مجلة النور للدراسات القانونية ، العدد (2) ، المجلد 1 ، ديسمبر 2024
ISSN: 3007-3340 , https://doi.org/10.69513/jnfls.v1.i2.a6 (180-152)

الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني

م.م عبدالرحمن شامل عبدالرحمن

جامعة نينوى/ كلية القانون

abdulrahman.shamel@uoninevah.edu.iq

ORCID: 0009-0004-2275-0862

م.د زيد لقمان

جامعة نينوى / كلية القانون

zaid.luqman01@gmail.com

ORCID: : 0009-0009-6270-8091

تاريخ الاستلام:2024/10/20 تاريخ القبول :2024/11/20
تاريخ النشر:2024/12/17

المخلص

توضح نتائج البحث بوضوح أن مبادئ القانون الدولي الإنساني، رغم شموليتها وعموميتها، تواجه تحديات كبيرة في تطبيقها على الهجمات السيبرانية. الطبيعة الافتراضية للهجمات السيبرانية وارتباطها بالبنية التحتية المدنية تجعل من الصعب تطبيق مبادئ مثل التمييز والتناسب بشكل دقيق وفعال، مما يخلق فجوات تنظيمية حقيقية في إطار القانون الحالي. وإلى جانب ذلك، يعد "دليل تالين" خطوة هامة نحو تنظيم الهجمات السيبرانية ضمن إطار القانون الدولي، ولكنه لا يغطي كل الجوانب المهمة، فهو غير ملزم ويواجه اعتراضات دولية. بناءً على هذه الفجوات، هناك حاجة ملحة لإنشاء إطار قانوني دولي خاص لتنظيم الحروب السيبرانية وتأثيراتها المتزايدة في عالم يعتمد بشكل متزايد على التكنولوجيا. كما يهدف هذا البحث إلى التعرف على الطبيعة القانونية للهجمات السيبرانية في إطار القانون الدولي الإنساني، وتحديد التكييف القانوني لهذه الهجمات، وبيان مدى الحاجة لتنظيم قانوني خاص. ونتبع في هذا البحث المنهج التحليلي بهدف تحليل الآراء الفقهية والنصوص القانونية الدولية المتعلقة بموضوع البحث للوصول لهدف البحث.

الكلمات المفتاحية: الهجمات السيبرانية ؛ القانون الدولي الإنساني ؛ حماية المدنيين؛ مبدأ التمييز.

مجلة النور للدراسات القانونية ، العدد (2) ، المجلد 1 ، ديسمبر 2024
ISSN: 3007-3340 , https://doi.org/10.69513/jnfls.v1.i2.a6 (180-152)

The Legal Nature of Cyber Attacks in Light of International Humanitarian Law

Dr. Zaid Luqman Ismail
University of Nineveh / College of Law
zaid.luqman01@gmail.com
ORCID: : 0009-0009-6270-8091

Asst.Lec. Abdulrahman Shamil Abdulrahman
University of Nineveh / College of Law
abdulrahman.shamel@uoninevah.edu.iq
ORCID: 0009-0004-2275-0862

Received:10/10/2024 Acceptance:20/10/2024
Published:17/12/2024

Abstract

The research findings clearly demonstrate that, despite the comprehensive and universal nature of international humanitarian law (IHL) principles, significant challenges arise in their application to cyberattacks. The virtual nature of cyberattacks and their connection to civilian infrastructure make it difficult to effectively and precisely apply principles such as distinction and proportionality, creating real regulatory gaps within the current legal framework. Furthermore, the "Tallinn Manual" represents an important step toward regulating cyberattacks within the framework of international law, but it does not cover all critical aspects. It is non-binding and faces international objections. Based on these gaps, there is an urgent need to establish a dedicated international legal framework to regulate cyber warfare and its growing impact in an increasingly technology-dependent world. This research aims to examine the legal nature of cyberattacks within the

framework of international humanitarian law, determine the legal characterization of such attacks, and highlight the necessity of a specific legal regulation. The research adopts an analytical methodology to analyze jurisprudential opinions and international legal texts related to the research topic to achieve its objectives.

Keywords: Cyberattacks; International Humanitarian Law; Civilian Protection; Principle of Distinction.

المقدمة

لا شك أن التطور التكنولوجي واستخدام وسائل الاتصال المتطورة من انترنت وغيره أصبح مسألة شبه حتمية في عالمنا المعاصر، وقد شهد الطلب على الإنترنت سواء كان في الإنتاج أو التوزيع أو الاتصال أو التمويل أو غيرها، تزايدًا واضحًا منذ عقد التسعينات من القرن الماضي، والآن أصبح الإنترنت واستخدام الوسائل السيبرانية ممتد ليس فقط للنشاطات المدنية وإنما كذلك إلى النشاطات العسكرية للدول، وواكب ذلك ظهور ما يسمى بالقرصنة المعلوماتية أو الهاكرز (Hackers)، وظهرت مصطلحات جديدة مثل الهجمات السيبرانية أو الحروب السيبرانية، والتي تشكل في عالم اليوم أحد التحديات التي يواجهها النظام القانوني الدولي، وذلك لصعوبة تحديد طبيعتها وعناصرها من ناحية، وصعوبة الوقوف على آثارها وتبعاتها من ناحية أخرى، ومن هذا المنطلق، رأينا أن نخصص هذه الورقة البحثية لمحاولة الوقوف على الطبيعة القانونية للهجمات السيبرانية في إطار القانون الدولي الإنساني، وذلك من خلال المحددات الآتية:

أولًا: أهمية البحث:

يكتسب هذا الموضوع أهمية على الصعيد القانوني، لأكثر من سبب فمن ناحية إن الهجمات السيبرانية الناتجة عن التقدم التكنولوجي وانتشار التقنيات الرقمية، أصبحت تهديدًا يتجاوز الحدود الجغرافية للدول، وأصبح يمس الأمن ليس الوطني فحسب وإنما الأمن الدولي كذلك، ومن ناحية أخرى، فإن الهجمات السيبرانية قد يترتب عليها آثار

خطيرة ومدمرة ليس فقط على الصعيد العسكري، وإنما على الصعيد المدني من تدمير للبنى التحتية وإصابة المدنيين، ولذلك فإن هذا الموضوع يكتسب أهميته من خطورة آثاره، الأمر الذي يستوجب البحث في أبعاده للوقوف على طبيعته القانونية، لتحديد طبيعة هذه الهجمات وموقف القانون الدولي الإنسان منها.

ثانيًا: إشكالية البحث :

تتمحور إشكالية البحث حول مدى قدرة القانون الدولي الإنساني الحالي على التعامل مع الهجمات السيبرانية، حيث تثير هذه الإشكالية عدة تساؤلات، منها: هل يمكن تصنيف الهجمات السيبرانية كأعمال عدائية تقع ضمن نطاق النزاعات المسلحة؟ وهل يستطيع القانون التقليدي تنظيم هذه الهجمات وتحديد طبيعتها وعناصرها؟ أم أن هناك حاجة إلى تطوير قواعد قانونية جديدة تتناسب مع خصوصية الفضاء السيبراني؟

ثالثًا: منهجية البحث:

يعتمد البحث على المنهج التحليلي؛ إذ سيتم تحليل النصوص القانونية المتعلقة بالقانون الدولي الإنساني، وبيان علاقتها وارتباطها بالواقع الحالي للهجمات السيبرانية، كما سيتم دراسة بعض الحالات العملية للهجمات السيبرانية وتأثيراتها على الصعيد الدولي.

رابعًا: أهداف البحث:

يهدف هذا البحث لتحقيق عدة أهداف منها:

- تحديد الطبيعة القانونية للهجمات السيبرانية في ظل القانون الدولي الإنساني.
- تحليل الهجمات السيبرانية وبيان مدى توافقها مع أحكام القانون الدولي الإنساني.
- تقديم مقترحات لتطوير الإطار القانوني بحيث يشمل الحماية من الهجمات السيبرانية.

خامسًا: الدراسات السابقة:

- دراسة بعنوان: **"المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"**، للباحث طلال ياسين العيسى

وعدي محمد عناب[1]، وتناولت هذه الدراسة المسؤولية الدولية الناشئة عن الهجمات السيبرانية، وأظهرت الدراسة العديد من النتائج والتي من أهمها أن أغلب الدول تفتقد إلى وجود تشريعات تختص بالفضاء السيبراني وفي حال وجود قوانين فإن يوجد ثغرات قانونية بهذا الخصوص، كما أوصت الدراسة بأهمية الحاجة إلى تعبئة الفراغ التشريعي في مجال مكافحة الجرائم السيبرانية.

ويتميز بحثنا عن هذه الدراسة، في كونه يبحث في تحديد الطبيعة القانونية للهجمات السيبرانية، ومن ثم البحث في مدى ملائمة قواعد القانون الدولي الإنساني التقليدية في التطبيق على هذه الهجمات.

- دراسة بعنوان: "**الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول**"، للباحث منزر رابح، و درويش سعيد[2]، حيث هدفت هذه الدراسة إلى بيان الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، من حيث كونها إما جريمة سيبرانية تخضع لأحكام دليل تالين لعام 2013 الخاص بقواعد القانون الدولي المطبقة على الحروب السيبرانية التي تتم في إطار نزاع مسلح، أو عبارة عن جريمة دولية ذات طابع خاص تطبيق عليها قواعد القانون الدولي العام، وبالتالي إثارة المسؤولية الدولية للدولة المعتدية المترتبة عليها باعتباره عدوانًا يحظره القانون الدولي.

وفي هذا الصدد يأتي بحثنا لمحاولة استكمال ما طرحته هذه الدراسة من حيث طبيعة الهجمات السيبرانية وعلاقتها بالقانون الدولي الإنساني.

- دراسة بعنوان: "**الهجمات السيبرانية في ضوء القانون الدولي**" للباحث الدكتور عبد الله عبد الكريم علي أحمد[3]، وقد ركزت هذه الدراسة على توضيح ماهية الهجمات السيبرانية ونشأتها وخصائصها، ومن ثم بيان التكييف القانون لها وجهود مكافحتها على الصعيد الدولي، ويتميز عنها بحثنا في كوننا سنسعى لبيان الطبيعة القانونية لهذه الهجمات ومدى انطباق قواعد القانون الدولي الإنساني عليها.

- دراسة بعنوان: "**Rewired Warfare: Rethinking the Law of Cyber Attack**" للباحث Michael N. Schmitt[4]، تركز هذه الدراسة على كيفية إعادة النظر في القوانين الدولية المتعلقة بالهجمات السيبرانية، مبيّنةً أن تطور تكنولوجيا المعلومات يستدعي تعديلات على

المبادئ الأساسية للقانون الدولي الإنساني، خاصة فيما يتعلق بمفهوم "الهجوم" نفسه. تُبرز الدراسة التعقيدات التي تواجهها الدول عند محاولة تطبيق قوانين تقليدية، مثل مبادئ التمييز والتناسب، على الهجمات السيبرانية التي لا تسبب أضرارًا مادية مباشرة ولكن قد تكون لها آثار مدمرة على البنية التحتية الحيوية والمدنيين، كما تنتهي إلى أن تزايد استخدام الهجمات السيبرانية يتطلب وضع معايير قانونية جديدة تأخذ في الحسبان طبيعة هذه العمليات وتحديات إثبات نسبتها إلى جهات فاعلة محددة، ويتميز عنها بحثنا في كونه يركز على كيفية تطبيق القانون الدولي الإنساني الحالي بشكل عملي، مع التركيز على تقديم توصيات محددة لإدراج هذه الهجمات ضمن النزاعات المسلحة. يسعى البحث إلى تحليل الفجوات الحالية في القانون وتقديم إطار قانوني مقترح لمواجهة التحديات المستقبلية.

سادسًا: خطة البحث:

المطلب الأول: ماهية الهجمات السيبرانية ونشأتها.

المطلب الثاني: التكييف القانوني للهجمات السيبرانية في ضوء القانون الدولي الإنساني.

المطلب الثالث: مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية.

المطلب الأول

ماهية الهجمات السيبرانية ونشأتها

يمكن اعتبار مفهوم الهجمات السيبرانية من أحدث المفاهيم المرتبطة بأساليب الجريمة الحديثة التي تعتمد بشكل أساسي على تكنولوجيا المعلومات، حيث تستهدف هذه الهجمات الأنظمة الحاسوبية والأجهزة الإلكترونية، وتتنوع بين محاولات لسرقة البيانات، أو تدميرها، أو تعديلها، وتشمل هذه الهجمات أيضاً زرع برامج ضارة تهدف إلى التجسس أو إحداث ضرر بأنظمة الحاسب المختلفة[5].

وواقع الأمر، فإن الهجمات السيبرانية تعتبر هجمات حديثة نسبيًا، نظرًا لارتباطها بالثورات التكنولوجية التي عرفها المجتمع، ومع تزايد اعتماد الأفراد على وسائل التكنولوجيا والاتصال وما واكبه من تحديات كبرى، وعليه سنعرض في هذا المطلب لمفهوم ونشأة الهجمات السيبرانية على التفصيل الآتي:

الفرع الأول: مفهوم الهجمات السيبرانية.
الفرع الثاني: نشأة وأنواع الهجمات السيبرانية.

الفرع الأول

مفهوم الهجمات السيبرانية

إن مسار الحروب لطالما ارتبط بالتطورات التقنية التي عرفتها المجتمعات البشرية، وسخرتها ما ساعدها على القيام بهجمات قتالية متطورة تعزز من قدرتها القتالية وصولًا لتحقيق أهداف الحرب، وتأمين المصالح الحيوية المنشودة من خوض النزاع المسلح، ومع وصولنا للعصر الحالي الذي أصبحت التقنيات الحديثة والمعلوماتية والإنترنت هم عنوان المرحلة، فقد أدى ذلك لظهور جيل جديد من المنظومات القتالية التي اعتمدت على هذه التقنية، بداية من الأسلحة ذاتية التشغيل، مرورًا بمنظومات القتال عبر الفضاء السيبراني، وهي ما تعرف بالهجمات السيبرانية أو الحرب السيبرانية، ومما تقدم أضحى من الضروري الوقوف على تعريف الهجمات السيبرانية، بيد أن الأمر ليس بهذه السهولة، إذ أنه لم يوجد حتى الآن تعريف موحد أو دقيق لهذا المفهوم، ويرجع هذا الغياب نتيجة غياب أو صعوبة التعرف على كافة عناصر هذه الهجمات سواء من حيث استخدامها أو من حيث آثار هذا الاستخدام، ومع ذلك فقد حاول بعض الباحثين وضع تعريف لهذه الهجمات، ونعرض منها ما يلي:

تعريف البعض لها بأنها: "استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها"[6]، وعرفها آخر بأنها: "أعمال تقوم بها دولة تحاول من خلال اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[7].

كما تُعرف الهجمات السيبرانية أيضاً بأنها: "تصرف يتم في عالم افتراضي معتمدًا على استعمال بيانات رقمية ووسائل اتصال تعمل الكترونيًا يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة من خلال اختراق مواقع الكترونية حساسة وفي العادة تقوم بوظائف تصنف بأنها ذات أولوية مثل أنظمة الحماية الخاصة بمحطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى"[8].

وعرفت كذلك من قبل الخبراء التابعين للناتو، والذي تم النص عليه في المادة 30 من دليل تالين المتعلق بتطبيقات القانون الدولي في مجال الصراع والحروب السيبرانية بأنها: "كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر أو إلحاق أذى بالأعيان سواء إضرارًا أو تدميرًا"[9].

ونفهم من هذه التعريفات، أن المقصود بالأضرار التي تترتب على الهجمات السيبرانية، ليس فقط الأضرار المباشرة، وإنما تشمل الأضرار غير المباشر المتمثلة في توقف المنشآت والأعيان المدنية عن العمل نتيجة الهجمات المستمرة، فذلك يعد ضررًا غير مباشر للهجمات السيبرانية[10].

كذلك يمكن أن نفهم من هذه التعريفات أن الهجمات السيبرانية تشمل تصرفات تتم في بيئة افتراضية، تعتمد على استخدام بيانات رقمية ووسائل اتصال إلكترونية لتحقيق أهداف عسكرية أو أمنية محددة. تطور مفهوم الهجمات السيبرانية ليشمل اختراق مواقع إلكترونية حساسة تنفذ مهام ذات أهمية خاصة، مثل أنظمة حماية محطات الطاقة النووية أو الكهربائية، المطارات، أو غيرها من نظم ووسائل النقل الحيوية. يشير هذا إلى أن الهجمات السيبرانية لم تعد مقتصرة على استهداف البيانات فحسب، بل تهدف أيضًا إلى إلحاق ضرر مباشر بالبنية التحتية الحيوية لتحقيق تأثيرات ملموسة على الأرض[11].

ومن جانبنا فإننا نرى أن الهجمات السيبرانية أو الحروب السيبرانية هي أنشطة عدائية تُنفذ عبر الفضاء الإلكتروني باستخدام تقنيات رقمية وأدوات اتصال تهدف إلى اختراق أنظمة الحواسيب والشبكات لاستهداف بيانات حساسة أو تعطيل بنية تحتية رئيسية، وهي تتنوع بين تحقيق مكاسب مالية أو سرقة معلومات أو إلحاق ضرر بمنشآت عسكرية ومدنية حيوية، وبين إيذاء الأشخاص وإلحاق أضرار مادية بهم.

وقد حاول الباحث في هذا التعريف أن يجمع بين جميع عناصر السيبرانية كما يراها، وهي:

- أن الهجمات السيبرانية تنفذ عبر الفضاء الإلكتروني وبوسائل رقمية وتقنية، كالحواسب والشبكات والانترنت، وبالتالي لابد أن نكون بصدد نشاط عدائي غير ملموس وعبر الفضاء السيبراني.
- أنها تهدف إلى المساس ببيانات حساسة أو تعطيل بنى تحتية، وقد تكون هذه البنى التحتية مدنية وقد تكون عسكرية وحيوية تمس الأمن القومي

للدول، بما يؤدي للإضرار بالأفراد والممتلكات، ومن ثم إذا كانت الهجمات هدفها هو سرقة بيانات شخصية لبعض الأفراد فلا نكون بصدد حرب سيبرانية، وإنما مجرد جريمة سيبرانية أو إلكترونية.

وبناء على ذلك، يمكن القول بأن، الهجمات أو الحروب السيبرانية تتميز بعدة خصائص منها[12]:

- أنها سهلة التنفيذ وواسعة النطاق، إذ يمكن لمرتكبيها تنفيذها على نطاق واسع، وباستخدام أدوات بسيطة.
- أنها صعبة تحديد المصدر، إذ لا دليل مادي أو فيزيائي يمكن تحديده في ذلك النوع من الخدمات، بل في أغلب الأحيان تظل مجهولة المصدر ما لم يعلن عنها مرتكبها أو تتبناها جهة محددة.
- أنها تتجاوز النطاق الجغرافي للدول، وبحيث يمكن القيام بهذه الهجمات في أي مكان وأي وقت، فالهجمات السيبرانية قد يصل مداها ليس لنطاق الأرض فحسب بل يمتد إلى الأقمار الصناعية والمجال الفضائي.

الفرع الثاني

نشأة الهجمات السيبرانية

بدأت ظهور صور الهجمات السيبرانية في الثمانينات من القرن الماضي وتحديدًا في عهد الرئيس الأمريكي "رونالد ريغان" والذي كان يرى أن بلاده قد تتعرض لخطر تلك الهجمات، ما أدى لإنشاء هيئة جديدة هي "وحدة السياسة القومية بشأن الاتصالات وأمن نظم المعلومات"[13]، بيد أن فكرة الهجمات السيبرانية بدأت في الحقيقة على صورة أنشطة فردية تستهدف سرقة البيانات واختراق الأنظمة الحاسوبية، حيث كان الدافع الأساس لهذه الهجمات في البداية هو استكشاف القدرات التكنولوجية الجديدة، وقد تم تطوير أول فيروسات الكمبيوتر وأدوات القرصنة التي استهدفت بشكل أساسي الأفراد والشركات الصغيرة. من الأمثلة المبكرة البارزة على هذا، "دودة موريس" عام 1988، التي أثرت على شبكة الإنترنت المبكرة وتسببت في أضرار واسعة النطاق[14].

ومع دخول الألفية الجديدة، زادت الهجمات السيبرانية تطورًا وتعقيدًا، ففي عام 2007 وقع هجوم روسي على دولة استونيا إثر قيام الحكومة الاستونية بتاريخ 26 أبريل 2007 بنقل نصب تذكاري يعود للحرب العالمية الثانية مخصصًا لتخليد الجيش الأحمر الروسي من وسط عاصمة استونيا تالين إلى

مقبرة عسكرية خارجها، ما أدى إلى حدوث مظاهرات شعبية للمجتمع الأستوني الناطق بالروسية، فضلًا عن إدانة روسيا لهذا القرار، وردًا على ذلك، تعرضت استونيا على مدار ثلاث أسابيع إلى سلسلة من الهجمات السيبرانية، التي طالت العديد من المواقع الحكومية والعسكرية والخاصة، ما أصاب الدولة بشلل تام، لاسيما في الإعلام والبنوك ومشغلي الهاتف المحمول وخدمات الطوارئ، وقد مثلت هذه الحادثة أول تجربة حقيقية لنظرية الحرب السيبرانية، حيث ظل الخبراء يعتبرون الحديث عن هذه الحرب مجرد مسألة نظرية وذلك حتى تم استخدام الفضاء السيبراني فيها لتدمير أهداف حيوية[15].

وفي عام 2010، أصبحت دودة "ستوكسنت" معروفة على نطاق واسع باعتبارها أول سلاح سيبراني حقيقي يستهدف البنية التحتية، حيث تم تطوير "ستوكسنت" خصيصًا لتعطيل برنامج تخصيب اليورانيوم الإيراني من خلال استهداف أنظمة التحكم الصناعية (ICS) المخصصة لتشغيل أجهزة الطرد المركزي[16]، وقد أشارت التحليلات إلى أن هذا الهجوم قد تم تطويره بدعم من دول كبرى نظرًا لتعقيده، ونجح في تعطيل ما يصل إلى 1000 جهاز طرد مركزي، مما أدى إلى تأخير البرنامج النووي الإيراني بشكل كبير، ويعتبر "ستوكسنت" نقطة تحول في مجال الحرب السيبرانية حيث أظهر إمكانية تحقيق تأثيرات مدمرة مادية عبر الإنترنت[17].

المطلب الثاني

التكييف القانوني للهجمات السيبرانية في ضوء القانون الدولي الإنساني

واقع الأمر، أن العديد من فقهاء القانون الدولي قد تطرقوا لموضوع الهجمات والحروب السيبرانية، وطرحوا عددًا من الإشكالات حولها، إلا أن أهم هذه التساؤلات كان ذلك المتعلق بتكييف هذه النوعية من الهجمات ومدى انطباق قواعد القانون الدولي لاسيما الإنساني عليها، وقد كانت الإجابة على هذا التساؤل محل جدل بين الفقهاء، فهناك من رأى انطباق قواعد القانون الدولي الإنساني عليها، وهناك من رأى عدم انطباق قواعد القانون الدولي عليها، ومن ثم الإقرار بوجود فراغ قانوني يستدعي العمل على سده، وسنعرض لوجهتي النظر، وذلك قبل العرض للقانون الواجب التطبيق على الهجمات السيبرانية، وذلك على النحو الآتي:

الفرع الأول

عدم تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية

يذهب جانب كبير من فقهاء القانون الدولي إلى عدم انطباق حكام القانون الدولي الإنساني على الهجمات السيبرانية، وذلك على أساس من القول أن الفضاء السيبراني الإلكتروني الافتراضي هو منطقة خالية من القانون، وهو ليس إلا عالم افتراضي لا يمكن تحديده بدولة أو جهة معينة، ومن ثم فلا يمكن أن يخضع لقواعد القانون العام من جهة أو لأحكام القانون الدولي الإنساني المتعلق بالنزاعات المسلحة الدولية وغير الدولية من ناحية أخرى[18].

ويستندون في هذا الرأي أو التوجه إلى أن القواعد القانونية التي تنظم أساليب ووسائل القتال في النزاعات المسلحة نشأت وتطورت عبر الزمن، بدءًا من اتفاقيات لاهاي لعامي 1899 و1907، مرورًا باتفاقيات جنيف الأربع لعام 1949، والبروتوكولين الإضافيين لعام 1977، هذه المعاهدات والقواعد العرفية المتراكمة تشكل أساس القانون الدولي الإنساني، الذي يسعى إلى تقييد استخدام العنف في الحروب وضمان حماية الأشخاص غير المشاركين في النزاع، وقد أسهمت هذه القواعد في تقنين بعض الأحكام التي كانت سابقًا معتمدة فقط كأعراف [19].

فضلا عن ذلك، فإنهم يستندون على حجة أن عالم الإنترنت عالم جديد لا يتفق مع الواقع المادي، وأنه لن يكون بإمكان أي سلطة أن تفرض أحكامها في ظل استقلالية الشبة وانفلاتها من مفهوم الخضوع، وقد أجابوا بانعدام السلطة القادرة على ذلك، حتى وإن وجد مثل هذا القانون، فإنها تبقى منطقة بلا قانون لاستحالة إخضاعها للتدخل التنظيمي التقليدي للدول، كونها تتسم بطابع عالمي مفتوح، ويتعذر إخضاعها لقانون واحد لاشتراك كل الدول فيها[20].

وبناءً على ذلك، يرى أصحاب هذا التوجه -ويتفق معه الباحث - أن تطبيق قواعد القانون الدولي الإنساني لا يمتد إلى الهجمات السيبرانية، إذ لا تحتوي أحكامه على قواعد محددة للتعامل معها في سياق النزاعات المسلحة. فرغم استخدام مصطلح "الحرب" للإشارة إلى هجمات الكمبيوتر، إلا أن هذا المفهوم يحتاج إلى إعادة تقييم. فتقليديًا، الحرب كانت ترتكز على استخدام جيوش نظامية وتسبقها إعلانات رسمية لحالة الحرب وتحديد لميدان القتال. أما في هجمات الفضاء السيبراني، فالنزاع لا يلتزم بحدود جغرافية أو أهداف واضحة، نظرًا لأن هذه الهجمات تنفذ عبر شبكات المعلومات والاتصالات التي تتجاوز الحدود الوطنية، وتعتمد على أسلحة إلكترونية تتناسب مع سياق

العصر الرقمي. هذه الأسلحة تُوجَّه نحو البنى التحتية الحيوية أو تُستخدم من خلال العملاء ضمن أجهزة الاستخبارات، وبسبب هذه العوامل، تصبح الهجمات السيبرانية في الصراعات السياسية أقرب إلى توصيف الإرهاب منها إلى الحرب التقليدية. كما أن تحديد طبيعة الأسلحة المعلوماتية يثير إشكالية في كيفية تنظيمها والتعامل معها وفقًا للقواعد القانونية الحالية[21].

الفرع الثاني

تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية

في مقابل الرأي السابق، يذهب رأي آخر إلى أن الهجمات السيبرانية يمكن تكييفها في ظل أحكام القانون الدولي العام على أساس أن الصورة الأولية تُظهر أن تلك الهجمات من الممكن أن يتم ارتكابها أثناء النزاعات المسلحة الدولية أو غير الدولية وفي أوقات السلم، وأن تكييف استخدام الهجمات السيبرانية يدور حول فرضيتين هما[22]:

الفرضية الأولى: عدم إمكانية إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية، ويعتبر ذلك أحد العقبات التي تواجه المتخصصين وذلك بخلاف وسائل الأخرى التي تترك أثر مادي محسوس عند الاستخدام.

الفرضية الثانية: أنه إذا ثبت أن الهجمات السيبرانية يترتب عليها أثر مادي ملموس على المستويات الاقتصادية والأمنية والعسكرية ، فهنا يكون المعيار في تكييف الهجمات السيبرانية، فيما إذا كانت من قبيل التصرف العدواني، أو كون هدفه رد العدوان، حيث تعتمد بصورة أساسية على القواعد القانونية ذات الصلة، لاسيما حكم المادة الثانية في فقرتها الرابعة من ميثاق الأمم المتحدة[23]، وكذلك المادة 51 من نفس الميثاق، فتؤكد على الحق الطبيعي للدول في الدفاع عن نفسها. وتنص على أن "ليس في هذا الميثاق ما يضعف أو ينتقص من الحق الطبيعي للدول في الدفاع عن أنفسها، بشكل فردي أو جماعي، إذا تعرضت لأي اعتداء مسلح حتى يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين."[24]هذا الحق يشمل اتخاذ تدابير الدفاع الذاتي فور وقوع الهجوم، على أن يتم إبلاغ مجلس الأمن بهذه التدابير.

بالإضافة إلى ما سبق، فإن القانون الدولي الإنساني ينطبق بمبادئه وقواعده العامة، على أي نزاع مسلحة بما فيها الحروب السيبرانية، فإذا كان من الصحيح أن القانون الدولي الإنساني لم يشر للحروب السيبرانية، إلا أن ذلك

ليس له أهمية، إذ أن شرط مارتينيز الذي يعتبر أحد المبادئ الراسخة في القانون الدولي الإنساني، ينص صراحة على أنه في حالة وجود حالة غير منصوص عليها في الاتفاقيات الدولية، فإن المدنيين والمقاتلين يبقون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة ومبادئ الإنسانية وما يمليه الضمير العام[25].

وعلى هذا الأساس يمكن القول بأن القانون الدولي الإنساني وفقًا لشرط مارتينيز[26]، ينطبق على جميع الحالات التي لا تنظمها قواعد القانون الدولي الإنساني، والتي تدخل في إطارها الحروب والهجمات السيبرانية، فالهدف من هذا الشرط هو سد الثغرات التي قد تعتري القانون الدولي الإنساني في هذا المجال، ولذلك سمي بالمبدأ البديل او الاحتياطي كونه يطبق عن عدم توفر نص قانوني صريح يحمي الأشخاص المعنيين بالحماية[27].

المطلب الثالث

مدى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية

تنص الفقرة الأولى من المادة 35 من البروتوكول الأول الإضافي لاتفاقيات جنيف لعام 1977 على أن حق أطراف النزاع في اختيار وسائل وأساليب القتال ليس حقًا مطلقًا، بل يجب أن يكون مقيدًا بالقواعد الأساسية للقانون الدولي الإنساني. وهذا يعني أنه حتى في حال نشوب شكوك حول معنى بعض الأحكام الواردة في القانون، يمكن الاستناد إلى مبادئ مثل "شروط مارتينز" لتفسيرها، حيث توفر قاعدة عامة لتطبيق مبادئ القانون الإنساني على جميع النزاعات، مهما كان نوع السلاح المستخدم[28].

كذلك أشارت المادة 36 من البروتوكول الإضافي إلى التزام كل طرف سام متعاقد عند دراسته أو تطويره أو اقتناءه لسلاح جديد أو أداة للحرب أو اتباع أسلوب الحرب، بالتحقق فيما إذا كان ذلك السلاح محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[29]، أي أنه إذا تم تكييف الهجمات السيبرانية على اعتبارها سلاح أو أسلوب من أساليب الحرب فعلى الدول التحقق من مدى مشروعية استخدامها وفقًا للبروتوكول، أو وفقًا لأي قاعدة من قواعد القانون الدولي، وهو ما يؤكد انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية[30].

أشارت محكمة العدل الدولية في رأيها الاستشاري بشأن الأسلحة النووية إلى أن مبادئ القانون الدولي الإنساني تسري على جميع أشكال النزاعات وجميع أنواع الأسلحة، بما في ذلك الأسلحة المستقبلية. بناءً على ذلك، إن الهجمات السيبرانية تندرج تحت نطاق القانون الدولي الإنساني عند وقوعها في سياق نزاع مسلح، حيث يجب أن تلتزم المبادئ الأساسية مثل التمييز والتناسب والاحتياط، بغض النظر عن التقنيات المستخدمة[31].

بيد أن التساؤل الذي يثور هنا هو هل انطباق القواعد الواردة في القانون الدولي الإنساني على الحروب السيبرانية، سيكون كافيًا لتنظيم هذه الهجمات؟ أم أن هناك إشكاليات فيما يتعلق بهذه المسألة؟ وهل هناك حاجة إلى تنظيمها بقواعد خاصة بها؟

واقع الأمر، فإن تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، ومع التسليم جدلًا بإمكان تطبيق هذه القواعد، يثير العديد من الإشكاليات لاسيما فيما يتعلق بتطبيق المبادئ والقواعد الخاصة بسلوكيات الحروب، والتي من أهمها مبادئ الضرورة العسكرية والتمييز وغيرها من المبادئ، وعليه نعرض لهذه الإشكاليات، ثم نعرض لمدى الحاجة لوجود قواعد دولية خاصة بالحروب السيبرانية، ومدى كفاية قواعد تالين لعام 2013 للتطبيق على الهجمات السيبرانية على النحو الآتي:

الفرع الأول

إشكاليات تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية

يثير تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، إشكاليات عدة تتعلق بالمبادئ السلوكية للحرب، وسنحاول أن نوضح ذلك على النحو التالي:

أولًا: الهجمات السيبرانية ومبدأ الضرورة العسكرية:

لا شك أن مبدأ الضرورة العسكرية يعتبر أحد أهم المبادئ التي يقوم عليها القانون الدولي الإنساني، وهو يعني التزام أطراف النزاع المسلح باستخدام القوة الضرورية فقط لتحقيق هدف القتال المتمثل في إخضاع العدو وتحقيق النصر عليه، دون القيام بأضرار لا داعي لها ولا هدف منها، وبالتالي فإن كل هدف لا يؤدي إلى كسب الحرب يعد مخالفًا لمبدأ الضرورة العسكرية، وهذا المبدأ مقررًا في اتفاقيات جنيف لسنة 1949 والبروتوكول الإضافي الثاني لسنة 1977[32].

ويثار التساؤل هنا حول كيفية تطبيق مبادئ القانون الدولي الإنساني على الهجمات والحروب السيبرانية؟ وواقع الأمر فإن هذا المبدأ يقوم على أساس أن استخدام القوة والعنف والخداع في الحرب يجب أن يقتصر على تحقيق الانتصار على العدو وتحقيق الهدف العسكري المشروع، إلا أن الهجمات السيبرانية تخلق صعوبة في التمييز بين الأهداف العسكرية والمدنية، مما يجعل من الصعب تحديد ما هو ضروري لتحقيق الهدف العسكري المشروع وما يتعداه إلى غير المشروع.

ومن التحديات الكبرى التي تطرحها الهجمات السيبرانية هي صعوبة تحديد الأهداف والمنشآت العسكرية في الفضاء الإلكتروني، نظرًا لأن العديد من المنشآت التي تؤدي دورًا عسكريًا قد تقدم أيضًا خدمات مدني، هذا التشابك بين الأهداف العسكرية والمدنية يعقد من عملية التمييز التي يجب أن تكون أساسًا للتقييم في حالات النزاعات المسلحة، خاصة في الهجمات السيبرانية، حيث قد تكون البنية التحتية المستهدفة مخصصة للاستخدامات المدنية والعسكرية على حد سواء، مما يزيد من صعوبة التزام الدول بمبادئ القانون الدولي الإنساني في هذا السياق. (33)

ثانيًا: الهجمات السيبرانية ومبدأ التناسب:

يعد مبدأ التناسب أحد المبادئ الأساسية في القانون الدولي الإنساني، ويهدف إلى تقليل الخسائر والمعاناة الناتجة عن العمليات العسكرية، سواء من حيث الأضرار البشرية أو المادية. ينص هذا المبدأ على ضرورة أن تكون الأضرار الناجمة عن أي هجوم عسكري متناسبة مع الفائدة العسكرية المتوقعة من هذا الهجوم. ويعتبر هذا التوازن أمرًا دقيقًا وصعب التطبيق أحيانًا خلال النزاعات المسلحة، حيث أن الالتزام بهذا المبدأ يتطلب من الأطراف المتحاربة اتخاذ كافة التدابير الممكنة لتجنب إلحاق ضرر غير ضروري بالمدنيين والممتلكات المدنية.

ويحظر القانون الدولي الإنساني الهجمات التي تكون غير متناسبة والتي قد تلحق أضرارًا مفرطة بالمدنيين مقارنةً بالهدف العسكري المراد تحقيقه. ويعد هذا الحظر أداة رئيسية لحماية المدنيين من الآثار المدمرة للحرب، إذ يُلزم الأطراف المتنازعة بتقييم ما إذا كانت الخسائر المحتملة على المدنيين والأعيان المدنية مبررة في ضوء المكاسب العسكرية المتوقعة من العملية(34).

ويبرز مبدأ التناسب تحديات وإشكاليات خاصة عند تطبيقه على الهجمات السيبرانية ، حيث تكون البرمجيات المستخدمة في هذه الهجمات غير قادرة على مراعاة متطلبات التناسب بشكل تلقائي. ويتطلب هذا المبدأ موازنة دقيقة بين الأضرار المحتملة والفائدة العسكرية المتوقعة، وهي معادلة معقدة حتى في سياق العمليات العسكرية التقليدية.

فبرغم أن تحقيق الهدف العسكري يُعد أساسيًا، إلا أن الالتزام القانوني يفرض ضبط الهجمات لتجنب إلحاق أضرار مفرطة بالأعيان المدنية. يتطلب تنفيذ هذا المبدأ ضابطًا عسكريًا خبيرًا يستطيع تقدير التوازن بين الضرر المتوقع والمكاسب المرجوة، ومع ذلك، تصبح هذه العملية أكثر تعقيدًا عندما يتعلق الأمر بالهجمات السيبرانية، حيث يمكن أن يكون نطاق الضرر غير متوقع ومتجاوزًا الحدود المطلوبة، خاصةً عندما تستهدف البنية التحتية الحيوية التي تستخدم لأغراض مدنية وعسكرية معًا، كما أنه في الهجمات السيبرانية، يُصعب تحديد التأثيرات المترتبة على المدنيين والأعيان المدنية، نظرًا للطبيعة غير المادية للهجوم. وعليه، فإن تطبيق مبدأ التناسب في هذا السياق يتطلب تطورًا في تقنيات التقييم ووسائل التحكم، ما يستدعي وجود معايير جديدة تساعد في ضمان التزام العمليات السيبرانية بمبادئ القانون الدولي الإنساني [35].

ثالثًا: الهجمات السيبرانية ومبدأ التمييز:

يعد مبدأ التمييز أحد أهم مبادئ القانون الدولي الإنساني التي تهدف إلى تنظيم العمليات العسكرية من خلال التمييز بين المقاتلين وغير المقاتلين[36]، مما يمنح المدنيين حصانة ضد الهجمات التي تُوجَّه إلى الأهداف العسكرية، ويتضمن هذا المبدأ أيضًا ضرورة التفريق بين الأعيان المدنية والأعيان العسكرية، بحيث يُحظر الهجوم على الأعيان المدنية تحت أي ظرف، وهذه القاعدة هي أساس قوانين الحرب وأعرافها. [37]

ومع ذلك، يطرح تطبيق هذا المبدأ تحديات كبيرة عندما يتعلق الأمر بالهجمات السيبرانية، حيث تكمن الصعوبة الأساسية في التمييز بين الأهداف العسكرية والمدنية في الفضاء السيبراني، حيث يمكن أن تكون البنى التحتية المستهدفة ذات استخدام مزدوج، مثل شبكات الاتصالات والبنوك أو الأنظمة الكهربائية، والتي قد تخدم الأغراض المدنية والعسكرية في الوقت نفسه، ففي الحروب التقليدية، يسهل على المقاتلين الموجودين في الميدان التفريق بين هذه الأهداف، لكن الهجمات السيبرانية، التي تنفذ عن بُعد عبر الفضاء الإلكتروني،

تجعل من الصعب تحديد الأهداف المسموح بها وتجنب الأضرار التي قد تلحق بالمدنيين[38].

هذا التداخل بين الأهداف المدنية والعسكرية يزيد من صعوبة تحديد الأضرار المحتملة على الأعيان المدنية، مما يشكل تحديًا أمام الدول والمقاتلين للامتثال الكامل لمبدأ التمييز في العمليات السيبرانية. وتتطلب هذه العمليات السيبرانية تطوير أدوات وتقنيات جديدة تمكن من التقييم والتحكم في الأضرار المتوقعة، وذلك لضمان التقيد بمبادئ القانون الدولي الإنساني حتى في سياق الحروب السيبرانية.

الفرع الثاني

مدى الحاجة لتنظيم الهجمات السيبرانية بقواعد خاصة

تتميز مبادئ القانون الدولي الإنساني بعموميتها وشموليتها، ولذلك فمن الناحية النظرية يمكن أن تنطبق هذه القواعد على الهجمات السيبرانية، إلا أن ذلك لا يخفي حقيقة الطبيعة الخاصة للهجمات السيبرانية، وكونها تنفذ في فضاء سيبراني مشترك مع المدنيين ووجود حالة مؤكدة من التشابك والتداخل بينهما، ما يجعل من الصعوبة بمكان توجيه الهجمات السيبرانية ضد العسكريين فقط، أو بالصورة التي تتناسب مع مبدأ الضرورة العسكرية، أو مبدأ التناسب، وفقًا لأحكام القانون الدولي الإنساني.

ولعل ذلك كان سببًا في البحث عن تنظيم خاص للهجمات السيبرانية، والتي من ضمنها دليل تالين[39]، وقد جاء هذا الدليل نتيجة القصور الذي يتسم به القانون الدولي الإنساني في مجال الحروب السيبرانية، إذ لوحظ عدم وجود أساس قانوني ينظم اللجوء لهذا النوع من الهجمات والعمليات العدائية المرتبطة به، ولذلك تم الاتفاق عليه كصك قانوني وحيد يمكن اللجوء إليه في مثل هذه الظروف.

ومع ذلك فإن هذا الدليل يعاب عليه أن نصوصه تنطبق فقط على النزاعات المسلحة التقليدية، حيث نص على ضرورة أنه لكي ينطبق على كل نشاط سيبري قانون النزاعات المسلحة، أن يتم هذا النشاط في سياق نزاع مسلح دولي أو غير دولي، فضلًا عن ذلك فإن هذا الدليل ليس ملزمًا فهو لا يرقى لمستوى الاتفاقية الدولية حتى بالإضافة إلى معارضة بعض الدول له مثل روسيا والصين، فضلًا عن عدم مراعاة التمثيل العالمي للدول عند إعداده[40].

وبناء على ما سبق، يمكن القول بأن الهجمات السيبرانية تتميز بخصائص وطبيعة خاصة بها، وإن كانت تسمح بتطبيق قواعد القانون الدولي الإنساني عليها بصورة غير مباشرة، إلا أن قواعد القانون الدولي الإنساني لا تتضمن معالجة هذه الهجمات بصورة مباشرة، وبالتالي فإن الحاجة إلى تنظيم هذه النوعية من الهجمات بشكل مباشر وخاص أصبح في عالم اليوم مسألة ذات أهمية كبيرة، لاسيما وأن استخدام الهجمات السيبرانية قد يؤدي لمخاطر وأضرار مدمرة في ظل اعتماد المجتمع الدولي بأكمله على التكنولوجيا في عالم اليوم، لاسيما وأننا أصبحنا في زمن الذكاء الاصطناعي الذي بدوره سيؤدي إلى مزيد من الاعتماد على التقنيات الحديثة، ما يعظم من مخاطر هذه الهجمات وتأثيراتها في حالة نجاحها.

ومن ناحية أخرى، فإنه وإن كانت قواعد القانون الدولي الإنساني تنطبق على الهجمات السيبرانية التي تقع أثناء النزاعات المسلحة سواء كانت دولية أو غير دولية، فإنها لا تنطبق في حالة السلم، ومن ثم ففي هذه الحالة يجب البحث عن آلية تطبيقها في حالة السلم، وهنا يمكن أن نجد تطبيقًا للمادة الثانية فقرة 4 من ميثاق الأمم المتحدة، التي تنص على حظر استخدام القوة بين الدول[41]، ومع ذلك يبقى الأصل أن هذه القواعد سواء الواردة في القانون الدولي العام أو القانون الدولي الإنساني لا تنطبق بصورة مباشرة على الهجمات السيبرانية، الأمر الذي يستدعي ضرورة العمل من قبل المجتمع الدولي أعضاء ومنظمات على إنشاء وإبرام اتفاقية دولية ملزمة تتعلق بحظر استخدام الهجمات السيبرانية في الحروب، أو على الأقل تقييدها بما يواءم أهداف ومبادئ القانون الدولي الإنساني.

الخاتمة

تناولت في هذه الورقة البحثية موضوع في غاية الأهمية وهو موضوع الهجمات السيبرانية وطبيعتها في إطار القانون الدولي الإنساني، وقد عرضت لمفهوم هذه الهجمات ونشأتها وتطورها، ثم عرضت لتكييفها القانوني وطبيعتها القانونية، وعرضت لرأي الفقهاء في مدى خضوع هذه الهجمات وتطبيقاتها لقواعد القانون الدولي الإنساني، ثم عرضت لأهم الإشكالات التي تواجه تطبيق القانون الدولي الإنساني ومبادئه على هذه الهجمات لما تتميز به من طبيعة خاصة.

ومما توصلت إليه من نتائج ومقترحات في هذا البحث، أن:

أولًا: النتائج:

- أن مفهوم الهجمات السيبرانية ما زال محل جدل وخلاف فقهي، وهو ما يصعب من معالجته من الناحية القانونية ويزيد من الجدل والخلاف بشأن طبيعتها وعناصرها.
- مبادئ القانون الدولي الإنساني رغم شموليتها وعموميتها تواجه تحديات كبيرة في تطبيقاتها على الهجمات السيبرانية.
- أن للهجمات السيبرانية طبيعة افتراضية، تجعل من تطبيق مبادئ القانون الدولي الإنساني كمبدأ التمييز والتناسب والضرورة العسكرية بشكل دقيق وفعال مسألة صعبة إن لم تكن مستحيلة.
- أن هناك فجوات تنظيمية حقيقية في إطار القانون الدولي الإنساني الحالي، تحول دون تطبيق قواعده بشكل فعال ومباشر على الهجمات السيبرانية.
- أن دليل "تالين" مثل خطوة هامة نحو تنظيم الهجمات السيبرانية ضمن إطار القانون الدولي، إلا أنه لا يغطي كل الجوانب الهامة، كما أنه غير ملزم ويواجه اعتراضات دولية، ما يجعل هناك حاجة ملحة لإنشاء إطار قانوني دولي خاص لتنظيم الحروب السيبرانية وتأثيراتها المتزايدة في عالم يعتمد بشكل متزايد على التكنولوجيا.

ثانيًا: المقترحات:

- نقترح على المجتمع الدولي وفقهاء القانون الدولي بصفة خاصة، بضرورة العمل على إيجاد تعريف موحد للهجمات السيبرانية، على أن يتضمن هذا التعريف عناصر هذه الهجمات بما يساعد على تحديد الطبيعة القانونية لها.
- نظرًا لأهمية حماية البنية التحتية العالمية من الهجمات السيبرانية، فإن العالم اليوم بحاجة إلى معاهدة دولية تضع قواعد واضحة لاستخدام الهجمات السيبرانية وتقييدها بما يتماشى مع أهداف ومبادئ القانون الدولي الإنساني.
- نقترح على المجتمع الدولي بضرورة العمل على اتخاذ خطوات جادة لإنشاء إطار قانوني يحدد آلية التعامل مع الهجمات السيبرانية ليس فقط في أوقات النزاعات المسلحة، وإنما في أوقات السلم كذلك، بحيث يجب أن يتضمن هذا الإطار مبادئ عامة تلزم الدول الأعضاء بتحمل مسؤولياتها في منع هذه الهجمات وضمان عدم تأثيرها على البنى التحتية المدنية وحياة

وممتلكات الأفراد، ويكون ذلك ليس فقط بالعمل على إنشاء اتفاقية دولية ملزمة تساهم في تنظيم الفضاء السيبراني وتحقيق الأمن والاستقرار الدولي، وإنما كذلك من خلال العمل على إدماج الهجمات السيبرانية ضمن المنظومة القانونية الدولية بداية من ميثاق الأمم المتحدة، مرورًا باتفاقيات جنيف الأربع لعام 1949 والبروتوكولات المضافة لها.

قائمة المصادر:

أولًا: المراجع العربية:

1. المؤلفات العامة:

1. إيهاب خليفة، كيفي يمكن أن تدير الدول شؤونها في عصر الإنترنت، دار العربي للنشر والتوزيع، القاهرة، 2017.
2. صلاح الحديثي، التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية، الطبعة الأولى، منشورات المجموعة العلمية للطباعة والنشر والتوزيع، مصر، 2021.
3. سهيل حسين الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2016.
4. هالة الرشيدي، الإرهاب السيبراني، ماهيته ووجوده ومكافحته، الطبعة الأولى، دار النهضة العربية، القاهرة، 2021.

2. المجلات الدورية:

1. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، العدد الرابع، السنة الثامنة، 2016، العراق.
2. طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، 2019.
3. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، المجلة المصرية للقانون الدولي، المجلد 77، 2021.
4. عمار ياسر زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، مركز بحوث الشرطة ، الشارقة، المجلد 30، العدد 118، 2021.
5. عمر محمود عمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة الشريعة والقانون، المجلد 46، العدد الثالث، 2019.

6. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من عدد 2002.
7. محمد حسن سعيد دراجي، عمر صالح العكور، الهجمات السيبرانية وفقًا لأحكام القانون الدولي الإنساني، مجلة الشريعة والقانون، العدد 51 المجلد الأول، 2024.
8. منزر رابح، ودرويش سعيد، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن، العدد الأول، 2021.
9. نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، المجلد السادس عشر، العدد الرابع، السنة 2021.
10. يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد 23، السنة 14، 2017.
11. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلد الرابع، العدد الرابع، 2018.

- مواقع الانترنت:

1. بشار خليل، ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي، مجلة المعلوماتية، العدد 154، الجمعية السورية للمعلوماتية، 2020، متاح عبر العنوان الإلكتروني: https://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=853
2. Stuxnet computer worm, available at: Stuxnet | Definition, Origin, Attack, & Facts | Britannica, available at: https://www.britannica.com/technology/Stuxnet
3. University of Maryland, Department of Computer Science. The Morris Worm: A Fifteen-Year Perspective. 2019, https://www.cs.umd.edu/class/fall2019/cmsc818O/papers/morris-worm.pdf

Sources

1- Ihab Khalifa, How Can Countries Manage Their Affairs in the Age of the Internet, Al-Arabi Publishing and Distribution, Cairo, 2017.
2- Salah Al-Hadithi, A Comprehensive Detailed Study of the Development of Legal Rules Regarding Cyber Warfare, First Edition, Scientific Group for Printing, Publishing, and Distribution, Egypt, 2021.
3- Suhail Hussein Al-Fatlawi, Cyber Attacks: A Legal Analytical Study, First Edition, Zain Legal Publishing, Beirut, 2016.
4- Hala Al-Rashidi, Cyber Terrorism: Its Nature, Existence, and Combating, First Edition, Al-Nahda Al-Arabia Publishing, Cairo, 2021.

Journals:

1- Ahmad Abis Ni'ma Al-Fatlawi, Cyber Attacks: Their Concept and the International Responsibility Arising from Them in Light of Contemporary International Organization, Al-Muhaqqiq Al-Hilli Journal, Issue 4, Vol. 8, 2016, Iraq.
2- Talal Yassin Al-Issa, Oday Mohammad Anab, International Responsibility Arising from Cyber Attacks in Light of Contemporary International Law, Zarqa Journal for Research and Humanities Studies, Vol. 19, Issue 1, 2019.
3- Abdullah Abdul Karim Ali Ahmad, Cyber Attacks in Light of International Law, Egyptian Journal of International Law, Vol. 77, 2021.

4- Ammar Yasser Zuhair, Contemporary Security Challenges of Cyber Attacks, Police Research Center, Sharjah, Vol. 30, Issue 118, 2021.
5- Omar Mahmoud Omar, Electronic Warfare in International Humanitarian Law, Sharia and Law Journal, Vol. 46, Issue 3, 2019.
6- Michael Schmidt, Warfare Through Communication Networks: Attacking Computer Networks and the Law of War, International Review of the Red Cross, Selected from the 2002 Issue.
7- Mohammed Hassan Saeed Daraji, Omar Saleh Al-Akor, Cyber Attacks According to the Provisions of International Humanitarian Law, Sharia and Law Journal, Issue 51, Vol. 1, 2024.
8- Manzer Rabeh, and Darwish Said, The Legal Nature of Cyber Attacks Between States, Voice of Law Journal, Vol. 8, Issue 1, 2021.
9- Naseeb Najib, Cyber Warfare from the Perspective of International Humanitarian Law, Critical Law Journal of Law and Political Science, Vol. 16, Issue 4, 2021.
10- Yahya Mufreh Al-Zahrani, Strategic and Legal Dimensions of Cyber Warfare, Research and Studies Journal, Issue 23, Vol. 14, 2017.
11- Yahya Yassin Saud, Cyber Warfare in Light of the Rules of International Humanitarian Law, Vol. 4, Issue 4, 2018.

Websites:

Bashar Khalil, What is Cyber Warfare? A Terrifying Future for Digital Conflict, Informatics Magazine, Issue 154, Syrian Informatics Association, 2020, available at:

https://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=853

4. Stuxnet computer worm, available at: Stuxnet | Definition, Origin, Attack, & Facts | Britannica, available at: https://www.britannica.com/technology/Stuxnet University of Maryland, Department of Computer Science. The Morris Worm: A Fifteen-Year Perspective. 2019, https://www.cs.umd.edu/class/fall2019/cmsc818O/papers/morris-worm.pdf

ثانيًا: المراجع الأجنبية:

1. Evelyne Akoto: Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?" : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014- 2015 .
2. K. Saalbach: Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014.
3. Michael N. Schmitt: Rewired Warfare: Rethinking the Law of Cyber Attack, International Review of the Red Cross, Cambridge University Press, 2017.

الهوامش:

(1) طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، 2019، ص82 – 95.

(2) منزر رابح، ودرويش سعيد، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن، العدد الأول، 2021، ص538 – 557.

(3) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، المجلة المصرية للقانون الدولي، المجلد 77، 2021، ص 1-37.

(4) Michael N. Schmitt: Rewired Warfare: Rethinking the Law of Cyber Attack, International Review of the Red Cross, Cambridge University Press, 2017, p. 189- 206.

(5) د. عمار ياسر زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، مركز بحوث الشرطة ، الشارقة، المجلد 30، العدد 118، 2021، ص27.

(6) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، العدد الرابع، السنة الثامنة، 2016، العراق، ص616.

(7) يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد 23، السنة 14، 2017، ص235.

(8) K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6.

(9) المادة 30 من دليل تالين المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية، وهو دليل لدراسة تداعيات الحروب والهجمات السيبرانية والقواعد المعيارية المنظمة لها، صدر عن مجموعة من الخبراء العسكريين والقانونيين بالناتو بالتعاون مع اللجنة الدولية للصليب الأحمر. يراجع: صلاح الحديثي، التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية، الطبعة الأولى، منشورات المجموعة العلمية للطباعة والنشر والتوزيع، مصر، 2021، ص 21.

(10) هالة الرشيدي، الإرهاب السيبراني، ماهيته ووجوده ومكافحته، الطبعة الأولى، دار النهضة العربية، القاهرة، 2021، ص 31.

(11) Saalbach," Cyber War, op. cit. p. 6.

(12) د. عبد الله عبد الكريم علي أحمد، مرجع سابق، ص 13.

(13) عبد الله عبد الكريم، مرجع سابق، ص9.

(14) ففي مساء يوم 2 نوفمبر 1988، خرج حريق هائل عن السيطرة على الإنترنت، مما تسبب في "إشعال" حواسيب عديدة، كان هذا الحدث أول تجربة للوكيل المتنقل على الإنترنت أو إضافة جديدة إلى سجل التخريب الحاسوبي: الدودة المشهورة باسم دودة

موريس. كانت من عمل روبرت تابان موريس، طالب الدراسات العليا في علوم الحاسوب في جامعة كورنيل، وقد أثارت الدودة قلقًا كبيرًا بين أولئك المتصلين بالإنترنت. للمزيد يراجع:

University of Maryland, Department of Computer Science. The Morris Worm: A Fifteen-Year Perspective. 2019, available at: https://www.cs.umd.edu/class/fall2019/cmsc818O/papers/morris-worm.pdf.

([15]) Evelyne AKOTO: Les cyberattaques étatiques constituent−elles des actes d'agression en vertu du droit international public ?" : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014− 2015, p. 13.

([16]) Stuxnet computer worm, available at: Stuxnet | Definition, Origin, Attack, & Facts | Britannica accessed in: 10/10/2024.

([17]) إيهاب خليفة، كيفي يمكن أن تدير الدول شؤونها في عصر الإنترنت، دار العربي للنشر والتوزيع، القاهرة، 2017، ص 205.

([18]) محمد حسن سعيد دراجي، عمر صالح العكور، الهجمات السيبرانية وفقًا لأحكام القانون الدولي الإنساني، مجلة الشريعة والقانون، العدد 51 المجلد الأول، 2024، ص4.

([19]) سهيل حسين الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2016، ص123.

([20]) نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، المجلد السادس عشر، العدد الرابع، السنة 2021، ص 226.

([21]) عمر محمود عمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة الشريعة والقانون، المجلد 46، العدد الثالث، 2019، ص137.

([22]) طلال ياسين، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مرجع سابق، ص88.

(23) حيث تنص على أن "يمتنع جميع أعضاء الأمم المتحدة في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو بأي أسلوب آخر لا يتوافق مع أهداف الأمم المتحدة".

(24) عبد الله عبد الكريم، مرجع سابق، ص 22.

(25) مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من عدد 2002، ص 90.

(26) وقد تم إدراج شرط ماتينيز في اتفاقيات لاهاي 1899 – 1907 وفي اتفاقيات جنيف الأربع لعام 1949، وفي الفقرة الثانية من المادة الأولى من البروتوكول الإضافي لسنة 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. يراجع، صلاح الحديثي، مرجع سابق، ص 120.

(27) محمد حسين دراجي، الهجمات السيبرانية وفقًا لأحكام القانون الدولي الإنساني، مرجع سابق، ص5.

(28) يراجع المادة 35 من البروتوكول الإضافي لاتفاقيات جنيف لسنة 1977.

(29) يراجع المادة 36 من البروتوكول الإضافي لاتفاقيات جنيف لسنة 1977.

(30) نسيب نجيب، مرجع سابق، ص 229.

(31) عبد الله عبد الكريم، مرجع سابق، ص22.

(32) فقد أشارت المادة 15 من البروتوكول إلى حظر مهاجمة المنشآت المحتوية على قوى خطرة حتى لو كانت أهدافًا عسكرية، إذا كان من شأن ذلك أن يلحق خسائر فادحة بالسكان المدنيين، كما حظرت المادة 17 من البروتوكول ذاته الترحيل القسري للمدنيين ما لم تبرره الضرورة العسكرية الملحة.

(33) د. عبد الله عبد الكريم، مرجع سابق، ص 24.

(34) نسيب نجيب، مرجع سابق، ص231.

(35) يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلد الرابع، العدد الرابع، 2018، ص97، 98.

(36) يعد التمييز يعد أحد أهم المبادئ الأساسية التي يقوم عليها القانون الحديث للنزاعات المسلحة. يتمحور هذا المبدأ حول فكرة أساسية مفادها أن المدنيين يجب أن يكونوا

محصنين من الاستهداف في سياق النزاعات المسلحة. ورغم أن أحكامًا صريحة بشأن حصانة المدنيين لم تُدرج حتى صدور البروتوكول الإضافي الأول عام 1977، إلا أن مبدأ التمييز يعتمد على قناعة أساسية عُبّر عنها في أحد أقدم القوانين المعاصرة التي تنظّم النزاعات المسلحة، وهو إعلان سانت بطرسبرغ لعام 1868، حيث ينص إعلان سانت بطرسبرغ على أن "تقدم الحضارة يجب أن يسهم في التخفيف قدر الإمكان من ويلات الحرب؛ وأن الهدف المشروع الوحيد الذي ينبغي للدول أن تسعى لتحقيقه أثناء الحرب هو إضعاف القوات العسكرية للعدو". كما ينص البروتوكول الإضافي الأول في المادة 48 منه على أن: " ضمان احترام وحماية السكان المدنيين والأعيان المدنية، يجب على أطراف النزاع التمييز في جميع الأوقات بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية. وبناءً على ذلك، يجب أن توجه عملياتهم فقط ضد الأهداف العسكرية".

(37) عبد الله عبد الكريم، مرجع سابق، ص 26.

(38) أحمد عبيس الفتلاوي، الهجمات السيبرانية، مرجع سابق، ص636.

(39) ويتعلق بقواعد القانون الدولي المطبقة على الحروب السيبرانية، وقد تم إعداده من قبل مجوعة خبراء في القانون الدولي تابعين لحلف شمال الأطلسي ومشاركة اللجنة الدولية للصليب الأحمر، وله اصداران الأول سنة 2013 وتكون من 95 مادة استمدت في مجملها في أحكام القانون الدولي المختلفة كميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني، والثاني عام 2017 ويتكون من 154 قاعدة قانونية، ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات السيبرانية الأخرى التي تحدث يوميا خلال وقت السلم بشار خليل، ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي، مجلة المعلوماتية، العدد 154، الجمعية السورية للمعلوماتية، 2020، متاح عبر العنوان الإلكتروني:
https://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=853
تاريخ الاطلاع 2024/10/11.

(40) منزر رابح ودرويش سعيد، الطبيعة القانونية للهجمات السيبرانية، مرجع سابق، ص548.

حيث تنص المادة 4/2 من ميثاق الأمم المتحدة على أن: "يمتنع أعضاء الهيئة جميعًا ([41]) 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".