مفهوم القانون الدولي الإنساني وإشكالية تطبيقه على الهجمات السيبرانية

أ.م.د/ نبيل عبدالرحمن ناصر الدين
أستاذ القانون الدولي المشارك جامعة الجزيرة
Tel:00967770774210
أ/ سلمان الحكمي
باحث ماجستير- جامعة الجزيرة
Tel:00967771449868

الملخص:

يتناول هذا البحث إشكالية تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، في ظل تنامي التهديدات الرقمية الحديثة، وتعدد أشكال النزاعات المسلحة في الفضاء السيبراني، يسلط البحث الضوء على المفاهيم القانونية الأساسية ذات الصلة، مثل مفهوم القانون الدولي الإنساني، ومفهوم الهجمات السيبرانية وخصائصها، كما تناقش البحث الاتجاهات الفقهية المختلفة حول مدى انطباق أحكام القانون الدولي الإنساني على الهجمات السيبرانية المستخدمة أثناء النزاعات المسلحة، وقد توصل البحث إلى ،أن الهجمات السيبرانية قد تشكل في بعض صورها نزاعًا مسلحًا فعليًا؛ مما يستوجب إخضاعها لأحكام القانون الدولي الإنساني، خاصة إذا استهدفت منشآت حيوية أو أوقعت أضرارًا جسيمة بالأشخاص أو الممتلكات، وأوصى البحث بصياغة نظام قانوني دولي واضح ينظم الفضاء السيبراني، وتحديث قواعد القانون الدولي الإنساني، بما يتلاءم مع طبيعة النزاعات الحديثة.

الكلمات المفتاحية: القانون الدولي الإنساني، الهجمات السيبرانية، الحرب السيبرانية، خضوع الهجمات، النزاعات المسلحة.

Abstract:

This study addresses the challenge of applying the rules of International Humanitarian Law (IHL) to cyberattacks, in light of the growing digital threats and the increasing variety of armed conflicts in cyberspace. The research highlights key legal concepts, including the definition of IHL and the nature and characteristics of cyberattacks. It also examines various scholarly perspectives on the applicability of IHL to cyberattacks carried out during armed conflicts, presenting the opposing view that rejects the subjection of cyberattacks to IHL regulations. The study concludes that certain forms of cyberattacks may constitute actual armed conflicts, thereby necessitating their subjection to the provisions of IHL—particularly when such attacks target critical infrastructure or cause significant harm to individuals or property. The study recommends the development of a clear international legal framework to regulate cyberspace and the modernization of IHL rules to align with the nature of contemporary conflicts.

Keywords: International Humanitarian Law, Cyberattacks, Cyber Warfare, Applicability of IHL, Armed Conflicts.

المقدمة:

يعد القانون الدولي الإنســـاني أحد فروع القانون الدولي العام الذي ينظم العلاقات الدولية أثناء النزاعات المسـلحة، وأرسـى العديد من القواعد القانونية الدولية، والتي تهدف إلى حماية ضـحايا النزاعات المسلحة، من المدنيين والأعيان المدنية، أو من الأسرى، أو المرضى أو الجرحى، وتقييد وسائل وأساليب القتال لأغراض إنسانية، تحقيقًا لمبدأ الضرورة العسكرية.

ومع نهاية القرن العشـرين وبداية القرن الواحد والعشـرين، ظهرت تكنولوجيا المعلومات، وشـبكة الإنترنت والاتصالات، والتي ارتبطت بمختلف نواحي الحياة، واعتماد البنية التحتية عليها لما تتميز به من سـرعة في إنجاز المهام وقلة التكاليف، ورغم هذه الإيجابية فإنه قد برز الجانب السـلبي منها، من خلال الاستغلال السيئ لها، وذلك عبر إمكانيات استخدامها في النزاعات المسلحة الدولية وغير الدولية، والتي بدورها نقلت ساحة الحرب التقليدية إلى ساحة افتراضية –الفضاء السيبراني– ليس لها حدود جغرافية، يتم من خلالها توجيه هجمات سـيبرانية من قبل دوله، أو أشـخاص تابعين لها، عن طريق التسـلل إلى أنظمة وبرامج غير مصـــرح الدخول إليها تابعة لدولة أخرى، بهدف تعطيلها أو تدميرها، وذلك عبر برامج إلكترونية تسـبب آثارًا مدمرة، وقد ينتج عنها التسـبب بجرح أو قتل الأشـخاص في الدولة المسـتهدفة من الهجوم السيبراني.

ولهذا كله فقد أرتأى الباحث أن يكون عنوان البحث مفهوم القانون الدولي الإنســـاني وإشـــكالية تطبيقه على الهجمات السيبرانية.

أهمية البحث:

يكتسب موضوع الهجمات السيبرانية أهمية بالغة في وقتنا الراهن، نتيجة للتطور العلمي والتكنولوجي الذي حقق كثيرًا من المنافع للإنسـانية، وحمل في الوقت نفسـه أسـلوبًا وسـاحة جديدة للحروب تختلف كليًا عن ميدان ووسائل وأساليب القتال في الحروب التقليدية.

ووضـــع كهذا يجعل السـكان المدنيين والأعيان المدنية في خطر، يقع على عاتق المجتمع الدولي إعطاء موضـــوع الهجمات الســـيبرانية اهتمامًا كبيرًا، والبحث عن حلول ومعالجات والحد منها، من خلال تقييم قواعد القانون الدولي الإنســاني المعنية بحماية السـكان المدنيين والأعيان المدنية، فلابد من مواكبة التشريعات لتلك التطورات، ووضع نصوص قانونية خاصة لمواجهتها.

ونتيجة للقصـور التشـريعي على المسـتوى الدولي والوطني لهذا النوع الجديد من الأسـلحة؛ تأتي أهمية البحث في التعريف بماهية الهجمات السيبرانية؛ باعتبارها أحد الأسلحة التي يمكن استخدامها أثناء

النزاعات المسلحة، وإيضاح أوجه القصور في التشريعات الدولية لمكافحة هذا النوع من الهجمات، حتى نصل بإجابة عن تساؤل البحث الرئيس.

إشكالية البحث:

تكمن مشكلة البحث في السؤال الرئيس الآتي:

ما مفهوم القانون الدولي الإنساني وإشكالية تطبيقه على الهجمات السيبرانية؟

ويتفرع عن إشكالية البحث العديد من التساؤلات، هي كالآتي:

- ما مفهوم القانون الدولي الإنساني؟
- ما مفهوم الهجمات السيبرانية؟
- ماهي خصائص الهجمات السيبرانية؟
- هل توجد إشكالية في تطبيق قواعد القانون الدولي الانساني علي الهجمات السيبرانية؟

أهداف البحث:

- توضيح مفهوم القانون الدولي الإنساني.
- تعريف الهجمات السيبرانية لغةً واصطلاحًا.
- بيان خصائص الهجمات السيبرانية.
- تحليل إشكالية تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية.

منهج البحث:

يستدعي موضوع البحث اتباع المنهج الوصفي التحليلي، مع الاستعانة بمناهج البحث الأخرى، من خلال وصف الهجمات السيبرانية، وحالاتها، والمواقف الفقهية منها، وتحليل قواعد ومبادئ القانون الدولي الإنساني لمحاولة معرفة مدى انطباقها على الإشكالية المطروحة.

تقسيمات البحث:

المبحث الاول– الإطار المفاهيمي للقانون الدولي الإنساني والهجمات السيبرانية.

المطلب الأول– مفهوم القانون الدولي الإنساني.

المطلب الثاني– مفهوم الهجمات السيبرانية وخصائصها.

المبحث الثاني– إشكالية تطبيق القانون الدولي الإنساني على الهجمات السيبرانية.

المطلب الأول– الرأي القائل بعدم خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني.

المطلب الثاني– الرأي القائل بخضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني.

المبحث الأول- الإطار المفاهيمي للقانون الدولي الإنســـاني والهجمات السيبرانية.

يعد مفهوم القانون الدولي الإنساني من الركائز الأساسية التي تحكم سلوك الدول والأطراف المتحاربة أثناء النزاعات المسلحة. ويهدف هذا القانون إلى حماية الأفراد الذين لا يشاركون في الأعمال القتالية، مثل المدنيين، والجرحى، وأسرى الحرب، وضمان احترام حقوقهم الأساسية. ومع ظهور الفضاء السيبراني كساحة جديدة للصراع، تبرز إشكالية تطبيق هذا القانون على الهجمات السيبرانية، التي تتميز بطبيعتها غير التقليدية والمعقدة.

وعليه سنقسم بحثنا في هذا المبحث إلى مطلبين، نخصص المطلب الأول لدراسة مفهوم القانون الدولي الإنساني، والمطلب الثاني للتعريف بمفهوم الهجمات السيبرانية وخصائصها، وذلك على النحو الآتي:

المطلب الأول- مفهوم القانون الدولي الإنساني:

يعد القانون الدولي الإنســاني (International Humanitarian law) اصــطلاحًا حديث الاستخدام نسبيًا إلا أن جذوره ضاربة في تاريخ القانون الدولي العام، وقد أطلق عليه عدة تسميات- قبل أن يتم الاستقرار على التسمية الحديثة له- تحمل في طياتها الدلالة على القواعد القانونية الدولية المندرجة تحت لواء القانون الدولي الإنساني، من تلك التسميات قانون الحرب الذي ظل سائدًا حتى نشأة منظمة الأمم المتحدة، ونص ميثاق إنشائها على حظر استخدام القوة أو التهديد باستخدامها لحل المنازعات الدولية، وبعد ذلك ساد استخدام مصطلح قانون النزاعات المسلحة، ثم ومع بداية السبعينيات تأثر هذا القانون بحركة حقوق الإنسان على الصعيد الدولي خاصة في أعقاب مؤتمر طهران عام 1968م، وشاع استخدام مصطلح «**القانون الدولي الإنساني.**» كدلالة على الطابع الإنساني التي تحميها قواعده القانونية الدولية [1].

[1] د. شريف عتلم، محاضرات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، الطبعة التاسعة، 2011م، ص10. كتاب منشور علي الإنترنت في الزيارة تاريخ 18 اغسطس 2020م، على الرابط الآتي:
https://www.icrc.org/ar/download/file/23990/0237_mohadarat_for_web.pdf

ويضم القانون الدولي الإنساني القواعد القانونية الدولية التي يجب احترامها في حال نشوب أي نزاع مسلح، ولا يقتصر الالتزام بقواعد القانون على الحكومات وقواتها المسلحة فحسب، وإنّما يمتد ليشمل أيضًا جماعات المعارضة المسلحة وغيرها من أطراف النزاعات [1]. فقواعد القانون الإنساني هي قواعد قانونية تستمد صفتها هذه من كونها جزءًا من القانون الدولي العام، ولها نفس خصائص القاعدة الدولية، وكذلك مصدرها هو نفس مصدر القانون الدولي العام من قواعد مكتوبة أو عرفية، وعلى هذا فإن هذه القواعد القانونية تنشأ وتتطور داخل إطار القاعدة القانونية الدولية، وعلى اعتبار أن المسؤولية الدولية أحد العناصر الأساسية الضرورية لتفعيل كافة فروع القانون الدولي العام المعاصر، بما فيها القانون الدولي الإنساني، وتعدُّ من المبادئ الأساسية لهذا القانون[2].

ولذا يمكن القول بأن القانون الدولي الإنساني هو مجموعة القواعد التي تسعى إلى الحد من التبعات الإنسانية للنزاعات المسلحة، ويشار إليه في بعض الأحيان بقانون النزاع المسلح، أو قانون الحرب، ويتمثل الهدف الأساسي للقانون الدولي الإنساني في تقييد وسائل وأساليب القتال التي قد تستخدمها أطراف نزاع معين، وضمان الحماية والمعاملة الإنسانية للأشخاص الذين لا يشاركون مشاركة مباشرة في العمليات العدائية، أو كفُّوا عن المشاركة فيها[3].

وبناءً على ما تقدم عرفت اللجنة الدولية للصليب الأحمر القانون الدولي الإنساني بأنه: مجموعة القواعد الدولية الاتفاقية أو العرفية التي يقصد بها خصيصًا، تسوية المشكلات الإنسانية الناجمة مباشرة عن النزاعات المسلحة، دولية كانت أم غير دولية، والتي تحد لأسباب إنسانية من حق أطراف النزاع في استخدام ما يحلو لها من وسائل القتال وطرقه، وتحمي الأشخاص والأعيان التي يلحق بها الضرر أو تتعرض له من جراء هذا النزاع[4].

---

[1] د. بلال علي النسور و د. رضوان محمود المجالي، الوجيز في القانون الدولي الإنساني "ما بين الاعتبارات القانونية والسياسية، جوانب نظرية وتطبيقية" دراسة في بعض من النماذج الدولية المعاصرة، الأكاديميون للنشر والتوزيع، عمان الأردن، 2012م، ص 36.

[2] د. ديب عكاوى، القانون الدولي الإنساني. أكاديمية العلوم الأوكرانية، كييف، 1995م، ص 206.

[3] نيلس ميلزر، القانون الدولي الإنساني مقدمة شاملة، إصدارات اللجنة الدولية للصليب الأحمر، آب/ أغسطس 2016م، ص 17. كتاب منشور على الإنترنت في الزيارة تاريخ 18 أغسطس 2023م، على الرابط الآتي:
https://blogs.icrc.org/alinsani/2020/08/13/3871/

[4] د. شريف عتلم، و د. عمر مكاوي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني، أصدارات اللجنة الدولية للصليب الأحمر، المجلد الثاني، 2017م ص11.

القانون الدولي الإنســـاني وفق مفهوم اللجنة الدولية للصـــليب الأحمر بأنه: جزء من منظومة القانون الدولي التي تحكم العلاقات بين الدول، ويهدف إلى حماية الأشخاص الذين لا يشاركون أو توقفوا عن المشــاركة في الأعمال العدائية، والمرضـــى والجرحى والســـجناء والمدنيين، وتحديد حقوق والتزامات أطراف النزاع في سير الأعمال العدائية[1].

إن تفســـير اللجنة الدولية للصـــليب الأحمر لا يختلف عمّا أتى به العديد من فقهاء القانون الدولي، فالقانون الدولي الإنســاني بشــكل عام، هو: ذلك الفرع من القانون الدولي العام الذي يســعى إلى التخفيف من سلوك النزاع المسلح، وتخفيف المعاناة التي يسببها[2].

يعرف الدكتور محمود شــريف بســيوني القانون الدولي الإنســاني بأنه: "مجموعة القواعد التي تحمي فئات معينة من الأشــخاص والممتلكات، وتحظر الهجمات ضــدهم أثناء النزاعات المسـلحة، سـواء كانت ذات طابع دولي أو غير دولي"[3].

ويعرفه جان بكته بأنه: ذلك الفرع المهم من فروع القانون الدولي العام الذي بوجوده يؤدي إلى الإحســـاس بالإنســـانية، ويركز على حماية الفرد، فقواعده تهدف إلى التخفيف من معاناة كل ضـــحايا النزاعات المسلحة ممن هم تحت رحمة أعدائهم، سواء أكانوا جرحى أم مرضى أم غرقى أم أسرى حرب أم مدنيين[4].

عرف دليل ســـان ريمون لعام 1994م القانون الدولي الإنســـاني بأنه: القواعد الدولية التي وضــعتها المعاهدات أو الأعراف، وتحدد حق أطراف أي نزاع في اختيار وســائل أو أســاليب الحرب، أو

---

(1) International Committee of the Red Cross (ICRC), War and International Humanitarian Law (29 October 2010), (last visited 3 September 2023). available at; www.icrc.org/eng/war-and-law/overview -war-and-law.htm

(2) Alexander, A. A Short History of International Humanitarian Law. European Journal of International Law 2015, 26 (1), 109–138. **https://doi.org/10.1093/ejil/chv002**.

(3) Bassiouni, C. M. The Normative Framework of International Humanitarian Law: Overlaps, Gaps, and Ambiguities. International Law Studies 2000, 75 (1), pp,1-55,p2.

(4) أ.د. محمد عزيز شكري، تاريخ القانون الدولي الإنساني وطبيعته، تقديم أد. مفيد شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، القاهرة، 2000م، ص 24.

تحمي الدول غير الأطراف في النزاع أو الأعيان والأشخاص الذين يتأثرون أو من المحتمل أن يتأثروا من النزاع[1].

عرفته الأستاذة ماريا تيريزا دوتلي بأنه: مجمل القواعد القانونية التي تكون الدول ملزمة باحترامها، والتي تستهدف توفير الحماية لضحايا النزاعات المسلحة، الدولية منها وغير الدولية[2].

من التعريفات سالفة الذكر يمكن القول وبحق أن القانون الدولي الإنساني هو: فرع من فروع القانون الدولي العام[3]، ويخضع للقواعد التي تحكم بقية فروع القانون الدولي العام، إلا أن هذا القول لا يمنع من أن هناك بعض القواعد الخاصة التي تتضمنها بعض المواثيق الدولية المتعلقة بالقانون الدولي الإنساني قد خرجت عن الأصل العام في اتفاقية فينا لقانون المعاهدات لعام 1969م، فعلى سبيل المثال تضمن البروتوكولان الإضافيان لعام 1977م الملحقان باتفاقيات جنيف لعام 1949م بعض القواعد الخاصة لا يقابلها مثيل في قانون فينا للمعاهدات، منها أن يدخل البروتوكولان حيز النفاذ بعد مرور ستة شهور من تاريخ إيداع صكين للتصديق على الأقل، ويرجع المهتمون هذا الأمر إلى أهمية قواعد هذين البروتوكولين، وضرورة تطبيقيهما بأسرع ما يمكن.

كما أنه من الملاحظ أنّ القانون الدولي الإنساني يخاطب بقواعده إلى جانب الدول، والأفراد، ويركز على حمايتهم؛ حيث أصبح الفرد في ظله- وعلى هدي التعاريف السابقة- يتمتع نوعًا ما فحسب، بشخصية قانونية دولية، رغم ما قد قيل عن عدم اكتمالها، فيرى بعض الباحثين ومنهم الدكتور محمد عزيز شكري بأن القانون الدولي في الزمن المعاصر لم يعد قانون الدول والمنظمات الدولية فحسب، بل

---

[1] د. شريف عتلم و د. محمد ماهر عبد الواحد، موسوعة اتفاقيات القانون الدولي الإنساني، إصدارات فرع اللجنة الدولية للصليب الأحمر، القاهرة، 2002م، ص638.

[2] د. مايا الدباس، و د. جاسم ذكريا، القانون الدولي الإنساني، منشورات الجامعة الافتراضية السورية، سوريا، 2018م، ص9.

[3] القانون الدولي الإنساني هو فرع من فروع القانون الدولي العام، ينطبق علية كافة العناصر الضرورية التي تكون الفرع، كما حددها البروفسور ديب عكاوى، وهي كما يأتي:

- وجود موضوع خاص تعالجه القواعد القانونية الدولية التي تشكل هذا الفرع.
- توفر قواعد قانونية عامة ملزمة داخل الفرع.
- وجود مبادئ خاصة تنظم تشكيل الفرع الجديد للقانون الدولي.
- رغبة المجتمع الدولي في إفراز فرع جديد للقانون الدولي.
- وجود على الأقل وثيقة قانونية واحدة تثبت قواعد هذا الفرع.

راجع البروفسور ديب عكاوى، القانون الدولي الإنساني، مرجع سابق، ص.61-62.

غدا أيضـــا قانون الفرد، مرجعين هذا الأمر إلى التطور الذي لحق بالقانون الدولي في الأزمنة الحديثة؛ حيث أصبح في بعض الحالات يخاطب الإنسان مباشرة بحقوق وواجبات معينة هذا من جهة، ومن جهة ثانية فإن عندهم – أي الباحثين– لو أخذت عبارة أو مصـــطلح القانون الدولي الإنســـاني على إطلاقها، فإنها تشمل قواعد القانون الخاص بالإنسان وحمايته[1]. والقانون الدولي الإنساني، ينقسم إلى فرعين:

قانون لاهاي، هو القانون الذي ينظم استخدام القوة ووسائل وأساليب القتال، وتشكل اتفاقية لاهاي لعامي 1907م، والاتفاقيات المعنية بحضـر الأسـلحة 1899م ومصـادره الأسـاسـية، وأنشـئت بموجبها القواعد القانونية الدولية التي تنظم حقوق وواجبات المحاربين في إدارة العمليات العسكرية والحربية، وتهدف إلى الحد من آثار العنف، بحيث لا تتجاوز ما تطلبه الضرورة العسكرية.

قانون جنيف، ويقصـــد به: القانون الذي يســـعى إلى حماية ضـــحايا النزاعات المســـلحة[2] المتمثل بمجموعة القواعد القانونية التي أقرتها اتفاقيات جنيف الأربعة 1949م، وبرتوكولاها الإضـافيان 1977م، المنظمة لســـير الأعمال الحربية، بما في ذلك حظر مهاجمة الوحدات الطبية، والأفراد العاملين بها، أو الأشـخاص العاجزين عن القتال بسـبب المرض أو الجروح، ويتدخل لحماية الإنسـان عمومًا، بما في ذلك حماية العسكريين الذين عجزوا عن مباشرة القتال، وحماية المدنيين وكل الأشخاص الذين لا يشتركون في العمليات الحربية[3].

يميل القانونيون الدوليون إلى إخفاء هذا البيان العام بالتعليق القائل بأن مصـــطلح "القانون الدولي الإنســـاني" يُطبق تقليديًا على جزء "جنيف" من قانون الحرب، والذي كان له تركيز إنســـاني، على عكس قانون "لاهاي"، والذي كان أكثر اهتمامًا بأساليب الحرب، ثم ذكروا، مع ذلك، أن هذا التقسيم "كان منذ فترة طويلة مصـــطنعًا". ويقال: إنّ كلا الجزأين من القانون يســـتندان إلى مخاوف إنســـانية، وبالتالي يتداخلان، في الواقع، كما يقول شريف بسيوني: "إنهما متشابكان للغاية ومتداخلان لدرجة أنه يمكن القول: إنهما وجهان لعملة واحدة". وبالتالي، يتم التأكيد على أنه يمكن استخدام مصطلح القانون الدولي الإنساني

---

[1] أ. د. محمد عزيز شكري، تاريخ القانون الدولي الإنساني وطبيعته، تقديم أ. د. مفيد شهاب، دراسات في القانون الدولي الإنساني، مرجع سابق، ص84.

[2] د. شريف عتلم، و د. عمر مكاوي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني، مرجع سابق، ص12.

[3] د. ديب عكاوى، القانون الدولي الإنساني، مرجع سابق، ص 32.

للإشارة إلى جميع قواعد القانون الدولي التي تتعلق بالنزاع المسلح، سواء كانت عرفية أو تقليدية أو لاهاي أو جنيف[1].

وفي جميع الحالات وعلى أمل أن تنتهي الخلافات حول المعنى الدقيق للمصطلح، فإن قانون الحرب، أو قانون النزاعات المسلحة، أو القانون الدولي الإنساني، بالمفهوم الواسع، يهدف إلى وضع قواعد منظمة للعمليات الحربية، وتخفيف الأضرار الناجمة عنها إلى أقصى حد نتيجة الضرورات الحربية، فعلى الرغم من أنّ القانون المتعلق بسير الأعمال العدائية (ما يسمى "قانون لاهاي") بدأ في التطور في مجموعة واحدة من المعاهدات، في حين أن القانون الذي يحمي الضحايا (ما يسمى "قانون جنيف") تم تطويره بشكل منفصل في اتفاقيات جنيف المختلفة، الا أن هذين الفرعين قد ارتبطا معًا في وقت لاحق في البروتوكولين الإضافيين لعام 1977م ليكونا مجموعة قانونية واحدة [2]، فمنذ ظهور بروتوكولي عام 1977 زالت هذه التفرقة [3]؛ إذ تضمن البروتوكول الإضافي الأول خاصة العديد من الأحكام الخاصة بوسائل وأساليب القتال، ولم يعد لهذا التمييز بينهما إلا قيمة تاريخية، وقد عبر الدكتور عامر الزمالي عن ذلك بأن: «بروتوكولي عام 1977 وخاصة الأول منهما تضمن قواعد صهرت القانونين معًا، وليس من الوجاهة الحديث عن قانونين منفصلين، والحال أن القانون الدولي الإنساني يشمل الاثنين»[4].

---

(1) Alexander, A. A Short History of International Humanitarian Law, Op, Cit, p. 112.

(2) Doswald-Beck, Louise.. "International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons". *International Review of the Red Cross Archive* 37(316) 1997, 35–55.p 36.

(3) في الواقع، لم يكن هناك مطلقًا تمييز بين "قانون لاهاي" و "قانون جنيف"؛ حيث تكشف القراءة المتأنية لقانون ليبر لعام 1862م، ومؤتمر بروكسل لعام 1874م، والكتب القانونية المبكرة أن "قوانين الحرب وأعرافها" في تلك الفترة لم تتضمن قواعد تحمي الأشخاص الواقعين في قبضة العدو، ولا سيما أسرى الحرب وسكان الأراضي المحتلة. وعلى العكس من ذلك، تضمنت اتفاقيات جنيف جوانب القواعد القانونية المتعلق بسير الأعمال العدائية، وهي حظر مهاجمة الوحدات الطبية وأفراد المهن الطبية أو الأشخاص العاجزين عن القتال بسبب المرض أو الجروح (هذا العنصر الثاني هو أحد عناصر القاعدة العرفية المتمثلة في الإبقاء على حياة العدو). لذلك، فإن أثر البروتوكولين الإضافيين لعام 1977 لم يكن إنشاء مجموعة موحدة من القانون الإنساني تحتوي على هذين العنصرين للمرة الأولى، وإنما إزالة التمييز الذي كان دائمًا اصطناعيًا وخاطئًا، فالقانون الدولي الإنساني مجرد مصطلح حديث لـ "قانون الحرب". راجع:

Doswald-Beck, Louise. "International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons, 1997. Op, Cit, p 36-37.

(4) د. شريف عتلم، و د. عمر مكاوي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني، مرجع سابق، ص12.

والواقع أن القانون الدولي الإنساني لا يقتصر على القواعد الإنسانية الواردة في اتفاقيات لاهاي، و اتفاقيات جنيف الأربعة، بل تجاوز ذلك ليشمل جميع القواعد الإنسانية المستمدة من أي مصدر آخر، سواء كانت مستمدة من اتفاق دولي آخر، أو كانت مستمدة من مبادئ القانون الدولي كما استقر بها العرف ومبادئ الإنسانية والضمير العام، وهذا ما أكدته اللجنة الدولية للصليب الأحمر في التقرير المقدم إلى "مؤتمر الخبراء الحكوميين المعني بإعادة تأكيد وتطوير القانون الإنساني الدولي المطبق في النزاعات المسلحة"؛ حيث ذكرت أنّه " قد يعني القانون الدولي الإنساني قواعد قانون النزاعات المسلحة ذات الطبيعة الإنسانية الواضحة، أي: تلك التي تحمي البشر وممتلكاتهم الأساسية، وبالتالي فإن المصطلح لا يشمل اتفاقيات جنيف فحسب، بل يشمل أيضًا قواعد المعاهدات أو القانون العرفي التي، لأسباب إنسانية، تضع حدودًا يجب مراعاتها في سير الأعمال العدائية، واستخدام الأسلحة، وسلوك المقاتلين، واللجوء إلى الأعمال الانتقامية، وكذلك القواعد التي تهدف إلى ضمان التطبيق السليم لتلك القواعد"[1].

أكدت محكمة العدل الدولية في رأيها الاستشاري الصادر في 8 يوليو / تموز 1996م، بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها؛ حيث خلصت المحكمة إلى أن "هذه القواعد – التي نظمتها كل من اتفاقات لاهاي، واتفاقيات جنيف– تبين ما يتوقع من الدول من تصرف وسلوك " وفيما يتعلق بالبروتوكول الإضافي الأول لعام 1977م، ذكرت المحكمة أن "جميع الدول ملزمة بهذه القواعد ... والتي عند اعتمادها، كانت مجرد تعبير عن القانون العرفي الموجود من قبل"[2].

وفي ختام هذا الجزء، يمكن القول: إن القانون الدولي الإنساني هو فرع من القانون الدولي العام، والذي يعرف كذلك بقانون النزاعات المسلحة، يهدف لتحقيق ما يأتي:

1- الحد من الأضرار الناجمة عن النزاعات المسلحة عن طريق تقييد حق أطراف النزاع على حرية اختيار أساليب ووسائل القتال في ميدان المعركة.

2- إلزام المتحاربين بالحفاظ على الأشخاص الذين لا يشاركون في العمل العسكري، أو توقفوا عن هذا الاشتراك، وكذلك الأعيان التي لا تساهم مساهمة مباشرة في هذا العمل.

---

(1) Alexander, A. A Short History of International Humanitarian Law, Op, Cit, p. 122.

(2) Doswald-Beck, Louise. "International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons, Op, Cit, p.36-37.

وفي سبيل ما ذكر هناك تحديات كبيره تواجه تطبيق القانون الدولي الإنساني خصوصًا تأثيرات التكنولوجيا الحديثة، مثل الطائرات بدون طيار، والأسلحة الذكية من بينها الهجمات السيبرانية، وغير ذلك من أساليب القتال الجديدة المستخدمة في النزاعات المسلحة الدولية وغير الدولية، وبالتالي يتطلب تطوير قوانين جديدة لمواكبة هذه التطورات، من خلال توسيع دور المنظمات الإنسانية، مثل الصليب الأحمر، وتعزيز التعاون بين الدول لتنفيذ القوانين الدولية الإنسانية، من خلال دعم الآليات الدولية، مثل الأمم المتحدة، والاتفاقيات الإقليمية في الحد من معاناة ضحايا النزاعات المسلحة.

المطلب الثاني- مفهوم الهجمات السيبرانية وخصائصها:

الهجمات السيبرانية مصطلح حديث ظهر في العقود الأخيرة، نتيجة لثورة تكنلوجيا المعلومات، ولم تكن الهجمات معروفة إلا في وقت قريب، فالهجمات السيبرانية يكتنفها الغموض والالتباس بشكل كبير؛ مما نتج عن ذلك صعوبات واجهها المختصون في القانون الدولي العام، والإنساني بشكل خاص، وذلك في وضع تعريف جامع مانع نتج عن ذلك عدم وجود تعريف محدد ودقيق، ومع ذلك نجد أن معظم التعاريف تشترك في معانى متقاربه، وهو استهداف مواقع وأنظمة إلكترونية، من خلال وسائل اتصال إلكترونية أخرى، تؤدي إلى تعطيل أو تدمير أو إتلاف تلك الأنظمة والأجهزة المرتبطة بالبنى التحتية، والتسبب بالإضرار بها.

وقد أطلق العديد من المصطلحات على الهجمات السيبرانية؛ حيث أطلق البعض عليها مصطلح الحرب الافتراضية، ومنهم من أطلق عليها الحرب الإلكترونية، ومنهم من أطلق عليها الحرب السيبرانية، وفي جميع الحالات، فإن مصطلح الهجمات السيبرانية أوسع نطاقًا من الحرب السيبرانية، وأكثر دلالة ومعنى، ويتماشى مع مقتضيات القانون الدولي المعاصر، بالإضافة إلى أنها قد تحدث خارج النزاعات المسلحة، وتكون سببًا لبدء نزاع مسلح، أو تحدث في نطاق النزاعات المسلحة، وتكون جزءًا من الحرب السيبرانية.

ولغاية الوقوف على مفهوم هذا المصلح حديث النشأة، سيتم تعريف الهجمات السيبرانية لغويًا في ضوء المعاجم اللغوية، فضلًا عن التطرق لتعريف الهجمات السيبرانية اصطلاحًا في ضوء الاجتهادات الفقهية والقانونية.

الفرع الأول- تعريف الهجمات السيبرانية.

أولًا- السيبرانية (cyber) في اللغة: إن كلمة السيبرانية اشتقت من الكلمة اللاتينية سايبر (Cyber) ومعناها تخيلي أو افتراضي، وهي صفة تطلق لأي شيء يرتبط بثقافة الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، وتعني أيضًا: علم التحكم الأوتوماتيكي والقيادة والتوجيه عن بعد[1].

وقد استخدم هذا المصطلح أكاديميًا لأول مرة من قبل عالم الرياضيات الأمريكي روبرت وينز عام 1948م في كتابه الشهير "علم التحكم الآلي" وذلك للإشارة إلى آليات التنظيم الذاتي، أي: السيطرة والاتصال في الحيوان والآلة [2].

وأما قاموس مصطلحات الأمن المعلوماتي فيعرف السيبرانية: بأنها هجوم عبر الفضاء السيبراني، يهدف إلى السيطرة على مواقع إلكترونية وبنى تحتية إلكترونية لتعطيلها، أو تدميرها والإضرار بها[3].

فيما عرف قاموس المصطلحات العسكرية الأمريكية السيبرانية بأنها: أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية[4].

أما في القواميس العربية، فقد أشار قاموس المورد في تعريف كلمة سايبر (Cyber) بالكمبيوتري أو عصري جدًا، كما عرفها بأنها: عالم الضبط ومصدرها (Cybernetics)، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي: ضبط الأشياء والتحكم بها عن بعد[5]، وجاء في قاموس المعاني بمعنى تخيلي[6].

ومما يجدر الإشارة إليه أن المختصين في اللغة العربية يواجهون تحديًا في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية؛ إلا أن الوثائق الصادرة عن الأمم المتحدة باللغة العربية تستخدم مصطلح السيبرانية بدلًا من الإلكترونية، وهو السبب في اختيار هذه التسمية في مجال دراستنا.

---

[1] منير البعلبكي، ورمزي منير البعلبكي، المورد الحديث، دار العلم للملايين، لبنان،2008، ص307.

وقاموس أكسفورد

https://www.oxordlearnersdictionaries.com/definition/American-englis/cyber

[2] Norbert Wiener, "Cybernetics or control communication in the animal and the machine" ,M.I.T. press ,second Edition, Cambridge, Massachusetts, 1948,Available At:

https://cutt.ly/akhwlob

[3] Richard kissel, "Glassory of Key information security Terms", National institute of standards and technology, U.S Department of Commerce",Revision,2,May,2013,p.57.

[4] U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, 2010, as amended through Feb. 15, 2016.

[5] منير البعلبكي، المورد، قاموس إنكليزي عربي، دار العلم الملايين، بيروت،2004، ص243.

[6] قاموس المعاني على شبكة الإنترنت، استرجعت بتاريخ 2 / 2/ 2023م. متاح على الرابط الآتي:

https://www.almaany.com/ar/dict/ar-en/cyber

ثانيًا- الهجمات السيبرانية اصطلاحًا:

ليس هناك إجماع واسع على تعريف جامع مانع لمصطلح الهجمات السيبرانية، ومع ذلك فقد اجتهد العديد من الخبراء والفقهاء القانونيين كلٌ في مجال اختصاصه في تقديم تعريف يحيط بهذا المفهوم تبعًا لوجهات النظر التي يتبناها أصحابها؛ لذلك سنستعرض بعض التعاريف لمحاولة الوصول إلى التعريف الراجح:

فقد عرف شميت (schmitt) الهجمات السيبرانية بأنها: عبارة عن مجموعة من الإجراءات تتخذها الدولة، من أجل الهجوم على نظم المعلومات تابعة للعدو؛ بهدف التأثير والإضرار بها، أو للدفاع عن نظم المعلومات الخاصة بدولة المهاجم[1].

وعرف دليل الجيش الأمريكي لعام 2005م الهجوم السيبراني بأنه: القيام عمدًا بأنشطة تخريبية لأجهزة الحاسوب أو الشبكات؛ بغرض التسبب بأضرار أو تحقيق أهداف اجتماعية أو دينية أو أيدلوجية أو سياسية أو أي أهداف مماثلة، أو ترهيب أي شخص أو أي جهة لتحقيق تلك الأهداف[2].

فيما عرفها زيمت وباري zimet & Bary بالقول بأنها: مجموعة من العمليات القائمة على الحرب الإلكترونية والخداع النفسي، فضلًا عن القيام باستهداف شبكة تواصل العدو العسكرية، وعملياته الأمنية الإلكترونية[3].

كما عرفها كل من الأستاذ "ريتشارد كلارك "روبرت كناكي "على أنها: أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى؛ بهدف تحقيق أضرار بالغةٍ أو تعطيلها[4].

ويعرفها(Marco Roscini) بأنها: تطويع الإمكانيات التقنية، بغرض التأثير على المواقع الإلكترونية الأخرى، أو تعطيلها أو تدميرها، سواء كانت تلك المواقع تقدم الخدمات المدنية أم العسكرية[5].

---

(1) Michael N. Schmitt , Computer network attack and the use of force in international law: Thoughts on a normative framework, Columbia journal of transnational law, 1998–1999, Vol . 37, P.890.

(2) US Army Training and Doctrine Command , DESIGN Handbook No. 1.02 ,Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook, 2005 , at VII - 2

(3) Zimet E.and C. L. Barry ," Military services Overview, Cyber power and National Security ", National Defense University Press Washington, DC, USA, 2009, P.291.

(4) Nathalie Caplan," Cyber War: the Challenge to National Security», Global Security Studies, vol . 4, no.1 (Winter 2013), p 94.

(5) Marco Roscini," World Wide Warfare – Jus ad bellum and the use of Cyber Force", Max Planck Yearbook of United Nations Law, Volume 14,2010,p.91.

وعرفت استراتيجية الأمن السيبرانية الألمانية الهجمات السيبرانية بأنها: هجوم يتم من خلال الفضاء السيبراني موجه للإضرار بأنظمة تكنولوجيا المعلومات للدولة، وذلك بتعديلها كلها أو بعضها أو تحريفها أو تدميرها[1].

وأوردت استراتيجية المملكة المتحدة أربع طرق مختلفة للهجوم الإلكتروني في استراتيجيتها الوطنية الإلكترونية بدلًا من تعريف المصطلح وهي: "الهجوم الإلكتروني" و "تخريب سلسلة التوريد" و" التلاعب في الطيف الراديوي" و "تعطيل الإلكترونيات غير المحمية، باستخدام ترددات عالية الطاقة[2].

وفي عام ٢٠١١م، نشرت قيادة إدارة الأمن السيبراني بالولايات المتحدة الأمريكية دليلًا، عرفت فيه الهجوم السيبراني بأنه: فعل عدائي يتم باستخدام الكمبيوتر، والشبكات والأنظمة السيبرانية ذات الصلة، ويهدف إلى تعطيل أو تدمير أو التلاعب بأنظمة الإنترنت لدولة، أو المعلومات المخزنة على الحاسبات الآلية لها، أو وظائف هذه الأجهزة، ويتم هذا الهجوم بوسائل متعددة، منها المراسلات الإلكترونية المزيفة، أو الرسائل المفخخة، ويتميز الهجوم بأن آثاره عادة ما تكون منفصلة من الناحية الجغرافية عن نقطة إطلاقه". ونلاحظ أن التعريف قد ركز على غرضين للهجوم، وهما إلحاق الضرر بالنظم الإلكترونية، أو المعلومات ذات الصلة، وتدمير البنية المادية المرتبطة بتشغيل واستخدام هذه النظم[3].

ويعرف شين(shin) الهجوم السيبراني بأنه: استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها وجهًا لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها[4].

ويعرف (Matthew C. Waxman) الهجمات السيبرانية بأنها: الجهود الرامية إلى تغيير أو تعطيل أو تدمير أنظمة الحاسوب أو الشبكات أو المعلومات أو البرامج الموجودة عليهما، والأضرار التي

---

(1) German Federal Ministry of the Interior, Cyber Security Strategy for Germany (Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011), 14-15.

(2) UK Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (November,2011),13-14. https://www.gov.uk/government/uploads/system/uploads/attachment-data/file/60961/ukcyber-security-strategy-final .pdf. 22/6/2019 .

(3) US DOD, Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories, Joint Terminology for Cyberspace Operations, November 2011, available at: https://www.nsciva.org/CyberReferenceLib/201011joint%20Terminology%20for%20Cyberspace%20Operations.pdf.2/4/2020

(4) Shin, Beomchul, "The Cyber warfare and the Right of Self - Defence: legal perspectives and the case of the United States, IFANS, Vol . 19, No. 1, June 2011. P. 105.

تسببها هذه الهجمات يمكن أن تصيب شبكة الحاسوب أو المرافق المادية أو الأشخاص، وتتراوح أضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الانترنت إلى الدمار واسع النطاق على البنية التحتية العسكرية والمدنية المرتبطة بتلك الشبكات[1].

فيما ذهبت المستشارة القانونية في اللجنة الدولية للصليب الأحمر كوردولا دروغيه إلى تعريف الهجمات السيبرانية بأنها: هجمات لاستغلال الشبكات التي تنفذ لأغراض جمع معلومات غير مشروعة، وتحصل خارج نطاق النزاعات المسلحة، غير أنه في حالة النزاعات المسلحة عندما تلجأ الأطراف إلى أساليب الحرب ووسائلها التي تعتمد على عمليات سيبرانية، فهنا ينطبق القانون الدولي الإنساني[2].

بينما يعرف هربرت لين الهجمات السيبرانية بأنها: الأفعال التي يتخذها أطراف نزاع ما لتحقيق ميزة على خصومهم في الفضاء السيبراني، باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على البشر، ومن الناحية النظرية 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- التجسس السيبراني أو الاستغلال السيبراني- ويتاح لطائفة متنوعة من الفاعلين الحصول على هذه الأدوات والتقنيات، ومنهم الدول القومية والأفراد ومجموعات الجريمة المنظمة والمجموعات الإرهابية، وتتباين بشدة الدوافع إلى استخدام الهجمات السيبرانية أو التجسس السيبراني، ويشمل ذلك التجسس أغراضًا مالية وعسكرية وسياسية وشخصية[3].

أما التعريف الذي طرحه البروفيسور (Fuertes) بأنه: هجوم يتم من خلال الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل البيانات المتوفرة أو إتلافها أو الاستحواذ عليها، وتتم من خلال سلسلة الهجمات تقوم بها دولة ضد دولة أخرى[4].

---

(1) Matthew C. Waxman, Cyber- Attacks and the Use of Force: Back to the Future of Article 2 (4), Yale Journal of International Law, 2011, Vol . 36, p. 422.

(2) كوردولا دروغيه، ما من فراغ قانوني في الفضاء السيبراني، مقالة منشورة في تاريخ ١٦/٨/٢٠١١ متوفر على الموقع الرسمي للجنة الدولية للصليب الأحمر، متاح على الرابط:
https://wwwicrc.org/ar/doc/resources/documentsinterview/2011/cyber-warare-interview-2011-08- htm.16.

(3) لين، هربرت،" النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ (886)، صيف ٢٠١٢م، ص 515-531، ص 519-518، متاح على الرابط: https://cutt.ly/RkoansD

(4) Micheal S. Fuertes, "Cyber warfare, Unjust Actins in a just war" Florida International University, Full 2013, p.1.

كما يعرف (Johan Sigholm) الهجمات السيبرانية بأنها: جزء من العمليات السيبرانية (العمليات في الفضاء السيبراني) والتي تعمل على توظيف إمكانيات الفضاء السايبر والاستخدام العدائي له، من قبل الدولة والجهات غير الحكومية الفاعلة في النزاعات، والتي تعمل نيابة عنها، من أجل التسبب بالضرر، الدمار أو سقوط الضحايا لتحقيق أهداف عسكرية أو سياسية[1].

والجدير بالذكر أن القاعدة رقم (30) من " دليل تالين 1 "، ونظيرتها رقم (٩٢) من " تالين ٢ "[2]، قد أوردتا تعريفًا للهجوم السيبراني باعتباره: عملية إلكترونية هجومية أو دفاعية، يتوقع وفقا للمجرى العادي للأمور أن تتسبب في أضرار جسيمة، كإصابة أو موت أشخاص، أو تلف أو تدمير أشياء. ونلاحظ أن الأمثلة التي أوردها التعريف لأضرار الهجوم السيبراني، منها ما لا يمكن تداركه كموت أشخاص، أو تلف أو تدمير أشياء، وهي نفس الآثار التي يمكن أن تحدث نتيجة استخدام القوة، أو الهجوم العسكري المسلح من دولة على أخرى[3].

وفي الفقه العربي نجد العديد من التعريفات للهجمات السيبرانية، منها تعريف الدكتور عبد القادر محمد فهمي بأنها: هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية الدولة، أو الفاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب، وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، أو تقليلها ، أو حتي تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوتها العسكرية، وبالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم[4].

كما عرفت الهجمات السيبرانية بأنها: وسيلة قتالية يتم استخدامها بذاتها من أجل التسلل للأنظمة الإلكترونية المعدة من أجل حماية أو تنظيم سير عمل منشآت حيوية، مثل محطات توليد الطاقة النووية

---

(1) Johan Sigholm, Non- State Actors in Cyberspace Operations, National Defense University, Finland and Finish Society of Military Sciences, 2013, Vol .4 ,No.1,p.6.

(2) دليل تالين تم إعداده من قبل الخبراء القانونيين بدعوى من منظمة شمال الحلف الأطلسي الناتو وذلك لتنظيم النزاعات المسلحة في الفضاء السيبراني؛ حيث صدر دليل تالين الأول عام 2013 ويتكون من 282صفحة ويحتوي على 95مادة ، كما صدر دليل تالين الثاني عام 2017.

(3) Michael N. Schmitt: Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published,2013, P. 92. Available At: https://cutt.ly/tkofrbK

(4) عبد القادر فهمي، الحروب التقليدية وحروب الفضاء الإلكتروني: دراسة مقارنة في قواعد الاشتباك، مجلة العلوم القانونية والسياسية العدد (2)، المجلد (16)، السنة الثامنة، 2018م، ص20.

أو السدود أو وسائل النقل، وذلك بغرض تطويعها والسيطرة عليها لتدمير ذاتها بذاتها، من خلال القيام بتغذيتها بمعلومات غير صحيحة لجهة التحكم والحماية الإلكترونية[1].

ومما سبق يمكن تعريف الهجمات السيبرانية بأنها: عبارة عن عمليات عدائية هجومية أو دفاعية تتم في الفضاء السيبراني من قبل أطراف دولية أو غير دولية، من خلال الدخول غير المشروع للشبكات و الأنظمة الإلكترونية المعدة لحماية وتنظيم سير عمل المنشئات الحيوية لخصم معين، بواسطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة بقصد تغيير أو تعطيل أو تدمير أنظمة الحاسوب أو الشبكات أو المعلومات أو البرامج المرتبطة بتشغيل واستخدام البنية التحتية الوطنية للدول المدنية والعسكرية، والتسبب بأضرار جسيمة للأشخاص أو الممتلكات تكافئ ما قد ينتج عن هجمات الأسلحة التقليدية، تزامنًا مع نزاع مسلح تقليدي أو تمهيدًا له، بدافع سياسي أو قومي أو اقتصادي....الخ.

الفرع الثاني– خصائص الهجمات السيبرانية:

تحتوي الهجمات السيبرانية على العديد من الخصائص التي تميزها عن غيرها من الهجمات، من أبرزها ما يأتي:

قلة الكلفة المادية للهجمات السيبرانية، مقارنة بتكاليف الأسلحة المستخدمة في الحروب التقليدية، فلا تحتاج الدول في سياق ذلك إلى تخصيص ميزانيات ضخمة في تصنيع أسلحة مكلفة جدًا، كحاملات الطائرات والمقاتلات المتطورة، وإنما يكفي تطوير البرمجيات اللازمة، وامتلاك الأجهزة الحاسبة لتفرض تهديدًا خطيرًا وحقيقيًا على دولة أخرى[2].

تتميز الهجمات السيبرانية بالسرعة والمرونة والمراوغة، وسهولة التنفيذ؛ حيث يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، وفي بيئة مماثلة فمن الصعب جدًا على أي عقلية التحصن لوحده أن ينجح، فالتحصن بهذا المعنى سيجعل من هذا الطرف عرضة لمزيدٍ من عمليات الاختراق، وبالتالي لمزيدٍ من الضغط.

الهجمات السيبرانية تخضع لعمليات التطوير والابتكار في تقنياتها ووسائلها بشكل دائم وسريع، الأمر الذي يترتب عليه زيادة فاعليتها في اختراق أكثر الأنظمة الحماية تعقيدًا وقدرتها التدميرية.

---

[1] طلال ياسين العيسي، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقاء للبحوث والدراسات الإنسانية، العدد1، المجلد 19، 2019م، ص84.

[2] فيصل محمد عبد الغفار، الحرب الإلكترونية، الطبعة الأولى، عمان، الجنادرية،2016، ص11.

اختفاء العامل الجغرافي في الهجمات السيبرانية، فبعد ظهور شبكات المعلومات لم يعد هناك صورة مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، وبالتالي لا يتواجد مفهوم السيادة بمعناه السائد في العالم الواقعي؛ إذ إن الحدود تتداخل مع بعضها البعض نتيجة لارتباط الدول بأنظمة تكنلوجية وشبكة أنترنت واحده؛ مما يجعل أي مركز أو منشأة بغض النظر عن مكان تواجده الفعلي هدفًا لتلك الهجمات[1].

الهجمات السيبرانية تحقق مبدأ إخلاء المسؤولية، نتيجة لصعوبة تحديد مصدرها وشخصية القائم بها؛ حيث إنها لا تترك في الغالب أثرًا ماديًا يمكن ضبطه على عكس الأدوات المستخدمة في الحروب التقليدية التي يمكن اكتشافها ورصدها ومن ثم الرد عليها، فأغلب الهجمات تظل مجهولة المصدر مالم يعلن عنها أو إذا تم اكتشافها عن طريق الصدفة، وبعد وقت طويل؛ وهو ما يلغي إمكانية تطبيق مبدأ الردع بالانتقام، حتى إذا ما تم تتبع مصدر تلك الهجمات وتبين أنها تعود إلى فاعلين غير حكوميين فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد[2].

الهجمات السيبرانية قد تستخدم أثناء السلم أو الحرب، من خلال الجيش والمجتمع؛ لتحقيق أهداف مختلفة، فهي لا تقتصر على الأهداف العسكرية فقط، بل قد تستهدف البنية التحتية المدنية كاستهداف شبكات المياه والكهرباء، وأنظمة المستشفيات والبنوك وغيرها من المنشآت الحساسة، عن طريق قصفها بالعديد من الفيروسات والبرامج الضارة والتي قد يترتب عليها خسائر مادية في الأرواح والممتلكات[3].

يمكن للهجمات السيبرانية أن تنفذ أهدافها دون إلحاق ضرر مادي بالبنية التحتية أو البشر، وذلك من خلال الولوج غير المصرح به للأنظمة الالكترونية لدولة ما، وللاطلاع على بيانات ومعلومات سرية، للاستفادة منها دون تغير شيء فيها ودون محاولة للسيطرة أو التحكم فيها، ويمكن أيضًا إحداث دمار هائل بالبشر يكافئ أو يفوق هجمات الأسلحة التقليدية[4].

---

[1] صلاح حيدر عبد الواحد، حرب الفضاء الإلكتروني، دراسة في مفهومها وخصائصا، وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، عمان، 2021، ص44.

[2] فيصل محمد عبد الغفار، الحرب الإلكترونية، مرجع سابق، ص12.

[3] عادل عبد الصادق، أسلحة الفضاء السيبراني في ضوء القانون الدولي الإنساني، سلسة أوراق العدد 32، وحدة الدراسات المستقبلية مكتبة الإسكندرية، مصر (القاهرة)، 2016، ص58.

[4] المرجع نفسه، ص61.

المبحث الثاني- إشـكالية تطبيق القانون الدولي الإنسـاني على الهجمات السيبرانية:

انقسم الفقه القانوني حول مسألة انطباق القانون الدولي الإنساني على الهجمات السيبرانية من عدمه إلى فريقين بين مؤيد ومعارض، ولكل فريق حججه وأسانيده ومبرراته القانونية، فهناك من يرى عدم خضوع الهجمات والحروب السيبرانية لأحكام وقواعد القانون الدولي الإنساني، وهناك من يرى خضوع الهجمات والحرب السيبرانية لأحكام وقواعد القانون الدولي الإنساني[1]، وعليه سوف نتناول ذلك فيما يأتي:

المطلب الأول- عدم خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني:

يعد الفضاء السيبراني مكانًا أو قارة أو فضاء مستقلًا بحد ذاته عن كل الفضاءات الأخرى، بما فيها فضائنا المادي الملموس، يعني أنه مجال افتراضي غير مادي مستقل عن أي مكان وزمان يتم التواصل من خلاله بين كل أنحاء العالم، وكذلك تخزين ونقل وتداول كم غير محدود من المعلومات لمختلف المجالات، ويعتمد وجود هذا المجال على عناصر مادية -أجهزة الحاسب الآلي التي تتصل مع بعضها عن طريق شبكة الإنترنت وما يرتبط بها من تقنيات وبرامج- وبشرية -العنصر البشري الذي يقوم بتشغيل وتفعيل العناصر المادي- ومصمم بحيث يستحيل على أي جهة أو كيان التحكم فيه؛ لأن معظم الاتصالات التي تتم من خلاله تستخدم وسائل تمويه وتشفير، ولا يمكن لأي نظام مراقبة التعرف بدقه على مصدرها[2].

وعلى هذا الأساس ذهب جانب من الفقه الأوروبي والأمريكي إلى اعتبار الفضاء السيبراني منطقة خالية من القانون، وكل شيء فيه مباح؛ حيث لا يمكن لأي شخص القيام بأنشطة معادية من دون قواعد أو ضبط النفس. فقد قيل بأن كلمات المرور وألواح المفاتيح وأجهزة الحواسيب هي التي تشكل حدودًا وفواصل بين العالمين، ولابد من الدخول إلى هذا العالم من خلالها، فهذا العالم لا يمكن أن يتحدد

---

[1] تعد الهجمات السيبرانية أوسع نطاقاً من الحروب السيبرانية، بمعنى: أن الهجمات السيبرانية قد تكون جزءًا من حرب سيبرانية أو جزءًا من حرب تستخدم فيه أسلحة تقليدية، أو تستخدم في أوقات غير الحرب في وقت السلم، كما أن الحرب السيبرانية تتمثل في شن عدة هجمات سيبرانية، سواء كانت دفعة واحدة أو على عدة مراحل.

[2] د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، كلية الحقوق، جامعة المنصورة، ص265.

بدولة معينة، وبالتالي لا يمكن إخضـــاعه حتى للقانون الدولي العام التقليدي، فهذا القانون لم ينجح بحكم الفضاء البحري أو الجوي أو الخارجيين[1].

ويذهب أنصـــار هذا الاتجاه الذي يعرف (بالمذهب الحر)، والذي يتزعمه بعض الســـياســـيين الأمريكيين وعلماء التقنية، وتســـاندهم فئة قليلة من فقهاء القانون، إلى أن الإنترنت لا يخضـــع لقانون، وحجتهم أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي[2]. وعلى أساس ذلك طرحوا سؤلًا وجيهًا، هو أنه إذا سلمنا بضرورة خضوع الإنترنت للقانون، فأي سلطة يكون بإمكانها اليقظة على فرض أحكامه في ظل استقلالية الشبكة وانفلاتها من مفهوم الخضوع؟ وأجابوا بانعدام السلطة القادرة على ذلك، وحتى إن 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[3].

وفيما يتعلق بتطبيق أحكام القانون الدولي الإنساني على الحرب السيبرانية، يرى أصحاب هذا الاتجاه بأنه لا توجد أي قواعد قانونية بأي وثيقة من مواثيق القانون الدولي الإنساني تتناول بشكل مباشر مسألة الهجوم على شبكات الحاسوب، أو تتطرق إلى حرب المعلومات أو العمليات المعلوماتية، كذلك لم توضع ضوابط للهجوم على الشبكات الحاسوبية أثناء النزاعات المسلحة؛ كون استخدام تكنولوجيا الإنترنت حديث نسبيًا، إضافة إلى أن تطوير واستخدام الهجمات السيبرانية على شبكات الحاسوب حصل في فترة لاحقة على إعداد صكوك القانون الدولي الإنساني، كما أنّ هناك رأيًا آخر يقول بأن عدم انطباق القانون الدولي الإنساني على هذه الأسلحة، هو أن القانون الدولي وضعت قواعده لتنظيم وسائل وأساليب القتال ذات الطبيعة المتحركة التي ينتج عنها آثار مادية غير متوفرة في الهجمات الســـيبرانية، وبالتالي تكون الهجمات السيرانية خارج نطاق القانون الدولي الإنساني، ولا ينطبق عليها وصف الهجوم المسلح[4].

ويؤيد أصـــحاب هذا الرأي حجتهم بأن عبارة الحرب الإلكترونية لم ترد ضـــمن ميثاق الأمم المتحدة واتفاقيات جنيف ولاهاي، ومعاهدة حلف شمال الأطلسي؛ حيث وقد استخدم ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسي على حد سواء مصطلحات، مثل مصطلح "هجوم المسلح" و"استخدام القوة

---

(1) طالب حسن موسى، عمر محمود أعمر، "الإنترنت قانونًا، مجلة الشريعة والقانون، العدد37، 2016، ص8.

(2) Lavenue, J., Cyberspace ET Droit International: pour UN nouveau Jus Communications: Revue de la Recherche , (1996),p.3.

(3) طالب حسن موسى، عمر محمود أعمر، "الإنترنت قانونا"، مرجع سابق، ص8.

(4) أسامه صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية، العدد7، 2013، ص8.

في النزاعات المسلحة" و"عمل من جانب القوات البرية أو البحرية أو الجوية" وهي مصطلحات لا تنسجم مع مفهوم الحرب الإلكترونية؛ مما يجعلها ظاهريًا خارج نطاق القانون الدولي، على سبيل المثال النزاع الإلكتروني بين إستونيا وجورجيا والذي استمر لعدة أيام، فعلى الرغم من جسامة الأضرار التي لحقت بالبنية التحتية لهاتين الدولتين، فإنها لم تعد بمثابة نزاع مسلح، ولم تخضع لقواعد الحرب. إضافة إلى ذلك بينت المادة (51) من ميثاق الأمم المتحدة" أنه ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة..."، وهذا النص يعطي للدول الحق في الدفاع عن نفسها في حال تعرضها لهجوم من قبل قوة مسلحة، أما في السياق السيبراني فلا يعد الهجوم السيبراني نزاعًا مسلحًا بالمعنى الحقيقي؛ لأنه لا يتضمن استخدامًا للقوة المسلحة ضد إقليم الدولة. كما أن الهجوم السيبراني قد لا يصاحبه أو ينتج عنه أضرار جسدية أو مادية مباشرة[1].

ويبين أصحاب هذا الرأي أنه وعلى الرغم من أن مسمى الحرب يطلق على هجمات الحاسوب، فهوا أيضًا بحاجة إلى نظر؛ كون الحرب مفهوم يرتكز بالأساس على استخدام الجيوش النظامية، ويسبقها إعلان واضح لحالة الحرب على ميدان قتال محدد، أما بالنسبة لهجمات الفضاء السيبراني، فإنها تفتقر إلى تلك المقومات المادية؛ حيث تتم عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، والتي يتم توجيهها ضد المنشآت الحيوية، وذلك باستعمال أسلحة إلكترونية جديدة تناسب التطور التكنولوجي لعصر المعلومات، وبالتالي يجعلها أقرب إلى وصف الإرهاب منها إلى وصف الحرب[2]. كما أن أحد الأسباب التي تدعو أصحاب هذا الرأي للاعتقاد بعدم خضوع الهجمات السيبرانية للقانون الدولي الإنساني هو عدم وجود تعريف دقيق ومحدد ضمن نصوص هذا القانون الذي يركز على النزاعات المسلحة التقليدية، وبالتالي قد لا يغطي الهجمات السيبرانية بشكل مباشر.

ويضيف أصحاب هذا الرأي أن تطبيق مبادئ العامة في القانون الدولي الإنساني على الفضاء السيبراني، تبدو غير واقعية؛ لأن وسائل وأساليب الحرب السيبرانية غير واضحة ومفهومة بشكل كاف، حيث ولا يزال فهم الآثار المحتملة لهذه التكنولوجيا غير واضح قياسًا على وسائل وأساليب النزاعات

---

(1) C , Stahn,"Jus ad bellum', jus in Bello" jus post bellum"? Rrthing the Conception of the Law of Armed Force", The European Journal of International of International Law, 17(5), (2007), p. 923,footnot,8.

(2) عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 46، عدد 3، 2019، ص 137. متاح على الرابط: https://cutt.ly/lkpBGCp.

المسلحة التقليدية. وتتسم كذلك هجمات الفضاء السيبراني بسرية تامة، واستباقية بدون سابق إنذار، غير محددة المجال والمدى، وتكون أهدافها غير مأمونة، بخلاف الحرب التقليدية التي يكون مكانها وأهدافها محددين، فهي متعددة الأوجه ومتشابكة مع غيرها من الحروب، كالحرب الإعلامية والسياسية والسيكولوجية والإرهاب[1].

بالإضافة إلى أن المقاتلين السيبرانيين ليس لهم مكان ثابت، ولا يحتاجون إلى التواجد في المكان الذي ينطلق منه الهجوم أو المكان الذي يظهر أن الهجوم ينشأ فيه، ويمكن للقائم بالتصرف السيبراني بإخفاء هويته، أو تزويرها باستخدام التقنيات التكنولوجية[2].

كما يصعب تتبع مصدر الهجمات السيبرانية وتحديد الفاعلين بدقه، وهذا يشكل تحديًا أمام تطبيق القانون الدولي الإنساني الذي يتطلب تحديد المسؤولية بشكل واضح. بالإضافة إلى أن الترابط بين الأنظمة الحاسوبية للبنى التحتية المدنية والعسكرية يعقد مسألة تطبيق قواعد القانون الدولي الإنساني التي تعتمد على التمييز بين المقاتلين، والتمييز بين الأهداف العسكرية والمدنية[3].

ومن خلال ما تقدم يمكن القول: إن القانون الدولي الإنساني الحالي لا يتماشى مع مستجدات العصر؛ لأنه وضع أساسًا للتعامل مع النزاعات المسلحة التقليدية، وبالتالي لا ينطبق على الهجمات السيبرانية؛ لأنه لا يعد تلك الهجمات نزاعًا مسلحًا بالمعنى الحقيقي، بسبب غياب المقومات المادية للأعمال العدائية التقليدية.

على الرغم من الحجج الواردة ضمن هذا الاتجاه، فلا ينبغي الاعتراف بوجود فراغ قانوني في الفضاء السيبراني، ولكن يجب التسليم بفكرة اتساع القانون الدولي الإنساني لاستيعاب هذه التطورات الحديثة، وما يؤيد ذلك ما أشارت إليه محكمة العدل الدولية بأنّ" مبادئ وقواعد القانون الدولي الإنساني المطبق في النزاع المسلح، تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة، بما في ذلك تلك المستقبلية[4]، بالإضافة إلى الالتزام المنصوص عليه في المادة 36 من البروتوكول الإضافي الأول لعام 1977 لاتفاقيات جنيف لعام 1949م، عند اقناء الأسلحة التحقق إن كانت محظورة أم لا. وبالتالي نؤيد

---

(1) عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مرجع سابق، ص 137.
(2) المرجع نفسه.
(3) عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مرجع سابق، ص 137.
(4) نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة السورية الافتراضية، 2021، ص44.

موقف اللجنة الدولية للصليب الأحمر، وهو أن القانون الدولي الإنساني ينطبق على العمليات الإلكترونية التي يتم إجراؤها في النزاعات المسلحة، بقدر ما تكون عواقب مثل هذه العمليات قابلة للمقارنة مع عواقب العمليات التقليدية[1].

المطلب الثاني- خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني:

يرى أنصار هذا الرأي والذي يعرف بالمذهب القانوني، كالفقيه ماركو روسيني (Roscini Marco) والفقيه شين(Shin) إلى أنه لا يوجد فراغ قانوني في الفضاء السيبراني، وأن القواعد القانونية العرفية والاتفاقية الموجودة في إطار القانون الدولي الإنساني كافية لتنظيمه، وأنه يمكن تطبيقها على الفضائيات الحديثة، والذي تشكل الإنترنت أحد وسائله الرئيسية، خاصة وأنه سبق تنظيم وسائل اتصال تشابهها، مثل الهاتف والفاكس وغيرها من الوسائل الإلكترونية[2].

كما وضح المستشار القانوني للجنة الدولية للصليب الأحمر Cordula Droege أن الإطار القانوني الدولي الإنساني الحالي يطبق على النزاعات السيبرانية، ويجب احترامه، بمعنى: أن القانون الحالي قادر على التعامل مع التطورات الجديدة دون الحاجة إلى وضع قواعد قانونية خاصة بالفضاء السيبراني[3]، فإذا كنا نجمع بأن اتفاقيات القانون الدولي الإنساني لم تشر على وجه الخصوص إلى الهجمات والحرب السيبرانية، إلا أن هذه الحجة ليس لها أهمية تذكر، في ظل وجود شرط مارتينز، والذي يعد جزءًا من القانون الدولي الإنساني العرفي، والذي ينص على أنه في الحالات التي لا يشملها هذا البروتوكول أو الاتفاقات الدولية الأخرى، يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المشتقة من الأعراف الراسخة، ومن مبادئ الإنسانية، ومن ما يمليه الضمير العام[4]، وهذا يعني

---

(1) Sergey, Sayapin."Chapter 25: Russian approaches to international law and cyberspace". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar Publishing, 2021), pp525-546.p.539. https://doi.org/10.4337/9781789904253.00038

(2) Koh, paul. International Law in Cyberspace, Harvard International Law Journal, Online, volume 54 (2012), p.3.

(3) كوردولا دروغيه، ما من فراغ قانوني في الفضاء السيبراني، مقالة منشورة في تاريخ ١٦/٨/٢٠١١ متوفر على الموقع الرسمي للجنة الدولية للصليب الأحمر، متاح على الرابط:
https://wwwicrc.org/ar/doc/resources/documentsinterview/2011/cyber-warare-interview-2011-08- htm.16.

(4) مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص9.

أنه ليس هناك خلو أو فراغ قانوني، وأن كل ما يقع في أثناء النزاعات المسلحة هو يخضع لقواعد ومبادئ القانون الدولي الإنساني بصفة عامة، بما في ذلك الهجمات والحروب السيبرانية.

حيث وقد أجمع الفقه الدولي على أن الحروب السيبرانية تعد حربًا بالمعنى الصحيح، عندما تكون عواقب مثل هذه العمليات قابلة للمقارنة مع عواقب العمليات التقليدية. وأن استخدام القوة، من خلال هذه الآلية الحديثة ضد دولة ما يشكل حقًا وطنيًا للدولة المعتدى عليها للدفاع عن نفسها[1]. ويؤيد هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس، ردًا على هجمات 11سبتمبر 2001 على الولايات المتحدة الأمريكية[2]، كما أوضحت محكمة العدل الدولية أن المادة(51) من الميثاق لا تشير إلى نوع محدد من الأسلحة، وطبقته على قضية نيكاراغوا ضد الولايات المتحدة الأمريكية في عام (1986م) بشأن الأنشطة العسكرية المستخدمة[3]. وفي هذا السياق أشارت المحكمة في رأيها الاستشاري بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها ما يأتي:

تم اختراع الأسلحة النووية بعد ظهور معظم مبادئ وقواعد القانون الإنساني المطبق في النزاعات المسلحة ؛ (...). ومع ذلك، لا يمكن أن نستنتج من ذلك أن المبادئ والقواعد الراسخة للقانون الإنساني المنطبقة في النزاعات المسلحة لا تنطبق على الأسلحة النووية. قد يكون هذا الاستنتاج غير متوافق مع الطابع الإنساني الجوهري للمبادئ القانونية المعنية التي تتغلغل في قانون النزاع المسلح بأكمله، وتنطبق على جميع أشكال الحرب، وجميع أنواع الأسلحة، تلك الموجودة في الماضي، وتلك الموجودة في الحاضر. وتلك من المستقبل. ومثل الحرب النووية، تخضع الحرب الإلكترونية لقانون النزاع المسلح و "مبادئه الأساسية"، وهي حظر المعاناة غير الضرورية، ومبدأ التمييز. ويقصر المرء نفسه على المواد (48، 51، 52) من البروتوكول الأول وقواعدها العرفية[4].

---

[1] في حال وقوع هجمات إلكترونية من دولة ما فإن للدولة المعتدى عليها الحق في الدفاع عن نفسها استنادًا لنص المادة (51) من ميثاق الأمم المتحدة، سواء كان ناتج عن عدوان مسلح في العالم الحقيقي أو الفضاء الإلكتروني، وهنا يكون الرد فرديًا أو جماعيًا، ويكون من حق الدولة الضحية اتخاذ تدابير للدفاع عن النفس في الفضاء الإلكتروني، وفي العالم الحقيقي، ولكنها تكون ضرورية ومتناسبة لمواجهة الهجوم المفاجئ:

Michael N. Schmitt, International Law in Cyberspace the Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, Volume 54, 2012. www.harvardilj.org/wp-content/.../12/HILJ-Online_54_Schmitt.pdf

مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، مرجع سابق، ص87.

[2] Marko, Roscini, World Wide Warfare– Jus ad bellum and Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14, 2010, p.115.

[3] ICJ Reports 1986, see note 64, 94 Para. 176.

[4] Karine, Bannelier, "Chapter 20 Is the principle of distinction still relevant in cyber warfare?

وبالتالي من الممكن وصف الأعمال التي ترتكبها الأسلحة غير الحركية بأنها هجمات عندما تكون آثارها عنيفة. وكما أوضح دورمان، فإن "استخدام العوامل البيولوجية أو الكيميائية التي لا تسبب انفجارًا ماديًا، مثل استخدام الغازات الخانقة أو السامة، سيشكل هجومًا؛ لأن التأثيرات الناتجة عنيفة بغض النظر عن الوسائل المستخدمة لتحقيقها. مثل استخدام العوامل الكيميائية أو العوامل البيولوجية، يمكن أن يشكل استخدام الأدوات الإلكترونية هجومًا. على سبيل المثال ، وفقًا للورقة الفرنسية حول القانون الدولي المطبق على العمليات في الفضاء السيبراني، أي عملية إلكترونية يتم تنفيذها في حالة نزاع مسلح وفيما يتعلق بها، وتشكل عملًا من أعمال العنف، سواء كانت هجومية أو دفاعية، ضد طرف آخر في النزاع، هو هجوم بالمعنى المقصود في المادة (49) من البروتوكول الإضافي الأول من اتفاقيات جنيف، وهذا يعني إمكانية خضوع الهجمات السيبرانية للقانون الدولي الإنساني[1].

وبالإضافة إلى ذلك منح دليل تالين الدولة الحق في الرد على الهجمات السيبرانية التي تتعرض لها من الدولة المعادية، مع إمكانية الرد باستخدام القوة العسكرية الحقيقية في حال تعرضت دولة ما لهجوم إلكتروني وأدى هذا الهجوم إلى خسائر مادية وبشرية؛ حيث يمكن معادلة العملية الإلكترونية باستخدام القوة عندما يكون نطاقها وتأثيراتها قابلة للمقارنة مع أثر وحجم الهجمات التقليدية، أي: مساوية أو قريبة منها[2].

ومن أجل تحديد العمليات السيبرانية التي يمكن وصفها على أنها استخدامات للقوة، ينص دليل تالين على العديد من العوامل– معايير شميت– التي يمكن أخذها في الاعتبار وهي: الخطورة، والفورية، والمباشرة، والغزو، وتدخل الدولة، والافتراض مشروعية قياس الآثار والطابع العسكري. ومع ذلك، فإن استخدام القوة لا يتطابق مع الهجوم المسلح. التمييز بين استخدام القوة في المادة (4/2) والهجوم المسلح في المادة (51) واضح من الميثاق. وهذا يعني أنه لكي تكون قادرًا على التصرف دفاعًا عن النفس، يجب أن تكون العملية الإلكترونية من حيث الحجم والتأثيرات مساوية لهجوم مسلح[3].

From doctrinal discourse to States practice". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar Publishing, 2021). P. 428.
https://doi.org/10.4337/9781789904253.00032

(1) Karine, Bannelier, "Chapter 20 Is the principle of distinction still relevant in cyber warfare? From doctrinal discourse to States practice", op. cit, p. 434.

(2) Michae N. Schmitt (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op. cit, comment (3) on Rule (13).

(3) Eric, myjer."Chapter 17: Some thoughts on cyber deterrence and public international law". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar

أما عن اشتراط ميثاق الأمم المتحدة استخدام القوة لعد الهجوم السيبراني نزاعًا مسلحًا، فإن المادة (4/2) من الميثاق قد حظرت على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدام ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة، لكن الميثاق ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعًا للظروف المحيطة بكل حالة على حدة،[1] على سبيل المثال تؤكد وزارة الدفاع الأمريكية أن حقيقة الهجوم السيبراني على شبكة الكمبيوتر، والذي يمكن أن يتسبب بأضرار واسعة النطاق، واضطراب اقتصادي وخسائر في الأرواح، من الممكن أن يعجل باتخاذ مجلس الأمن إجراء بموجب المادة (39) من الميثاق، إذا وصف الهجوم السيبراني بأنه تهديد للأمن والسلم الدوليين أو إخلال به أو كان وقع عملًا من أعمال العدوان، وقد يلجأ مجلس الأمن بوجب المادة (40) من الميثاق إلى اتخاذ تدابير لمنع تفاقم الأزمة في حال رأى المجلس في موقف معين تهديدًا للسلم، كما يمكن لمجلس الأمن اتخاذ تدابير تنطوي على استخدام القوة أو لا تنطوي عليها بموجب المادة (41،42) من الميثاق[2].

وبالتالي يستطيع المجلس بموجب الصلاحيات المخولة له القطع الكلي أو الجزئي لوسائل التواصل أو فرض الحصار الإلكتروني على الدولة المسؤولة عن الهجوم السيبراني من أجل منع استمراره أو تكراره، وكل هذا يعني أن الفقرة الرابعة من المادة الرابعة من ميثاق الأمم المتحدة والمواد ذات الصلة تنطبق على الهجمات السيبرانية[3].

وفي هذا السياق نصت المادة(36) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف 1949م، المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام 1977م، على ما يأتي:" يلتزم أي طرف سام متعاقد، عند دراسة، أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو بعضها بمقتضى هذا الملحق" البروتوكول" أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد. يدل هذا النص على قابلية تطبيق قواعد القانون الدولي الإنساني على وسائل وأساليب الحرب المرتكزة إلى التكنولوجيا السيبرانية،

Publishing, 2021).pp366-386. p.382 . https://doi.org/10.4337/9781789904253.00028

(1) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية، مجلة المحقق المحلي للعلوم القانونية والسياسية، جامعة بابل، السنة الثامنة، العدد الرابع، 2016، ص 49.

(2) Roscini, Marco. "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force." Max Planck Yearbook of United Nations Law Online 14, no. 1 (2010): 85–130.P.110. https://doi.org/10.1163/18757413-90000050.

(3) Ibid, p.111.

تماما كما يخضع لها أي سلاح جديد عندما يستخدم في نزاع مسلح اعتمادًا على معيار النتائج التي تحدثها هذه الأسلحة.

أما بالنسبة لحجة اعتبار الهجوم السيبراني على شبكات الحاسوب ليس نزاعًا مسلحًا لغياب الأعمال العدائية التقليدية؛ لأن وجود النزاع المسلح الدولي أو الداخلي هو شرط لتطبيق القانون الدولي الإنساني، كما تنص المادة الثانية المشتركة من اتفاقيات جنيف لعام 1949م، على انطباق هذه الاتفاقية- بغض النظر عن الشروط المحددة التي تتعلق بوقت السلم- على جميع حالات الحرب المعلنة أو أي نزاع مسلح آخر ينشب بين طرفين أو أكثر من الأطراف المتعاقدة، حتى لو لم يعترف أحدهما بحالة الحرب ... وأصبحت الحرب المعلنة شكل من أشكال النزاعات المسلحة[1]. بمعنى: أن هذه المادة أخذت بالحالة الواقعية للحرب لكي يطبق عليها القانون الدولي الإنساني، بغض النظر عن أي معيار شكلي آخر.

ونظرًا للتقدم في ووسائل وأساليب الحرب، ولاسيما حرب المعلومات، فلا يكفي لتطبيق القانون الدولي الإنساني الاعتماد على معيار الفاعل فقط (القوات المسلحة)، بل يجب الاعتماد بدرجة أكبر على معيار جسامة الآثار واتساع النطاق. على سبيل المثال تخضع الحرب الكيميائية والحرب البيولوجية للقانون الدولي الإنساني على الرغم من أنها لا تتضمن استعمال أسلحة حركية.

ومما يجدر الإشارة إليه أن النهج القائم على النتائج تؤيده أيضًا حقيقة أنه مادام النزاع المسلح قد بدأ، فإن الوسائل التي تستخدم لإحداث الأذى أو الموت أو إحداث التلف أو الدمار للبنى التحتية للدولة المستهدفة بغض النظر عن الوسيلة أو الطريقة التي استخدمت، كالتجويع، والضرب، والرمي بالرصاص، وإلقاء القنابل، وكذلك الهجمات السيبرانية كلها تخضع للقانون الدولي الإنساني، على سبيل المثال الهجمات السيبرانية التي تستهدف الشبكات الوطنية لتوليد الطاقة، ومحولات الكهرباء ومرافق الأسلحة النووية، وكذلك مراكز التحكم بحركة الملاحة الجوية، بحيث يجعلها تدمر نفسها، وينتج عن ذلك التسبب بأضرار مساوية لأضرار النزعات التقليدية، وعلى نطاق واسع (مثل تدمير البنية التحتية الحيوية أو التسبب في خسائر بشرية أو تعطيل القوات العسكرية)، وبالتالي يقتضي خضوع هذه الهجمات لأحكام

(1) Jean S, Pictet. the Geneva Conventions of 12 August 1949. Commentary Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, International Committee Of The Red Cross, (1952), P. 27-37.

القانون الدولي الإنساني حتى ولو لم يتم استخدام القوات المسلحة التقليدية، ويكون للدول حق الرد عليها[1].

وترتيبًا على ما سبق يمكن القوال إن أنصار هذا الاتجاه يذهبون إلى أنه لا يوجد فراغ قانوني في الفضاء السيبراني، وهو ما يرجحه الباحث، وأن القواعد القانونية العرفية ولاتفاقيات الموجودة في إطار القانون الدولي الإنساني قابلة للتمديد لتشمل الهجمات والحروب السيبرانية، ما دام تأثير هذه الهجمات مشابهًا لتأثير الهجمات التقليدية، كإجراء مقبول إلى حين التوصل إلى تشريع قانون دولي إنساني ذي نصوص قانونية واتفاقيه، واضحة وصريحة في إشارتها للهجمات والحروب والعمليات السيبرانية بشكل تفصيلي، وبما يتلاءم مع طبيعتها؛ لأن القواعد السارية لا تواكب طبيعة هذا التطور بكل تفاصيله، لاسيما توضيح كيفية تطبيق تلك المبادئ في الحالات التي تكون البنية التحتية المستهدفة في خدمة أغراض مدنية وعسكرية على حد سواء، وغير ذلك من الإشكاليات القانونية، لعل من بينها تحديد هوية المسؤول عن الأفعال ومصدرها، وذلك لاحتواء هذا النوع الجديد من الحروب، وبما يتماشى مع ميثاق الأمم المتحدة.

الخاتمة:

موضوع البحث الموسوم بـــ "مفهوم القانون الدولي الإنساني وإشكالية تطبيقه على الهجمات السيبرانية" تناولت بالبحث فيه العديد من المفاهيم المتعلقة بتوضيح مفهوم القانون الدولي الإنساني، وتعريف الهجمات السيبرانية وخصائصها، وذلك في المبحث الأول، ومن ثم تم دراسة إشكالية تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية، وقد خلص البحث الي العديد من النتائج والتوصيات علي النحو الآتي:

أولًا- النتائج:

1- الهجمات السيبرانية كتحدٍ للقانون الدولي الإنساني: أكد البحث أن الهجمات السيبرانية تمثل نوعًا جديدًا من الحروب؛ حيث تُنفذ في فضاء افتراضي لا يخضع للحدود الجغرافية. هذا التحول أحدث إشكاليات متعددة، منها صعوبة تحديد مصدر الهجمات وتحديد المسؤول عنها، سواء كان دولة أو جهة

[1] مايكل ن. شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، مرجع سابق، ص 94-95.

غير حكومية. كما أن الأضـــرار الناتجة عن هذه الهجمات قد تتجاوز الأضـــرار التقليدية، مثل تعطيل البنية التحتية الوطنية، وتعطيل أنظمة المستشفيات أو المرافق الحيوية؛ مما يجعلها تهديدًا جوهريًا للسكان المدنيين.

2- توصل البحث إلى أن أحكام القانون الدولي الإنساني يمكن أن تنطبق على الهجمات السيبرانية، عندما تشكل الهجمات الإلكترونية جزءًا من نزاع مسلح حركي مستمر، وعندما لا يكون استخدام الأسلحة التقليدية كافيًا بحد ذاته، ولكنه يستند أيضًا إلى هجمات سيبرانية واسعة النطاق، كما ينطبق القانون الدولي الإنساني على الهجمات السيبرانية إذا كان تبادل العمليات السيبرانية بين الدول يرقى بحد ذاته إلى "اللجوء إلى القوة المسلحة".

3- قصور التشريعات الدولية: أشار البحث إلى وجود نقص واضح في التشريعات الدولية المتعلقة بتنظيم الفضاء السيبراني؛ مما يترك فجوات قانونية تعيق التصدي للهجمات السيبرانية بفاعلية، في ظل تزايد خطر الهجمات السيبرانية، بما يجعلها تمثل تهديدًا متناميًا للسلم والأمن الدوليين.

ثانيًا- التوصيات:

1- يوصي البحث بضرورة تطوير قواعد القانون الدولي الإنساني لإدراج الهجمات السيبرانية بوضوح ضمن النصوص القانونية، بحيث تُعد هذه الهجمات وسيلة قتال حديثة تستوجب تنظيمًا دقيقًا. ويشمل ذلك وضع معايير دولية لتحديد طبيعة الهجمات السيبرانية، وتحديد المسؤولية الدولية.

2- أوصى البحث بتأسيس إطار دولي للتعاون بين الدول لمكافحة الهجمات السيبرانية. يشمل هذا التعاون تبادل المعلومات حول التهديدات الســـيبرانية، وتطوير آليات الردع والعقوبات الدولية على الجهات التي تستخدم الفضاء السيبراني لأغراض عدائية.

3- رفع الوعي وبناء القدرات: أوصـــى البحث بضـــرورة دعم الجهود الرامية إلى زيادة الوعي بأهمية الأمن السيبراني، وتدريب الكوادر الفنية المتخصصة والقانونية والقضائية في الدول على التعامل مع القضايا المرتبطة بالفضاء السيبراني، بما في ذلك فهم طبيعة الهجمات السيبرانية وآليات توثيقها، وملاحقة الفاعلين، وكيفية تطبيق القانون الدولي الإنساني على النزاعات الســـيبرانية، وكذلك تزويد الجيوش بتقنيات ومهارات التعامل مع التهديدات السيبرانية.

قائمة المصادر والمراجع

أولًا- قائمة المراجع العربية:

1- أ.د. محمد عزيز شكري، تاريخ القانون الدولي الإنساني وطبيعته، تقديم أ. د. مفيد شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، القاهرة- 2000م, متاح على الرابط:

https://blogs.icrc.org/alinsani/2020/08/13/3871/

2- د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية، مجلة المحقق المحلي للعلوم القانونية والسياسية، جامعة بابل، السنة الثامنة، العدد الرابع، 2016.

1- د. بلال علي النسور و د. رضوان محمود المجالي، الوجيز في القانون الدولي الإنساني "ما بين الاعتبارات القانونية والسياسية، جوانب نظرية وتطبيقية" دراسة في بعض من النماذج الدولية المعاصرة، الأكاديميون للنشر والتوزيع، عمان الأردن, 2012م.

2- د. ديب عكاوى، القانون الدولي الإنساني. أكاديمية العلوم الأوكرانية، كييف، 1995م.

3- د. شريف عتلم و د. محمد ماهر عبد الواحد، موسوعة اتفاقيات القانون الدولي الإنساني، إصدارات فرع اللجنة الدولية للصليب الأحمر، القاهرة، 2002م.

3- د. شريف عتلم، محاضرات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، الطبعة التاسعة, 2011م.

4- د. شريف عتلم، و د. عمر مكاوي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني، إصدارات اللجنة الدولية للصليب الأحمر، المجلد الثاني، 2017م.

5- د. عامر الزمالي، مدخل إلى القانون الدولي الإنساني، منشورات المعهد العربي لحقوق الإنسان، ط1، 1993م.

6- د. عامر الزمالي، مدخل الى القانون الدولي الإنساني، إصدارات المركز العربي لحقوق الإنسان، ط2، تونس، 1997م.

7- د. مايا الدباس، و د. جاسم ذكريا، القانون الدولي الإنساني، منشورات الجامعة الافتراضية السورية، سوريا، 2018م.

8- د. محمد طلعت الغنيمي، نظرة عامة في القانون الدولي الإنساني الإسلامي، بحث ضمن مقالات في القانون الدولي الإنساني في الإسلام، جمع وترتيب د، عامر الزمالي، إصدارات اللجنة الدولية للصليب الأحمر.

9- أسامه صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية، العدد7، 2013.

10- د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس

وقت السلم، كلية الحقوق، جامعة المنصورة، 2020.

11-صلاح حيدر عبدالواحد، حرب الفضاء الإلكتروني، دراسة في مفهومها وخصائصا، وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، عمان، 2021.

12-طالب حسن موسى، عمر محمود أعمر، "الإنترنت قانوناً، مجلة الشريعة والقانون، العدد37، 2016.

13- طلال ياسين العيسي، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقاء للبحوث والدراسات الإنسانية، العدد1، المجلد 19، 2019.

14- عادل عبدالصادق، أسلحة الفضاء السيبراني في ضوء القانون الدولي الإنساني، سلسة أوراق العدد 32، وحدة الدراسات المستقبلية مكتبة الإسكندرية، مصر(القاهرة)، 2016.

15-عبد القادر فهمي، الحروب التقليدية وحروب الفضاء الإلكتروني: دراسة مقارنة في قواعد الاشتباك، مجلة العلوم القانونية والسياسية العدد (2)، المجلد (16)، السنة الثامنة، 2018.

16- عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 46، عدد 3، 2019. متاح على الرابط: https://cutt.ly/lkpBGCp.

17- فيصل محمد عبد الغفار، الحرب الإلكترونية، الطبعة الأولى، عمان ،الجنادرية،2016.

17- كوردولا دروغيه، ما من فراغ قانوني في الفضاء السيبراني، مقالة منشورة في تاريخ ١٦/٨/٢٠١١ متوفر على الموقع الرسمي للجنة الدولية للصليب الأحمر، متاح على الرابط:
https://wwwicrc.org/ar/doc/resources/documentsinterview/2011/cyber-warare-interview-2011-08- htm.16.

18- لين، هربرت،" النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ (886)، صيف ٢٠١٢م، ص 515-531، ص 519-518، متاح على الرابط:
https://cutt.ly/RkoansD

19- مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002.

20-محمود داوود, مراحل واتجاهات تطور القانون الدولي الإنساني, مجلة القانون, م 9، عدد 1، جامعة البحرين، يناير، 2012، ص 129-201.

21-منير البعلبكي ورمزي منير البعلبكي، المورد الحديث، دار العلم للملايين، لبنان،2008.

22- منير البعلبكي، المورد، قاموس إنكليزي عربي، دار العلم الملايين، بيروت،2004.

23- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة السورية

الافتراضية،2021.

4- نيلس مليزر، القانون الدولي الإنساني مقدمة شاملة، إصدارات اللجنة الدولية للصليب الأحمر, آب/ أغسطس 2016م, ص 17. كتاب منشور علي الإنترنت في الزيارة تاريخ 18 اغسطس 2020م, على الرابط التالى:-

24- قاموس أكسفورد، متاح على

الرابط:https://www.oxordlearnersdictionaries.com/definition/American-englis/cyber

ثانيًا- المراجع الأجنبية:

1. Alexander, A. A Short History of International Humanitarian Law. European Journal of International Law 2015, 26 (1), 109–138. https://doi.org/10.1093/ejil/chv002. International Committee of the Red Cross (ICRC), War and International Humanitarian Law (29 October 2010), available at www.icrc.org/eng/war-and-law/overview-war-and-law.
2. Bassiouni, C. M. The Normative Framework of International Humanitarian Law: Overlaps, Gaps, and Ambiguities. International Law Studies 2000, 75 (1), pp1-55,.
3. C , Stahn,"Jus ad bellum', jus in Bello" jus post bellum"? Rrthing the Conception of the Law of Armed Force", The European Journal of International of International Law, 17(5), (2007).
4. Doswald-Beck, Louise. 1997. "International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons". International Review of the Red Cross Archive 37(316): 35–55.
5. Eric, myjer."Chapter 17: Some thoughts on cyber deterrence and public international law". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar Publishing, 2021).pp366-386. https://doi.org/10.4337/9781789904253.00028
6. German Federal Ministry of the Interior, Cyber Security Strategy for Germany (Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011), 14-15.
7. ICJ Reports 1986, see note 64, 94 Para. 176.
8. Jean S, Pictet. the Geneva Conventions of 12 August 1949. Commentary Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, International Committee Of The Red Cross, (1952).
9. Johan Sigholm, Non- State Actors in Cyberspace Operations, National Defense University, Finland and Finish Society of Military Sciences, 2013, Vol .4 ,No.1.
10. Karine, Bannelier, "Chapter 20 Is the principle of distinction still relevant in cyberwarfare? From doctrinal discourse to States practice". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar Publishing, 2021). https://doi.org/10.4337/9781789904253.00032
11. Koh, paul. International Law in Cyberspace, Harvard International Law Journal,

Online, volume 54 (2012).

12. Lavenue, J., Cyberspace ET Droit International: pour UN nouveau Jus Communications: Revue de la Recherche , (1996).
13. Marco Roscini," World Wide Warfare – Jus ad bellum and the use of Cyber Force", Max Planck Yearbook of United Nations Law, Volume 14,2010.
14. Matthew C. Waxman, Cyber- Attacks and the Use of Force: Back to the Future of Article 2 (4), Yale Journal of International Law, 2011, Vol . 36.
15. Michael N. Schmitt , Computer network attack and the use of force in international law : Thoughts on a normative framework , Columbia journal of transnational law, 1998– 1999, Vol . 37.
16. Michael N. Schmitt, International Law in Cyberspace the Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, Volume 54, 2012. www.harvardilj.org/wp-content/.../12/HILJ-Online_54_Schmitt.pdf
17. Michael N. Schmitt: Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published,2013, P. 92. Available At: https://cutt.ly/tkofrbK
18. Micheal S. Fuertes, "Cyber warfare, Unjust Actins in a just war" Florida International University, Full 2013.
19. Nathalie Caplan ," Cyber War : the Challenge to National Security », Global Security Studies, vol . 4, no.1 (Winter 2013).
20. Norbert Wiener, "Cybernetics or control communication in the animal and the machine" ,M.I.T. press ,second Edition, Cambridge, Massachusetts, 1948,Available At: https://cutt.ly/akhwlob
21. Richard kissel, "Glassory of Key information security Terms", National institute of standards and technology, U.S Department of Commerce",Revision,2,May,2013.
22. Schindler, D. International Humanitarian Law: Its Remarkable Development and Its Persistent Violation. Journal of the History of International Law / Revue d'histoire du droit international 2003, 5 (2), 165–188. https://doi.org/10.1163/157180503770735821.
23. Sergey, Sayapin."Chapter 25: Russian approaches to international law and cyberspace". In Research Handbook on International Law and Cyberspace, (Cheltenham, UK: Edward Elgar Publishing, 2021), pp525-546. **https://doi.org/10.4337/9781789904253.00038**
24. Shin, Beomchul, "The Cyber warfare and the Right of Self - Defence: legal perspectives and the case of the United States, IFANS, Vol . 19, No. 1, June 2011.
25. U.S. Department of Defense , Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, 2010, as amended through Feb. 15, 2016.
26. UK Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the

UK in a Digital World (November,2011),13-14. https://www.gov.uk/government/uploads/system/uploads/attachment-data/file/60961/ukcyber-security-strategy-final .pdf. 22/6/2019 .

27. US Army Training and Doctrine Command , DESIGN Handbook No. 1.02 ,Critical Infrastructure Threats and Terrorism : Cyber Operations and Cyber Terrorism Handbook , 2005 , at VII – 2
28. US DOD, Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories, Joint Terminology for Cyberspace Operations, November 2011.
29. Zimet E.and C. L. Barry ," Military services Overview, Cyber power and National Security " , National Defense University Press Washington , DC , USA , 2009.