السيبرانية كأسلحة مستخدمة في النزاعات المسلحة سواء بشكل منفرد أو متواز ومتزامن مع استخدام الأسلحة التقليدية.

وعليه، سيتم تناول هذا مدى انطبقا مبادئ القانون الدولي الإنساني على الهجمات السيبرانية، وذلك من خلال المطالب الآتية:

المطلب الاول: مبدأ الضرورة العسكرية بين الشمولية، وخصوصية الهجمات السيبرانية

المطلب الثاني: مبدأ التناسب بين الشمولية، وخصوصية الهجمات السيبرانية

الفرع الثالث: مبدأ التمييز بين الشمولية، وخصوصية تطبيقه على الهجمات السيبرانية

المطلب الرابع: مبدأ الانسانية بين شموليته، وخصوصية الهجمات السيبرانية

المطلب الاول: مبدأ الضرورة العسكرية بين الشمولية وخصوصية الهجمات السيبرانية

أشار دليل (تالين) إلى أنه في حالات يكون فيها الخيار ممكناً بين أهداف عسكرية عديدة من أجل الحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره من أجل الهجوم السيبراني، هو الهدف الذي يتوقع منه أن يسبب خطرا أقل على المدنيين، والأعيان المدنية، ويتطلب تطبيق مبدأ الضرورة العسكرية ومراعاته، أن يختار الهجوم الذي يؤدي لتسبب إصابات وأضرارا أقل، أما في حال وجود عدد من الأهداف، وأن إحداها تحقق ميزة عسكرية أكثر من مثيلاتها، فهنا من حق المهاجم أن يوجه الهجمات السيبرانية المباشرة ضد الهدف العسكري الذي يحقق أكثر ميزة عسكرية ممكنة في إطار النزاع المسلح (شميت، 2002، ص105).

وبالنظر للخصوصية التي تتميز بها الهجمات السيبرانية عند استخدامها كسلاح في النزاعات المسلحة نظرا للطبيعة الخاصة بها، وبقدر تعلق الأمر بتطبيق مبدا الضرورة العسكرية عليها، فإنه في الحالات التي يكون هنالك خيار بين عدة أهداف عسكرية؛ لتحقيق غاية الميزة العسكرية المطلوبة، ويتم اختياره من خلال تنفيذ هجمات سيبرانية، فتكون الجهة المستخدمة له ملزمة بمراعاة مبدأ الضرورة العسكرية، وتقليل الأخطار التي قد يتعرض لها المدنيين والأعيان المدنية وغير المشتركين في العمليات والنزاعات المسلحة. حيث يتم مراعاة تقليل المخاطر والآثار المدمرة أو التي تؤثر على الحياة العامة للمدنيين. (الحديثي، 2021، ص130).

ومبدأ الضرورة العسكرية يسمح فقط باستخدام النوع والدرجة من القوة غير المحظورة، التي تكون ضرورية من أجل تحقيق الغرض المقصود والمشروع من النزاع المسلح، وهو اخضاع العدو بشكل كامل أو جزئي، وبأقل قدر ممكن من التضحية في الأرواح والموارد، وبالتالي يمنع في هذا الشأن

تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تستوجب هذا التدمير والحجز(فقرة 3 من المادة 57 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة.1977). كما يحظر بموجب مبدأ الضرورة العسكرية، إلحاق الإصابة والألم التي ليس لها مبرر، بالتالي فإن هذا المبدأ يحظر اللجوء للوسائل والأساليب الحربية التي لا تحظر استخدامها قاعدة أخرى من قواعد القانون الدولي الإنساني مبرر(الفقرة 2 من المادة 35 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة 1977).

المطلب الثاني: مبدأ التناسب بين الشمولية وخصوصية الهجمات السيبرانية

مبدأ التناسب من المبادئ المهمة التي تمثل القانون الدولي الإنساني، وهو مبدأ ذو شمولية تتسع لجميع النزاعات المسلحة الدولية وغير الدولية، التي تستخدم مختلف الأسلحة فيها بالعادة، ومبدأ التناسب ذو طبيعة ميدانية عملية، والذي يحظر شن هجوم مسلح، قد يؤدي إلى خسائر جانبية في أرواح المدنيين وممتلكاتهم أو بالأعيان المدنية والبنى التحتية. ولابد من الإشارة الى أنه تم اعتماد هذا المبدأ في المواد 51 و57 من البروتوكول الإضافي الملحق باتفاقيات جنيف لعام 1977.

وفي إطار خصوصية الهجمات السيبرانية عندما تكون سلاح أو أداة عسكرية في إطار النزاعات المسلحة، نجد أن هنالك صعوبة في تطبيق هذا المبدأ ترتبط بعدم إمكانية الفصل بين الفضاء السيبراني المستخدم للأغراض المدنية أو من قبل المدنيين، وبين الفضاء السيبراني المستخدم للأغراض العسكرية عندما تستخدمه أطراف النزاعات المسلحة، ولأن مبدأ التناسب يتضمن إجراء نوع من الموازنة بين المعاناة أو التدمير، وبين الميزة العسكرية المبتغاة؛ لأننا أمام فقدان لمعايير واضحة لتقييم ما هو مقبول من درجة المعاناة الإنسانية المقبولة عند تعطيل بعض المنشآت المدنية التي توفر أو تضمن استمرار تقديم الخدمات الأساسية للمدنيين، كالكهرباء والاتصالات والخدمات الطبية مثلا، التي سوف يكون لتوقفها أو تدميرها أثر حقيقي للهجمات السيبرانية التي يترتب على القيام بها إيقاف تلك الخدمات المرتبطة بالجانب الإنساني (الحديثي، 2021، ص132).

وبالرغم من تلك الصعوبات في تطبيق مبدأ التناسب وفقا لما ينبغي في إطار ارتكاب هجمات سيبرانية، إلا أننا نجد أن دليل (تالين) المطبق في حالة الحروب والهجمات السيبرانية، قد أشار إلى تطبيق مبدأ التناسب من حيث منع القيام بهجمات سيبرانية يترتب عليها خسائر بين أرواح المدنيين أو إصابات أو أضرار تصيب الأعيان المدنية، والتي يكون فيها نوع من المغالاة والإفراط غير المبرر لا يتناسب مع غاية تحقيق الميزة العسكرية التي يراد الحصول عليها أو تحصيلها باستخدام هجمات سيبرانية (شميت، 2002، ص107).

المطلب الثالث: مبدأ التمييز بين الشمولية وخصوصية تطبيقه على الهجمات السيبرانية

نتيجة المآسي التي كانت تترتب على النزاعات المسلحة، عندما كان المدنيون والعسكريون والأعيان المدنية هدفا مشروعا لتلك النزاعات على حد سواء، ونتيجة لتطور قواعد القانون الدولي الإنساني، فقد اختلفت النظرة تجاه الجهات التي يمكن أن يسمح بأن تكون هدفا للعمليات العسكرية بحيث يحصل اهتمام كبير بالفئات المستضعفة، لاسيما المدنيين الذين كانوا من أكثر ضحايا النزاعات المسلحة سابقا؛ لعدم وجود قواعد قانونية تحميهم، والمقصود بالمدنيين هنا هم غير المقاتلين، والذين لا يشتركون في العمليات العسكرية حسب المفهوم العام، ومنهم المدنيين طبعا، بالإضافة للأعيان المدنية، فأسبغ عليهم القانون الدولي الإنساني الحماية القانونية ومنع استهدافهم (الطراونة، 2016، ص191).

وتكون الهجمات العشوائية، هي الهجمات التي لا تكون موجهة لهدف عسكري معين، أو تلك التي تستخدم أسلوب أو وسيلة قتال لا يمكن توجيهها إلى هدف عسكري محدد، أو هي الهجمات التي تستخدم طريقة أو وسيلة قتال لا يمكن تحديد آثارها على النحو الذي يقتضيه القانون الدولي الإنساني، بالتالي فمن شأنها في كل حالة من تلك الحالات أن تصيب أهدافاً عسكرية وأعيان مدنية ومدنيين دون تمييز (الفقرة (9)من المادة (59)من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة 1977).ونظرا لأهمية حماية الأعيان المدنية، فقد وضعت قواعد وبنود لحمايتها ضمن الإعلانات والمواثيق والاتفاقيات الدولية، ومنها إعلان سان بطرسبرغ لعام 1868 وكذلك ما نصت عليه لائحة لاهاي لعام 1907(نصت لائحة لاهاي لعام 1907 على "أن حق الأطراف المتحاربين في اختيار وسائل القتال وأساليبه ليس بالحق غير المحدد).وكذلك ما نصت عليه اتفاقية جنيف الرابعة الخاصة بحماية المدنيين، ومن ثم البروتوكول الأول لعام 1977وما نصت عليه المادة 48 منه(نصت المادة 48 من البروتوكول الإضافي الأول لعام 1977 على: تعمل أطراف النزاع على التمييز بين السكان المدنيين المقاتلين، وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجيه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تامين احترام، وحماية السكان المدنيين والأعيان المدنية).

ونظراً لشمولية وعمومية والزامية تلك القواعد، فإنه من الممكن أن تنطبق على الهجمات السيبرانية، ولكن ونظرا للطبيعة الخاصة للهجمات السيبرانية باعتبارها سلاح في النزاعات المسلحة، ولكونها ترتكب أو تنفذ في فضاء سيبراني مشترك مع المدنيين ووجود حالة مؤكدة من التشابك والتداخل بينهما، مما يمثل صعوبة في توجيه الهجمات السيبرانية ضد العسكريين فقط دون المساس بالمدنيين، وفقا لأحكام القانون الدولي الإنساني. (شميت، 2002، ص 109).

المطلب الرابع: مبدأ الإنسانية بين شمولية وخصوصية الهجمات السيبرانية

يلعب مبدأ الإنسانية دورا مهما في احترام وحماية حقوق الإنسان خلال النزاعات المسلحة الدولية وغير الدولية، ويؤكد على المكانة المهمة التي يتمتع بها الإنسان وفقا لأحكام القانون الدولي الإنساني، ويؤكد هذا المبدأ على الابتعاد عن الأعمال الوحشية والانتقامية والبربرية التي تتعارض مع الطبيعة البشرية والإنسانية، وبالتالي يؤكد هذا المبدأ على احترام كرامة الإنسان في جميع الأوقات بما في ذلك أوقات النزاعات المسلحة.(الطراونة، 2016، ص192).

ويمكن القول، أنه إذا ما أردنا تطبيق مبدأ الإنسانية على الهجمات السيبرانية، والذي من تطبيقاته عدم التسبب بالآلام غير مبررة أو مجازر لا مبرر لها، فنستطيع القول إن تطبيق مبدأ الإنسانية على الهجمات السيبرانية يكون قريب جدا من صور وآليات تطبيقه في النزاعات المسلحة التي تستخدم فيها الأسلحة التقليدية من حيث ضرورة الالتزام بعدم التسبب بالآلام، وايقاع ضحايا لا مبرر لها. كما أن هنالك إشكالية في إمكانية تطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية نظرا للطبيعة الخاصة للهجمات السيبرانية كنوع جديد من الأسلحة دخلت ميدان النزاعات المسلحة حديثا. وهنا يمكننا إضافة مبدأ مهم آخر ربما يكون أوضح من غيره، يتعلق بتحريم استخدام أنواع معينه من الأسلحة في النزاعات الدولية، وهو مبدأ مهم جدا يتعلق بما هو مسموح أو محرم استخدامه من الأسلحة خلال النزاعات المسلحة.

كما استغلت روسيا سلاح الهجمات السيبرانية في نزاعاتها الأخيرة، كغزوها لجورجيا في عام 2008، وللقِرم في عام 2014، ومنذ ذلك الحين، أصبحت أوكرانيا "ساحة تدريب" لعمليات الحرب الروسية السيبرانية، إذ أنه بين عامي 2015 و2016، عطَّلت الهجمات المنسوبة لروسيا شبكات الطاقة في أوكرانيا لعدة ساعات، وهو ما دفع روسيا لتبقي أسلحتها السيبرانية الأقوى في جعبتها، لتزيد وتيرة هجماتها السيبرانية في حالة تعثُّر الحرب البرية، أو تضرُّرها من العقوبات المالية، (جيني، 2022).

وعليه، وبخلاف ما تقدم، فإن استخدام القوة في العلاقات الدولية، يعتبر عملاً غير مشروع وفق ميثاق الأمم المتحدة، والذي نص على: "يمتنع أعضاء المنظمة جميعاً في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو أي وجه آخر غير متفق مع مقاصد الأمم المتحدة (فقرة 4 من المادة 2 من ميثاق الأمم المتحدة).

وإذا كنا قد تطرقنا لشمولية مبدأ الإنسانية في قواعد القانون الدولي الإنساني، إلا أن ذلك لا يعني أن ننكر حقيقة التغيرات التي شهدتها طبيعة الحروب منذ أن تم اعتماد اتفاقية جنيف الأصلية، حيث أصبحت أداة ووسائل للحروب المتطورة لدرجة لم يكن يتصورها واضعي تلك الاتفاقية، ولعل استخدام الفضاء السيبراني المتزايد من أجل الأغراض العسكرية يعتبر أحد أبرز المبررات التي تدعو لإعادة النظر في القواعد التي تنظم سير النزاعات المسلحة، وصياغتها بشكل يتلاءم وطبيعة تلك الاستخدامات(Jeffrey, 2008) .

وعليه يمكننا القول إن المنظومة القانونية الدولية الحالية بحاجة إلى تشريع قواعد قانونية على شكل اتفاقيات دولية ملزمة وواضحة، تتفق مع الطبيعة الخاصة للهجمات السيبرانية أثناء ارتكابها أو القيام بها خلال النزاعات المسلحة الدولية وغير الدولية.

الخاتمة والنتائج والتوصيات

في خاتمة الدراسة التي تناولنا فيها بيان مدى إمكانية تطبيق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية، باعتبارها سلاح وأداة تستخدم في النزاعات المسلحة الدولية وغير الدولية مع مراعاة الطبيعة الخاصة التي تتميز بها الهجمات السيبرانية عن غيرها من الأسلحة التقليدية المستخدمة في النزاعات المسلحة، فقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات، كما يلي:

اولا: النتائج:

في نهاية هذه الدراسة تم التوصل إلى النتائج الآتية:

1- مازال مفهوم الهجمات السيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي على تعريفها حتى هذا اليوم، وبالرغم من ذلك لا تحدث في فراغ قانوني، إذ يمكن الاستناد في ذلك للمادة 36 من البروتوكول الإضافي لعام 1977. وقرارات محكمة العدل الدولية من خلال رأيها بمشروعية التهديد بالأسلحة النووية أو استخدامها.

2- تستخدم الهجمات السيبرانية في أوقات النزاعات المسلحة؛ فتخضع لأحكام القانون الدولي الإنساني أو تقع في أوقات السلم؛ لكنها تمثل أيضا اعتداء على أمن وسيادة الدول، فتعتبر انتهاك لأحكام ميثاق الأمم المتحدة، وتوجب المسؤولية الدولية.

3- تخضع الهجمات السيبرانية التي تحدث في سياق النزاع المسلح الحركي للقانون الدولي الإنساني، إلا أن التحدي الأكبر هو تلك الهجمات التي تحدث خارج سياق النزاع المسلح الحركي، ومدى إمكانية اعتبارها نزاع مسلح، وإثبات نسبة الهجوم لدولة ما، بالتالي إمكانية تطبيق القانون الدولي الإنساني عليها أيضاً.

4- من أجل معرفة مدى إمكانية انطباق قواعد ومبادئ القانون الدولي على الهجمات السيبرانية التي تحدث ضمن النزاع المسلح الحركي، يجب

تكييف الهجوم السيبراني لمعرفة مدى انطباق مصطلح النزاع المسلح سواء الدولي أم غير الدولي، من ثم يأتي دور تطبيق المبادئ، وقواعد القانون الدولي الإنساني.

5- هنالك توجهين مختلفين في مسالة خضوع وعدم خضوع الهجمات السيبرانية لأحكام القانون الدولي، لكن الرأي الراجح هو خضوعها لتلافي الوقوع في إشكالية التهرب من المسؤولية الدولية، وبالتالي ارتكاب المزيد من المجازر بحق المدنيين نتيجة استخدام الهجمات السيبرانية كسلاح.

6- إن ظهور الهجمات السيبرانية كأسلوب جديد يستخدم في النزاعات المسلحة الدولية وغير الدولية ومع عدم وجود منظومة قانونيه واضحة تحكم التعامل مع هذا التطور التكنولوجي والنوعي إلا انه في نفس الوقت لا يمكن التسليم بعدم القدرة على اخضاع الهجمات السيبرانية لأحكام القانون الدولي من خلال استغلال ما هو متوفر من أحكام القانون الدولي الإنساني العرفي.

7- إن مبادئ القانون الدولي الإنساني كمبدأ الضرورة العسكرية والتناسب والتمييز والإنسانية هي مبادئ تتمتع بصفة الشمولية والعمومية، وقابليتها للتطبيق على الهجمات السيبرانية مع مراعاة خصوصية تلك الهجمات باعتبارها سلاح جديد ومتطور، قد دخل حديثا في ميدان النزاعات المسلحة الدولية وغير الدولية.

8- تعد الهجمات السيبرانية الروسية إحدى أهم أدوات موسكو في إطار حربها على أوكرانيا والغرب، وقد شكلت سابقاً آداه مرنة لضرب مجموعة من الأهداف في أوكرانيا وخارجها.

ثانيا: التوصيات:

في ضوء ما توصلت إليه الدراسة من نتائج، تم صياغة التوصيات الآتية:

1- توصي الدراسة بأهمية استمرار الجهود الدولية لتطويع ما توفر من أعراف دولية، ونصوص اتفاقيه في إطار القانون الدولي الإنساني لتطبيقها على الهجمات السيبرانية كلما كان ذلك ممكننا، خصوصا مع وجود هذه المكنة نتيجة عمومية وشمولية مبادئ وقواعد القانون الدولي الإنساني لحين التوصل إلى اتفاق دولي؛ لتشريع قانون دولي إنساني يشمل الهجمات السيبرانية.

2- قيام المجتمع الدولي بالإسراع في الوصول إلى قانون دولي إنساني صريح، وملزم يتضمن الهجمات السيبرانية باعتباره سلاح نوعي جديد، دخل ميدان النزاعات المسلحة والتعاملات الدولية بقوة، ولا مناص من خضوعه للمنظومة القانونية في القانون الدولي.

3- ضرورة إدخال تعديلات جوهريه كي تتسع الاتفاقيات الدولية للهجمات السيبرانية، ومنها ميثاق الأمم المتحدة فيما يتعلق باعتبار الهجمات السيبرانية اعتداء يعطي الحق باعتماد الاستثناء أو التصريح باستخدام القوة دفاعا عن النفس أو تدابير الأمن الجماعي من خلال مجلس الأمن الدولي، وينص على ذلك صراحة. وكذلك تعديل النصوص الحاكمة في اتفاقيات جنيف الأربعة لعام 1949 والبروتوكولين الإضافيين الملحقين بها، وكذلك أحكام اتفاقيات لاهاي إلى حين التوصل إلى اتفاقيات دوليه ملزمة في إطار القانون الدولي الإنساني يشمل بشكل واضح وصريح الهجمات السيبرانية.

4- العمل على تزويد الجيوش بمهارات وتقنيات التعامل مع التهديدات السيبرانية، وذلك من خلال تدريب المهندسين المعلوماتيين في القوات المسلحة وتعليمهم، وإكسابهم مهارات الأمن السيبراني؛ ليكونوا قادرين على تولي مسؤولية حماية البنى التحتية الوطنية من تهديدات الهجمات السيبرانية الحالية والمستقبلية.

5- ضرورة التواصل مع خبراء معلوماتيين من أجل إيجاد برمجية ما، تعمل على فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية، وذلك من أجل حماية السكان المدنيين من مخاطر الهجمات السيبرانية.

6- على الدول الكبرى استغلال التطور التكنولوجي في مجال الثورة المعلوماتية بما يخدم رفاه الدول بشكل عام، والإنسان على وجه الخصوص، بدلا من تسخيرها في الحروب والصراعات.

المصادر والمراجع

جيني، إ. (2022). *باحثون يحللون استراتيجية الحرب السيبرانية الروسية التي خالفت التوقعات*، مجلة نيتشر 20 on أبريل 2022، المجلد (31)، العدد(2)، منشورة على الرابط: https://www.scientificamerican.com/article/where-is-russias-cyberwar-researchers-decipher-its-strategy/

الحديثي، ص. (2021). *التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية*. (ط1). مصر: منشورات المجموعة العلمية للطباعة والنشر والتوزيع.

الرشيدي، هـ. (2021).*الإرهاب السيبراني*، ماهيته ووجوده ومكافحته. (ط1). القاهرة: منشورات دار النهضة العربية للنشر والتوزيع.

سعود، آ.(2018). *شرح مبسط لشرط مارتينز في أحكام القانون الدولي الإنساني*، الحوار المتمدن-العدد: 5810 – 2018 / 3 / 9 – 22:12: https://www.mohamah.net/law

سعود، ي. (د.ت). الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، *المجلة القانونية- مجلة متخصصة في الدراسات والبحوث العلمية، 1(1)*: 18-37.

سمودي، ر. (2018). حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، *مجلة جامعة الشارقة للعلوم القانونية*، 15(2):341-342

شميت، م.(2002). الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكومبيوتر، *المجلة الدولية للصليب الأحمر*، 2(4): 37-71.

الطراونة، م. (2016). *الوسيط في القانون الدولي الإنساني*. (ط1). عمان: منشورات دار وائل للنشر والتوزيع.

العبيدي، ع. (2021). *مكافحة الجرائم السيبراني كآلية لتعزيز الأمن الإقليمي*. (ط1). مصر: منشورات مركز الدراسات العربية.

الفتلاوي، أ. (2016). الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، *مجلة المحقق للعلوم القانونية والسياسية*،4(8): 610-678.

الفتلاوي، أ.(2018).*الهجمات السيبرانية، دراسة قانونية تحليلية*. (ط1). بيروت: منشورات زين الحقوقية.

كلنتر، ز. (2016). *المسؤولية الدولية الناشئة عن الهجمات السيبرانية*، رسالة ماجستير، جامعة الكوفة-كلية القانون، جمهورية العراق

الموصلي، ن. (2021). الهجمات السيبرانية في ضوء القانون الدولي الإنساني، بحث مقدم استكمالاً لمتطلبات نيل درجة الماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية.

ناي، ج.(1997)، *المنازعات الدولية– مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل*، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة.

نعوس، م. (2013). حقوق والتزامات الدول في الحرب المعلوماتية، مجلة دراسات علوم الشريعة والقانون، المجلد(1)، العدد(2)

التشريعات والوثائق والاتفاقيات الدولية

ميثاق الأمم المتحدة

اتفاقيات جنيف الأربع لعام 1949

البروتوكولان الإضافيان الملحقان باتفاقيات جنيف لعام 1977

اتفاقيات لاهاي لعام 1899-1907

دليل تالين المتعلق بإخضاع الهجمات السيبرانية لأحكام القانون الدولي الإنساني لعام 2015-2017

اتفاقية شيكاغو للطيران المدني الدولي لعام 1944، المادة 3.

اتفاقية مونتريال لعام 1971 لقمع الأعمال غير المشروعة ضد الطيران المدني،

بروتوكول مونتريال لعام 1988 لقمع أعمال العنف غير المشروعة في المطارات التي تخدم الطيران المدني الدولي.

اتفاقية الأمم المتحدة لقانون البحار لعام 1982

اتفاقية مونتريال لعام 1971 لقمع الأعمال غير المشروعة ضد الطيران المدني.

دستور الاتحاد الدولي للاتصالات، موقع الجزيرة، نشر في2020/12/4،الموقع الرسمي:https://www.itu.int/ar/Pages/default.aspx

References

Jeffrey, T. (2008). Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 106(7), Available at: *https://repository.law.umich.edu/mlr/vol106/iss7/6*.

Micheal S. Fuertes, (2013). *Cyber warfare*, Unjust Actins in a just War, Florida International University.

Moreno-Ocampo, L. (2010). The role of the international community in assisting the International Criminal Court to secure justice and accountability. In *Confronting genocide* (pp. 279-289). Dordrecht: Springer Netherlands.

Moreno-Ocampo, L. (2010). The role of the international community in assisting the International Criminal Court to secure justice and accountability. In *Confronting genocide* (pp. 279-289). Dordrecht: Springer Netherlands.

Reydams, L., Wouters, J., & Ryngaert, C. (Eds.). (2012). *International prosecutors*. Oxford University Press, 5, 926-944.

Saalbach,K. (2014). *Cyber War, Methods and Practice*", Version 9.0, University of Osnabruck-

Schmidt, M. (2002). War through Communication Networks Attack on computer networks, *International Journal of the Red Cro*ss. 1(1): 17-41.

Shin. B. (2011). The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, *IFANS*,19(1).

Thomas, F. (2005). Legitimacy after Kosovo and Iraq in international law, *The American Journal of International Law*, 100(1): 88-106.

Tomar, S. (2014). Proxy Warfare", *Journal of Defense Studies*,8(2).

Legislation, documents and international agreements:

Charter of the United Nations

The four Geneva Conventions of 1949

The Hague Conventions of 1899-1907

The Tallinn Guide on the Subjecting of Cyber Attacks to the Provisions of International Humanitarian Law 2015-2017

The two Additional Protocols to the Geneva Conventions of 1977.