المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 6 - الإصدار 62
تأريخ النشر: 20 ديسمبر 2024 م

القانون الدولي الإنساني والنزاعات المسلحة

International Humanitarian Law and Armed Conflicts

إعداد: الدكتور/ صابر محمد محمود المزعل

قسم القانون، كلية إدارة الأعمال، جامعة الأمير سطام بن عبد العزيز، الخرج، المملكة العربية السعودية

Email: s.elmezel@psau.edu.sa

الباحثة/ ياسمين محمد حسن يونس

قسم القانون، كلية إدارة الأعمال، جامعة الأمير سطام بن عبد العزيز، الخرج، المملكة العربية السعودية

Email: y.younis@psau.edu.sa

الملخص

في ظل التطورات العلمية والتكنولوجية المتسارعة التي يشهدها العالم في هذا الوقت، يواجه القائمون على تطبيق قواعد القانون الدولي الإنساني (IHL)، تحديات جديدة تتعلق بتكييف أحكامه مع واقع النزاعات المسلحة المعاصر، كالحرب السيبرانية (Cyber Warfare). نهدف من خلال هذه الدراسة؛ إلى تحديد دور قواعد القانون الدولي الإنساني في حماية المدنيين والبنى التحتية الحيوية في الحروب السيبرانية، ومناقشة مدى ملاءمة القواعد القانونية القائمة للتعامل مع الطبيعة المتفردة لهذا النوع من الحروب، على أننا سوف نتبع من خلال هذه الدراسة على الأسلوب التحليلي لقواعد القانون الدولي الإنساني والاتفاقيات الدولية ذات الصلة.

وقد توصلنا من خلال هذه الدراسة إلى إن قواعد القانون الدولي الإنساني صيغت بصورة عامة لتشمل كافة أنواع النزاعات المسلحة، بما في ذلك الحروب السيبرانية. وعلى الرغم من أن مبادئ القانون الدولي الإنساني تتميز بالمرونة وقابلية التكيف مع النزاعات الحديثة، غير أن الطبيعة المتفردة للحروب السيبرانية مازالت تثير شكوكًا حقيقية حول فاعلية قواعد القانون الدولي الإنساني في توفير الحماية القانونية للمدنيين والبنى التحتية، وضمان التزام أطراف النزاع بتطبيق المبادئ الأساسية للقانون الدولي الإنساني، كمبدأ التمييز وقاعدة التناسب بشكل كامل. وقد أوصى الباحثين إلى ضرورة تطوير قواعد القانون الدولي الإنساني وإبرام اتفاق دولي جديد يتناول حصرياً الأمن السيبراني ومكانته في القانون الدولي، قادر على حماية المدنيين والبنى التحتية من الأضرار الناشئة عن الحروب السيبرانية. وإعداد بروتوكول إضافي خاص بحماية المدنيين والبنى التحتية الحيوية المتضررة من الحروب السيبرانية؛ ووضع معيار واضح للتفرقة بين الأنماط المختلفة للحروب السيبرانية، يمكن من خلاله تحديد ما إذا كان الهجوم السيبراني يشكل عدوانًا مسلحًا واستخدامًا للقوة يتيح للدول حق الدفاع عن نفسها من عدمه.

الكلمات المفتاحية: القانون الدولي الإنساني، النزاعات المسلحة، الحرب السيبرانية، حماية المدنيين، البنى التحتية الحيوية.

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 6 - الإصدار 62
تأريخ النشر: 20 ديسمبر 2024 م

International Humanitarian Law and Armed Conflicts

Dr/ Sabir M. Al-Meze'l
Department of Law, College of Business Administration, Prince Sattam bin Abdulaziz University, 165, Al-Kharj, 11942, Saudi Arabia.
s.elmezel@psau.edu.sa
Mrs/ Yasmeen M. Younis
Department of Law, College of Business Administration, Prince Sattam bin Abdulaziz University, 165, Al-Kharj, 11942, Saudi Arabia.
y.younis@psau.edu.sa

Abstract

In light of the rapid advancements in science and technology, those tasked with enforcing the rules of International Humanitarian Law (IHL) face new challenges in adapting its provisions to the realities of contemporary armed conflicts, such as cyber warfare. This study aims to determine the role of IHL rules in protecting civilians and critical infrastructure in cyber warfare, and to discuss the adequacy of existing legal rules in addressing the unique nature of this type of warfare. This study will employ an analytical approach to the rules of IHL and relevant international agreements. Through this study, we have found that the rules of IHL were formulated in a general manner to encompass all types of armed conflicts, including cyber warfare. Although the principles of IHL are flexible and adaptable to modern conflicts, the unique nature of cyber warfare still raises genuine doubts about the effectiveness of IHL rules in providing legal protection for civilians and infrastructure, and ensuring that parties to the conflict fully comply with the basic principles of IHL, such as the principle of distinction and the rule of proportionality. The researchers recommended the need to develop the rules of IHL and conclude a new international agreement that exclusively addresses cybersecurity and its place in international law, capable of protecting civilians and infrastructure from damages resulting from cyber wars. They also recommended the preparation of an additional protocol to protect civilians and vital infrastructures affected by cyber wars; and the establishment of a clear standard to differentiate between the different types of cyber wars, through which it can be determined whether a cyber-attack constitutes armed aggression and the use of force that allows states the right to defend themselves or not.

Keywords: International Humanitarian Law (IHL), Armed Conflict, Cyber Warfare, Protection of Civilians, Critical Infrastructure.

1. مقدمة:

منذ العصور القديمة كانت هنالك رغبة بدافع ديني أو فلسفي، بجعل الحروب أكثر إنسانية. وعلى ذلك، لم يشرع الدين الإسلامي الحنيف الحرب، بل شرع الجهاد الذي يعد ضرورة لا يتم اللجوء إليه إلا دفعًا للعدوان، وحين لا يكون هُنالك مفرٌ مِنه، أما الحرب العدائية فلم يَعرفُها الإسلام تماشيًا مع مبادئه المتمثلة بالسلام والتعايش بين مختلف الأمم والأديان، ولو كانت على غير الدين الإسلامي (الساجي: 2017). كما اعتمد فلاسفة عصر الأنوار مبدأ الكرامة الإنسانية، حيث نجد في كتاب فن الحرب للكاتب الصيني "سان زو" منذ القرن الخامس قبل الميلاد، أقدم النصوص لما يمكننا تسميته في وقتنا الحاضر بقواعد القانون الدولي الإنساني، والتي كانت تهدف إلى التخفيف من معاناة ضحايا النزاعات المسلحة، والسيطرة على أعمال العنف، والتخفيف من أضرار الحروب بوجه عام (الخفاجي: 2021).

يعد القانون الدولي الإنساني مجموعة القواعد والقيم والمبادئ التي تهدف إلى حماية الكرامة الإنسانية في سياق النزاعات المسلحة. وهو ينظم سلوك الأطراف المتحاربة، ويحدد القيود المفروضة على وسائل وأساليب الحرب. يستمد القانون الدولي الإنساني قوته من مجموعة متنوعة من المصادر القانونية، بما في ذلك المعاهدات الدولية، مثل اتفاقيات جنيف وبروتوكولاتها الإضافية، والعرف الدولي، والمبادئ القانونية العامة. وعلى الرغم من أهميته، فإن القانون الدولي الإنساني لا ينظم حق الدول في اللجوء إلى القوة المسلحة، بل يركز على حماية المدنيين وتنظيم الأعمال العدائية بمجرد اندلاع النزاع. وتعد اتفاقيات جنيف لعام 1949، التي اعتمدتها غالبية دول العالم، الإطار الأساسي للقانون الدولي الإنساني. وقد شهد هذا النظام القانوني تطوراً ملحوظاً بفضل البروتوكولات الإضافية لعام 1977، والتي أضافت أحكاماً جديدة لتعزيز الحماية الممنوحة لضحايا النزاعات المسلحة (Bouvier: 2020).

ارتبط مسار الحروب عبر تاريخها الطويل، بالتطورات التقنية التي عرفتها الجماعات البشرية، وسخرتها في سبيل تطوير قدراتها القتالية، وصولًا لتحقيق أهدافها، وتأمين مصالحها الحيوية (نجيب: 2021). ومع التوسع الكبير في اعتمادنا على البنية التحتية الرقمية وظهور ما يسمى بالحروب السيبرانية، باتت الحاجة ماسة لتطوير آليات قانونية فعالة لحماية المدنيين والبنية التحتية الحيوية. فقد أدى التقدم التكنولوجي إلى جعل الدول والمجتمعات والأفراد يعتمدون بشكل كامل على أجهزة الكمبيوتر وأنظمة الحاسب الآلي وشبكة الانترنت، وفي الوقت نفسه جعلهم عرضة للخطر من خلال الهجمات السيبرانية (Islam: 2017).

وعلى الرغم؛ من الدور الكبير الذي لا يزال يلعبه القانون الدولي الإنساني في حماية المدنيين والبنى التحتية الحيوية من مخاطر هذه الحروب، من خلال التزام كافة الأطراف بالمبادئ العامة والأطر الأساسية والبروتوكولات الخاصة بهذا القانون. إلا أن الحروب السيبرانية تتميز بسرعتها ومداها الواسع، مما يجعلها تشكل تهديدًا مباشرًا على المدنيين والبنى التحتية الحيوية في الدولة. حيث يمكن للهجمات السيبرانية أن تؤدي إلى تعطيل الخدمات الأساسية، مثل: الرعاية الصحية والاتصالات، وتسبب أضرارًا واسعة النطاق للبنية التحتية الحيوية، مثل: شبكات الكهرباء والنقل. الأمر الذي تظهر معه الحاجة المُلحة لتطوير قواعد القانون الدولي الإنساني لتشمل الحروب السيبرانية، وضمان تطبيقه بشكل فعال لحماية المدنيين والبنى التحتية الحيوية من الآثار المدمرة لهذه الحروب.

1.1. إشكالية الدراسة:

تتمثل الإشكالية الأساسية التي تبحث فيها هذه الدراسة، في تحديد مدى ملاءمة القواعد القانونية التقليدية "القائمة" في القانون الدولي الإنساني مع الطبيعة المتفردة للحروب السيبرانية،

وبيان مدى القدرة على الاستناد على الأحكام القانونية في القانون الدولي الإنساني لتغطية الأضرار الناشئة عن هذا النوع من الحروب والتي قد تصيب المدنيين والبنى التحتية الحيوية.

2.1. أهمية الدراسة:

تكتسب دراسة دور القانون الدولي الإنساني في النزاعات المسلحة، وتغطية عواقب الحروب السيبرانية على وجه التحديد، أهمية بالغة في ظل التطورات التكنولوجية المتسارعة التي تشهدها البشرية. فمع تزايد الاعتماد على الأنظمة الرقمية في كافة مناحي الحياة، باتت الحروب السيبرانية تشكل تهديداً جدياً للسلم والأمن الدوليين. لذا، تكمن أهمية هذه الدراسة في أنها تتناول موضوعًا حديثًا لا يزال في طور التبلور، وذلك من خلال تحديد المقصود بالحروب السيبرانية، وبيان مدى قابلية قواعد القانون الدولي الإنساني للتطبيق على الحروب السيبرانية من أجل حماية المدنيين والبنى التحتية الحيوية.

3.1. أسئلة الدراسة:

سوف نحاول من خلال هذه الدراسة الإجابة عن التساؤلات التالية:

- ما هو القانون الدولي الإنساني؟
- ما هي أهداف القانون الدولي الإنساني؟
- ما هي المبادئ الأساسية التي تقوم عليها فلسفة قواعد القانون الدولي الإنساني؟
- ماهي النزاعات المسلحة، وهل تعتبر الحرب السيبرانية نوعًا جديدًا من هذه النزاعات؟
- ماهي الحرب السيبرانية، وماهي الآثار الناشئة عنها؟ وهل ترقى لاعتبارها عدوانًا خارجيًا يمنح الدولة المعتدى عليها حق الدفاع عن النفس؟
- كيف يمكن تغطية عواقب الحروب السيبرانية طبقًا للقواعد القانونية القائمة في القانون الدولي الإنساني؟
- هل القواعد القانونية التقليدية في القانون الدولي الإنساني كافية لتغطية آثار الحروب السيبرانية؟
- ما هي التحديات التي تواجه تطبيق قواعد القانون الدولي الإنساني لمواجهة آثار الحروب السيبرانية؟
- كيف يمكن التغلب على التحديات التي تعيق تطبيق قواعد القانون الدولي الإنساني لتغطية آثار الحروب السيبرانية؟

4.1. أهداف الدراسة:

نحاول من خلال هذه الدراسة تحقيق الأهداف التالية:

- تحديد الإطار العام للقانون الدولي الإنساني والمبادئ الأساسية التي يقوم عليها.
- تحديد المقصود بالحروب السيبرانية، ومدى اعتبارها نوعًا جديدًا من النزاعات المسلحة.
- تحديد مدى اعتبار الحرب السيبرانية عدوانًا خارجيًا يعطي الدولة المعتدى عليها الحق بالدفاع عن النفس.
- تحديد المبادئ التي يقوم عليها القانون الدولي الإنساني والتي يمكن الاستناد إليها لتغطية عواقب الحروب السيبرانية.
- تحديد الثغرات القانونية في قواعد القانون الدولي الإنساني في مواجهة النزاعات المعاصرة، كالحروب السيبرانية.

5.1. منهج الدراسة:

سيعتمد الفريق البحثي في هذه الدراسة على المنهج التحليلي لدراسة مدى ملائمة القواعد القانونية الحالية في القانون الدولي الإنساني للطبيعة الخاصة التي تمتاز بها الحروب السيبرانية. حيث سنقوم بدراسة قواعد القانون الدولي الإنساني والأحكام القانونية

للاتفاقيات والمعاهدات الدولية ذات الصلة، بما في ذلك اتفاقيات جنيف وبروتوكولاتها الإضافية، واتفاقية لاهاي، وميثاق الأمم المتحدة. وسنسعى من خلال هذا التحليل إلى تحديد الثغرات القانونية وتحديد مواطن القصور في النظام القانوني القائم والتي قد تقف حائلًا دون توفير الحماية القانونية الكافية للمدنيين والبنى التحتية الحيوية المتضررة من الحروب السيبرانية.

6.1. خطة الدراسة:

سوف نقسم هذه الدراسة إلى مبحثين رئيسيين، وعلى النحو الآتي:

المبحث الأول: الحروب السيبرانية كصورة مُتطورة للنزاعات المسلحة.

المبحث الثاني: أدوات القانون الدولي الإنساني لتغطية عواقب الحروب السيبرانية.

2. الحروب السيبرانية كصورة مُتطورة للنزاعات المسلحة:

لطالما ارتبط مفهوم الحرب بالنزاعات المسلحة، حيث كان مصطلح "الحرب" هو المصطلح السائد في المؤلفات القانونية والدراسات العسكرية لفترات طويلة، وقد تجسد ذلك في التشريعات الدولية والوطنية، وفي الكتابات التاريخية التي تناولت الحروب العالمية وغيرها من النزاعات المسلحة. كما انعكس هذا الاستخدام على التشكيلات الحكومية للدول، حيث كانت الوزارات الحربية هي المعنية بشؤون القتال. مع ذلك، شهدت العقود الأخيرة تحولاً لافتاً في المصطلحات المستخدمة، حيث ظهرت مصطلحات مثل "النزاعات المسلحة" و"العمليات العدائية" و"عمليات الدفاع عن النفس" بدلاً من مصطلح "الحرب". ويعود السبب الرئيسي لهذا التحول إلى ميثاق الأمم المتحدة الذي حظر الحرب واللجوء إلى استخدام القوة المفرطة كأداة لحل الخلافات الدولية، ما لم تكن دفاعاً عن النفس وفقاً للشروط والضوابط التي حددها الميثاق.

وعلى هدي ذلك، فإنه من الضروري بدايةً تحديد المقصود بالحروب السيبرانية، وما إذا كان هذا النوع من الحروب يرقى لاعتبارها صورة متطورة من النزاعات المسلحة وفقًا لمفهوم القوة تعطي للدول المستهدفة حق الدفاع عن النفس، أما أنها مجرد هجمات عدائية تهدف إلى تحقيق أهداف اقتصادية أو سياسية. من جهة أخرى؛ فإنه لابد من بيان الأنماط المختلفة لهذا النوع من الحروب، وذلك في مطلبين رئيسيين، وعلى النحو الآتي:

المطلب الأول: مفهوم الحرب السيبرانية.

المطلب الثاني: أنماط الحرب السيبرانية.

1.2. مفهوم الحرب السيبرانية:

منذ بدء الخليقة والحرب حقيقة واقعة من حقائق الحياة، حتى أضحت ظاهرة اجتماعية وإنسانية صاحبة الإنسان منذ ظهوره على الأرض ولازمته في مسيرته عبر القرون، فهي سجال بين البشر طالما هنالك تضارب في المصالح (الساجي:2017). تعتبر الحروب السيبرانية أحدث أنواع النزاعات المسلحة في العصر الحديث، ورغم أن هذا النوع من الحروب قد يبدو حديث العهد، إلا أن جذوره تمتد إلى عقود مضت. على أنه لا يمكن تحديد تاريخ مُحدد لبداية الحروب السيبرانية، حيث ظهر هذا النوع من الحروب تزامنًا مع الثورة المعلوماتية وتطور تدريجياً مع تطور قطاع التكنولوجيا والاتصالات. فقد أدى ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مختلف المجلات، إلى ظهور الآثار السلبية والمخاطر الناجمة عن التوسع الكبير في الاعتماد على تكنولوجيا المعلومات، وبالتزامن مع التطور الكبير في تكنولوجيا المعلومات والاتصالات ظهر ما يسمى بالهجمات السيبرانية التي تتم في الفضاء السيبراني. والتي تستهدف بدرجة كبيرة المواقع الحيوية ذات الأهمية، كالمواقع العسكرية، والبنى التحتية للخدمات الأساسية (نجيب: 2021).

أطلق العديد من المصطلحات والمفاهيم للدلالة على الحرب السيبرانية، فقد استخدم جانب من الفقه مصطلح "الحرب الافتراضية" في بعض الأحيان للدلالة على هذا النوع من الحروب، كما استخدم مصطلح "الحرب الإلكترونية" في أحيان أخرى، وكذا مصطلح "الهجمات السيبرانية"، فضلًا عن مصطلح "الهجمات المعلوماتية" (البلداوي:2022).

تشير الحرب السيبرانية إلى تلك الهجمات التي تندرج ضمن تعريف النزاعات المسلحة، وعلى الرغم من أن المحللين والخبراء يتوقعون أن الهجمات السيبرانية لها أضرار اقتصادية ومادية جسيمة وواسعة النطاق للسكان المدنيين، إلا أنه لم يتم التوقيع على أي وثيقة على المستوى الدولي تقدم تعريفًا شاملاً للحرب السيبرانية وتنص على أحكام تنظم الحرب السيبرانية (Islam: 2017).

وعلى ذلك، فإنه ليس هنالك ثمة إجماع على كافة المستويات حول تحديد المفهوم الدقيق لما يعرف بـ "الحرب السيبرانية" حتى الآن، وتكمن المشكلة الأساسية في غياب هذا التعريف إلى الطبيعة المتفردة والمتسارعة للعمليات السيبرانية (محمد:2013). ولعل التعريف الأكثر استشهادًا حول الحرب السيبرانية، هو التعريف الذي قدمه رئيس هيئة الأركان العامة في الجيش الأمريكي "ريتشارد كلارك" وزميله في الأمن الدولي في مجلس العلاقات الخارجية "روبرت نايك" بأن الحرب السيبرانية هي "أعمال من جانب دولة قومية لاختراق كمبيوتر أو شبكات دولة أخرى بغرض التسبب في الضرر أو التعطيل". كما يرى ريتشارد بأن الحرب السيبرانية تشكل أكثر من مجرد مسألة أمنية عسكرية، بل أنها قضية أمن قومي حقيقية تتطلب استراتيجية منسقة بالكامل للمجتمع بأكمله، حكومة وقطاع خاص (Richard & Robert:2010).

كما يرى جانب من الفقه بأن الحرب السيبرانية تنطوي على هجوم مُتعمد لتعطيل أو تدمير شبكات الكمبيوتر في دولة أخرى، غير أنه من غير الواضح كم من الضرر يتوقع أن يحدث قبل اعتبار العملية السيبرانية بمثابة عملًا حربيًا بموجب ميثاق الأمم المتحدة (Tom: 2010).

وقد عرف "Michael N. Schmitt" الحرب السيبرانية، بأنها: مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة (سعود:2018).

ولعل من أحدث التعريفات للحرب السيبرانية ما جاء به مجموعة الفقهاء التابعين للناتو، وفقًا للمادة (30) من دليل "تالين" المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية، والتي تنص على أنه: "تشمل الحرب السيبرانية: كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف أو ضرر للأشياء المادية" (درويش:2017).

بدورها، تعرف (ICRC) الحرب السيبرانية، بأنها: "الأفعال التي يتخذها أطراف النزاع، لتحقيق ميزة على خصومهم في الفضاء الإلكتروني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على الطاقة البشرية من الناحية النظرية، حيث يمكن تحقيق المزايا عن طريق إتلاف أو تدمير أو إعطاب أو نهب أنظمة الحاسوب لدى الخصم، أو بالحصول على معلومات يفضل الخصم أن تبقى سرية، أو من خلال الاستغلال السيبراني (باكير: 2010).

من وجهة نظر قانونية، فإنه من المهم التفرقة بين الهجمات السيبرانية التي تدخل ضمن سياق النزاعات المسلحة وتعتبر بمثابة هجمات عدوانية تثير تطبيق قواعد القانون الدولي وقواعد القانون الدولي الإنساني، عن الهجمات الأخرى التي تتم في الفضاء السيبراني والتي تشنها جماعات إجرامية خارجة عن القانون، والتي لا تنطبق عليها قواعد القانون الدولي؛

حيث أن مصطلح الحرب السيبرانية يجب أن يشير إلى الهجمات السيبرانية التي تشنها دولة ضد دولة أخرى، والتي قد تحدث بالاتساق مع الحروب التقليدية "الحركية" المسلحة، أو قد تتم بشكل منفصل، والتي تستخدم فيها الدول الأسلحة السيبرانية أو الأسلحة المعلوماتية التي قد تصل بتأثيرها ومداها إلى حد استخدام الأسلحة التقليدية في النزاع المسلح (بن تغري:2020).

وعلى ذلك، يرى جانب من الفقه بأنه لا يمكن إطلاق مصطلح الحرب السيبرانية إلا إذا كان الهجوم السيبراني في سياق نزاع مسلح قائم، أو كهجمات عدوانية من دولة ضد دولة أخرى، إذ لا يمكن اعتبار الهجمات التي يقوم بها كيان غير مشروع نوعًا من الحروب السيبرانية التي يطبق عليها قواعد القانون الدولي (هديب:2024).

من جهتنا، يمكن تعريف "الحرب السيبرانية" على أنها هجمات إلكترونية معلوماتية متطورة، تشنها دولة معادية ضد دولة أخرى معتدى عليها، للسيطرة على شبكات الكمبيوتر الخاصة بالمرافق العسكرية والحيوية في الدولة المعتدى عليها، والتحكم بها أو التشويش عليها، وقد تكون هذه الهجمات متزامنة مع النزاع المسلح القائم بينهما، وقد تجري في حالات أخرى بشكل منفصل وبصورة مفاجئة.

2.2. أنماط الحرب السيبرانية:

في عالم الحرب السيبرانية، هناك عمليات مرئية للغاية، مثل القرصنة على محطة طاقة أو محطة تليفزيونية، وهناك العمليات الأكثر سرية، كما حدث بين الصين والولايات المتحدة الأمريكية، حيث جاء في تقرير استخباراتي أمريكي في منتصف عام 2021، محاولة بكين التسلل إلى البنى التحتية الحيوية في الولايات المتحدة الأمريكية، الأمر الذي دفع الأخيرة إلى تشكيل أكبر تحالف استخباراتي يضم بالإضافة إلى الولايات المتحدة الأمريكية، كلًا من بريطانيا واستراليا وكندا ونيوزيلندا، للتصدي لأية هجمات سيبرانية متوقعة من الدول المعادية. ولا تشكل هذه الحادثة في الوقت الحاضر سوى غيض من فيض من الهجمات السيبرانية التي تحدث حول العالم (جراليه:2023).

وقد تبين لنا في المطلب السابق بأنه لا يوجد إجماع دولي حول ما يعتبر حربًا سيبرانية تعطي الحق للدولة الدفاع عن نفسها، حيث أن مفهوم القوة في الحروب السيبرانية له مدلولاته عن مفهومها التقليدي وفقًا لما قصده واضعي ميثاق الأمم المتحدة، فإن هنالك إطار تفسيري آخر لاستخدام القوة في الفضاء السيبراني تختلف درجته وتأثيره وفقًا لأنماط متعددة من الحروب السيبرانية.

تُرتكب أنواع مختلفة من الهجمات السيبرانية عن طريق أنظمة الكمبيوتر من قبل الأفراد أو المنظمات غير الحكومية أو من قبل حكومات بعض الدول، ليس مفهومًا إن كانت هذه الهجمات ترقى لاعتبارها عدوانًا خارجيًا يعطي الدول المعتدى عليها حق الدفاع عن النفس، غير أنه من الواضح مؤخرًا بأن العديد من الهجمات السيبرانية أصبحت تشكل خطرًا حقيقيًا ومصدر قلق كبير للمجتمعات العالمية. وقد أدى تقاعس المجتمع الدولي عن وقف الهجمات السيبرانية، وصعوبة تحديد مرتكبيها، إلى تزايد نسب وقوعها وتوسع نطاقها، وارتفاع حجم الأضرار الناتجة عنها، الأمر الذي دفع مرتكبي هذه الهجمات إلى توسيع نطاقها من خلال تطوير تقنياتهم، وارتكابهم هجمات أكبر حجمًا وأوسع نطاقًا، ومع مرور الوقت إلى شن حروب سيبرانية. وفي ظل هذا الوضع الراهن؛ فإنه من غير الواضح من اتفاقيات جنيف وبروتوكولاتها الإضافية، فيما إذا كان القانون الدولي الإنساني ينطبق على الحرب السيبرانية (Islam: 2017).

كأصل عام، تتوقف فعالية تطبيق قواعد ومبادئ القانون الدولي الإنساني على التمييز بين أنواع النزاعات المسلحة. وهو ما يمكن اتباعه أيضاً بالنسبة للحروب السيبرانية التي تتباين في أشكالها وأنماطها، وذلك تبعاً لطبيعة الصراع والأهداف المرجوة من ورائه والقدرات التقنية المتاحة للأطراف المتحاربة، وللضرورة التي تستدعي استخدام أي نمط من هذه الأنماط.

وبهذا الصدد؛ يمكن تصنيف الحروب السيبرانية إلى ثلاثة أنماط رئيسية: الحروب السيبرانية الباردة، والحروب السيبرانية متوسطة الشدة، والحروب السيبرانية الساخنة. على أننا سوف نتناول هذه الأنماط تباعًا، وعلى النحو الآتي:

1.2.2. الحروب السيبرانية الباردة.

يصنف هذا النوع من الحروب بأنه من الحروب طويلة الآجل، أو من الحروب المستمرة ذات الطبيعة الممتدة. ويُعبر هذا النوع من الحروب عن الصراعات الناشئة بين دولتين كنتيجة لخلافات أيديولوجية أو عرقية أو دينية، فطبيعة الخلاف بين الدولتين له جذور تاريخية ممتدة. غالبًا ما يتخذا هذا النمط من الحروب السيبرانية أنشطة سيبرانية منخفضة الشدة، يتم اللجوء إليها كبديل عن الحروب المسلحة والمعلنة، ولا تتطور بالضرورة إلى استخدام الأسلحة التقليدية، أو شن حرب سيبرانية واسعة النطاق (هديب:2024).

تلجأ الدول في الحرب السيبرانية الباردة إلى استخدام عدة وسائل، منها: التجسس على المرافق الحيوية والمواقع العسكرية، سرقة المعلومات أو القرصنة، شن هجمات تخريبية، اختراق المواقع الحساسة. كما قد تنشط في هذا النمط من الحروب السيبرانية جماعات دولية للقرصنة للتعبير عن مواقف سياسية، او حقوقية، أو دينية، كجماعة ويكيليكس، وأنونيموس (بن تغري:2020).

ويتجلى هذا النوع من الحروب السيبرانية في الصراعات السياسية ذات البعد الديني الممتد، مثل الصراع العربي الإسرائيلي، أو الصراع الهندي الباكستاني. ويعد من أبرز الأمثلة على هذا النوع من الحروب السيبرانية، ما تعرضت له دولة "إستونيا" إحدى دول الإتحاد السوفييتي المنهار، من هجمات سيبرانية في عام 2007 طالت العديد من المواقع الحكومية شملت مواقع لرئيس الوزراء الأستوني ورئيس البرلمان، فضلًا عن بعض المواقع الخاصة، بما في ذلك البنوك وشركات الهاتف المحمول وخدمات الطوارئ، ما أدى إلى إصابتها بالشلل التام. وقد اتهمت الحكومة الأستونية دولة روسيا بالوقوف خلف هذه الهجمات، واعتبرتها بمثابة مواقف إنتقامية بسبب نقلها للنصب التذكاري المخلد للجيش الروسي خارج العاصمة تالين (Shackelford:2009).

2.2.2. الحروب السيبرانية متوسطة القوة.

يظهر هذا النوع من الحروب السيبرانية بالتزامن مع الحروب التقليدية المسلحة الدائرة بين دولتين، والتي تسير جنبًا إلى جنب وبالتوازي مع النزاع المسلح القائم، أو التي قد تكون سابقة في بعض الأحيان للحرب المسلحة الحركية، أو تمهيدًا للتدخل العسكري المسلح. فنمط الحرب السيبرانية في هذه الحالة إما أن يكون موازي أو مرافق أو مرتبط أو سابق للحرب التقليدية الدائرة على الأرض (سعود:2018).

وتتخذ الحرب السيبرانية في هذا النوع من الحروب أنشطة أكثر حدية مقارنة بالحروب السيبرانية الباردة، وقد تطال مواقع عسكرية واستخباراتية حساسة، وتعطيل شبه كامل لأنظمة الاتصالات السلكية واللاسلكية والأنظمة الرادارية (هديب:2024).

ومن أمثلة هذا النوع من الحروب السيبرانية متوسطة الشدة، الهجوم السيبراني التي تعرض له المفاعل النووي الإيراني في عام 2010، والذي يعد الهجوم السيبراني الأخطر على الإطلاق حتى ذلك الوقت، والذي اتهمت من خلاله إيران الولايات المتحدة وإسرائيل، وقد شنت هذه الهجمات من خلال فيروس يستهدف أجهزة الطرد المركزية في المفاعل النووي في مدينة "ناتانيز" بهدف تعطيل البرنامج النووي لتخصيب اليورانيوم (خليفة:2021).

3.2.2. الحروب السيبرانية الساخنة.

يعبر هذا النوع من الحروب السيبرانية عن الحروب التي قد تنشأ في الفضاء السيبراني بشكل منفرد، وغير موازي أو مرافق للحرب التقليدية أو النزاع المسلح الحركي. فخلافًا للنوعين السابقين الذين تعرض لهما المجتمع الدولي بالفعل، فإن العالم لم يشهد

هذا النوع من الحروب السيبرانية، وإن كانت احتمالات حدوثه قائمة ومتوقعة في ظل ما يشهده العالم من تطور متسارع في القدرات التكنولوجية، وارتفاع نسب اعتماد الدول على الوسائط الإلكترونية في شتى المجالات (بن تغري:2020).

ويستهدف هذا النوع من الحروب السيطرة المطلقة على المواقع الإلكترونية الخاصة بإطلاق الأسلحة في الدولة، وقد يرافق ذلك استخدام للأسلحة ذاتية التشغيل من قبل الدولة المهاجمة، وتوجيه ضربات إلكترونية شديدة القوة للبنية التحتية للدولة المقصودة بالهجوم، وتدمير المنشآت الحيوية كالسدود، ومحطات توليد الطاقة، وتعطيل قطاع الاتصالات والمواصلات، وإيقاف للخدمات المصرفية، بما يصل إلى أكبر قدر من التدمير الشامل أو الشلل شبة التام للدولة التي تتعرض لمثل هذا الهجوم (هديب:2024).

وفي هذا الصدد، يرى "جاك جولدسميث" أستاذ القانون بجامعة هارفارد: بأنه "إذا لم تكن الدول على دراية بالقواعد الخاصة بالحروب السيبرانية، فقد تنشأ كل أنواع المشاكل العرضية. فقد تقوم دولة ما بعمل تعتبره دولة أخرى عملاً حربياً، حتى لو لم تكن الدولة الأولى تقصد أن يكون هذا العمل عملاً حربيًا" (Goldsmith:2010).

وعلى ذلك؛ يثور التساؤل حول مدى اعتبار الهجمات السيبرانية نوعًا جديدًا من الحروب المسلحة العدائية التي تعطي الدولة ضحية هذه الهجمات الحق في الدفاع عن النفس، أم أنها لا تعدو أن تكون أعمال تخريبية تنفذها منظمات إجرامية أو جماعات من القراصنة في الفضاء السيبراني؟

للإجابة عن هذا التساؤل، ذهب جانب من الفقه إلى القول بأن الحرب السيبرانية هي دائمًا هجوم سيبراني، ولكن ليست كل الهجمات السيبرانية تشكل حربًا سيبرانية، فالهجوم السيبراني يصبح حربًا سيبرانية إذا حدث الهجوم بتأثيرات تعادل آثار الهجوم المسلح التقليدي، أو حدث في سياق صراع مسلح تقليدي (Islam:2017).

ويعتقد جانب آخر من الفقه، بأن أحد الاعتبارات المهمة لاعتبار ما إذا كان الهجوم السيبراني يشكل حربًا، تحديد ما إذا كان الهجوم من عمل قراصنة منفردين، أو مجموعة إجرامية، أو حكومة، ذلك أن قانون الحرب ينطبق في المقام الأول على الصراعات بين الدول، وبالتالي فإن الأعمال المارقة لا تشملها القوانين عادة. فبموجب ميثاق الأمم المتحدة، يحق للدول أن تشن حرباً إذا تعرضت لـ"هجوم مسلح" من دولة أخرى. ولكن لا يوجد إجماع حتى الآن بشأن ما يعنيه هذا الحق في حالة تعرض شبكات الكمبيوتر التابعة لدولة ما لهجوم سيبراني (Tom:2010). بينما يعتقد جانب آخر من الفقه بأن الهجوم السيبراني المباشر على البنية التحتية المدنية الذي يتسبب في الأضرار، وحتى فقدان أرواح المدنيين، سيكون بمثابة جريمة حرب (Ryan:2010).

إن قواعد حق اللجوء إلى الحرب الواردة في ميثاق الأمم المتحدة تبدو مرنة بما يكفي لتوسيعها لتشمل الحروب التي لم تكن موجودة عندما وضعَت، كما هو الحال فيما يتعلق بالحرب السيبرانية. وأن القوة السيبرانية يمكن وصفها بأنها استخدام للقوة "المسلحة" بالمعنى الوارد في المادة 2 (4). ومن ناحية أخرى؛ فإن الهجمات السيبرانية واسعة النطاق على البنى التحتية الحيوية والتي تسفر عن خسائر في أرواح المدنيين أو أضرار مادية كبيرة بالبنى التحتية الحيوية مماثلة لتلك التي تنجم عن هجوم مسلح باستخدام أسلحة تقليدية، هي وحدها التي تمنح الدولة الضحية الحق في الاستعانة بالدفاع عن النفس بموجب المادة (51) من ميثاق الأمم المتحدة (Roscini:2010).

ويعتقد جانب من الفقه، بأنه مهما يكن الاختلاف حول المعيار الذي يجب الاعتماد عليه لتحديد ما إذا كان الهجوم السيبراني يشكل حربًا عدائية أم لا، فإن الحقيقة الثابتة في هذا الشأن تتمثل في أن العمليات السيبرانية أصبحت جزءًا لا يتجزأ من الحروب المسلحة. فقد استخدمت روسيا قواتها السيبرانية مرارًا وتكرارًا، ولا سيما ضد جورجيا في عام 2008، وخلال صراعها المسلح المستمر مع أوكرانيا (Schmitt:2022).

وتأسيسًا على ذلك، فإنه لا يوجد إجماع دولي حتى الآن على ما يعتبر استخدام للقوة ويشكل حربًا عدائية فيما يتعلق بالهجوم السيبراني، يتيح للدولة المتضررة الحق بالدفاع عن نفسها باعتبار الهجوم من قبيل النزاع المسلح، كما أن هنالك تخوف دولي من اعتبار الهجمات السيبرانية من قبيل الهجوم المسلح، حتى لا يؤدي ذلك إلى خلق حالة من عدم الاستقرار في العلاقات الدولية، أو التأثير على مبدأ السلم والأمن الدوليين من خلال التوسع في استخدام القوة تحت غطاء حق الدفاع عن النفس، تطبيقًا للالتزام الوارد في الفقرة الرابعة من المادة (2) من ميثاق الأمم المتحدة، والتي تنص على أنه: (4- يمتنع أعضاء الهيئة جميعًا 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). فالخلاف مازال قائمًا بين الدول فيما يتعلق بما قد يرقى إلى مستوى التهديد باستخدام القوة في الفضاء السيبراني، والذي يُعطي الدولة المعتدى عليها حق الدفاع عن نفسها طبقًا لما ورد في نص المادة (51) من ميثاق الأمم المتحدة، والتي تنص على أنه: (ليس في هذا الميثاق ما يُضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، ...).

صفوة القول: مازالت الحرب السيبرانية تثير إشكالية واضحة تتعلق بالقواعد التي تعطي الدول حق اللجوء إلى القوة للدفاع عن نفسها، على اعتبار الحرب السيبرانية نوعًا جديدًا من النزاع المسلح، وبالتالي وصف اللجوء إلى القوة بالمشروع أو غير المشروع وفقًا للأحكام القانونية القائمة في ميثاق الأمم المتحدة. والأمر يزداد صعوبة في ظل عدم وجود اتفاق دولي موحد حول مفهوم القوة التي تشكل عدوانًا مسلحًا يمنح الدولة المعتدى عليها حق الدفاع عن نفسها في حالة تعرضها للهجمات السيبرانية.

3. أدوات القانون الدولي الإنساني لتغطية عواقب الحروب السيبرانية:

إن المعاهدات الدولية المختلفة وميثاق الأمم المتحدة واتفاقيتي لاهاي وجنيف والبروتكولات الإضافية الخاصة بها، قادرة بلا شك على التمييز بين الضحايا والمعتدين، وهي بمثابة مبادئ توجيهية توفر عند احترامها بعض الحماية للمدنيين. غير أنه من غير المستغرب في الوقت الراهن؛ أن يناقش العديد من الخبراء القانونيين والدبلوماسيين والقادة العسكريين في مختلف أنحاء العالم كيفية توسيع نطاق قانون الحرب ليشمل الحروب السيبرانية، ذلك أن ظهور القدرات القتالية السيبرانية يشكل التطور العسكري الأكثر أهمية منذ عقود من الزمان، ولكن ليس من الواضح بعد كيف قد تنطبق المعاهدات والاتفاقيات القائمة في هذا المجال الجديد من الصراع (Tom: 2010).

وعلى ذلك، فإننا سوف نناقش في هذا المبحث آلية تطبيق قواعد القانون الدولي الإنساني القائمة لتوفير الحماية للمدنيين والبنى التحتية من الحروب السيبرانية (مطلب أول)، ومن ثم نعرض لأبرز التحديات التي تقف حائلًا أمام تطبيق مبادئ النزاع المسلح على الحروب السيبرانية (مطلب ثانٍ).

1.3. آلية تطبيق قواعد القانون الدولي الإنساني:

لقد كان القانون الدولي بطيئاً في التكيف مع التطورات التي شهدها العالم مؤخرًا فيما يتعلق بالحرب السيبرانية. ذلك أن الحقائق على الأرض، والاستخدام الواسع النطاق وغير الواضح للإنترنت، تشكل تحديات حقيقية لسيادة الدولة. ولعل أفضل السُبل لضمان نظام قانوني شامل يحكم الحروب السيبرانية يتلخص في إبرام اتفاق دولي جديد يتناول حصرياً الأمن السيبراني ومكانته في القانون الدولي، قادر على تغطية الأضرار الناشئة عن الحروب السيبرانية. غير أنه لما كان المجتمع الدولي يفتقر إلى الإرادة

السياسية اللازمة لمعالجة هذه القضية بشكل مباشر، وإلى أن يصبح مثل هذا الاتفاق قابلاً للتطبيق سياسياً، فمن الأهمية بمكان؛ أن نبحث في كيفية الاستفادة من القواعد القانونية القائمة في القانون الدولي الإنساني لتغطية الآثار التي تخلفها الحروب السيبرانية.

بتفحص قواعد القانون الدولي الإنساني القائمة، يتضح لنا بأن واضعوا هذا القانون لم يشيروا إلى الأضرار الناشئة عن الحروب السيبرانية على وجه الخصوص، غير أن عدم توافر أحكام قانونية خاصة بتغطية الأضرار التي تخلفها الحروب السيبرانية لا يعني - البتة- بأن القواعد القانونية القائمة لا تشمل الأضرار الناشئة عن هذه الحروب، ذلك أن قواعد القانون الدولي الإنساني جاءت عامة تشمل كافة الأساليب والوسائل المتبعة في الحروب المسلحة، بحيث تكون قادرة على تغطية كافة الأضرار الناشئة عن استخدام القوة وحماية المدنيين والبنى التحتية الناشئة عن استخدام القوة في الحروب المسلحة.

وعلى ذلك، ظهر اتجاه فقهي يؤكد عدم وجود فراغ قانوني فيما يتعلق بتغطية الأضرار الناشئة عن الحروب السيبرانية، ويرى أنصار هذا الاتجاه عدم وجود أي عوائق تعيق تطبيق قواعد القانون الدولي الإنساني وإعمال مبادئه بصفة عامة على أي نزاع مسلح بما في ذلك الحروب السيبرانية (Koh:2012).

وقد بينت محكمة العدل الدولية في قضية نيكارغوا مع الولايات المتحدة الأمريكية والمتعلقة بالأنشطة ذات الطابع العسكري في عام 1986، بأن المادة (51) لا تشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على أي استخدام للقوة. وبغض النظر عن حقيقة أن الهجمات السيبرانية لا تستخدم الأسلحة الحركية التقليدية، فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون مسلحة، ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة بالمدنيين والبنى التحتية الحيوية مستوف لشروط الهجوم المسلح، وبالتالي تطبق أحكام القانون الدولي الإنساني. أما الهجوم على شبكات الحاسب الآلي إذا لم يكن مصاحبًا للنزاع المسلح أو كانت آثاره لا تشكل خسائر في المدنيين أو تأثير على البنى التحتية الحيوية، فإنه لا يخضع لأحكام القانون الدولي الإنساني، بل يخضع للقوانين الجنائية الداخلية (Roscini:2010).

وعلى هدي ذلك، فإننا سوف نعرض لأهم لأبرز المبادئ العامة في القانون الدولي الإنساني والتي يمكن الاستناد إليها لتغطية عواقب الحروب السيبرانية في عدة فروع، وعلى النحو الآتي:

1.1.3. شرط مارتنز (Martinez's condition):

أكدت اتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية الملحقة بها لعام 1977 على قاعدة هامة من أجل ضمان تطور أحكام القانون الدولي الإنساني، بأنه عند وجود حالة لا تغطيها اتفاقية دولية، فإنه يطبق العرف الدولي والمبادئ الإنسانية وما يمليه الضمير العام فيما يخص سير العمليات الحربية. فما لم يحظر صراحةً في الاتفاقيات الدولية لا يمكن أن يكون مباحًا إذا كان يتعارض مع مبادئ الإنسانية وما استقر عليه الضمير العام. وعليه؛ فإنه كلما عجز القانون الدولي الإنساني المطبق على النزاعات الدولية المسلحة عن توفير الحماية المطلوبة لتغطية الآثار المترتبة عن هذه النزاعات، تلتزم الدول بتطبيق أحكام القانون الدولي الإنساني العرفي (صبر:2024).

وقد عُرف هذا الشرط " بشرط مارتنز" والذي جاء النص عليه لأول مرة في ديباجة اتفاقية لاهاي الثانية عام 1899، والتي نصت على أنه: "إن المدنيين والعسكريين يبقون تحت مبادئ القانون الدولي الذي نشأ بحكم العادة بين الأمم المتحضرة من خلال مبادئ الضمير العام والقوانين الإنسانية بين المواطنين والمحاربين لحين استكمال قانون الحرب (علي:2011).

وتبدو أهمية هذا الشرط في أنه يعبر صراحة عن النقص الذي يمكن أن يشوب قانون الحرب، وكذلك عن أهمية العرف الدولي في سد هذا النقص ونظرًا لأهمية هذا الشرط فقد تواترت اتفاقيات القانون الدولي الإنساني على النص عليه، فقد نصت عليه المادة

(63) من اتفاقية جنيف الأولى لعام 1949، وكذلك المادة (62) من اتفاقية جنيف الثانية، والمادة (44) من اتفاقية جنيف الثالثة، والمادة (152) من اتفاقية جنيف الرابعة، والمادة الأولى من البرتوكول الأول وديباجة البرتوكول الثاني (حمدي:2014).

وعلى ذلك، فإنه وفقًا لشرط مارتنز فإن المدنيون والمقاتلون في الحروب السيبرانية يبقون تحت حماية وسلطة مبادئ القانون الدولي الإنساني المستمدة من التقاليد العرفية الراسخة، ومبادئ الإنسانية، وما يمليه الضمير العام (Schmitt:2022). وأما القول بأن ميثاق الأمم المتحدة اشترط القوة لاعتبار الهجوم نزاعًا مسلحًا، وأن الهجوم السيبراني ليس من قبيل النزاعات المسلحة كونه لا يتضمن استخداما للقوة المسلحة، فإنه يمكن الرد عليه بما تضمنته المادة (39) من الميثاق نفسه التي تمنح مجلس الأمن سلطة تقديرية لتقرير المعنى الحقيقي لاستخدام القوة والتي يقررها تبعًا للظروف المحيطة بكل حالة على حدة، وبالتالي يبقى لمجلس الأمن وحده سلطة تقرير ما إذا كان الهجوم السيبراني يشكل تهديد للأمن والسلم الدوليين من عدمه، وما إذا كان يتضمن استخدامًا للقوة أو عملًا من أعمال العدوان (البلداوي:2022). وعلى هذا الأساس فإن كل ما يقع من أضرار نتيجة للحروب السيبرانية يخضع لمبادئ القانون الدولي الإنساني وفقًا لشرط مارتنز، وعليه فإنه لا يمكن القول بوجود فراغ قانوني فيما يتعلق بالحروب السيبرانية (نجيب:2021).

ويمكن الاستدلال على صحة هذا التحليل أيضًا، بما ورد في حكم لمحكمة الولايات المتحدة الأمريكية العسكرية في قضية "كروب" لعام 1948، والتي أشارت إلى أن شرط مارتنز أكثر من مجرد إعلان صوري غير قابل للتطبيق، بل أنه شرط عام يجعل من العادات المستقرة بين الأمم المتحضرة وما يمليه الضمير العام جزءًا من المعايير القانونية التي يلزم تطبيقها كلما كانت أحكام الاتفاقيات الدولية لا تغطي حالات محددة (سعود:2018).

2.1.3. مبدأ التمييز (The principle of distinction):

إن أحد المفاهيم الجوهرية في القانون الدولي الإنساني هو مبدأ التمييز، حيث يتمتع بعض الأشخاص والأشياء بالحماية ضد الهجمات بسبب وضعهم المدني. ويقضي مبدأ التمييز بألا توجه هجمات إلا نحو أهداف عسكرية. كقاعدة عامة؛ يسمح مبدأ التمييز لأطراف النزاعات المسلحة بتوجيه الهجمات المباشرة ضد القوات المسلحة، وتجنيب المدنيين المسالمين وحمايتهم من آثار الأعمال العدائية (Melzer:2008).

نشأ مبدأ التمييز في إعلان سانت بطرسبرغ عام 1868، بهدف الحد من الخسائر المدنية في الحرب. وقد تم تدوين المبدأ بموجب المادة 48، والفقرة الثانية من المادة (51)، والفقرة الثانية من المادة (52) من البروتوكول الإضافي الأول لعام 1977 لاتفاقية جنيف. ويتجلى المبدأ بشكل أكثر وضوحًا في المادة (48) والتي تقضي بالتزام أطراف النزاع بالتميز في جميع الأوقات بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، وبالتالي يجب أن توجه عملياتها ضد الأهداف العسكرية فقط، من أجل ضمان احترام وحماية السكان المدنيين والأعيان المدنية. وتنص الفقرة الثانية من المادة (51) على القاعدة التي تنص على أنه لا يجوز استهداف المدنيين في الهجمات العسكرية. وتنطبق هذه القاعدة على السكان المدنيين والأفراد المدنيين. كما تحظر هذه القاعدة أعمال العنف أو التهديد به بهدف أساسي وهو نشر الرعب بين الجماعات المذكورة. وتكرر الفقرة الثانية من المادة (51) القاعدة التي تنص على أن الهجمات يجب أن تقتصر بشكل صارم على الأهداف العسكرية. كما تحدد هذه القاعدة ما هي الأهداف العسكرية (Ribbenvik:2018).

وعلى ذلك، فمبدأ التمييز لا يستهدف حماية المدنيين فحسب؛ بل أنه لابد من التمييز بين الأهداف العسكرية والأعيان المدنية. وتخضع أطراف النزاع في الحرب السيبرانية لنفس القواعد التي تنطبق على الحروب الحركية، حيث تلتزم الأطراف بتطبيق

المبدأ الأساسي في القانون الدولي الإنساني المتمثل بمبدأ التمييز، فتعتبر الهجمات ضد المدنيين أو الأهداف المدنية عملًا محظورًا وفقًا لأحكام القانون الدولي الإنساني، فلا يجب أن يكون الضرر الجانبي المتوقع الذي يلحق المدنيين من جراء الحروب السيبرانية "مفرطًا" مقارنة بالميزة العسكرية المتوقعة عندما يتم مهاجمة أهداف مشروعة، فلا بد من اتخاذ الاحتياطات الممكنة قبل بدء أي هجوم سيبراني (Dinstein:2012).

وتأسيسًا على ذلك، فقد استندا وأضعوا دليل "تالين" على مبدأ التمييز، عندما حظر الدليل أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية، فلا يجوز توجيه الهجمات السيبرانية لتدمير أنظمة البنى التحتية الحيوية، ما لم تكن من قبيل الأهداف العسكرية التي يجوز استهدافها طبقًا لقواعد القانون الدولي (Schmitt:2022).

3.1.3. قاعدة التناسب (The rule of proportionality):

تقضي قاعدة التناسب التحقق من مدى مشروعية السلاح المستخدم في النزاعات المسلحة، وبأنه ليس من قبيل الاسلحة المحظورة دوليًا، وأن تلتزم الأطراف المتنازعة بعدم استخدام أي وسائل أو أسلحة لا يمكن من خلالها توجيهها إلى أهداف عسكرية، أو استخدام طريقة لا يمكن السيطرة على آثارها على النحو الذي يقتضيه القانون الدولي الإنساني، وبالتالي تلحق أضرارًا جسيمة بالبنى التحتية الحيوية، دون التمييز بين الأهداف العسكرية والأعيان المدنية، أو دون التفرقة بين المدنيين والعسكريين (سعود:2018).

وعلى ذلك نصت المادة (36) من البرتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949، والمتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام 1977، على أنه: "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب، أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد".

وتأسيسًا على ذلك، تلتزم الدول بالتحقق من مدى مشروعية استخدام الهجمات السيبرانية باعتبارها سلاح جديد أو أسلوب حديث من أساليب الحرب طبقًا لما جاء في نص المادة (36) من البرتوكول الإضافي الأول، وعلى ذلك فإن مبادئ القانون الدولي الإنساني تنطبق على الهجمات السيبرانية متى ما كانت صادرة من دولة ضد دولة أخرى، سواء كانت مصاحبة لنزاع مسلح قائم بين الدولتين، أو تمت بطريقة منفصلة عن أي نزاع مسلح، وأن تسفر هذه الهجمات عن إلحاق أضرار جسيمة بالمدنيين أو إحداث أضرار كبيرة بالبنى التحتية المدنية. حيث أنه من غير الممكن اعتبار كل هجوم سيبراني ينشأ عن قرصنة أو اختراق لشبكات حاسوبية من قِبل جماعات إجرامية خارجة عن القانون بمثابة نزاع مسلح (البلداوي: 2022).

وتجدر الإشارة في هذا المقام، إلى التداخل أو التقاطع بين قاعدة "التناسب" وبعض المبادئ العامة المعمول بها بموجب القانون الدولي الإنساني، كمبدأ "الضرورة" العسكرية الذي نصت عليه الفقرة الثالثة من المادة (57) من البروتوكول الإضافي الاول، والذي يضع قيودًا على أطراف النزاع بضرورة استخدام نوع الأسلحة الذي تقتضيه الضرورة العسكرية، وبالقدر والدرجة اللازمة لتحقيق الهدف المقصود والمشروع من النزاع المسلح، وبأقل قدر ممكن من التضحية في الأرواح والموارد. وكذلك مبدأ "الإنسانية" المنصوص عليه بموجب الفقرتين الأولى والثانية من المادة (35) من البرتوكول ذاته، والذي يحظر إلحاق الآلام والإصابات التي لا مبرر لها، وبالتالي حظر استخدام الأسلحة والقذائف والمواد ووسائل القتال التي من شأنها إحداث إصابات أو آلام لا مبرر لها.

صفوة القول: يتضح لنا مما تقدم أن المبادئ والأحكام القانونية المعمول بها بموجب القانون الدولي الإنساني هي في الحقيقة مبادئ عامة لا تخص نوع محدد من الأسلحة، أو تنطبق على أسلوب معين من أساليب القتال، بل أن واضعوا هذه المبادئ قاموا بوضعها بطريقة تستشرف المستقبل، بحيث تكون هذه المبادئ قابلة للتطبيق على ما قد يظهر من وسائل جديدة من وسائل القتال، أو ما قد يظهر من أسلحة متطورة لم تكن معروفة وقت إعداد القواعد القانونية الخاصة بالقانون الدولي الإنساني.

2.3. معوقات تطبيق مبادئ النزاع المسلح على الحرب السيبرانية:

أصبح من الثابت لنا بأن قواعد القانون الدولي الإنساني لم تتطرق للأضرار الناشئة الحروب السيبرانية، كما أشرنا في موضع سابق، فالهجمات السيبرانية غير منظمة من ضمن الحروب المسلحة، ذلك أن ظهور الحروب السيبرانية وتطورها حصل في فترة لاحقة على إعداد قواعد القانون الدولي الإنساني، فقواعد القانون الدولي الإنساني وضعت أساسًا لتغطية الأضرار الناشئة عن استخدام القوة في الحروب الحركية المسلحة. وعلى ذلك، فإن تطبيق قواعد القانون الدولي الإنساني لتغطية عواقب الحروب السيبرانية متوقف على تقرير اعتبار الحروب السيبرانية نوعًا جديدًا من الحروب المسلحة المشمولة بقواعد القانون الدولي الإنساني.

عرفت المادة الثانية من اتفاقية جنيف "النزاع المسلح" بأنه: "نزاع مسلح ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب". وقد أضافت المادة الأولى من البروتوكول الإضافي الأول لاتفاقية جنيف في فقرتها الرابعة عناصر للنزاع المسلح الدولي: "النزاعات المسلحة التي تناضل بها الشعوب ضد التسلط الاستعماري والاحتلال الأجنبي وضد الأنظمة العنصرية، وذلك في ممارستها لحقها في تقرير المصير، كما كرسه ميثاق الأمم المتحدة والإعلان المتعلق بمبادئ القانون الدولي الخاصة بالعلاقات الودية والتعاون بين الدول طبقًا لميثاق الأمم المتحدة". كما أضافت المادة الأولى من البرتوكول الإضافي الثاني تعريفًا لما يعتبر نزاع مسلح غير دولي، بأنه: "كل نزاع يدور على إقليم أحد الأطراف السامية المتعاقدة بين قواته المسلحة وقوات مسلحة منشقة أو جماعات نظامية مسلحة أخرى وتمارس تحت قيادة مسؤولة على جزء من إقليمية من السيطرة ما يمكنها من القيام بعمليات عسكرية متواصلة ومنسقة" (خوي:2022).

والنزاع المسلح كما عرفته المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية "تاديتش" هو النزاع الذي يوجد حيثما يكون هنالك استخدام للقوة بين الدول" دون الإشارة إلى متطلبات أخرى لوجود النزاع (Prosecutor v. Tadić:1995). وفي ذات الاتجاه يرى "جان بكتيه" بأن: "أي خلاف ينشب بين دولتين ويفضي إلى تدخل القوات المسلحة هو نزاع مسلح بالمعنى المقصود، حتى لو لم يعترف أحد الطرفين بحالة الحرب، ولا يعول في هذا الصدد على المدة التي تستمر خلالها النزاعات أو حصيلة القتلى" (J.Pictet: 1952).

غير أن اتجاهًا حديثًا يتزعمه بعض السياسيين الأمريكيين وخبراء في التكنولوجيا وبعض فقها القانون الدولي ظهر مؤخرًا، يرفض اعتبار الهجمات السيبرانية من قبيل الحروب المسلحة، ويرفض التعامل القانوني مع الإنترنت، حيث يعتبر الإنترنت منطقة بلا قانون (البلداوي:2022).

يستند أنصار هذا الاتجاه إلى أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي، فلا يوجد سلطة قادرة على فرض أحكامه في ظل استقلالية شبكة الإنترنت وانفلاتها من مفهوم الخضوع، واستحالة إخضاع الشبكة للتنظيم القانوني التقليدي للدول، كونها تتسم بطابع عالمي مفتوح (موسى:2016).

وينتقد أصحاب هذا الاتجاه وصف "الحرب" الذي يطلق على هجمات الكمبيوتر، كون الحرب مفهوم يرتكز بالأساس على استخدام الأسلحة من قبل الجيوش النظامية ضمن إقليم محدد، يسبقها إعلان لحالة الحرب، في حين لا تكون الهجمات السيبرانية محددة النطاق والأهداف، ذلك أنها تنفذ عن طريق شبكات معلوماتية تتعدى الحدود الدولية، وبالتالي هي أقرب لاعتبارها "إرهاب" من كونها "حرب" أو "نزاع مسلح" (أعمر: 2009).

وعلى ذلك، يرى أنصار هذا الاتجاه أن تطبيق قواعد القانون الدولي الإنساني القائمة على الحروب السيبرانية تبدو غير واقعية، لأن وسائل وأساليب الحروب السيبرانية غير واضحة ومفهومة بشكل كافٍ، ولأنها تتم بسرية مطلقة وبشكل مفاجئ ودون إعلان لحالة الحرب (نجيب: 2021).

من جهة أخرى، فإنه لما كانت اتفاقية لاهاي وجنيف تلزم الجيوش بتقليص الأضرار التي قد تلحق بالمدنيين في زمن الحرب، حيث إن قانون الحرب يتطلب الالتزام بمبدأ "التمييز"، فلا يجوز تدمير مدينة بأكملها بهدف تدمير وحدة عسكرية واحدة موجودة هناك. فإن تطبيق هذا الالتزام في الحروب السيبرانية يعني أنه لا يجوز لك أن تخطط لشن هجوم حاسوبي ضخم، حتى على شبكة عسكرية، دون مراعاة شبكات الحاسوب المدنية التي قد تتأثر بهذا الهجوم. وعلى هذا فإن الصراع السيبراني من المفترض أن يميز الأهداف العسكرية عن الأهداف المدنية، وبالتالي حظر استهداف شبكات الكمبيوتر المدنية. غير أن القانون الدولي غير واضح إلى حد ما، فيما يتصل بكيفية استخدام الدول للأسلحة السيبرانية في زمن الحرب، ولكن مع الترابط الشديد بين شبكات الكمبيوتر، فسوف يكون الالتزام بمبدأ التمييز أو قاعدة التناسب في صراع سيبراني أكثر صعوبة مقارنة بالحرب التقليدية. ذلك أن أجهزة الكمبيوتر لا تحمل دائماً لافتات مكتوب عليها "أنا هدف عسكري" أو "أنا هدف مدني"، بل أن الشبكات المدنية تتداخل بالعادة مع شبكات الكمبيوتر العسكرية (Tom:2010).

كما يعتقد جانب من الفقه أن الهجمات السيبرانية على شبكات الكمبيوتر لا تندرج تلقائيًا ضمن إطار تعريف "الهجوم" وفقًا لقانون النزاع المسلح، وبالتالي فإن بعض الهجمات على شبكات الكمبيوتر، وخاصة تلك التي تستخدم فقط كوسيلة لجمع المعلومات الاستخباراتية، لا تندرج تحت بند "الهجمات" التي تنطوي على استخدام القوة، وبالتالي لا يمكن إخضاع هذا النوع من الهجمات لأحكام القانون الدولي الإنساني (Dinstein:2012).

من جهة أخرى، يشكك جانب من الفقه بالقدرة على تقرير المسؤولية القانونية المترتبة على شن الهجمات السيبرانية، والقدرة على تحديد الجهة المسؤولة عن هذه الانتهاكات؛ فهل تقع على القائد العسكري، أم على المصنع، أم تقع على المبرمج، لا سيما إذا تعلق الأمر بالمسؤولية الجنائية الفردية، وعليه يرى أنصار هذا الاتجاه بضرورة وضع قواعد قانونية تتفق مع الطبيعة الخاصة للحرب السيبرانية (سعود:2018).

صفوة القول: على الرغم من التزام الدول الأطراف السامية في الاتفاقيات الدولية بالمبادئ العامة والأطر الأساسية في القانون الدولي الإنساني، إلا أنه ثمة حاجة مُلحة لتطوير قواعد هذا القانون وموائمة أحكامه للطبيعة المُتفردة للحرب السيبرانية، فالإبقاء على القواعد القانونية القائمة، دون النظر للجوانب الخاصة بالحرب السيبرانية من شأنه أن يُسفر عن خرق للعديد من الأحكام القانونية القائمة في اتفاقية جنيف، وكذا البرتوكول الإضافي الأول المتعلق بحماية ضحايا الحرب، فضلًا عن اتفاقيات لاهاي، وقد يسهم التطور المستمر الذي تشهده الحروب السيبرانية، إلى إخراج هذه الحرب من تغطية هذه القوانين تمامًا.

4. الخاتمة

تعد الطبيعة المتفردة للحرب السيبرانية تحديًا حقيقيًا للمفاهيم السائدة حول الأمن القومي أمام المنظمات الدولية المُكلفة بالحفاظ على السِلم والأمن الدوليين، كمنظمة الأمم المتحدة ممثلة بمجلس الأمن ومحكمة العدل الدولية، وغيرها من الاتحادات والجمعيات والهيئات الدولية والهيئات متعددة الأطراف المهتمة بحفظ السلام، وكذا اللجنة الدولية للصليب الأحمر (ICRC) المختصة بتطبيق قواعد القانون الدولي الإنساني. يرجع ذلك؛ الى صعوبة تحديد المقصود بالحروب السيبرانية، نظرًا لصعوبة تحديد طبيعتها وعناصرها وآثارها، وكذلك صعوبة تحديد الجهات المسؤولة عنها في كثير من الأحيان، فضلًا عن السرعة الفائقة التي تتسم بها عملية تنفيذ الهجمات السيبرانية مقارنة بالحروب الحركية المسلحة، الأمر الذي يضع الجهات الرقابية في مأزق حقيقي وتحدٍ كبير، نظرًا لصعوبة التحقق من امتثال أطراف الحرب السيبرانية بـالمبادئ والعامة والالتزامات الأساسية التي تفرضها أحكام الاتفاقيات الدولية، كاتفاقية لاهاي وجنيف بهدف الحد من الأضرار التي يمكن أن تلحق بالمدنيين وقت الحرب. ولما كانت الفكرة الأساسية التي تمثل فلسفة القانون الدولي الإنساني، تتمثل في كون الحرب لها حدود لا يمكن تجاوزها، فإن هذه الفكرة لا تزال إلى وقتنا الحاضر تشكل المبدأ الثابت الذي تقوم عليه قواعد القانون الدولي الإنساني، حتى في ظل التغيير العالمي والتقدم العلمي الذي نشهده. غير أنه لتلبية متطلبات العصر، ينبغي على صُناع القرار العمل على تطوير وتحديث قواعد القانون الدولي الإنساني. فبينما نستلهم من الماضي قيمة هذا المبدأ؛ يتعين علينا أن ننظر أيضًا - في الوقت ذاته- إلى المستقبل لضمان استمرار وتطوير وتكييف قواعد القانون الدولي الإنساني، بما يتناسب مع التحديات الجديدة والمتغيرة، وذلك بهدف ضمان حماية أفضل للأشخاص المدنيين المتأثرين بالنزاعات المسلحة على اختلاف أشكالها وتنوع أساليبها.

كثيرًا ما تحدد التغيرات في طبيعة الحرب مسار القانون الدولي الإنساني نحو التطور المستمر، فإذا ما أوريد للقانون الدولي الإنساني أن يبقى فاعلًا، فلابد أن يظل متجاوبًا مع السياق الذي ينبغي تطبيقه فيه. ولعل الطريقة الأكثر ملاءمة لتحقيق ذلك هي من خلال المعاهدات التي تتناول التطورات في ساحة المعركة، على أن الصعوبات العملية التي قد تعترض عملية التفاوض بشأن المعاهدات متعددة الأطراف، لا يجب أن يكون، في أي حال من الأحوال؛ سببًا في توقف تطور قواعد القانون الدولي الإنساني لمواجهة التطورات المعاصرة في النزاعات المسلحة، فالممارسات الدولية قد تكون كافية لتشكل الرأي القانوني للإعلان عن نشوء قاعدة عرفية جديدة، وتطبيقها في مواجهة التطورات الجديدة في القانون الدولي الإنساني.

1.4. النتائج:

- تزايد المخاطر الناشئة عن الهجمات السيبرانية بشكل مُطرد مع ارتفاع نسب اعتماد المجتمعات على التكنولوجيا ووسائل الاتصال الإلكترونية في مختلف القطاعات، حيث تعتمد الدول بشكل كبير على الفضاء الإلكتروني الذي يعتقد بأنه سوف يستمر بالنمو، الأمر الذي يتوقع معه ارتفاع معدل التأثير الناشئ عن الهجمات السيبرانية.
- تتقاعس الدول والمنظمات الدولية في التعامل مع العمليات السيبرانية من خلال المعاهدات الدولية متعددة الأطراف والبرتوكولات الإضافية الخاصة بها، حيث لا يوجد إلى الآن معيار واضح لتحديد متى تشكل الهجمات السيبرانية عدوانًا مسلحًا يتيح للدولة المعتدى عليها حق الدفاع عن النفس.

2.4. التوصيات:

- إبرام اتفاق دولي جديد يتناول حصرياً الأمن السيبراني ومكانته في القانون الدولي، قادر على حماية المدنيين والبنى التحتية من الأضرار الناشئة عن الحروب السيبرانية. وإعداد بروتوكول إضافي خاص بحماية المدنيين والبنى التحتية الحيوية المتضررة من الحروب السيبرانية.
- وضع معيار واضح للتفرقة بين الأنماط المختلفة للحروب السيبرانية، يمكن من خلاله تحديد ما إذا كان الهجوم السيبراني يشكل عدوانًا مسلحًا واستخدامًا للقوة يتيح للدول حق الدفاع عن نفسها من عدمه.
- الموازنة بين أهداف ميثاق الأمم المتحدة في تحقيق الاستقرار في العلاقات الدولية والحفاظ على السلم والأمن الدوليين وعدم السماح للدول الأعضاء التوسع في استخدام القوة تحت غطاء حق الدفاع عن النفس من جهة، ومخاطر الحروب السيبرانية الدائرة فعلًا على الأرض والتي قد تشكل تهديدًا حقيقيًا باستخدام القوة يُعطي الدولة حق الدفاع عن نفسها طبقًا لأحكام ميثاق الأمم المتحدة من جهة أخرى.

5. الشكر

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2024/02/30540)

6. المراجع:

1.6. المراجع العربية

- **أعمر، عمر محمود (2009):** الحرب الإلكترونية في القانون الدولي الإنساني، مجلة الشريعة والقانون، المجلد 46، العدد 3.
- **باكير، علي حسين (2010):** الحروب الإلكترونية في القرن الواحد والعشرين، مركز الجزيرة للدراسات، قطر.
- **البلداوي، حامد محمد علي (2022):** مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني، مجلة الجامعة العراقية، مركز البحوث والدراسات الإسلامية، الجامعة العراقية، ع 57، المجلد 2.
- **بن تغري، موسى (2020):** الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القانوني، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، مجلد 12، عدد خاص.
- **جراليه، جيوم (2023):** الوجه الحقيقي للحرب السيبرانية، المركز العربي للبحوث والدراسات، ع 119.
- **حمدي، صلاح الدين أحمد (2014):** العدوان في القانون الدولي العام، منشورات زين الحقوقية، بيروت.
- **الخفاجي، خالد علي (2021):** القانون الدولي الإنساني والتحديات المعاصرة، المجلة المغربية للإدارة المحلية والتنمية، ع 158، 203-231.
- **خليفة، إيهاب (2021):** الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة.
- **خوي، محمد مفتاح أحمدو (2022):** النزاعات المسلحة، مجلة القانون والأعمال، الكلية العلوم القانونية والاقتصادية والاجتماعية، جامعة الحسن الأول، ع79.
- **درويش، سعيد (2017):** الحروب السيبرانية وأثرها على حقوق الإنسان، دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 54، العدد 5.

- **الساجي، علام (2017):** النزاعات المسلحة في الشريعة الإسلامية والقانون الإنساني، مجلة حقوق الإنسان والحريات العامة، ع3، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 80-107.
- **سعود، يحيى ياسين (2018):** الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، المجلد (4)، العدد (4).
- **صبر، نور عبد الرضا (2024):** العرف الدولي وفقًا لشرط مارتنز، مجلة كلية الحقوق والعلوم السياسية، الجامعة العراقية، المجلد 25- 4، العدد 24.
- **علي، أحمد سي (2011):** دراسات في القانون الدولي الإنساني، دار الاكاديمية، الجزائر.
- **محمد، أسامة صبري (2013):** الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية، العدد (7).
- **موسى، طالب حسن (2016):** الإنترنت قانونًا، مجلة الشريعة والقانون، العدد 37.
- **نجيب، نسيب (2021):** الحرب السيبرانية من منظور القانون الدولي الإنساني، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، المجلد 16، العدد 4، 218-236.
- **هديب، إسلام رمضان (2024):** الحرب السيبرانية في ضوء القانون الدولي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة بني سويف، س 36، عدد 1.

2.6. المراجع الإنجليزية:

- **Bouvier, Antoine A. (2020):** International Humanitarian Law and the Law of Armed Conflict, third edition, Peace Operations Training Institute, Williamsburg. VA. USA.
- **Dinstein**, Y. (2012): The Principle of Distinction and Cyber War in International Armed Conflicts, Oxford University Press, Vol. 17, No. 2.
- **Goldsmith, Jack (2010):** Cyber Crime & Doing Time, A Blog about Cyber Crime and related Justice issues, September 22, 2010.
- **Islam, Mohammad S. (2017):** Cyber Warfare and International Humanitarian Law: A Study, International Journal of Ethics in Social Sciences, Vol. 5, No. 1.
- **J.Pictet (1952):** commentary on the Geneva Convention for the Amelioration of the condition of the wounded and Sickin Armed Forces in the field, ICRC, Geneva.
- **Koh, H. (2012):** International Law in Cyberspace, Harvard International, Vol 54.
- **Melzer, N. (2008):** Targeted Killing in International Law, Oxford University Press.
- **Prosecutor v. Tadić (1995):** Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2,1995.

- **Ribbenvik, A. (2018):** The Principle of Distinction in Modern Warfare, Essay in Legal Science, Faculty of Law, Lund University.
- **Richard, A. Clarke & Robert, K. Knake (2010):** Cyber War: the next Threat to National Security and What to Do About it. Review by: David S. Fadok. Strategic Studies Quarterly, Vol. 5, No. 4 (WINTER 2011), pp. 133-135.
- **Roscini, M. (2010):** World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, pp. 85-130.
- **Ryan, Daniel (2010):** We don't know when or if a cyberattack rises to the level of an 'armed attack. National Defense University.
  https://www.npr.org/2010/09/22/130023318/extending-the-law-of-war-to-cyberspace
- **Schmitt, M. N. (2022):** International humanitarian law and the conduct of cyber hostilities: quo vadis, Journal of International Humanitarian Legal Studies, 13 (2).
- **Shackelford, Scott J. (2009):** From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkley Journal of International Law (BJIL), Vol. 25, No.3.
- **Tom, Gjelten (2010):** Extending the Law of War to Cyber space. Viewed 15 September 2013.

Doi: https://doi.org/10.52133/ijrsp.v6.62.2