The Extent Of The Applicability And Compulsion Of International Humanitarian Law In The Cyberwarfare

Dr. Maya Shawkat Saftly [*]
Najah M. Maher Al- Dakkak [**]

(Received 4 / 10 / 2021. Accepted 31 / 1 / 2022)

□ ABSTRACT □

After the four Geneva Conventions for the Protection of Victims of Armed Conflicts of 1949 and the Additional Protocols attached thereto of 1977 laid the foundations of the rules of contemporary international humanitarian law, and its provisions are no longer subject to controversy, whether in terms of the provisions of those rules or in terms of their binding for the parties to both international and non-international armed conflict; The controversy arises again and from time to time whenever a new type of confrontation arises between the parties to the conflict, whether in its form or its tools, in order to find out whether this new confrontation that has developed is a type of armed conflict and whether the provisions of international humanitarian law apply to it accordingly as well. Cyber-attacks constitute one of the subjects of this controversy in international jurisprudence and jurisdiction today, as we can attribute it to one reason, which is the absence of international legal rules regulating its provisions. So that one group says that Cyber-attacks are not subject to the provisions of the rules of international humanitarian law, and another group says that they occur, and this is what prompted the research into those problems that hinder the application of the provisions of international humanitarian law in the absence of texts regulating its provisions to know the consequences and to avoid the negative ones and prevent their occurrence.

Keywords: Cyber-attacks- Cyber Space- Cyber Armed Conflicts- Electronic Wars- Space Wars- Cyber Wars- International Humanitarian Law.

[*] **Professor, Section of International Law, Faculty of Law, Tishreen University, lattakia,Syria.**
[**] **Postgraduate Student ,Section of International Law, Faculty of Law, Tishreen University, lattakia,Syria. E-mail: najah3maher@gmail.com**

مدى انطباق القانون الدولي الإنساني وإلزاميته في الحروب السيبرانية

الدكتورة مايا شوكت صفطلي*

نجاح محمد ماهر الدقاق**

(تاريخ الإيداع 4 / 10 / 2021. قُبِل للنشر في 31 / 1 / 2022)

□ ملخّص □

بعد أن أرست اتفاقيات جنيف الأربع لحماية ضحايا النزاعات المسلحة لعام 1949 والبروتوكولان الإضافيان الملحقان بها لعام 1977 دعائم قواعد القانون الدولي الإنساني المعاصر ولم تعد أحكامه محل جدال أو خلاف سواء لجهة أحكام تلك القواعد أو لجهة إلزاميتها لأطراف النزاع المسلح الدولي منه وغير الدولي؛ يثور الجدل مرة أخرى وبين الفينة والأخرى كلما استجد نوع جديد من أنواع المواجهة بين أطراف النزاع سواء في شكلها أو أدواتها وذلك لمعرفة فيما إذا كانت هذه المواجهة الجديدة التي استجدت نوعا من أنواع النزاعات المسلحة وفيما إذا كانت أحكام القانون الدولي الإنساني تنطبق عليها تبعا لذلك أيضا، وتشكِّل الهجمات السيبرانية إحدى مثارات هذا الجدل في الفقه والقضاء الدوليين اليوم لما يمكن أن نرده إلى سبب واحد وهو عدم وجود قواعد قانونية دولية تنظم أحكامها، ففريق يقول بعدم خضوع الهجمات السيبرانية لأحكام قواعد القانون الدولي الإنساني، وفريق آخر يقول بوقوعها، وهذا ما دفع إلى البحث في تلك المشكلات التي تعترض انطباق أحكام القانون الدولي الإنساني في غياب نصوص تنظم أحكامها لمعرفة ما يترتب عليها من آثار ولتلافي السلبي منها والحؤول دون وقوعه.

الكلمات المفتاحية: الهجمات السيبرانية– الفضاء السيبراني– النزاعات المسلحة السيبرانية– الحروب الإلكترونية– حروب الفضاء– الحروب السيبرانية– القانون الدولي الإنساني.

* **الدكتورة– قسم القانون الدولي– كلية الحقوق– جامعة تشرين– اللاذقية– سورية.**

** **طالب ماجستير– قسم القانون الدولي– كلية الحقوق– جامعة تشرين– اللاذقية– سورية.**

مقدمة:

لم تعد النزاعات المسلحة بنوعيها الدولي وغير الدولي محل اختلاف في مدى إلزامية أحكامها لأطراف النزاع المسلح بل ولم تعد الحرب خيارا مشروعا يمارسه الطرف الذي يعلن الحرب في مواجهة الطرف الآخر مثلما كان عليه الأمر في ظل القانون الدولي التقليدي، ومثل أي تطور يطرأ على موضوعات أي قانون؛ تبرز إلى المجتمع الدولي مسائل مستجدة غير معالجة ضمن قواعد قانونية اتفاقية مقننة ملزمة للأطراف مثلما كانت عليه الأسلحة النووية واليوم الطائرات بدون طيار والروبوتات المتَحكَّم بها عن بعد.

وتُعدُّ "**الحروب السيبرانية**" أو ما يُعرَف **بـ"حروب الفضاء الإلكترونية**" مسألة من تلك المسائل المستجدة إذ اصطدم المجتمع الدولي في مدى عدها نزاعات مسلحة وخضوعها تبعا لذلك لأحكام القانون الدولي الإنساني، وظهر في لذك اتجاهان بين مؤيد ومعارض، وتمحورت المشكلات الرئيسة في هذه المسألة حول ثلاث نقاط وهي: تحديد الحالات التي يمكن أن ينطبق فيها القانون الدولي الإنساني وهي الحالة التي يمكن فيها وصف الهجمات السيبرانية بوصف الحرب أو النزاع المسلح، ومعرفة مدى إلزامية أحكامه للأطراف في مثل هذه الحالات، ومواءمة انطباق قواعد هذا القانون ومبادئه عليها بسبب اختلاف طبيعتها وأساليبها وأدواتها عن النزاعات المسلحة التقليدية.

لذلك سيتم البحث في هذه المشكلات الثلاث من خلا مطلبين:

يتناول **المطلب الأول: الهجمات السيبرانية ومدى انطباق القانون الدولي الإنساني عليها.**

أما **المطلب الثاني: مدى إلزامية القانون الدولي الإنساني في الحروب السيبرانية وتطبيقه عليها.**

مشكلة البحث:

تتمحور النقطة الأولى من البحث حول التساؤل الآتي:

- **ما حالات الهجمات السيبرانية؟ وفي أي منها يمكن أن تشكِّل نزاعا مسلحا؟**

ويتفرع عن هذا السؤال الرئيس التساؤلات الفرعية الآتية:

1) هل يمكن تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية؟

2) وما مدى إلزامية هذه القواعد لأطراف النزاع؟

3) وكيف يمكن مواءمة تطبيق هذه القواعد مع مثل هذا النوع من النزاعات المسلحة؟

أهمية البحث وأهدافه:

1) تظهر أهمية هذا البحث بحسبان أن **الهجمات السيبرانية أصبحت سمة من سمات المواجهة في هذا العصر وقد ظهرت في المواجهات بين الدول بما فيها القوى العظمى** مما يقتضي ضرورة البحث فيها وتحديد أبرز جوانبها ومشكلاتها.

2) إضافة إلى أن تحديد مشكلات الحروب السيبرانية يكشف عن **ضرورة وضع الحلول لها وذلك من أجل الحد من آثارها السلبية وضبط أفعال الأطراف فيها.**

وانطلاقا مما سبق؛ فإن البحث يهدف إلى حل المشكلات الرئيسة للنزاعات المسلحة السيبرانية، وهي:

1) تحديد حالات النزاع السيبراني التي يمكن أن يُطبَّق عليها القانون الدولي الإنساني.

2) تحديد مدى إلزامية قواعد القانون الدولي الإنساني للأطراف في الحروب.

3) تحديد كيفية مواءمة قواعد القانون الدولي الإنساني لهذا الشكل المستجد من النزاعات المسلحة.

الدراسات السابقة:

1) الدراسة الأولى: هربرت لين: "**النزاع السيبراني والقانون الدولي الإنساني**"، **لعام 2012**، إذ هدف الباحث إلى تحديد مفهوم النزاعات السيبرانية وتحديد عناصرها، ووصل إلى نتيجة مفادها أن مشكلات الحماية السيبرانية المعادية وردعها بلا حل من الناحية الفكرية، ولميثاق الأمم المتحدة واتفاقيات جنيف صلة وثيقة بالعمليات السيبرانية، لكن سمات هذه الصلة غير واضحة اليوم لأن الفضاء السيبراني شيء جديد بالمقارنة بهذه الصكوك.

2) الدراسة الثانية: يحيى ياسين سعود: "**الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني**"، **لعام 2018**، إذ هدف الباحث إلى إيجاد مقاربات إنسانية بين الحروب التقليدية وحروب الفضاء الإلكتروني، وتوصَّل إلى نتيجة مفادها صعوبة مواءمة هذه المقاربات في ظل غياب قواعد اتفاقية واضحة تحكم هذا النوع من الهجمات.

3) الدراسة الثالثة: عمر محمود أعمر: "**الحرب الإلكترونية في القانون الدولي الإنساني**"، **لعام 2019**، وقد هدف الباحث إلى تحديد مدى إمكانية تطبيق مبادئ القانون الدولي الإنساني على الحروب السيبرانية وتكييفها من جهة كونها نزاعا مسلحا أم لا، وخلص إلى أن القانون الدولي الإنساني يمكن تطبيقه على الهجمات السيبرانية عندما تُرتكَب في إطار نزاع مسلح.

4) الدراسة الرابعة: موسى بن تغري: "**الحرب السيبرانية والقانون الدولي الإنساني**"، **لعام 2020**، وقد هدف الباحث إلى إيجاد قواعد القانون الدولي الإنسان واجبة التطوير من أجل مواءمتها للنزاعات المسلحة السيبرانية وانطباقها عليها، وخلص إلى نتيجة مفادها أن الحرب السيبرانية حرب حقيقية ويمكن تطبيق قواعد القانون الدولي الإنساني عليها بعد تطويرها.

وتهدف هذه الدراسة موضوع البحث إلى تحديد المشكلات الثلاث الرئيسة التي تتطلب الحروب السيبرانية الإجابة عنها، وهي: متى نقول عن الهجمات السيبرانية أنها نزاعات مسلحة حقيقية لتطبيق القانون الدولي الإنساني عليها؟، وهل تُعدُّ هذه القواعد في حال انطباقها ملزمة للأطراف على الرغم من غياب أي نص إلزامي حولها؟، وكيف يمكن أن نطبق هذه القواعد في حال انطباقها على هذا الشكل الجديد غير المألوف بالنسبة للنزاعات المسلحة التقليدية؟!

منهجية البحث:

تم اعتماد المنهج الوصفي التحليلي من خلال وصف الهجمات السيبرانية وحالاتها والمواقف الفقهية منها، وتحليل النصوص القانونية فيما يتعلق بمدى انطباقها عليها.

خطة البحث:

1. المطلب الأول: الهجمات السيبرانية ومدى انطباق القانون الدولي الإنساني عليها.

1) الفرع الأول: مفهوم الهجمات السيبرانية.

2) الفرع الثاني: أنواع الهجمات السيبرانية ومدى انطباق أحكام القانون الدولي الإنساني عليها.

2. المطلب الثاني: مدى إلزامية القانون الدولي الإنساني في الحروب السيبرانية وتطبيقه عليها.

1) الفرع الأول: مدى إلزامية القانون الدولي الإنساني لأطراف النزاع المسلح السيبراني.

2) الفرع الثاني: مدى مواءمة القانون الدولي الإنساني في تطبيقه على الحروب السيبرانية.

الجانب النظري للبحث:

المطلب الأول: الهجمات السيبرانية ومدى انطباق القانون الدولي الإنساني عليها:

لقد عرف القانون الدولي الإنساني المعاصر من خلال اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977 فئتين تقليديتين من النزاعات المسلحة؛ وهما النزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية[1].

وتكون النزاعات المسلحة دولية وفق ما ذهبت إليه المادة 2 المشتركة من اتفاقيات جنيف الأربع والبروتوكول الإضافي الأول إذا ما دارت رحاها بين طرفين دوليين (أي بين الدول) أو في إطار حروب التحرير الوطنية التي تناضل فيها الشعوب:

1. ضد التسلط الاستعماري؛
2. وضد الاحتلال الأجنبي؛
3. وضد الأنظمة العنصرية، وذلك في ممارستها لحق تقرير مصيرها[2].

أما النزاعات المسلحة غير الدولية؛ فهي تلك التي تنشأ بين القوات الحكومية من جهة والقوات المتمردة من جهة أخرى وذلك عند مستوى معين من التنظيم والشدة لهذه القوات[3]، أو تلك التي تنشأ بين القوات غير الحكومية بعضها دون بعض دون تدخُّل من جهة الحكومة[4].

وبما أن هذا التصنيف القانوني الدولي للنزاعات المسلحة يعتمد في تقسيمه على الأشكال التقليدية التي تدور بها الحرب وهي استعمال الجيوش النظامية العسكرية البرية منها والبحرية والجوية؛ فإن هذا التصنيف يثير إشكالية تتعلق بمدى انطباق قواعد النزاعات المسلحة على شكل جديد من أشكال هذه النزاعات ظهرت نتيجة التطور العلمي والتقني لأنظمة المعلومات وظهور تكنولوجيا جديدة تعتمد على التحكم بالأسلحة عن بعد مثل تكنولوجيا النانو والأسلحة ذاتية التشغيل المتزايدة، ومنها أيضا "**الحروب السيبرانية – Cyberwarfare**" التي قد تحدث من خلالها تلك النزاعات دون أن تتلاقى الجيوش وفق المفهوم التقليدي للحرب أو النزاعات المسلحة.

الفرع الأول: مفهوم الهجمات السيبرانية:

كلمة "**سيبرانية**" في اللغة مُشتقَّة من الكلمة اليونانية (**Kybernetes**) التي تعني القيادة والتحكم عن بعد[5].

وتُعرَّف **الهجمات السيبرانية** بأنها: "هجمات تتم بوساطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة وتهدف إلى تعطيل أو تدمير أنظمة الإنترنت أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم، ويُستَخدم هذا المصطلح

---

[1] – تعرّف اللجنة الدولية للصليب الأحمر القانونَ الدولي الإنساني على أنه: "مجموعة القواعد الدولية المستمدة من الاتفاقيات والأعراف التي تهدف بصورة خاصة إلى تسوية المشكلات الإنسانية الناجمة بصورة مباشرة عن النزاعات المسلحة الدولية أو غير الدولية التي تقيِّد لأسباب إنسانية حق أطراف النزاع في استخدام أساليب الحرب وطرقها التي تروق لها أو تحمي الأشخاص والأملاك المعرَّضين أو الذين يمكن أن يتعرضوا لأخطار النزاع".

عبد العزيز، مصلح حسن أحمد. (2013). مبادئ القانون الدولي الإنساني. (ط1). عمَّان: دار الحامد للنشر والتوزيع. ص 22. الهامش رقم 1.

[2] – المادة 2 المشتركة من اتفاقيات جنيف الأربع لعام 1949، والمادة 4 من البروتوكول الإضافي الملحق بها لعام 1977.

[3] – المادة 1\1 من البروتوكول الإضافي الثاني لعام 1977 الملحق باتفاقيات جنيف الأربع لعام 1949.

[4] - Vite´, Sylvain. (2009). Typology of armed conflicts in international humanitarian law: legal concepts and actual situations. *International Review of the Red Cross.* 91 (873). p 76.

[5] – الفتلاوي، أحمد عبيس نعمة. (2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. *مجلة المحقق الحلي للعلوم القانونية والسياسية*. 8 (4). العراق: جامعة بابل. ص 614.

للإشارة إلى وسائل القتال وأساليبه التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تجري في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني"[1].

ويعرِّفها "هربرت لين" 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 (الهجوم السيبراني)، أو بالحصول على معلومات يُفضِّل الخصم أن تبقى سرية (التجسس السيبراني أو الاستغلال السيبراني)، ويُتاح 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 أغراضا مالية وعسكرية وسياسية وشخصية[2].

ويعرِّفها "مايكل شميت" بأنها: "الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والإضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة"[3].

وقد حاول دليل تالين للقانون الدولي المطبق على الحروب الإلكترونية والمنشور من قبل اللجنة الدولية للخبراء تقديم تعريف للحرب السيبرانية على أنه: "عمليةٌ إلكترونيةٌ سواءً هجوميةً أو دفاعيةً، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان "الأهداف""[4].

ويُلاحظ من التعريفات المقدمة وبغض النظر عن الزاوية التي عرَّفت منها الحرب السيبرانية –عدا تعريف دليل تالين الذي عرفها بوصفها حربا– أنها تتصف بالعمومية والشمول في التعريف لتتناول جميع أنماط الهجمات الإلكترونية بما فيها الهجمات التي تشكِّل مجرد اعتداءات عادية أو هجمات قد ترقى إلى مستوى النزاعات المسلحة –وهو ما سيتضح في الفرع القادم–، وهنا يتضح الفرق بين مصطلح "**الهجمات الإلكترونية**" ذات المعنى الواسع لمثل هذه الهجمات، ومصطلح "**الحروب الإلكترونية**" **أو** "**الحروب السيبرانية**" التي يمكن أن ينطبق عليها وحدها القانون الدولي الإنساني.

ويُعرَّف "**الفضاء السيبراني**" حسب وزارة الدفاع الأمريكية بأنه: "مجال يتسم باستخدام الإلكترونيات (أي تكنولوجيا المعلومات) والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها"[5].

ولا يقتصر أثر الحروب الإلكترونية أو السيبرانية على البيانات في أجهزة الكومبيوتر أو أنظمتها؛ بل تتعداه إلى خلق تأثير مادي في العالم الحقيقي، كاختراق أنظمة الكومبيوتر للسيطرة على الحركة الجوية وخطوط أنابيب النفط ومحطات

---

[1]– أعمر، عمر محمود. (2019). الحرب الإلكترونية في القانون الدولي الإنساني. *دراسات، علوم الشريعة والقانون*. 46 (3). الأردن: جامعة البلقاء التطبيقية. ص 134 من المقدمة.

[2]– لين، هربرت. (2012). النزاع السيبراني والقانون الدولي الإنساني. *مختارات من المجلة الدولية للصليب الأحمر*. 94 (886). جنيف: اللجنة الدولية للصليب الأحمر. ص 551.

[3]- 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.

[4]– دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية. (2013). إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو). (ترجمة علي محمد كاظم موسوي). إنجلترا: جامعة كامبردج. الجزء الثاني: قانون النزاعات المسلحة السيبرانية. القسم الثالث: الهجمات بصورة عامة. المادة 30– تعريف الهجمات السيبرانية.

[5]– لين، هربرت. مرجع سابق. ص 516.

الطاقة النووية ومراقبة الحركة الجوية والبرية والبحرية والسدود، والتصادم بين الطائرات وإطلاق مواد سامة من المصانع الكيماوية، وانقطاع تشغيل البنية التحتية مثل شبكات إمدادات المياه والكهرباء بما ينعكس على المدنيين سلبا ويكونون هم الضحايا لمثل هذه العمليات، بل إن كثيرا من الدول بوصفها سلطات حكومات كانت عرضة لمثل هذه الاعتداءات وبدرجات متفاوتة من جهة الشدة والضرر، وذلك كما تعرضت أستونيا في عام 2007 لهجمات كبيرة استمرت لأيام عدة، وفي عام 2008 لجأت روسيا إلى الحرب الإلكترونية لتعطيل أنظمة اتصال القوات الجورجية، والغارات الإسرائيلية في عام 2007 على مشروع المفاعل النووي لدير الزور عندما لجأت إلى الحرب الإلكترونية لتعطيل أجهزة الدفاع السورية وشوشت عليها[1].

ويمكننا أن نعطي تعريفا مبسَّطا لـ"**الحرب الإلكترونية/ أو السيبرانية**" تبعا لذلك على أنها: "**الهجمات التي تحدث بين الأطراف الدولية أو غير الدولية المتنازعة ضمن نطاق الفضاء الإلكتروني مما يؤدي إلى نتائج مادية على أرض الواقع مماثلة لتلك التي تنتج عن النزاعات المسلحة التقليدية يمكن أن ينطبق عليها القانون الدولي الإنساني تبعا لذلك**".

الفرع الثاني: أنواع الهجمات السيبرانية ومدى انطباق أحكام القانون الدولي الإنساني عليها:

تتعدد أنماط الحروب السيبرانية تبعا لطبيعة الصراع والضرورة التي تفرض استخدام أي نمط من هذه الأنماط وقدرة العدو على التصدي لها، وتتعدد الحالات التي يثور التساؤل حول مدى انطباق القانون الدولي الإنساني عليها تبعا لذلك أيضا؛ وهي:

1. الحرب السيبرانية الباردة: ويكون الفضاء الإلكتروني فيها ساحة للصراع منخفض الشدة، وهو يعبِّر عن صراع مستمر بين الفاعلين المتنازعين، وهو نزاع متداخل له نواح متعددة ثقافية أو اقتصادية أو اجتماعية وتُسمَّى هذه الحالة أيضا بـ"**القوة الناعمة في الحروب السيبرانية**" وهي لا تتطور بالضرورة إلى استخدام القوة المسلحة بالمعنى التقليدي أو شن حرب إلكترونية واسعة النطاق، هدفها شن الحروب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وحرب الأفكار، كالصراع الإلكتروني العربي الإسرائيلي والصراع الهندي الباكستاني، والتوتر بين روسيا وأستونيا في عام 2007، وبين الولايات المتحدة وروسيا والصين، وبين طهران وواشنطن، وهي حروب إلكترونية ذات بعد اجتماعي ديني ممتد تنشط فيها الجماعات الفاعلة للتعبير عن مواقف سياسية وحقوقية.

2. الحرب السيبرانية متوسطة الشدة: وهي التي يتحول فيها الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية (نزاع مسلح) على الأرض وذلك تعبيرا عن حدة الصراع القائم بين الأطراف، وتدور الحرب السيبرانية هنا من خلال اختراق المواقع الإلكترونية وتخريبها وشن حروب معلوماتية وتجسسية مستمدة ذلك من قوة أطرافها وارتباطها بالنزاع المسلح على أرض الواقع، خاصة أنها أقل كلفة بكثير من النزاعات المسلحة التقليدية بما يمكن من تمويل حرب سيبرانية كاملة بكلفة دبابة، ومن أمثلتها هجمات حلف الناتو في عام 1999 على يوغسلافيا لتعطيل شبكات اتصال الخصوم، وبرزت أيضا في خلال الحرب بين لبنان وإسرائيل في عام 2006، والمواجهات بين حركة حماس وإسرائيل في عامي 2008 و2012.

3. الحرب السيبرانية الساخنة: وهي تعبِّر عن نشوء حرب في الفضاء الإلكتروني منفردة وغير متوازية مع الأعمال العسكرية التقليدية، ومع أن العالم لم يشهد هذا النوع من الحروب بعد إلا أن احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية واتساع الاعتماد بين الدول والفواعل من غير الدول في الفضاء الإلكتروني، وينطوي هذا

[1]– **أعمر، عمر محمود. مرجع سابق. ص 134 – 135.**

النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية؛ إذ تُستخدَم الأسلحة الإلكترونية ضد منشآت العدو وكذلك الروبوتات الآلية والطائرات بدون طيار واستهداف الحياة المدنية والبنية التحتية المعلوماتية، ومن أمثلتها هجمات فيروس ستكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة الأمريكية في عام 2010[1].

وتكمن المشكلة التي تثور بعد عرض أنواع الهجمات السيبرانية هذه في مدى انطباق أحكام القانون الدولي الإنساني عليها، خصيصا أن منها كما في النوع الأول مثلا لا يتعدى نطاق الأعمال غير المشروعة أو الجرائم العالمية في أبعد تقدير.

ترى اللجنة الدولية للصليب الأحمر أن العمليات السيبرانية التي تُنفَّذ في أثناء النزاعات المسلحة –شأنها شأن أي أسلحة أو أساليب حرب أخرى يلجأ إليها المتحاربون في النزاع، جديدة كانت أم قديمة– تخضع في تنظيمها للقانون الدولي الإنساني"[2]، وقد اعتمدت محكمة العدل الدولية هذا الرأي أيضا[3].

لكن المشكلة تثور أكثر عندما تُرتكَب هذه الهجمات في خارج إطار النزاع المسلح أي عندما يبدأ هجوم سيبراني –كما في حالة الحرب السيبرانية الباردة أو الساخنة– دون التزامن مع وجود نزاع مسلح تقليدي على أرض الواقع فيما إذا كان بالإمكان انطباق أحكام القانون الدولي الإنساني عليها أم لا.

إن ميثاق الأمم المتحدة قد حظر على الدول في المادة 4\2 منه اللجوء إلى الحرب أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة.

وقد ترك الميثاق تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها في كل حالة على حدة تبعا للظروف المحيطة ليقرر فيما إذا كانت العملية المستخدمة (وهي هنا الهجمة الإلكترونية) تشكل تهديدا للسلم والأمن الدوليين أو خرقا لهما أو عملا من أعمال العدوان، وإن نص المادة 51 من الميثاق لا يشير إلى استخدام نوع محدد من الأسلحة لعدها تهديدا للسلم والأمن الدوليين أو خرقا لهما أو عمل عدوان، مما يعني أن نوع السلاح المستخدم في الهجمات ليس له تأثير في نفي استخدام القوة، **وأن ما يُعتدُّ به هو الآثار المادية للسلاح على أرض الواقع**، لذلك أجمع الفقه الدولي على أن الحرب الإلكترونية تُعدُّ حربا بالمعنى الحقيقي للكلمة عندما تكون آثارها على العالم المادي مدمرة (كتدمير مشفى مثلا من جراء هجوم إلكتروني يستخدم الأسلحة عن بعد أو نشر وباء بيولوجي أو إطلاق سلاح نووي... إلخ)[4].

---

[1] – **بن تغري، موسى. (2020). الحرب السيبرانية والقانون الدولي الإنساني. *مجلة الاجتهاد القضائي*. 12 (عدد خاص). الجزائر: جامعة محمد خيضر بسكرة. ص 204.**

[2] – **اللجنة الدولية للصليب الأحمر. الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية. بيان ألقته السيدة "فيرونيك كريستوري" منشور على موقع اللجنة الدولية بتاريخ 10 أيلول (سبتمبر) 2019. تم استرجاعه في: 2021/09/21 على الرابط:** https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection

[3] – **اللجنة الدولية للصليب الأحمر. الحرب السيبرانية والقانون الدولي الإنساني. مجموعة أسئلة تتعلق بالحرب السيبرانية على موقع اللجنة الدولية للصليب الأحمر منشورة في 25 شباط (فبراير) 2021. تم استرجاعه في 2021/09/21 على الرابط:**
https://www.icrc.org/ar/document/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A

[4] – **أعمر، عمر محمود. مرجع سابق. ص 138.**

نخلص من هذا إلى أن الهجمات السيبرانية إن كان لها النتائج المادية نفسها للنزاعات المسلحة التقليدية فإنها تُعدُّ نزاعات مسلحة بمفهوم القانون الدولي الإنساني وتخضع لأحكامه حتى لو لم تتزامن مع نزاع مسلح تقليدي دولي كان أو غير دولي.

المطلب الثاني: مدى إلزامية القانون الدولي الإنساني في الحروب السيبرانية وتطبيقه عليها:

المشكلة الأخرى التي تتبع معرفة الحالات التي يمكن أن تُطبَّق فيها أحكام القانون الدولي الإنساني على الحروب السيبرانية تكمن في معرفة مدى إلزامية هذه الأحكام في مثل هذه الحروب خصوصا أن أحكام القانون الدولي الإنساني في اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين لعام 1977 وميثاق منظمة الأمم المتحدة لم تتطرق لمثل هذا النوع من الحروب؛ مما يعني ضرورة الوصول إلى حل لتقرير الإلزامية من عدمها في هذه الحروب الخطيرة التي تتطور يوما بعد يوم وقد تصبح الصورة الرئيسة للحروب المستقبلية.

الفرع الأول: مدى إلزامية القانون الدولي الإنساني لأطراف النزاع المسلح السيبراني:

انقسم الفقهاء إلى تيارين بين مؤيد ومعارض لخضوع الحروب السيبرانية لأحكام القانون الدولي الإنساني:

أ. أما أنصار **الاتجاه المعارض** الذي يُعرَف **بـ«المذهب الحر»** ويتزعمه بعض السياسيين الأمريكيين وسايره جانب من الفقه القانوني الأوروبي والأمريكي معا؛ فيذهبون إلى أن الإنترنت لا يخضع لقانون، وحجتهم أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي، وأن هذا العالم لا يتحدد بدولة معينة ولا يمكن إخضاعه للقانون الدولي العام التقليدي الذي لم ينجح إلى الآن حتى في حكم الفضاء البحري أو الجوي الخارجيين[1].

أما حجج أنصار هذا الاتجاه فتتلخص في النقاط الآتية:

1. عدم وجود نص قانوني دولي إنساني يتحدث عن الهجمات السيبرانية أو يعالج وضعها كون استخدام تكنولوجيا الإنترنت حديث نسبيا، وأن القانون الدولي الإنساني لا يتلاءم مع هذا النوع من الحروب كون المعاهدات النافذة حاليا يرجع تاريخها إلى ما قبل ظهور الهجمات السيبرانية بل وحتى قبل الإنترنت نفسه.

2. عدم ورود عبارة "**الحرب الإلكترونية**" في ميثاق الأمم المتحدة واتفاقيات جنيف ولاهاي ومعاهدات حلف شمال الأطلسي، فنص المادة 51 من ميثاق الأمم المتحدة على 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..."، والنص يربط –من وجهة نظرهم– الهجوم بالنزاع المسلح وهو ما لا يتوفر للحرب السيبرانية.

3. إن الحروب التقليدية يسبقها إعلان واضح لحالة الحرب ويتوفر فيها جيوش منظمة وميادين قتال حقيقية، أما الهجمات السيبرانية التي تفتقر إلى تلك المقومات المادية إضافة إلى قدرة التحكم فيها عن بعد يجعلها أقرب إلى وصف الإرهاب منها إلى وصف الحرب.

4. صعوبة تطبيق مبادئ القانون الدولي الإنساني على الفضاء الإلكتروني؛ وذلك لأن أساليب الحرب الإلكترونية غير مفهومة وواضحة قياسا على النزاعات المسلحة التقليدية؛ فهي تتسم بأنها تتم بسرية تامة، استباقية دون سابق إنذار، غير محددة المجال والمدى، متعددة الأوجه ومتشابكة مع غيرها من أنواع الحروب كالحرب الإعلامية والسياسية والسيكولوجية والإرهاب ...إلخ، والمقاتلون فيها ليس لهم مكان ثابت، إضافة إلى صعوبة تحديد مصدر الهجمات بسبب إمكان تشفير البيانات وإخفاء الهوية وهناك مشكلة أكثر تعقيدا تتعلق بترابط أنظمة الكمبيوتر المدنية والعسكرية[2].

---

[1]– أعمر، عمر محمود. مرجع سابق. ص 136.

[2]– أعمر، عمر محمود. مرجع سابق. ص 136 – 137.

ب. على الجهة الفقهية المعاكسة يرى أنصار **الاتجاه المؤيِّد** الذي يُعرَف **بـ«المذهب القانوني»** أنه يمكن تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية وأن هذه ليست المرة الأولى التي يحدث فيها تطور وتغير في التكنولوجيا المستخدمة، وقد تعامل معها القانون الدولي الإنساني من قبل، بمعنى أن القانون النافذ قادر على التعامل مع التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء الإلكتروني[1].

وتتلخص حجج أنصار هذا الاتجاه في الأسباب الآتية:

1. أما عن اشتراط ميثاق منظمة الأمم المتحدة استخدام القوة لعد الهجوم السيبراني نزاعا مسلحا؛ فإن المادة 4\2 من الميثاق قد حظرت على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، وقد ترك الميثاق تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقرر وجود اللجوء إلى القوة وفق الظروف المحيطة في كل حالة على حدة، بل وقد يلجأ المجلس إلى اتخاذ إجراءات قسرية وقهرية بعيدا عن نص المادة 4\2 في حال رأى موقفا معينا يهدد السلم والأمن الدوليين وهذا يعني أن العبرة للنتيجة لا للوسيلة في تطبيق أحكام الميثاق والقانون الدولي الإنساني، ولقد أجمع الفقه الدولي على أن الحرب الإلكترونية تُعدُّ حربا بالمعنى الصحيح عندما تكون آثارها على العالم المادي آثارا مدمرة.

2. إن البروتوكول الإضافي الأول لعام 1977 الملحق باتفاقيات جنيف الأربع لعام 1949 ينص في المادة 36 منه تحت بند الأسلحة الجديدة على: "بأنه عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى هذا اللحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"، وهذا النص يدلل على قابلية انطباق قواعد القانون الدولي الإنساني على كل حرب أو تقنية مستجدة مستعملة فيها ومنها الحروب السيبرانية.

3. إن كثيرا من التقنيات والاختراعات التكنولوجية لم تثر هذه الإشكالية مع أن القوانين التي كانت نافذة لم تنص عليها كالهاتف واللاسلكي والطائرة؛ فلم ينادِ أحد عند ظهور الثورة الصناعية الأولى بوجوب التخلي عن القوانين النافذة أو عدم انطباقها على هذه التقنيات المستحدثة[2].

4. ذهبت محكمة العدل الدولية في رأيها الاستشاري بشأن التهديد باستخدام الأسلحة النووية إلى أن: "المبادئ والقواعد الإنسانية قد وُضِعَت قبل اختراع الأسلحة النووية، ولكن هذا لا يمنع من تطبيق القانون الدولي الإنساني عليها، ولا يمكن التمسك بعدم انطباق القانون الإنساني على هذه الأسلحة بحجة أنها لم تكن معروفة عند وضع قواعده، وهذا ما لا يمنع من تطبيقه على الأسلحة النووية"[3]، وذكر القاضي "هرشغ" أيضا أن: "السلاح النووي هو من عدة نواح إنكار للاعتبارات الإنسانية التي تكمن وراء القانون المنطبق في النزاع المسلح... فالسلاح النووي لا يمكنه التمييز بين الأهداف المدنية والعسكرية"، والأمر نفسه ينطبق بالقياس على الحرب السيبرانية[4].

---

[1]– أعمر، عمر محمود. مرجع سابق. ص 138.

[2]– أعمر، عمر محمود. مرجع سابق. ص 138 – 139.

[3]– أعمر، عمر محمود. مرجع سابق. ص 137.

[4] – اللجنة الدولية للصليب الأحمر. القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها. مقال منشور على موقع اللجنة بتاريخ 16 آذار (مارس) 2016. تم استرجاعه في 2021/09/21 على الرابط: https://www.icrc.org/ar/publication/lhl-advisory-opinion-icj-legality-threat-or-use-nuclear-weapons

5. أكثر من ذلك؛ فإن "**شرط مارتنز**" الذي اعتُمِدَ لأول مرة في مؤتمر لاهاي الأول للسلام في عام 1899 وأُعيدَت صياغته منذ ذلك الحين وأُدمِجَ في العديد من الصكوك الدولية نص على أنه: "في الحالات غير المشمولة بالقانون التعاهدي، يظل السكان والمتحاربون تحت حماية وسلطان مبادئ القانون الدولي، كما هي التقاليد التي استقرت عليها الحال بين الشعوب المتمدنة والقوانين الإنسانية ومقتضيات الضمير العام"[1]، ويُفسَّر هذا الشرط عموما هكذا: "أي شيء لا يحظره القانون الدولي الإنساني صراحة لا يُعدُّ جائزا تلقائيا، ويجب على المحاربين أن يتذكروا دائما أن أعمالهم لا بدَّ وأن تكون متوافقة مع المبادئ الإنسانية ومع ما يمليه الضمير العام"[2].

6. إن القانون الدولي الإنساني المعاصر لم يشترط في اتفاقيات جنيف الأربع لعام 1949 الإعلان المسبق للحرب لانطباق قواعده عليها؛ بل أخذ بالمنهج الموضوعي في تطبيق أحكامه على كل نزاع مسلح ولو لم يكن معلنا على خلاف ما كان سائدا في القانون الدولي الإنساني التقليدي الذي لا يعترف إلا بالحرب القانونية المعلنة[3].

مما تقدم يتضح تفنيد حجج أنصار الاتجاه الأول من خلال حجج أنصار الاتجاه الآخر المؤيد لتطبيق أحكام القانون الدولي الإنساني على الحروب السيبرانية، وهي من الوضوح بما يكفي سواء لجهة شمولية النصوص والمواثيق الدولية لكل مستجد من أشكال وصور ووسائل النزاعات المسلحة، أو لجهة أحكام القضاء الدولي والتقنيات المستحدثة التي لم تثر هذه الإشكاليات من قبل، أو لجهة المصلحة المتوخاة من تطبيق أحكام القانون الدولي الإنساني وهي حماية ضحايا النزاعات المسلحة وحماية الأعيان المدنية وتخفيف أثر حدتها ونتائج كوارثها ما أمكن، وهو ما لا يمكن إلا بتطبيق أحكام القانون الدولي الإنساني على الحروب السيبرانية في الحالات التي يمكن انطباقه فيها.

لكن مع ذلك تبقى صعوبة وحيدة أثارها أنصار الاتجاه الأول الحر المعارض، وهو يكمن في كيفية تطبيق مبادئ القانون الدولي الإنساني على مثل الحروب السيبرانية أو في مدى ملاءمتها لها، وهذه هي المشكلة الثالثة.

الفرع الثاني: مدى مواءمة القانون الدولي الإنساني في تطبيقه على الحروب السيبرانية:

لا بدَّ لانطباق أحكام القانون الدولي الإنساني على الحروب السيبرانية وخصوصا الاتفاقيات المهمة فيه مثل اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977 واتفاقيات لاهاي 1899 – 1907 الخاصة باحترام قوانين الحرب البرية وأعرافها ونظام روما الأساسي للمحكمة الجنائية الدولية؛ لا بدَّ من موائمة الحرب السيبرانية مع هذه القواعد، وكذلك مع مبادئ القانون الدولي الإنساني التي تواجه صعوبات في تطبيقها على هذا النوع من النزاعات الفضائية وأهمها: مبدأ الإنسانية ومبدأ التمييز ومبدأ الضرورة العسكرية ومبدأ التناسب وغيرها من المبادئ الأخرى المتفرعة عنها[4].

وإذا كان من المسلَّم به والمتَّفق عليه أن "**شرط مارتنز**" يُطبَّق على الحروب أيا كان شكلها وأسلوبها ووسيلتها كما في الحرب السيبرانية، فإن بعض المبادئ والقواعد تستلزم بعض التطوير والإضافات وفقا للتطبيق العملي لها في مثل هذا النوع من الحروب[5].

---

[1]– ميلتسر، نيلس. (2016). القانون الدولي الإنساني مقدمة شاملة. جنيف: منشورات اللجنة الدولية للصليب الأحمر. ص 24.

[2]– اللجنة الدولية للصليب الأحمر. (2014). القانون الدولي الإنساني إجابات على أسئلتك. جنيف: منشورات اللجنة الدولية للصليب الأحمر. ص 7.

[3]– عتلم، حازم محمد. (2002). قانون النزاعات المسلحة الدولية – المدخل / النطاق الزماني. (ط2). القاهرة: دار النهضة العربية. ص 199.

[4]– بن تغري، موسى. مرجع سابق. ص 207.

[5]– سعود، يحيى ياسين. (2018). الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني. *المجلة القانونية*. (4). مصر: جامعة القاهرة. ص 93.

فبالنسبة لمبدأ الإنسانية؛ فإنه يهدف إلى حماية كرامة بني البشر سواء وقت السلم أو الحرب، ومعاملة الضحايا بإنسانية في وقت الحرب من خلال احترام شرفهم ودمائهم وأموالهم وصيانة الذات البشرية وكرامتها حتى في أشد الظروف قسوة وأكثرها ضراوة، وينبع هذا المبدأ من الإنسانية التي يتصف بها الإنسان، وتبعا لذلك؛ فإن وقوع الحرب لا يلغي الإنسانية المتأصلة لدى البشر كلهم، فالحرب حالة واقعية من صنع البشر، فإذا لم نستطع منعها، فبالإمكان الحد من آثارها[1].

وأما مبدأ التمييز الذي أشار إليه دليل تالين –على الرغم من عدم إلزامية قواعده– بأنه لا يجوز أن تكون الأعيان المدنية هدفا للهجمات السيبرانية، وهو يعني التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، إذ يؤمن الاحترام والحماية اللازمة للمدنيين والأعيان ذات الطابع المدني، وبالمحصلة؛ حصر توجيه الضربات العسكرية بالأهداف العسكرية، وتحريم الهجمات العشوائية[2]، فلا يجوز مثلا توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنى التحتية ما لم تُعدُّ من قبيل الأهداف العسكرية التي يجوز استهدافها وفقا للظروف السائدة[3].

ويبدو أن هذين المبدأين لا يثيران إشكالية بالنسبة للهجمات السيبرانية كونهما يظلان مبدأين نظريين من حيث الأصل يظهر تطبيقهما الفعلي ضمن المبادئ الأخرى.

أما مبدأ التناسب أي التناسب بين الفعل ورد الفعل، وهو المبدأ الذي يوازن بين المبدأين الرئيسين؛ «**الإنسانية**» و«**الضرورة العسكرية**»، فعندما لا يمكن تفادي إحداث الضرر العرضي بين المدنيين أو الأعيان المدنية، فإن الأمر يخضع لهذا المبدأ، ومن ثم يتعين على من يخططون لهجوم أو يقررون شنَّه أن يمتنعوا عنه أو يعلِّقوا القيام به، ولا يمكن أن يكون «**مبدأ التناسب**» قابلا للتطبيق إلا إذا أمكن تطبيقه وقت اتخاذ القرارات العسكرية؛ إذ سيكون غير فعال ومجد إذا تأخر إدراكه[4].

وأما مبدأ الضرورة العسكرية؛ يجمع فقهاء القانون الدولي على تعريف الضرورة الحربية على أنها:

"الحالة التي تكون ملحَّة لدرجة أنها لا تترك وقتا كافيا للأطراف المتحاربة لاختيار الوسائل المستخدمة في أعمالها أو هي الأحوال التي تظهر في أثناء الحرب وتفرض حال قيامها ارتكاب أفعال معينة على وجه السرعة بسبب موقف أو ظروف استثنائية في اللحظة ذاتها"[5].

وعلى الرغم من أن دليل تالين قد نص على وجوب الالتزام بهما في نطاق الحرب السيبرانية؛ إلا أنهما يواجهان صعوبات عملية؛ ذلك أن الأضرار العرضية أمر لا مفرَّ منه بسبب عدم وجود فاصل في كثير من الأحيان في الفضاء السيبراني المُستخدَم من قِبَلِ المدنيين وذلك المُستخدَم من قِبَلِ القوات المسلحة[6].

---

[1]– مركز الميزان في فلسطين. (2008). دليلك في: القانون الدولي الإنساني سؤال وجواب؛ السلسلة رقم 12. غزة: إصدارات مركز الميزان لحقوق الإنسان. ص 4.

[2]– إعلان سان بطرسبرغ المتعلق بتنظيم وحكم اختيار الأسلحة وحظر أسلحة معينة وتقييد استعمالها لعام 1868. الديباجة.

[3]– شميت، مايكل. (2002). الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب. المجلة الدولية للصليب الأحمر؛ *مختارات من أعداد 2002*. ص 105.

[4]- L. Brown, Bernard. (1976). The Proportionality Principle in the Humanitarian Law of Warfare: Recent Efforts at Codification. *Cornell International Law Journal. Vol. 10, N°. 1,* Art 5, P 140.

[5]– مركز الميزان في فلسطين. (2008). المبادئ الأساسية للقانون الدولي الإنساني؛ السلسلة رقم 02 غزة: إصدارات مركز الميزان لحقوق الإنسان. ص 6.

[6]– الفتلاوي، أحمد عبيس نعمة. مرجع سابق. ص 638.

ولا تقتصر ضرورة الموائمة بين الحروب السيبرانية وأحكام القانون الدولي الإنساني على المبادئ فقط؛ وإنما هناك كثير من الإشكاليات التي تثيرها الهجمات السيبرانية في إطار النزاعات المسلحة مثل تحمُّل مسؤولية الأفعال غير القانونية التي يمكن أن تتضمن خيارات القائد العسكري والمبرمج والمصنِّع، لا سيما إذا تعلق الأمر بالمسؤولية الجنائية الفردية، وكذلك المركز القانوني لأسير الحرب الذي يصعب تطبيقه في إطار الحروب السيبرانية[1].

لذلك فإنه من الضروري –وعلى الرغم من ضرورة التأكيد على انطباق أحكام القانون الدولي الإنساني على الحروب السيبرانية في الوقت نفسه– صياغة قواعد اتفاقية ملزمة مكملة لاتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977 تتناول بالتنظيم وبالتحديد الحروب السيبرانية لضبط قواعد هذه الحرب ونتائجها دون التي تكاد لا تختلف عن نتائج النزاعات المسلحة التقليدية، بحيث تكون ملزمة للأطراف الفاعلة من جهة وغير مُختلَف على مدى إلزاميتها وحالات انطباقها من جهة أخرى.

الاستنتاجات والتوصيات:

إن الحروب السيبرانية أضحت أمرا واقعا اليوم بوصفها أحد أهم أدوات الحرب الرئيسة بين الدول اليوم، وإن تحديد المشكلات الرئيسة التي تحد من تقييد أحكامها بقواعد منظمة مثل قواعد القانون الدولي الإنساني والبحث عن حلول لها يساهم بتلافي نتائجها السلبية التي لا تختلف عن نتائج النزاعات المسلحة التقليدية سوى لجهة الأدوات المُستخدَمة بها، ونخلص مما سبق إلى الاستنتاجات والتوصيات الآتية:

➢ **الاستنتاجات:**

1. إن الهجمات السيبرانية منها ما يبقى ضمن نطاق الجرائم الداخلية أو الدولية التي لا ترقى إلى مستوى النزاع المسلح ومنها ما يُعدُّ فعلا نزاعا مسلحا.

2. إن المعيار في عدِّ الهجمات السيبرانية نزاعات مسلحة من عدمها يكمن في النتيجة المادية المترتبة عن تلك الهجمات وليس في ارتباط الأفعال بالهجوم المسلح التقليدي وأساليبه.

3. إن القانون الدولي الإنساني ينطبق بالضرورة على الحروب السيبرانية وهو ملزم لأطرافها حتى ولو بغياب نص اتفاقي ملزم ينظم قواعدها صراحة إعمالا للنصوص الاتفاقية الدولية نفسها بما أفسحته من مجال لتطبيقها على ما يستجد من حروب وأدوات وإعمالا للعرف وقياسا على مسائل قضائية أخرى مشابهة كالأسلحة النووية.

4. إن أحكام القانون الدولي الإنساني تواجه صعوبة في تطبيقها في بعض القواعد والمبادئ نظرا لأنها خُصِّصَت أساسا لتُطبَّق على النزاعات المسلحة التقليدية مما يوجد صعوبة في مواءمتها مع الحروب السيبرانية التي تدور في فضاء خاص بها وميدان مختلف عن ميدان العالم الواقعي.

5. إن الهجمات والحروب السيبرانية أصبحت إحدى وسائل الحرب الأساسية حتى بين القوى العظمى في العالم، وهي مؤهَّلة مع تطور وسائل التكنولوجيا وتقنيات التحكم عن بعد لتكون ميدان الحرب الرئيس في النزاعات المستقبلية.

➢ **التوصيات:**

1. إلحاق بروتوكولات باتفاقيات جنيف الأربع لعام 1949 بما يشير صراحة إلى عد الهجمات السيبرانية نزاعات مسلحة عند استيفائها لشروط النزاع المسلح لإزالة كل لبس أو اختلاف فقهي وقضائي حول القواعد التي تحكمها.

[1]– **سعود، يحيى ياسين. مرجع سابق. ص 95.**

2. عد الاتفاقيات المعدِّلة أو البروتوكولات المضافة ملزمة للدول الموقعة عليها بحسبانها نزاعات مسلحة غير أنه تدور في الفضاء الإلكتروني، وذلك تبعا لمعيار النتيجة المادية التي لا تختلف في آثارها عن تلك المماثلة للنزاعات المسلحة التقليدية.

3. إعادة صياغة تلك القواعد بما يتناسب مع هذا الشكل الجديد من النزاعات المسلحة لإمكان تطبيقها عليها دون مواجهة أية عقبات تحد من ذلك.

4. ضرورة العمل والتعاون الدوليين على إيجاد شبكة معلومات مدنية منفصلة تماما عن تلك المستخدمة لأغراض عسكرية وسياسية وأمنية للحد من آثار الهجمات السيبرانية في المستقبل.

References:

➢ **Books:**

1. Atlam, H. *The Law of International Armed Conflicts - Introduction / Time Scope.* 2ded. Cairo: Arab Renaissance House, 2002, 435.
2. Abdulaziz, M. *Principles of International Humanitarian Law.* 1st ed. Al-Hamed House for Publishing and Distribution, Amman, 2013, 336.
3. Melzer, N. *International Humanitarian Law; A Comprehensive Introduction.* ICRC, Geneva, 2016, 326.

➢ **Journals:**

1. L. Brown, B. *The Proportionality Principle in the Humanitarian Law of Warfare: Recent Efforts at Codification.* Cornell International Law Journal. Vol. 10, No. 1, Art 5, 1976, 133 – 155.
2. Michael N. Schmitt, M. *Computer network attack and the use of force in international law: Thoughts on a normative framework.* Columbia journal of transnational law, 1999, Vol. 37, 885 – 937.
3. N. Schmitt, M. *War by Communication: The Attack on Computer Networks and the Law of War.* International Review of the Red Cross; Selections from 2002 issues, 2002, 87 – 114.
4. Vite´, S. *Typology of armed conflicts in international humanitarian law: legal concepts and actual situations. International Review of the Red Cross,* Vol. 91, No 873, 2009, 69 – 94.
5. Lynn, H. *Cyber conflict and international humanitarian law.* Selections from the International Journal of the Red Cross. Vol. 94, No. 886, Geneva: International Committee of the Red Cross, 2012, 515 – 531.
6. Al-Fatlawi, A. *Cyber-attacks: their concept and the international responsibility arising from them in the light of contemporary international organization.* Al-Mohaqiq Al-Hilli magazine for legal and political sciences, Vol. 8, No. 4, Iraq: University of Babylon, 2016, 610 – 687.
7. A'mar, O. *Electronic warfare in international humanitarian law.* Studies, Sharia and Law Sciences. Vol. 46, No. 3, Jordan: Al-Balqa Applied University, 2019, 134 – 155.
8. Ben Taghri, M. *Cyberwarfare and international humanitarian law.* Journal of Judicial Jurisprudence. 12 (special issue). Algeria: University of Mohamed Khider, Biskra, 2020, 199 – 218.

➢ **Periodicals:**

1. *Basic Principles of International Humanitarian Law.* Publications of Al Mezan Center for Human Rights, Gaza, Series N^{o}. 2, 2008. 12.
2. *Your Guide to: International Humanitarian Law Q&A.* Publications of Al Mezan Center for Human Rights, Gaza, Series N^{o}. 12, 2008. 25.
3. The international group of experts at the invitation of The NATO Cooperative Cyber Defense Center of Excellence. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press, Cambridge, 2013. 215.
4. *International Humanitarian Law; Answers to Your Questions.* ICRC, Geneva, 2014. 100.

➢ **Conventions:**

1. *Petersburg Declaration on the Regulation and Provision of the Selection of Weapons and the Prohibition and Restriction of Certain Weapons of.* 1868.
2. *The Four Geneva Conventions.* 1949.
3. *The Two Additional Protocols attached to The Four Geneva Conventions.* 1977.

➢ **Websites:**

1. *The United Nations:* < https://www.un.org/>
2. *International Committee of The Red Cross:* < https://www.icrc.org/>