بجـــــــامعة يـــحي فـــارس بالمدية

كليـــة الحقوق والعلوم السياسية

قسم الحقوق


# الحرب السيبرانية على ضوء مبادئ القانون الدولي الإنساني

**مذكرة مقدمة لنيل شهادة ماستر في الحقوق**

**تخصص: قانون دولي عام**


**من إعداد الطالبتين :**

- زكية هتشان
- شيماء كاك

**تحت إشراف الأستاذة :**

د/ فاطمة بابا


**لجنة المناقشة :**

| الاسم واللقب | المؤسسة الأصلية | الدرجة العلمية | الصفة |
|---|---|---|---|
| أسامة غربي | جامعة المدية | أستاذ التعليم العالي | رئيسا |
| فاطمة بابا | جامعة المدية | أستاذ محاضر "أ" | مشرفا ومقررا |
| الحسين عمروش | جامعة المدية | أستاذ التعليم العالي | مناقشا |

السنة الدراسية: 2025/2024 م

# شكر وعرفان

الحمد لله رب العالمين الذي بنعمته تتم الصالحات، والشكر له سبحانه وتعالى على نعمته وتوفيقه لإنجاز هذه المذكرة، والصلاة والسلام على خاتم الأنبياء والمرسلين محمد وعلى آله وصحبه أجمعين.

أما بعد: لا يسعنا في هذا المقام إلا أن نشكر الأستاذة المشرفة د. بابا فاطمة على تفضلها بالإشراف على هذه المذكرة، وعلى ما قدمته لنا من ملاحظات وإرشادات كان لها بالغ الأثر في إنجاز هذه المذكرة، جزاها الله كل خير وأطال الله في عمرها.

كما لا يفوتنا أن نتقدم بجزيل شكرنا إلى السادة أعضاء لجنة المناقشة على تكرمهم بقراءة ومناقشة هذه المذكرة وإثرائها.

إلى كل من ساعدنا من قريب ومن بعيد ولو بكلمة طيبة شجعتنا على العمل والاجتهاد.

# إهداء

أهدي ثمرة تخرجي هذا إلى من علمني العطاء، وإلى من أحمل اسمه بكل افتخار وأرجو من الله يمد في عمره إلى سندي "أبي"

إلى معنى الحب والحنان وسر الوجود، ومن كان دعاؤها سر نجاحي إلى غاليتي "أمي"؛

إلى إبنتي ميسان التي هي سبب فرحتي ودافعي في الحياة؛

إلى إخوتي وعائلاتهم الصغيرة،

إلى كل من مد لي يد العون في إنجاز هذا العمل المتواضع وإتمامه خاصة حبيبة وحليمة وحورية

وإلى العاملين معي بمؤسسة "شواي بن عيسى"

أهدي هذا العمل بالأخص لنفسي لأنه يعتبر ثمرة مجهوداتي، وتعبي خلال مشواري الدراسي والجامعي.

زكية

# إهداء

إلى العزيزالذي حملت إسمه نفخرا وإلى من كلله الله بالهبة و الوقار

إلى من حصد الأشواك عن دربي و زرع الراحة لي بدلا منها

"أبي"

إلى التي علمتني الأخلاق قبل أن أتعلمها، الى الجسر الصاعد بي إلى الجنة

واليد الخفية التي أزالت عن طريقي العقبات ومن ظلت دعواتها تحمل إسمي ليلا ونهارا

"أمي"؛

إلى من وهبني الله نعمة وجودهم إلى مصدر قوتي و أرضي الصلبة و جدار قلبي المتين و سندي في هذه الحياة

إخوتي وأخواتي وعائلاتهم الصغيرة.

الذين إن ضاقت بي الدنيا وسعت بخطاهم ، وإن سقطت كانوا أول من رفعوني بكلماتهم

إلى من رافقني بالقلب قبل الدرب .

ها أنا اليوم طويت صفحة من تعب دام سنين و ستشاركون معي فرحة نهاية طريقي.

و آخر دعوانا الحمد الله رب العالمين



# مقـــدمـــة

**مقدمـــة :**

شهد المجتمع الدولي على مر العصور أشكالا متعددة من النزاعات المسلحة، تطورت في أدواتها وطبيعتها مع تطور البشرية والتقدم التكنولوجي، وقد فرضت هذه النزاعات تحديات جسيمة على البشرية، مما استدعى ضرورة وجود قواعد قانونية تنظم سلوك أطراف النزاع وتحد من آثار الحرب على المدنيين والممتلكات، ويعد القانون الدولي الإنساني الإطار القانوني الذي ينظم الحروب التقليدية، لكن بروز الحرب السيبرانية كوجه جديد من الحروب ضاعف التهديدات التي تمس الأمن والسلم الدوليين، حيث أصبحت الفضاءات الرقمية ميدانا جديدا للنزاع تستخدم فيه الدول وأحيانا فاعلون من غير الدول وسائل تكنولوجية لتوجيه هجمات قد تكون مدمرة لبنى تحتية حيوية، أو مؤثرة على سير العمليات العسكرسة والسياسية.

هذا التحول النوعي في طبيعة النزاعات طرح تساؤلات جوهرية حول مدى قدرة قواعد ومبادئ القانون الدولي الإنساني على مواكبة هذه الحرب ومدى قابليته للتطبيق على النزاعات السيبرانية، التي غالبا ما تغيب فيها الحدود الجغرافية الواضحة وتتشابك فيها المسؤوليات القانونية بين الأطراف المتعددة.

تكمن أهمية تناول موضوع الحرب السيبرانية على ضوء مبادئ القانون الدولي الإنساني في ضرورة إعادة قراءة القواعد التقليدية للقانون الدولي الإنساني في ضوء التحديات التي تطرحها التكنولوجيا الحديثة، خصوصا على مستوى تحديد مفهوم النزاع المسلح وتمييز الأهداف العسكرية عن المدنية، وتقدير مبدأ التناسب في ظل هجمات قد تكون آنية وخفية وعابرة للحدود. كما يسهم هذا البحث في إثراء النقاش الفقهي حول آليات تطوير مبادئ القانون الدولي الإنساني، أو إيجاد مبادئ جديدة تكفل فعاليته في النزاعات الرّاهنة، وتحدد المسؤوليات وتضمن حماية الأشخاص المتأثرين وفقا لما يقتضيه القانون والإعتبارات الإنسانية.

هناك أسباب ذاتية وأخرى موضوعية دفعتنا لإختيار هذا الموضوع؛ وتتمثل الأسباب الذاتية في رغبتنا الشخصية في دراسة الحرب السيبرانية وتحديد طبيعتها القانونية ومدى انطباق مبادئ القانون الدولي الإنساني عليها، والمسؤولية الدولية الناشئة عنها بإعتبارها نوع جديد من الحروب، ولأنّ لها تأثير كبير في قلب موازين العالم وتهديد الأمن والسلم الدوليين.

أما الأسباب الموضوعية التي دفعتنا لاختيار هذا الموضوع هو أنّ الحرب السيبرانية نوع جديد يكتنفه الغموض في كثير من النواحي، خاصة الجانب القانوني لأنه لحد الساعة لا يوجد إطار قانوني دولي مفصل ينظم إستخدام القوة السيبرانية أثناء النزاعات المسلحة، ما يستدعي البحث في إمكانية تطبيق مبادئ القانون الدولي الإنساني على هذا النوع من الحروب، خاصة في ظل تصاعد التهديدات

السيبرانية، مما يعز الحاجة إلى تحليل مدى حماية القانون الدولي الإنساني للمدنيين والأعيان المدنية. هذا الموضوع أثار الكثير من الجدل بين القانونين، ودفعهم إلى البحث عن حلول قانونية وتقنية لمواجهة هذا الخطر.

وبخصوص أهداف الدراسة، فيمكن تلخيصها في النقاط التالية:

ـ تحديد المفاهيم النظرية لكل من الحرب السيبرانية والقانون الدولي الإنساني.

ـ تحليل مدى إنطباق مبادئ القانون الدولي الإنساني على الحروب السيبرانية: وذلك من خلال دراسة المبادئ الأساسية (التمييز، التناسب الضرورة العسكرية والإنسانية) في سياق الحرب السيبرانية.

- التطرق إلى دليل تالين كأساس قانوني للحرب السيبرانية (مشروع قانون).

ـ تسليط الضوء على الثغرات القانونية المتعلقة بالحرب السيبرانية، وذلك بالكشف عن النقاط التي لا يغطيها القانون الحالي ومحاولة اقتراح الحلول لسد هذه الثغرات.

ـ دراسة مسؤولية الفاعلين السيبرانيين، سواءا كانوا دولا أو جهات غير حكومية وتحديد سبل محاسبتهم لخرقهم القواعد الإنسانية.

ـ تعزيزالمعلومات المتعلقة بالحرب السيبرانية ومبادئ القانون الدولي الإنساني، من أجل توفير مرجع علمي يسهم في النقاشات القانونية حول تنظيم الحرب السيبرانية.

الدراسات السابقة في هذا الموضوع قليلة نوعا ما، نظرا لحداثة الموضوع وقلة المصادر القانونية والإهتمام المتأخر به، ومن أهم الدراسات التي لها علاقة بالموضوع: الدراسة الأولى للطالبتين غجاتي سهيلة و راهم أميرة، الهجمات السيبرانية وأثرها على تهديد الأمن والسلم الدوليين، حيث طرحتا إشكالية مدى تأثير الهجمات السيبرانية على السلم و الأمن الدوليين،وأهم النتائج التي توصلتا إليها هي أن الحرب السيبرانية مازالت من المفاهيم الحديثة،و القانون الدولي يكفل حماية البنية التحتية ،لكنه يعاني من قصور في بعض المواد ،كما أن القانون الدولي الإنساني يطبق على الهجمات السيبرانية مع وجود صعوبة في تطبيق مبادئه

أما الدراسة الثانية فكانت للطالبة أمينة بوطاطة، الحروب السيبرانية في العلاقات الدولية (المفهوم والظاهرة) ، حيث طرحت إشكالية مدى تأثير ظاهرة الحروب السيبرانية على واقع العلاقات الدولية ، ودرست نماذج واقعية من الحروب (حرب الولايات المتحدة الأمريكية ضد كل من الصين وروسيا وكوريا الشمالية، الحرب السيبرانية لروسيا ضد أوكرانيا، استونيا وجورجينا).

أما بخصوص دراستنا فقد ركزنا على جانب مدى إمكانية تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية وهذا ما يميز دراستنا، حاولنا إظهار إشكالات تطبيق مبادئ القانون

الدولي الإنساني على هذه الحرب و إبراز الحلول المقترحة، والتي لا تزال قيد التطور وتناولنا فكرة الحماية من خلال الجهود الدولية المبذولة(قانونية،تقنية)بطريقة مختلفة .

بما أنّ الحرب السيبرانية لها تكييف قانوني خاص بالنظر إلى خصائصها وطبيعتها القانونية، لذلك ثارت عدة تساؤلات حول مدى قابلية تطبيق مبادئ القانون الدولي الإنساني على النزاعات السيبرانية، لا سيما فيما يتعلق بمبادئ التمييز، التناسب، الضرورة العسكرية والإنسانية، ومدى إمكانية مساءلة الأطراف الفاعلة. لذلك الإشكالية التي يمكن طرحها بخصوص موضوع مذكرتنا هي: **إلى أيّ مدى يمكن تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية؟**

تندرج تحت هذه الإشكالية عدة أسئلة فرعية :

- ما هو مفهوم الحرب السيبرانية؟
- ما هو الفرق بين الحرب السيبرانية والهجمة السيبرانية والجريمة السيبرانية ؟
- ما هو مفهوم القانون الدولي الإنساني ؟
- ما هي التحديات القانونية التي تواجه تطبيق مبادئ القانون الدولي الإنساني على هذا النوع من الحروب؟
- ما هي الآليات والجهود الدولية المبذولة لمواجهة الحرب السيبرانية ؟
- ما هو الأساس القانوني لقيام المسؤولية الدولية في الحرب السيبرانية ؟

من أهم الصعوبات التي واجهتنا أثناء إعداد مذكرتنا، نقص المراجع في جانب الحروب السيبرانية نظرا لحداثة الموضوع خاصة في الفصل الثاني الذي ربط القانون الدولي الإنساني بالحروب السيبرانية فاعتمادنا الأكبر كان على المجلات القانونية والمواقع الإلكترونية ودراسات اللجنة الدولية للصليب الأحمر، فالدراسات المتخصصة تكاد تكون منعدمة، لأن بعض الكتب المتخصصة غير متوفرة أو غير متاحة إلكترونيا إضافة إلى ضيق الوقت.

تطلّب إعداد هذه المذكرة اعتماد منهجين هما: المنهج الوصفي، حيث استدعت طبيعة البحث إستعراض مفهوم الحرب السيبرانية وأنواعها، ونفس الأمر بالنسبة للقانون الدولي الإنساني، بالإضافة إلى المنهج التحليلي وذلك بغرض دراسة مضمون الحرب السيبرانية وأبعادها القانونية من خلال تحليل النصوص القانونية ومبادئ القانون الدولي الإنساني، بهدف إظهار مدى انطباق هذه المبادئ على الحرب السيبرانية. كما لا ننسى مسألة المسؤولية الدولية، أين ساعدتنا هذه الدراسة في تفكيك الإشكاليات النظرية والعملية المرتبطة بالموضوع.

للإجابة على الإشكالية المطروحة قسمنا البحث إلى فصلين؛ تناولنا في الفصل الأول الإطار المفاهيمي للحروب السيبرانية والقانون الدولي الإنساني، وقسم هذا الفصل إلى مبحثين، المبحث الأول الإطار النظري للحروب السيبرانية، والمبحث الثاني الإطار النظري للقانون الدولي الإنساني.

أما الفصل الثاني تناولنا فيه علاقة الحروب السيبرانية بمبادئ القانون الدولي الإنساني، وقسمناه بدوره إلى مبحثين، المبحث الأول تناولنا فيه الإطار القانوني للحرب السيبرانية وإشكالية تطبيق مبادئ القانون الدولي الإنساني، والمبحث الثاني تناولنا فيه الجهود الدولية في تنظيم الحرب السيبرانية وتقرير المسؤولية.

# الفصل الأول:

## الإطـار المفاهيمي للحروب السيبراية والقـانون الدولي الإنساني

## الفصل الأول: الإطـار المفاهيمي للحروب السيبراية والقـانون الدولي الإنسانـي

لم تعد الحروب تقتصر على الميادين التقليدية بل إمتدت إلى مجال التكنولوجيا و الإتصالات، ما أدى ظهور شكل جديد من الصراع عرف بالحرب السيبرانية ، والتي برز عنها عدة إشكاليات دفعتنا الى ضرورة فهمها.

يعد الإطار النظري أساسا ضروريا لفهم أي إشكالية بحثية بشكل صحيح، خاصة عندما يتعلق الأمر بموضوع معقد وحديث مثل الحرب السيبرانية وعلاقتها بالقانون الدولي الإنساني، فهذه الحرب تطرح تحديات قانونية وأخلاقية غير مسبوقة .

في هذا الفصل سنتناول الإطار المفاهيمي للحرب السيبرانية في المبحث الأول، وفي المبحث الثاني نتناول الإطار المفاهيمي للقانون الدولي الإنساني.

## المبحث الأول: الإطار المفاهيمي للحروب السيبرانية

شهد العالم خلال العقود الأخيرة تطورا هائلا في تكنولوجيا المعلومات والإتصالات، الأمر الذي أفرز تحولات عميقة في مفاهيم الأمن والصراع بين الدول، حيث لم تعد الحروب التقليدية الوسيلة الوحيدة لتحقيق الأهداف السياسية والعسكرية، بل برز نوع جديد من الحروب يتم عبر الفضاء الرقمي، يعرف بالحرب السيبرانية .

تكمن خطورة هذا النوع من الحروب في أنه يشن عن بعد، ويصعب تحديد الفاعل بدقة، يستهدف البنية التحتية الحيوية للدول ويهدد أمن الأفراد والمجتمعات. وفي هذا الإطارسنوضح المفاهيم العامة المتعلقة بالحرب السيبرانية، وذلك من خلال المطلب الأول الذي سنتناول فيه مفهوم الحرب السيبرانية، والمطلب الثاني سنتناول فيه الطبيعة القانونية للحرب السيبرانية وخصائصها، والمطلب الثالث سنتناول فيه أنماط الحرب السيبرانية والتمييز بينها وبين غيرها من الحروب .

### المطلب الأول: مفهوم الحرب السيبرانية

أعطيت للحرب السيبرانية عدة تعريفات، كونها حديثة النشأة وتتميز بالغموض، لذلك حاول الكثيرون تعريفها بغرض الوصول إلى تعريف موحد و شامل لها .

نتناول ما جاء به الفقهاء القانونيين في شأن تعريف الحرب السيبرانية في الفرع الأول، وفي الفرع الثاني نتناول نشأتها وتطورها .

#### الفرع الأول: تعريف الحرب السيبرانية

نتناول في هذا الفرع المقصود بالحرب السيبرانية (أولا)، ثم نقوم بالتمييز بين الحرب السيبرانية وغيرها من المفاهيم المشابهة (ثانيا) على النحو التالي :

**أولا: المقصود بالحرب السيبرانية**

قبل التطرق للمقصود بالحرب السيبرانية لا بد من توضيح معنى السيبرانية :

**أ- المقصود بمصطلح "السيبرانية":** مصطلح السيبرانية Cybermetic أشتق من المصطلح الإغريقي Kybernetes ويعني الطيار أوقائد الدفة أوالحاكم[1]، أما في العصر الحديث فإن كلمة سيبرانية معناها

[1]. جيلالي شويرب ، فائزة مراد ، **مفهوم الحروب السيبرانية والأمن السيبراني**، مجلة الحقوق والحريات، المجلد 11، العدد الأول، جامعة محمد خيضر،بسكرة، الجزائر، 2023، ص 160.

إحتواء آليات تعقيب تتيح وظائف القيادة والتحكم في الأنظمة المغلقة. ومصطلح السيبرانية مأخوذة من كلمة Cyber وتعني صفة لأي شيئ مرتبط بثقافة الحواسيب أوتقنية المعلومات أوالواقع الإفتراضي[1] .

مصطلح Cyber الإنجليزي متأصل في الكثير من الكلمات التي يشيع استخدامها في مجال تكنولوجيات المعلومات والإتصالات مثل الفضاء السيبراني Cyber space والخيال العلمي[2] Cyber punk

قاموس المورد فجاء فيه بأن السيبرانية هي علم الضبط ومصدرها Cyber netics، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية أي ضبط الأشياء بعد السيطرة عليها[3].

بالنسبة لقاموس مصطلحات الأمن المعلوماتي فعرف السيبرانية بأنها هجوم عبر الفضاء إلكتروني، يهدف الى السيطرة على المواقع الإلكترونية أو البنية المحمية إلكترونيا لتعطيلها أو تدميرها.

عرف قاموس المصطلحات العسكرية الأمريكية السيبرانية بأنها: "أي فعل يستخدم عن طريق الشبكات الإلكترونية بهف السيطرة أوالتعطيل لبرامج إلكترونية أخرى"[4].

**ب- المقصود بعبارة "الحرب السيبرانية":** اختلفت التعريفات بشأن "الحرب السيبرانية"، ومنها ما يلي:

1- عرفت الحرب السيبرانية بأنها: "إستخدام القدرة الشبكية للدولة أوالفاعلين من غير الدول لتعطيل أو حرمان أو تقليل كفاءة أو التحكم أو حتى تدمير البيانات والمعلومات الموجودة في أجهزة أوشبكات أجهزة الحسابات للفاعلين الآخرين أوحتى تدمير تلك الأجهزة والشبكات ذاتها"[5] .

2- جاء في تعريف آخر أن الهجمات السيبرانية هي: "الهجمات التي تطلقها الدول أو مجموعات من الدول، أو الجماعات السياسية المنظمة ضد البنية التحتية السيبرانية لدولة أخرى، وذلك بالتزامن مع هجمة عسكرية"[6] .

3- البنتاغون عرف الحرب السيبرانية ب"توظيف القدرات السيبرانية ، حيث يكون الغرض الأساسي هو تحقيق الأهداف أو تأثيرات عسكرية في الفضاء السيبراني"[7].

4- كما عرفت أيضا على أنها، هجمات على نظم المعلومات بهدف الإضرار بها وفي الوقت نفسه للدفاع عن نظام المعلومات الخاصة بالدولة المهاجمة، كذلك يقصد بالحرب السبرانية مجموعة الأعمال التي

---

[1]. جيلالي شويرب ، فائزة مراد ، مرجع سابق، ص161.

[2]. ناجي محمد أسامة الشاذلي، **الجوانب القانونية للحرب السيبرانية: دراسة في إطار القانون الدولي الإنساني**، مجلة روح القوانين، الجزء الثاني، العدد 103، مصر، جويلية 2023، ص 1245.

[3].نفس المرجع ، نفس الصفحة.

[4]. نفس المرجع، ص 1246.

[5]. نفس المرجع، ص 1242.

[6]. نفس المرجع، نفس الصفحة.

[7]. أمينة بوطاطة، **الحروب السيبرانية في العلاقات الدولية (مفهوم و الظاهرة)**، مذكرة مكملة لنيل شهاة الماسترفي العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955، سكيكدة، الجزائر، 2021/2020، ص 22.

تقوم بها دولة ما، تحاول من خلالها إختراق أجهزة الكمبيوتر وشبكات المعلومات التابعة لدولة أخرى، بهدف تحقيق أضرار بالغة أو تعطيلها .

5- أيضا عرفت الحرب السيبرانية على أنها نزاع يحدث في الفضاء الإلكتروني، ويكون له طابع دولي، إن صفة السيبرانية تعني علم التحكم الأوتوماتيكي أوعلم الضبط، ومن بين التعاريف التي ذهب إليها خبراء ومختصين في القانون الدولي الإنساني، وأولهم الأستاذ SHIN الذي عرف السيبرانية بأنها: "إستخدام الطيف الإلكتروني أوالكهرومغناطيسي لتخزين وتعديل المعلومات وتبادل البيانات وجه لوجه مع أنظمة تحكم لبنى تحتية مرتبطة بها"[1] .

6- هناك العديد من الفقهاء والقانونيين الذين إعتبروا الحرب السيبرانية إستمرارا للحروب التقليدية والمادية، ويتألف جندها من الدنيين والعسكريين في آن واحد، وهي حرب أدمغة بالدرجة الأولى لأنها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية، وذلك لغرض إيقاف وتحطيم البنية التحتية للدولة، وذلك بإضعاف شبكات النقل والإمددات اللوجستية، وضرب المعلومات الإقتصادية، والعبث بالمحتوى الرقمي والتقني .

7- فقهاء آخرون تابعون للناتو، عرفوا الحرب السيبرانية في القاعدة ثلاثون من دليل تالين، المتعلق بتطبيقات القانون الدولي في مجال الصراع والحروب السيبرانية، والتي تنص على أنها "كل العمليات السيبرانية سواء كانت دفاعية أوهجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلفا أو ضررا للأشياء المادية"[2].

8- تعرف اللجنة الدولي للصليب الأحمر هذه الحرب بأنها: "الأفعال التي يتخذها أطراف النزاع لتحقيق ميزة على خصومهم، في الفضاء الإلكتروني بإستخدام أدوات تقنية مختلفة، وتقنيات تعتمد على الطاقة البشرية، من الناحية النظرية يمكن تحقيق المزايا عن طريق إتلاف أوتدميرأوإعطاب أونهب أنظمة الحاسوب لدى الخصم (الهجوم السيبراني)، أوبالحصول على معلومات يفضل الخصم أن تبقى سرية التجسس السيبراني أومن خلال إستغلال سيبراني[3] .

9- أما الفقه العربي وبالرجوع إلى المختصين في اللغة العربية، فنجد أنهم واجهوا تحديا في إختيارالمصطلح المقارب لمصطلح (Syber) في اللغة الإنجليزية، وهذا ما أكدته الترجمة الحرفية للغة العربية لعنوان اتفاقية "مجلس أوربا" المتعلقة بالهجمات السيبرانية التي ترجمتها ترجمة غير صائبة، إن ترجمة العنوان Convention on Cybercrime إلى اللغة العربية بأنه: "الإتفاقيات المتعلقة بالجريمة

---

[1]. حامد محمد علي البلداوي، **مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني**، مجلة الجامعة العراقية، العدد 57، الجزء الثاني، الجامعة العراقية، العراق، بدون سنة، ص 372.

[2]. نفس المرجع، نفس الصفحة.

[3]. نفس المرجع، نفس الصفحة.

الإلكترونية"، ويعود السبب إلى عدم وجود اصطلاح مناظر له في اللغة العربية، وهذا ما جعل الوثائق الصادرة عن الأمم المتحدة باللغة العربية استعملت اصطلاح السيبرانية بدل الإلكترونيةأمن السيبراني .

خلاصة القول هو وجود عدة تعاريف، ولكنها جميعا متشابهة وتصب في قالب واحد وهو أنّ : الحرب السيبرانية (Cyber warfare) هي صراع يستخدم فيها الفضاء السيبراني كبيئة رئيسية للعمليات الهجومية والدفاعية بين الدول أوبين جهات غير حكومية بهدف تحقيق أهدف عسكرية، سياسية، أقتصادية وايديولوجية، وتعتمد هذه الحرب على الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية والأنظمة العسكرية والمؤسسات الحكومية والشركات الكبرى وغالبا ما تكون مدفوعة بأهداف استراتيجية مثل: التجسس، التخريب أو بغرض فرض النفوذ، هذه الحرب أصبحت ساحة جديدة للمواجهة بين الدول والجماعات وهي تشكل تهديد للأمن القومي والإنسانية .

**ثانيا: التمييز بين الحرب السيبرانية وغيرها من المفاهيم المشابهة**

في هذا العنوان سنميز بين الحرب السيبرانية، الهجمة السيبرانية والجريمة السيبرانية، لأنّ هناك من يخلط بينهم، فالتمييز بين هذه المفاهيم الثلاثة يساعد على فهم طبيعة الأفعال المرتكبة عبر الفضاء الإلكتروني والإطار القانوني المناسب لها، وفيما يلي نعرض لمفهوم كل مصطلح ثم نوضح الفرق في الجدول أدناه:

**أ- الحرب السيبرانية:** الحرب السيبرانية –مثلما تم التوصل إليه أعلاه- هي نزاع مسلح يتم عبر الفضاء الإلكتروني، تستخدم فيه الدول والفاعلون المرتبطون بها الوسائل السيبرانية كوسيلة لتحقيق الأهداف العسكرية أو السياسية ضد دولة أخرى، فهي مرتبطة بالقانون الدولي الإنساني خاصة إذا بلغت أعمالها حد النزاع المسلح .

**ب- الهجوم السيبراني:** الهجوم السيبراني هو عمل عدائي يتم عبر الفضاء الإلكتروني، يهدف إلى تعطيل أوتدمير أوالتلاعب بأنظمة المعلومات أوشبكات الإتصال أوالبنية التحتية المعلوماتية، ولا يشترط فيه أن يرتقي إلى درجة الحرب، إذ يمكن أن يكون عملا منفردا، إجراميا أوأداة في سياق نزاع عسكري، وقد يحدث تداخل بين الهجمات والحروب السيبرانية كما حدث لدولة استونيا في 27 أفريل 2007 حيث وقع هجوم سيبراني شامل استهدف المواقع الإلكترونية الحكومية والبرلمان وحسابات البنوك والصحف، تسبب هذا الهجوم في عزل الدولة عن العالم وانقطاع الخدمات عن تلك المواقع[1].

[1]. سهيلة غجاتي، أميرة راهم، **الهجمات السيبرانية و أثرها على تهديد السلم و الأمن الدوليين**، مذكرة مكملة لمتطلبات نيل شهادة ماستر في القانون، كلية الحقوق، جامعة 8 ماي 1945 قالمة، الجزائر، 2024/2023 ، ص 18 .

**ج- الجريمة السيبرانية:** الجريمة السيبرانية هي عمل غير مشروع يرتكب عن طريق الانترنت أو باستخدام أنظمة المعلومات، بهدف تحقيق مكاسب مادية أو الإضرار بأشخاص أو مؤسسات، هذه الجريمة تحكمها قوانين الجرائم التقليدية مع تطويعها لخصوصية البيئة الرقمية، وقد تناولتها اتفاقية بودابست لمكافحة الجرائم الإلكترونية[1]، وكذلك عرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين عام 2000 أنها: "أيّ جريمة يمكن ارتكابها على نظام حاسوبي أوشبكة حاسوبية وتشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية"[2].

والجدول التالي يوضح خلاصة التمييز :

**الجدول رقم (01) : الفرق بين الحرب السيبرانية والهجوم السيبراني والجريمة السيبرانية**

| | الحرب السيبرانية | الهجوم السيبراني | الجريمة السيبرانية |
|---|---|---|---|
| **الفاعل** | دول أو أطراف مدعومة من الدول | دول، مجموعات وأفراد مستقلون | أفراد أوجماعات إجرامية |
| **الهدف** | تحقيق أهداف سياسية أوعسكرية | تخزين أو تدمير أنظمة معلوماتية | تحقيق مكاسب مادية أو شخصية |
| **الإطار القانوني** | القانون الدولي الإنساني | قد يكون ضمن نزاع أو مستقل | قانون العقوبات الوطنية أو الدولية |
| **الطابع** | نزاع مسلح | عمل عدائي إلكتروني | فعل إجرامي |

**المصدر:** من إعداد الطالبتين اعتمادا على ما سبق.

من خلال هذا الجدول يظهر أنّ المعيار الأساسي للتمييز بين هذه المفاهيم الثلاثة يكمن في طبيعة الفاعل، الهدف من الفعل، الإطار القانوني الذي ينطبق عليه، بينما ترتبط الحرب السيبرانية بالنزاعات المسلحة وتنظمها قواعد القانون الدولي الإنساني. وحاصل القول: "إن الحرب السيبرانية يمكن أن تشكل هجوما وجرائم سيبرانية في ذات الوقت"[3].

**الفرع الثاني: نشأة وتطور الحروب السيبرانية**

الحرب السيبرانية مرت بعدة مراحل، تزامنا مع تطور التكنولوجيا الرقمية والانترنت، ويمكن تقسيم هذا التطور إلى المراحل التالية: المرحلة الأولية (الخمسينات وأواخر التسعينات)، المرحلة المتوسطة (2000 _2010) بداية استخدام السيبرانية في الصراعات، المرحلة الحديثة (2011 حتى اليوم) تصاعد الحرب السيبرانية والهجمات المتقدمة، المرحلة المستقبلية للحروب السيبرانية.

[1]. إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية:معاهدة دولية أعدت من قبل مجلس أوروبا في عام 2001،تعنى بتحديد الجرائم الإلكترونية و تنظيم الإجراءات القانونية المتعلقة بها وتسهيل التعاون الدولي في مكافحة هذه الجرائم

[2]. سهيلة غجماتي وأميرة راهم، المرجع السابق، ص 16.

[3]. ناجي محمد أسامة الشاذلي، المرجع سابق، ص 1253.

**أولا: المرحلة الأولية (الخمسينات وأواخر التسعينات)**

في منتصف الخمسينات من القرن المنصرم تم استحداث أجهزة الكمبيوتر كأداة لمعالجة وحفظ المعلومات رقميا (DIGITAL)، وتظافرت جهود عدة شركات ليصلوا إلى تطوير وحدة المعالجة المركزية (CPU) وذلك لتسهيل المهام الموكلة إليه[1].

في الستينات وبالولايات المتحدة الأمريكية ظهر ما يسمى بـ: انترنت (Internet)، وزارة الدفاع شكلت لجنة من الخبراء وكلت إليهم مهمة إنشاء شبكة تربط بين الحواسيب، وبذلك أنشأت أول شبكة انترنت، سميت شبكة وكالة مشاريع الأبحاث المتطورة Advenced Research projects Agency Network مختصرة في (ARPANET)[2].

في هذه المرحلة ظهرت أولى الإختراقات الأمنية، لكنها لم تكن ذات طابع عسكري واضح، حيث تم تطوير أولى الفيروسات والبرمجيات الخبيثة مثل فيروس Creeper عام 1971 وفي بداية الثمانينات بدأت الحكومة الأمريكية تستشعر أهمية أمن المعلومات مع ظهور عملية التجسس الإلكتروني[3] .

في عام 1982 وقع هجوم على أنظمة الغاز السوفياتية عبر برمجيات تخريبية تسببت في إنفجار خط الأنابيب (حادثة سيبيريا).

في عام 1986 وقعت حادثة Cuckoo's.Egg"بيضة الوقواق" وهي من أوائل حوادث التجسس الإلكتروني، حيث تم إكتشاف قراصنة يعملون لصالح الإستخبارات السوفياتية من طرف عالم الفلك الأمريكي كليفورد ستول، حيث لاحظ نشاط غير معتاد على شبكة الحواسيب بالمختبر الوطني لورنس بريكلي بالولايات المتحدة[4].

**ثانيا: المرحلة المتوسطة (2000 _2010) بداية استخدام السيبرانية في الصراعات**

لقد تحولت الهجمات من مجرد عمليات قرصنة فردية إلى هجمات إلكترونية منظمة من قبل الدول والجماعات الإرهابية، حيث تم استخدام الفيروسات وأحصنة طراودة (Trojans) والهجمات الموزعة (D-Dos) لتعطيل البنية التحتية للخصوم. ففي ديسمبر 2006 أجبرت ناسا على حجب رسائل البريد الإلكتروني التي تأتي مع مرفقات قبل إطلاق المركبات الفضائية خشية إختراقها. كما شهد عام 2007

[1].أمينة بوطاطة، مرجع سابق، ص 16.
[2]. نفس المرجع، ص 17.
[3]. ويكيبيديا، **متى ظهرت الحرب السيبيرانية**، على الرابط: http :llar .m.WiKipedia.org/wiki/d8، تاريخ الاطلاع: 12-03-2025، وقت الإطلاع: 12:00
[4].مجدي عبد العزيز الشاذلي، **الحروب السيبرانية :المفهوم ـ السمات ـ الأنماط ـ التحديات القانونية الدولية**،بدون رقم الطبعة، دار النهضة العربية، مصر، 2021 ،ص102

هجوما سيبرانيا على إستونيا عطّل مواقع حكومية وبنكية، ويعتبر أول هجوم إلكتروني واسع النطاق ضد دولة، حيث تعطلت الخدمات الحكومية الإلكترونية والخدمة المصرفية عبر الإنترنت ووسائل الإعلام، وأصيبت العديد من الأحزاب السياسية بالشلل، حيث قطع الإتصال بحوالي 58 موقعا، وهذا كله بعد الخلاف مع روسيا حول إزالة نصب تذكاري[1].

في عام 2008 حدث هجوم على أنظمة وزارة الدفاع الأمريكية عبر USB مصاب بفيروس "Agent .btz"، وفي نفس السنة تم إختراق شبكة حواسيب في جورجينا من قبل مجهولين خلال فترة الصراع مع روسيا[2]. أما في نهاية عام 2009 الحكومة الكورية الجنوبية قدمت تقريرا عن تعرضها لهجوم من قبل كوريا الشمالية بغرض سرقة خطط دفاعية تتضمن معلومات عن شكل التحرك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية[3].

في عام 2010 تم إكتشاف فيروس "Stuxnet" الذي استخدم لإستهداف منشآت نووية إيرانية، مما كشف لأول مرة عن إمكانية استخدام البرمجيات الخبيثة كأسلحة رقمية[4]. وفي نفس السنة من شهر جويلية ألمانيا صرحت أنها تعرضت لعمليات تجسس شديدة من قبل الصين وروسيا، استهدفت قطاعات صناعية وبنى تحتية حساسة في البلاد منها شبكة الكهرباء[5]. كما قامت إسرائيل بتعطيل الرادارات السورية عند إغارتها على موقع الكير النووي السوري.

**ثالثا: المرحلة الحديثة (2011 حتى اليوم) تصاعد الحرب السيبرانية والهجمات المتقدمة**

بعد عام 2011 تطورت الحرب السيبرانية بشكل أكبر، وبدت سمات أخرى لها أهمها :

أ- تطورت الهجمات الإلكترونية لتشمل إستخدام الذكاء لإصطناعي والهجمات المستمرة المتقدمة (APT).

ب- تحولت الحرب السيبرانية إلى أداة استراتيجية في الصراعات الجيوسياسية .

ج- زيادة إستهداف البنية التحتية الحساسة مثل شبكات الطاقة والأنظمة المالية والمستشفيات .

---

[1]. ويكيبيديا، الموقع السابق.
[2]. اختراقات إلكترونية، **البداية اشارة موريس**، قناة الجزيرة، على الرابط: https://2u.pw-mtkkj، تاريخ الاطلاع: 12-03-2025، وقت الإطلاع: 10:15.
[3]. نفس الموقع.
[4]. ويكيبيديا، نفس الموقع .
[5]. نفس الموقع.

د- ظهور مجموعة قرصنة مدعومة من الدول مثل: APT28 و APT29 المرتبطين بروسيا و Charming Kitten المرتبطين بإيران[1] .

من أبرز الأحداث المهمة التي حدثت في هذه الفترة :

أنه في عام 2013 مع بداية مواجهة روسيا لأوكرانيا وتطور الخلاف بينهما، عملت روسيا على تطوير وتحديث برمجياتها وطرق هجومها، وسجلت أول هجماتها السيبرانية على الأنظمة المعلوماتية الخاصة بالمؤسسات الحساسة لأوكرانيا بهدف التجسس وجمع المعلومات سميت هذه العملية بـــ: عملية هرمجدون[2] .

في عام 2014 وقع هجوم Sany Pictures المنسوب إلى كوريا الشمالية ردا على فعل يسخر من زعيمها، وكذلك عملية "سنايك" التي تم خلالها إستخدام برمجيات خبيثة متطورة لإختراق شبكات الحاسوب الأوكرانية مما أدى إلى سرقة بيانات حساسة، وفي نفس السنة أيضا تم هجوم آخر في جويلية إستهدف النظام الآلي للإنتخابات في أوكرانيا بهدف تعطيل العملية الإنتخابية والتلاعب بالنتائج[3]، بعدها عامي 2015 و2016 تعرضت شبكة الكهرباء الأوكرانية لهجات سيبرانية أدت إلى إنقطاع واسع في الكهرباء.

في عام 2017 انتشر فيروس الفدة "Wanna cry" الذي ضرب مستشفيات وشركات حول العالم وتسبب في خسائر مالية كبيرة وقد سمي بهجوم نوت بيتيا، في نفس السنة قامت إيران بالهجوم على البرلمان البريطاني، إستهدفت الحسابات البريدية الإلكترونية لأعضاء البرلمان حيث إخترقت تسعون حسابا، في شهر أوت 2018 كشفت تقاريرعن قيام قراصنة إيرانيين بإستهداف ستة وسبعون جامعة في أربعة عشر دولة لسرقة أبحاث وبيانات أكاديمية حساسة[4].

في عام 2020 تم إختراق Solar winls الذي إستهدف شركات أمريكية وحكومات غربية، ويعتقد أنه من تنفيذ روسيا، وفي عام 2023 دارت حرب سيبرانية بين إسرائيل وحماس، فبعد هجوم 2023/10/07 تم إستهداف المواقع الإلكترونية الإسرائيلية لحجب الخدمة بشكل مكثف[5].

في عام 2024 شهد العالم زيادة كبيرة في هجمات الفدية (Ransom war) المدعومة بالذكاء الإصطناعي، حيث أصبحت أكثر دقة وبلغت الخسائر العالمية حوالي عشرة مليارات يورو، كما برزت

---

[1]. ويكيبيديا،الموقع السابق.
[2]. اختراقات إلكترونية، موقع سابق.
[3]. نفس الموقع.
[4]. اختراقات إلكترونية،نفس موقع .
[5]. نفس الموقع.

مجموعات قرصنة مثل "فولت تايفون الصينية" و"ساندروم الروسية"، حيث إستهدفت البنية التحتية لأمريكا وأوكرانيا .

**رابعا: المرحلة المستقبلية للحروب السيبرانية**

وهي المرحلة المدعومة بالذكاء الإصطناعي والكمبيوتر الكمي، حيث يتم فيها ما يلي:

أ- استخدام الذكاء الإصطناعي في تنفيذ الهجمات والدفاعات السيبرانية.

ب- تطوير الهجمات القائمة على الجوسسة، مما سيجعل تقنيات التشفير التقليدية غير فعالة.

ج-تزايد الهجمات على شبكات الجيل الخامس والانترنت.

د- إحتمال ظهور حرب سيبرانية شاملة تستهدف دولا بأكملها وليس مجرد مؤسسات محددة[1].

كخلاصة لما سبق، يمكننا القول بأنّ الحرب السيبرانية أصبحت اليوم جزءا أساسيا من النزاعات الحديثة، وتتطور بشكل متسارع مع تقدم التكنولوجيا، ولهذا السبب بدأ القانون الدولي الإنساني بمناقشة كيفية التعامل مع هذه الهجمات من الناحية القانونية ومدى إعتبارها أعمالا عدائية أوحتى جرائم حرب، لأننا أصبحنا نرى اليوم ضحايا في معارك خالية من الجنود، فما حدث في لبنان جراء تفجير أجهزة "بـيـجـر" التي تملكها عناصر تابعة لحزب الله يعطي دلالة واضحة على تطور الحرب الإلكترونية، فضغطة زر واحدة كافية لتخفي مناطق وأحياء وتعطل مصالح وتشل نظام كامل، هذا وما زال التطور مستمر والخطر على البشرية والكون يزداد ويزداد في ظل عجز قانون دولي.

**المطلب الثاني: الطبيعة القانونية للحرب السيبرانية وخصائصها**

تعد الحرب السيبرانية نمطا جديدا من الحروب التي تدور في الفضاء الرقمي، مستهدفة البنى التحتية الحيوية والمعلوماتية للدول، دون الحاجة لإستخام القوة العسكرية التقليدية. ويطرح هذا النوع من الحروب إشكاليات قانونية معقدة تتعلق بطبيعتها وحدود خضوعها لقواعد القانون الدولي وعلى رأسها القانون الدولي الإنساني، من هذا المنطلق تبرز أهمية تحديد الطبيعة القانونية للحرب السيبرانية التي سيتم تناولها في الفرع الأول وفي الفرع الثاني يتم إبراز أهم الخصائص لفهم مدى إمكانية إخضاعها للأطر القانونية القائمة .

**الفرع الأول: الطبيعة القانونية للحرب السيبرانية**

إن الحرب السيبرانية هي تحدي من التحديات الحديثة التي يواجهها القانون الدولي، فهي لا تندرج بسهولة ضمن الفئات التقليدية للنزاعات المسلحة، مما يثير تساؤلات حول كيفية تنظيمها وفقا للقواعد القانونية القائمة، ويمكن تحليل طبيعتها القانونية من خلال عدة أطر قانونية دولية هي: القانون الدولي

[1].إختراقات إلكترونية، نفس الموقع.

العام (أولا)، القانون الدولي الإنساني (ثانيا)، القانون الدولي لحقوق الإنسان (ثالثا) والإتفاقيات الدولية والمبادرات الحديثة (رابعا).

**أولا: الحرب السيبرانية في إطار القانون الدولي العام**

فيما يلي نتناول الحرب السيبرانية من زاوية المبادئ الأساسية للقانون الدولي العام :

أ. **مبدأ السيادة وعدم التدخل**: إن مبدأ السيادة هو حجر الأساس في القانون الدولي، وهو يمنع الدول من التدخل في الشؤون الداخلية للدول الأخرى، وبالتالي فالهجمات السيبرانية التي تستهدف بنية دولة أخرى تعتبر إنتهاك لسيادة الدولة، ما لم تكن هناك مبررات قانونية مثل الدفاع عن النفس[1]، ولكن بعض الدول تعتبر التجسس عمل غير عدائي، بينما دول أخرى تعتبه إنتهاك واضح للسيادة.

ب. **مبدأ عدم إستخدام القوة**: هناك نصوص مدونة في ميثاق الأمم المتحدة تتلاءم مع طبيعة الحرب السيبرانية ويمكن أن تطبق عليها، حيث تنص المادة 4/2 من ميثاق الأمم المتحدة على أنه: "يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد بإستعمال القوة أو إستخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق مع مقاصد الأمم المتحدة"[2].

في هذه الحالة ثار تساؤل حول تفسير مصطلح "القوة"؛ هل هواستخدام القوة المسلحة في إطار عدوان أو هجوم مسلح ترتكبه الدول بإستخدام قواتها المسلحة أوجماعات منظمة تابعة لها أومسندة من قبلها، وهناك من يرى أن القوة ليس معناها إستخدام القوة المسلحة فقط، بل يمكن أن يشمل الضغوطات الأخرى كالضغوط الإقتصادية أوالسياسية.

إنّ الأخذ بالمعيار الأول المعتمد على العنصر الحركي للقوات المسلحة لا يستقيم والكثير من الاستخدامات للقوة أثناء الحروب، وذلك لوجود الهجمات البيولوجية والجرثومية وكذلك الهجمات السيبرانية، وذلك بغض النظرعن مشروعية تلك الحرب من عدمها، كما أنّ إعتماد المعيار الثاني قد يوسع كثيرا من مفهموم القوة والتهديد ليشمل الإكراه الإقتصادي والسياسي، وقد يخالف المقصود بما ورد في مياق الأمم المتحدة من مقاصد وفقا لأغلبية الفقهاء، كونه يوسع من مفهوم العدوان بما يعطي مسوغا لإستخدام القوة المضادة إستنادا لحق الدفاع الشرعي[3]. إتجاه آخر يرى أن القوة تشمل كافة صور إستخدام القوة المسلحة إضافة إلى صور أخرى يترتب عنها انتهاك أوتأثير واضح على الأمن القومي لدولة أخرى.

---

[1]. يحي ياسين سعود، **الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني**، المجلة القانونية، المجلد 4، العدد 4، جامعة القاهرة، مصر، 2018، ص 86.

[2]. نفس المرجع، نفس الصفحة.

[3]. نفس المرجع، ص 87.

أصبح التفوق التكنولوجي عنصرا حيويا في تنفيذ عمليات ذات فاعلية في البحر والبر والجو والفضاء الخارجي، من خلال إعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة، وبهذا يتغير مفهوم القوة، حيث أصبح من الممكن تعريفها على أنها: "مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة وتؤثر في سلوك الوحدات السياسية الأخرى"[1]. معنى ذلك أنّ التغيير في مفهوم القوة يؤدي بالضرورة إلى تغيير مفهوم الحرب فالحروب التقليدية كانت قائمة على تدمير الخصم أوإحتلاله أوالإستيلاء موارده، أما الحرب الحديثة فهي قائمة على سرقة الأسرار الإقتصادية والعلمية والعمل على إختراق الأمن القومي لدولة أخرى .

**ج- مبدأ الدفاع الشرعي عن النفس**: الدولة المعتدى عليها لها حق اللجوء للقوة بحكم المادة 51 من ميثاق الأمم المتحدة والتي جاء فيها: "ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول، فرادى أو جماعات في الدفاع عن أنفسهم، إذا إعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة"[2]، كما جاء في البروتوكول الإضافي الأول سنة 1977 المتعلق بالأسلحة الجديدة في مادته 36: "يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو إقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب جديد للحرب، بأن يتحقق ما إذا كان محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"[3]. وهكذا نصل إلى فكرة ضرورة التحقق من مدى مشروعية إستخدام وسائل وأساليب الحرب الجديدة وفقا لقواعد القانون الدولي.

د. **مسؤولية الدولة عن الأعمال السيبرانية**: وفقا للمشروع المتعلق بـ "المسؤولية الدولية عن الأفعال غير مشروعة دوليا" الصادر عن لجنة القانون الدولي، تتحمل الدولة المسؤولية عن الأفعال السيبرانية إذا إرتكبتها جهات رسمية حكومية أو دعمت أو تواطأت مع جهات غير حكومية لشن هجمات سيبانية أو فشلت في منع الهجمات التي تنطلق من أراضيها[4] .

**ثانيا: الحرب السيبرانية في إطار القانون الدولي الإنساني**

القانون الدولي الإنساني ينظم النزاعات المسلحة لكنه لم يوضع خصيصا للحروب السيبرانية، لأنه يوجد خلاف حول ما إذا كانت الهجمات السيبرانية ترقى إلى النزاع المسلح، خاصة إذا لم تؤد إلى

---

[1]. يحي ياسين سعود، مرجع سابق، ص 87.
[2]. أمينة بوطاطة، مرجع سابق، ص 61.
[3]. نفس المرجع، ص 62.
[4].لجنة القانون الدولي، **مشروع مواد حول مسؤولية الدول عن الأفعال غير مشروعة دوليا مع التعليقات**، الأمم المتحدة ، الجمعية العامة، الدورة 56، الوثيقة A/56/10،2001، ص 35.

خسائر بشرية أوحصار مادي واسع. فدليل تالين[1] الذي وضعه خبراء القانون الدولي يرى أن القانون الدولي الإنساني ينطبق على الحرب السيبرانية إذا بلغ النزاع مستوى معينا من العنف.

**ثالثا: الحرب السيبرانية في إطار القانون الدولي لحقوق الإنسان**

حتى في زمن السلم يمكن أن تنتهك الهجمات السيبرانية حقوق الإنسان الأساسية مثل الحق في الخصوصية والحق في التعبير، فبعض الدول تستخدم الحرب السيبرانية لقمع المعارضين، أو شن عمليات مرقابة واسعة النطاق، وهو ما قد يشكل إنتهاكا للقانون الدولي لحقوق الأنسان[2]، لهذه الأسباب منظمات حقوق الإنسان تدعو إلى وضع ضوابط قانونية تحمي الأفراد من الإستخدام غير المشروع للقوة السيبرانية.

**رابعا: الإتفاقيات الدولية والمبادرات الحديثة**

ظهرت عدة محاولات من أجل تنظيم الحرب السيبرانية و تقنينها، ويمكن حصر هذه المحاولات في الإتفاقيات الدولية و الدراسات القانونية أهمها :

**أ ـ دليل تالين**: هو محاولة أكاديمية لتفسير كيفية تطبيق القانون الدولي الإنساني على الحرب السيبرانية، لكنه ليس ملزما قانونا.

**ب ـ مبادرة الأمم المتحدة للأمن السيبراني**: تسعى لتطوير معايير دولة تنظم إستخدام القوة السيبرانية.

**ج ـ إتفاقية بودابيست لمكافحة الجرائم السيبرانية**: تركز هذه الاتفاقية على التعاون الدولي لمكافحة الجرائم الإلكترونية، إلّا أنها لا تعالج الحرب السيبرانية بشكل مباشر.

بالنظر إلى ما تم طرحه يظهر جليا أن التكييف القانوني للحرب السيبرانية لم يصل بعد مرحلة إبرام إتفاقية دولية واضحة المعالم، ولا يزال ضمن درجة القياس والإجتهاد بسبب الدول المهيمنة على العالم، والتي تتجنب طرحه أو وضع إطار قانوني له حتى تبقى مهيمنة ومسيطرة، إذن لا يوجد حاليا إطار قانوني شامل ينظم الحرب السيبرانية في القانون الدولي .

[1]. دليل تالين أول دراسة منهجية أجراها مجموعة من الخبراء الدوليين تحت إشراف المركز التعاوني لقانون الدفاع السيبراني التابع لحلف الناتو سنة 2013 (سنتطرق إليه بالتفصيل في دراستنا) "لاحقا".

[2]. مصطفى كامل فرطاس، **الأمن السيبراني وحقوق الإنسان الرقمية**، المفوضية العليا لحقوق الإنسان، قسم النشر والتثقيف، شعبة البحوث والدراسات، جمهورية العراق، 2023، ص 15.

**الفرع الثاني: خصائص الحرب السيبرانية**

أفرز التقدم النكنولوجي واستخدام الفضاء السيبراني في النزاعات المسلحة نوعا جديدا من الحروب، يتميز بجملة من الخصائص التي تجعله مختلفا عن الأشكال التقليدية للصراع، تتمثل هذه الخصائص فيما يلي :

**أولا: الطبيعة غير المادية (الإفتراضية)**

تتميز الحرب السيبرانية بكونها تخاض في فضاء غير مادي، حيث تستخدم أدوات رقمية كالفيروسات والبرمجيات الخبيثة بدلا من الأسلحة التقليدية، هذا الطابع يجعل آثارها غير مرئية في الغالب رغم قدرتها على التسبب بخسائر مادية وبشرية كبيرة[1].

**ثانيا: صعوبة التتبع ونسبة الهجوم**

يصعب غالبا تحديد الجهة التي تقف وراء الهجمات السيبرانية، بسبب إستخدام أدوات التمويه الرقمي مثل الخوادم الوسيطية والتشفير، مما يعقد عملية إسناد المسؤولية ويعيق التفاعل القانوني والدبلوماسي مع هذه الهجمات[2].

**ثالثا: تجاوز الحدود الجغرافية**

لا تعترف الحرب السيبرانية بالحدود الدولية، إذ يمكن تنفيذ الهجمات من أي مكان في العالم، ما يعقد مسألة السيادة ويثير تساؤلات حول نطاق قواعد النزاع[3].

**رابعا: التكلفة المنخفضة والعائد المرتفع**

بالمقارنة مع الحرب التقليدية، فإن الحرب السيبرانية تتطلب موارد مالية أقل، ما يجعلها في متناول دول صغيرة أو حتى جماعات غير حكومية[4].

**خامسا: الطابع الوقائي**

كثير من العمليات السيبرانية تنفذ بشكل استباقي لتعطيل أنظمة الخصم قبل إندلاع النزاع، ما يطرح إشكالية حول مدى قانونية هذه الأفعال في إطار القانون الدولي[5].

---

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 495.
[2]. نفس المرجع، نفس الصفحة.
[3]. نفس المرجع، نفس الصفحة.
[4]. نفس المرجع، نفس الصفحة.
[5]. نفس المرجع، نفس الصفحة.

**سادسا: إستهداف البنية التحتية الحيوية**

غالبا ما تستهدف الهجمات السيبرانية منشآت مدنية حيوية، مثل: الكهرباء، المياه والاتصالات، وهو ما قد يعرض المدنيين لأضرار مباشرة رغم أن الهدف الظاهر قد يكون ذو طبيعة عسكرية[1].

**سابعا: إستخدام الذكاء لإصطناعي والأنظمة الذاتية**

تدار بعض الهجمات السيبرانية بواسطة أنظمة ذكية تتخذ قرارات هجومية دون تدخل بشري مباشر، ما يطرح تحديات أخلاقية وقانونية فيما يخص المراقبة والمساءلة[2].

**ثامنا: الإزدواجية بين السلم والحرب**

إن أدوات الحرب السيبرانية يمكن إستخدامها لأغراض مدنية أو عسكرية، فمثلا التكنولوجيا التي تستخدم في التعليم والإتصالات يمكن إستخدامها لتدمير شركات ومؤسسات مدنية وعسكرية[3].

**تاسعا: السرعة الفائقة وإمكانية المراوغة**

يتم تنفيذ الهجوم السيبراني في دقائق أوثواني، والأثر قد يكون لحظي أو طويل، كما أن الأفضلية تكون للمهاجم على المدافع[4].

**عاشرا: الطبيعة الغامضة للحرب السيبرانية**

لا يمكن بسهولة تحديد بداية النزاع المسلح السيبراني، وبالتالي قد تتأثر قواعد القانون الدولي الإنساني في التطبيق، مما يترك المدنيين دون حماية في المرحلة الأولى للهجوم[5].

**إحدى عشر: فشل نماذج الردع المعروفة**

الهجمات السيبرانية في الغالب لا تترك أثرا أو دليلا، كما أن الدمار الذي قد تخلفه الحرب السيبرانية قد يتضمن التجسس والتسلل والنسف دون دماء أوأنقاض، فضلا على أنّ أطرافه غير واضحة وتداعياته خطيرة من خلال تدمير مواقع الإنترنت بوابل من الفيروسات، كما أنّ سعة هذا الفضاء تسمح بزيادة عدد المهاجمين وإمتداد الصراع في الزمان والمكان[6].

---

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 495.
[2]. نفس المرجع، نفس الصفحة.
[3]. نفس المرجع، نفس الصفحة.
[4]. نفس المرجع، نفس الصفحة.
[5]. نفس المرجع، ص 496.
[6]. جيلالي شويرب، فائزة مراد، مرجع سابق، ص 163.

**اثنا عشر: تعدد الفاعلين**

الفاعل قد يكون شخص واحد أومجموعة من الأشخاص أو دولة أو هيئة أو شركة متعددة الجنسيات أو مجموعة إرهابية مثل جماعة Wikileaks[1](Wikileaks هي جماعة تنتمي لمنظمات غير حكومية، تقوم بنشر الملفات السرية عن الحكومات، تحتوي على معلومات سرية وهامة وبدون ذكر الهوية Anonymous).

**المطلب الثالث: أنماط الحرب السيبرانية والتمييز بينها وبين الحرب التقليدية**

الحرب السيبرانية –كما ذكرنا سابقا- هي حرب غير تقليدية تعتمد على التكنولوجيا والفضاء الرقمي، ويمكن أن تكون سرية وغير مكلفة بالمقارنة مع الحروب التقليدية التي تتطلب وجودا ماديا وقوة عسكرية، فالحرب السيبرانية تعتمد على الإختراقات الرقمية والتأثيرالإعلامي، فـ "الحرب السيبرانية هي نوع من الهجمات السيبرانية التي تحدث أثناء النزاع المسلح الحركي أو التي تنتج آثار مادية تشبه وتعادل في آثارها الهجمات التقليدية"[2].

على ضوء ما سبق نتناول هذا المطلب في فرعين: الفرع الأول يتضمن الأنماط الرئيسية للحرب السيبرانية، والفرع الثاني نوضح فيه الفوارق الجوهرية بين الحرب السيبرانية وبين الحروب التقليدية .

**الفرع الأول: أنماط الحرب السيبرانية**

تتعدد أنماط الحرب السيبرانية وفقا للأهداف والأساليب المستخدمة ومن أبرز هذه الأنماط نجد :

**أولا: التصنيف الأول**

يتضمن التصنيف الأول الهجمات التالية :

**أ ـ الهجمات السيبرانية التخريبية (Cyber disruption attacks)**: هدف هذه الهجمات تعطيل أو شل البنية التحتية الرقمية للخصم، وأسلوبها تنفيذ هجمات الحرمان من الخدمة (DDos) أو إستهداف الأنظمة الحيوية مثل شبكات الكهرباء والمواصلات، ومن الأمثلة على ذلك الهجوم على الأنظمة المالية أوشبكات الطاقة كما حدث في أوكرانيا عام 2015[3] .

**ب ـ الهجمات السيبرانية التجسسية ( Cyber Espionage)**: الهدف من هذه الهجمات هو جمع المعلومات السرية والإستخباراتية دون علم الطرف المستهدف، ومن أساليب هذا النوع إستخدام

[1]. شويرب جيلالي، مراد فائزة، مرجع سابق، ص 163.
[2]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1253
[3]. نفس المرجع، ص 1273.

البرمجيات الخبيثة (Mal ware) والتصيد الإلكتروني (Phishing) وإختراق الأنظمة، ومثال ذلك حملة "Stuxnet" التي إستهدفت البرنامج النووي الإيراني[1].

**ج ـ الهجمات السيبرانية التأثيرية (Cyber influence operations)**: الهدف منها التأثير على الرأي العام أو زعزعة استقرار المجتمع، والأساليب المستعملة في هذا النوع هو نشر الأخبار الزائفة ( Fake news) والتلاعب بمنصات التواصل الإجتماعي، ومن الأمثلة على ذلك التدخلات السيبرانية في الإنتخابات الأمريكية عام 2016[2].

**د ـ الحروب السيبرانية الهجومية (Offensive cyber operations)**: تلحق الضرر مباشرة بالأنظمة العسكرية أوالمدنية للدولة المستهدفة، ومن أساليبها تدمير قواعد البيانات، تعطيل أنظمة الدفاع الجوي مثل مراكز القيادة، ومن الأمثلة على ذلك هجوم "Not petya" الذي ألحق أضرارا عالمية[3] .

**ه ـ الدفاع السيبراني (Cyber defence)**: الهدف منه حماية الأنظمة والشبكات من الهجمات السيبرانية، الأسلوب المتبع هو بناء أنظمة تشفير قوية، مراقبة الشبكات، استخدام الذكاء الإصطناعي لرصد الهجمات، ومن الأمثلة على ذلك برنامج الأمن السيبراني الوطني لحماية البنى التحتية الحرجة[4].

**ثانيا: التصنيف الثاني**

هناك من أعطى تصنيفا آخر أو أنماط أخرى للهجمات السيبرانية (الحرب السيبرانية) وهو كالآتي:

**أ ـ هجمات التصعيد الإحتيالي (PHISHING ATTACKS)**: هو نمط من هجمات الهندسة الإجتماعية، يستخدم غالبا لسرقة بيانات المستخدم بما في ذلك بيانات إعتماد تسجيل الدخول وأرقام بطاقات الإئتمان[5].

**ب ـ هجمات التصعيد الإحتيالي بالرمح (SPEAR PHISHING)**: التصعيد بالرمح هو أيضا عملية إحتيال تتم عبر البريد الإلكتروني أو الإتصالات الإلكترونية، تستهدف فردا أو منظمة أو شركة على الرغم من أن مجرمي الإنترنت يسعون إلى سرقة البيانات لأغراض ضارة، وقد يعملون أيضا على تثبيت البرامج الضارة على جهاز حاسوب الضحية[6].

---

[1]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1253.
[2]. نفس المرجع، نفس الصفحة.
[3]. نفس المرجع، ص 1254.
[4]. نفس المرجع ، ص 1253.
[5]. يحي الحياني، وآخرون، **الأمن السيبراني في كل ما يخص مركز عمليات المراقبة (sos)**، بدون رقم الطبعة، بدون دار النشر، بدون سنة، ص 51.
[6]. نفس المرجع، نفس الصفحة.

**ج ـ هجمات تصيد الحيتان (WHALE PHISHING)**: تصيد الحيتان هو مصطلح يستخدم لوصف هجوم التصعيد الذي يستهدف الوصول إلى معلومات حساسة وسرية لشخصيات قوية، إذا أصبح فرد ما ضحية لهجوم تصيد إحتيالي من هذا النوع، فيمكن إعتبار تصيد كبير أو ما يسمى "حوت"[1].

**د ـ هجمات (DRIVE _BY)**: يشير هذا الهجوم إلى برنامج نصي ضار، يثبت على جهاز الضحية دون إذن صريح منه، ويمكن أن يحدث هذا النوع من الهجمات السيبرانية على أي جهاز مستخدم يعمل بنظام تشغيل، وتحدث هذه الهجمات عند تنقل المستخدم إلى صفة ويب يتم إختراقها وتصفحها[2].

**ه ـ برنامج الفدية (RANSOM WARE)**: تعتبر هذه البرامج الأكثر خطورة في هذا العصر والتي تمكن من جعل معلومات حساسة وخطيرة للأفراد والمنظمات على المحك[3]، في هذا النوع من الهجمات يظطر الضحية إلى حذف جميع المعلومات الضرورية من نظامه إذا فشل في دفع الفدية ضمن جدول زمني يقدمه مجرمي الإنترنت.

**و ـ الهجوم بكلمة المرور**: في هذا النوع من الهجمات السيبرانية يحاول السيبرانيون إختراق حسابات الضحايا من خلال إختراق ملفاتهم الشخصية، فهم يصلون إلى المعلومات بطريقة غير قانونية ليتم إستخدامها في التصعيد الإحتيالي أو إدخال برامج ضارة على الشبكات[4].

**ز ـ هجمات التنصت (SNIFFING) أوالتطفل (SNOOPING):** هدفها سرقة المعلومات، حيث يتم نقلها عبر شبكة عن طريق جهاز الحاسوب أو الهاتف الذكي أو جهاز آخر متصل به[5] .

**ح ـ هجمات البرامج الضارة (MAL WARE_ATTACKS)**: وهي نوع من البرامج الضارة المصممة لإحداث ضرر أو تلف جهاز حاسوب أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي[6].

**ط ـ حصان الطراودة (TROJAN HORSES)**: هو نوع من البرامج الضارة ويمكن إخفاءه عادة كمرفق في رسالة إلكترونية أو ملف مجاني للتنزيل، ثم ينتقل إلى جهاز المستخدم بمجرد التنزيل، ثم ينفذ الكود الضار المهمة التي صمم من أجلها مثل الوصول لأنظمة الشركات، التجسس، سرقة البيانات الحساسة[7].

---

[1]. يحي الحياني، وآخرون، مرجع سابق، ص 51.
[2]. نفس المرجع، نفس الصفحة .
[3]. نفس المرجع، نفس الصفحة.
[4]. نفس المرجع، نفس الصفحة.
[5]. نفس المرجع، نفس الصفحة.
[6]. نفس المرجع، نفس الصفحة.
[7]. نفس المرجع، ص 52.

**ي ـ القوة الغاشمة:** يعمل المهاجمون في هذا النوع من الهجمات السيبرانية على تجربة مجموعات مختلفة من أسماء المستخدمين وكلمات المرور حتى يعثروا على واحدة تعمل، المهاجم يعمل على تخمين المفتاح الذي تم إنشاءه ككلمة سر (DERIVATION FUNCTION)، يعرف بالبحث الشامل على المفتاح وبالحصول عليه يمكن تنفيذ أخطر الهجمات كإيقاف نظام كامل (الكهرباء والماء)[1].

تجسد البرمجيات الخبيثة السابقة الذكر بمختلف أشكالها وجها من أوجد الحرب السيبرانية، إذ تستخدم كوسائل عدائية توجه عمدا لتعطيل البنى الحيوية والتجسس على المعلومات الحساسة، ما يجعل إستخدامها يشكل عملا عدائيا يرقى إلى مستوى النزاع المسلح في الفضاء السيبراني .

**ثالثا: التصنيف الثالث**

فئة أخرى من الباحثين في مجال الحرب السيبرانية أعطوا أنماطا أخرى للحرب السيبرانية (تحت مسميات مختلفة)، وهي تتمثل في :

**أ ـ الحرب السيبرانية الباردة:** يتم فيها إستخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويعبر هذا النمط عن صراع مستمر بين المتنازعين، ويكون ذو طبيعة ممتدة ودائمة النشاط العدائي أو غير السلمي، وهو عميق الجذور ومتداخل وله نواة متعددة؛ ثقافية، إقتصادية وإجتماعية، وعادة يتم اللجوء إلى القوة الناعمة ـالحروب السيبرانية ـ في مثل هذه الصراعات، وإن كانت لا تتطور إلى إستخدام القوة المسلحة بشكلها التقليدي[2]. هذا النوع من الحروب السيبرانية يعتمد على عدة وسائل منها الحرب النفسية، الإختراقات المتعددة، سرقة المعلومات، التجسس، حرب الأفكار، التنافس بين الشركات التكنولوجية العالمية وأجهزة الإستخبارات الدولية، كما يكون هذا النوع من الحروب في حالات الصراع السياسي ذو البعد الإجتماعي الديني، مثل الصراع العربي الإسرائيلي، والصراع الهندي الباكستاني، فيما سبق اتهمت روسيا بشن هجمات إلكترونية على النرويج والشيك وبريطانيا، وشنت إيران هجمات إلكترونية على منشآت نفطية في منطقة الخليج العربي، وذلك ردا على تعرض الأقليات الشيعية للتمييز، كذلك كانت هجمات فيروس دوكو عام 2012 وهجمات فيروس شمعون 2 ضد السعودية في جانفي 2017[3].

**ب ـ الحرب السيبرانية متوسطة الشدة:** هذا النوع من الحروب السيبرانية يتم عن طريق إختراق المواقع الإلكترونية وتخريبها، وشن حرب معلوماتية وتجسسية ضد الخصم، في هذه الحالة الصراع يكون قائم

[1]. يحي الحياني، وآخرون، مرجع سابق، ص 52.
[2]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 491.
[3]. نفس المرجع، ص 492.

في الجانبين، حرب إلكترونية مع حرب تقليدية تعبيرا عن حدة الصراع بين الطرفين أو قد تمهل لعمل عسكري، تستمد هذه الحرب السيبرانية شدتها من قوة أطرافها وعدم إرتباطها بعمل عسكري تقليدي خاصة في ظل تكلفة الحرب التقليدية، فتمويل حملة حربية كاملة عبر الإنترنت يوازي تكلفة دبابة واحدة. والحروب السيبرانية متوسطة الشدة استخدمت في هجمات حلف الناتوعام 1999 على يوغسلافيا، حيث تم تعطيل شبكات الإتصال للخصوم، وخلال الحرب بين لبنان وإسرائيل عام 2006، وبين روسيا وجورجيا عام 2008، وبين حماس وإسرائيل في عامي 2008 و2012[1] .

**ج ـ الحرب السيبرانية الساخنة**: هي حرب في الفضاء الإلكتروني فقط وغير متوازية مع الأعمال العسكرية التقليدية عكس النوع السابق. ينطوي هذا النمط من الحروب على السيطرة على البعد التكنولوجي في إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، مع اللجوء إلى الروبوتات الآلية في الحروب والطائرات بدون طيار مع تطوير قدرات مجال الدفاع والهجوم الإلكتروني والإستحواذ على القوة الإلكترونية .

هذه الحرب قائمة على الفضاء الإلكتروني وقيام الدول بتدريبات على توجيه ضربة أولية لأجهزة الكمبيوتر الخاصة بالعدو وإختراق العمليات العسكرية عالية التقنية، واستهداف الحياة المدنية والبنية التحتية المعلوماتية، وذلك لغرض الهيمنة الإلكترونية الواسعة وبشكل أسرع في حالة نشوب الحرب. وقد شهدت الأسلحة الإلكترونية تطورا أكبر في قدرتها على التأثير على الخصوم مثل أسلحة الميكروويف والهجمات الإلكترونية عبر الفيروسات، فقد شنت إسرائيل هجمات فيروس "ستاكسنت" ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة الأمريكية عام 2010، وكان قد تم تطوير هذا الفيروس وتجربته في إسرائيل خلال عام 2007[2] .

**رابعا: التصنيف الرابع**

تبنى آخرون تصنيفا آخر معتمدين على طبيعة الصراع السيبراني، فإذا كانت المواجهات العسكرية تدور في ثلاثة فضاءات؛ الجوية، البرية، البحرية، إلا أنه في عصر الإنترنت وشبكات المعلومات ظهر فضاء جديد هو الفضاء الإلكتروني، مما أدى إلى ظهور تطورات على أساليب القتال والهجوم والدفاع، ونتج عنه تغيرات على مستوى الأهداف الطروحة مع تغير طبيعة الأسلحة المستخدمة وقواعد الإشتباك المتبعة. وتختلف الحروب الإلكترونية وفقا لطبيعة الصراعات السيبرانية، وذلك على النحوالتالي :

[1]. نبيلة عبد الفتاح قشطي، المرجع سابق، ص 493.
[2]. نفس المرجع، ص 493.

**أ ـ صراع سيبراني ذو طبيعة سياسية**: هذا الصراع تحركه دوافع سياسية ويأخذ شكلا عسكريا، يتم فيه إستخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية، ويتضمن توظيف أسلحة إلكترونية من قبل الفاعلين داخل المجتمع المعلوماتي أو من خلال التعاون مع قوة أخرى لتحقيق أهداف سياسية[1] .

**ب ـ صراع سيبراني ذو طبيعة ناعمة**: هو صراع حول الحصول على المعلومات والتأثير على المشاعر والأفكار وشن حرب إعلامية ونفسية، ويتم من خلالها تسريب المعلومات واستخدامها عبر منصات إعلامية، مما يؤثر في طبيعة العلاقات الدولية كالدور الذي لعبه موقع "ويكيليكس" في الدبلوماسية الدولية[2].

**ج ـ صراع سيبراني على التقدم التكنولوجي**: هذا الصراع له طابع تنافسي حول الإستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الإقتصادية والعلمية، وقد يمتد إلى محاولة السيطرة على الإنترنت والطاقات وعناوين المواقع والتحكم بالمعلومات، وكذلك العمل على إختراق الأمن القومي للدول الأخرى بدون إستخدام الطائرات أوالمتفجرات أو حتى إنتهاك حدود هذه الدول كهجمات قراصنة الكمبيوتر، وتدمير مواقع التجسس، وهذا ما يؤدي إلى دمار الإقتصاد والبنية التحتية[3].

**د ـ صراع سيبراني على المعلومات والإستخبارات**: يعد الفضاء الإلكتروني بيئة مناسبة للصراعات المعلوماتية، حيث يسهم في دعم قوة الأجهزة الأمنية للدول أو حتى الجماعات المختلفة على تشكيل شبكة عالمية من العملاء، وبدون تورط مباشر، بالإضافة إلى رخص التكلفة وسهولة الإتصال وصعوبة الرقابة التقليدية على التفاعلات الإلكترونية، وهذا يمثل عنصر جذب لإستخدام الأسلحة الإلكترونية وتوظيفها لتحقيق أهداف سياسية وعسكرية[4].

من خلال هذا التصنيف نكون قد وصلنا إلى ثلاثة أهداف أساسية للحرب السيبرانية، وهي كالآتي :

1ـ جمع المعلومات الإستخباراتية من بيانات العدو وشبكاته حول خططه وكيفية إنتشاره، وما ينوي القيام به.

2ـ الدفاع وحماية البيانات الإلكترونية والشبكات الخاصة بالدول والوقوف دون التعرض لها أو إتلافها.

3ـ مهاجمة أنظمة كمبيوتر العدو وخاصة المرتبطة بالمؤسسات الحساسة والبنية التحتية، وضرب مراكز الإتصال لديه وجعله عاجزا، مما يؤدي إلى إضعاف قياداته السياسية والعسكرية .

---

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 493.
[2]. نفس المرجع، نفس الصفحة.
[3]. نفس المرجع، ص 494.
[4]. نفس المرجع، ص 495.

**الفرع الثاني: التمييز بين الحرب السيبرانية والحرب التقليدية**

يعد التمييز بين الحرب السيبرانية وغيرها من أنماط الحروب -لا سيما بالنسبة للحرب التقليدية- مسألة جوهرية لفهم الخصوصيات التي تنفرد بها الهجمات السيبرانية، سواء من حيث الوسائل المستخدمة أو طبيعة الأهداف أو البيئة أو الفاعلون والنتائج المترتبة عنها. وعليه فإن فهم أوجه الإختلاف بين الحرب السيبرانية والحرب التقليدية (أولا) والتداخل بينهما (ثانيا)، يكتسي أهمية خاصة في السياق القانوني والأمني على حد سواء. وهو ما سيتم توضيحه فيما يلي :

**أولا: أوجه الاختلاف بين الحرب السيبرانية والحرب التقليدية**

تختلف الحرب السيبرانية عن الحرب التقليدية في عدة جوانب؛ فبينما تعتمد الحرب التقليدية على إستخدام الأسلحة المادية والوجود الملموس للقوات المسلحة على الأرض، تتميز الحرب السيبرانية بكونها تنفذ عبر الفضاء الرقمي، مما يجعل تحديد الأطراف المتورطة والمسؤوليات القانونية أكثر تعقيدا، علاوة على ذلك فإن الهجمات السيبرانية قد تستهدف البنية التحتية الحيوية مثل شبكات الكهرباء والماء والمستشفيات، مما يسبب أضرارا جسيمة للمدنيين دون أن تترك آثارا مادية واضحة.

من جهة أخرى فإن الحروب التقليدية تخضع لقواعد القانون الدولي الإنساني بشكل أكثر وضوحا، حيث تحدد الأهداف العسكرية وتحظر الهجمات على المدنيين، أما في الحرب السيبرانية فإن تطبيق هذه القواعد يصبح أكثر تحديا نظرا للطبيعة غير الملموسة للهجمات وصعوبة تحديد المسؤولية، لذلك يعتبر التمييز بين الأهداف العسكرية والمدنية في الهجمات السيبرانية أمر بالغ الأهمية لضمان الإمتثال للقانون الدولي الإنساني[1].

والجدول التالي يوضح الفرق بين الحرب السيبرانية وغيرها من الحروب:

[1]. اللجنة الدولية للصليب الأحمر، **الحرب السيبرانية والقانون الدولي الإنساني: التمييز بين الحروب السيبرانية وغيرها**، على الرابط: https://www.icrc.org/ar/document/cyber-and-international-humanitarian-law ، تاريخ الاطلاع: 12-03-2025. وقت الإطلاع: 14:30.

**جدول رقم (02): الفرق بين الحرب السيبرانية وغيرها من الحروب**

| | الحروب الهجينة[1] | الحرب التقليدية | الحرب السيبرانية |
|---|---|---|---|
| **البيئة** | مزيج بين البيئة الرقمية والفيزيائية | الأرض،البحر،الجو، الفضاء الخارجي | الفضاء الإلكتروني (الشبكات والأنظمة الرقمية) |
| **الأدوات** | مزيج بين الأسلحة التقليدية والبرمجيات | الأسلحة التقليدية (مدافع، دبابات، طائرات) | البرمجيات الخبيثة، الفيروسات، الذكاء الإصطناعي |
| **الفاعلون** | دول، ميليشيات، مجموعة قرصنة | دول ذات سيادة، جيوش نظامية | دول، جماعات منظمة، قراصنة، مستقلون |
| **الأهداف** | كلا النوعين: المادية والسيبرانية | أهداف مادية مثل:المعسكرات والمدن | الأنظمة الرقمية، البنية التحتية الحيوية |
| **القانون المنظم** | مزيج من القوانين التقليدية والسيبرانية | قوانين الحرب التقليدية، إتفاقيات جنيف | القانون الدولي الإنساني مع تحديات التطبيق |
| **التأثير** | مزدوج (سيبراني، مادي ) | مادي ومباشر مع تأثير ملموس | سريع واسع النطاق مع إمكانيات خفيفة |

**المصدر:** من إعداد الطالبتين اعتمادا على ما سبق

**ثانيا: أوجه التداخل بين الحرب السيبرانية والحرب التقليدية**

رغم اعتبار الحرب السيبرانية شكلا حديثا من أشكال النزاعات المسلحة، إلا أنها لا تشكل قطيعة مع أنماط الحروب التقليدية، بل تمثل إمتدادا وتطورا لها في ضوء التقدم التكنولوجي، فالحروب على إختلاف أشكالها، تشترك في أهدافها الإستراتيجية مثل التأثير على الخصم، وتحقيق مكاسب سياسية وإقتصادية وعسكرية وفرض الإرادة. ومن هذا المنطق يمكن النظر إلى الحرب السيبرانية على أنها جزء من منظومة الحروب المعاصرة، حيث تتكامل أدواتها مع أدوات الحروب التقليدية والحديثة. وهوما سنبرزه فيما يلي:

**أ- تكامل الحرب السيبرانية مع الحرب التقليدية:** أصبحت الحروب السيبرانية جزء لا يتجزأ من الحروب التقليدية، فعلى سبيل المثال تستخدم الدول الهجمات السيبرانية لتعطيل أنظمة الدفاع الجوي قبل شن ضربات عسكرية تقليدية .

**ب- الحرب السيبرانية كبديل للحرب التقليدية:** بعض الدول تفضل إستخدام الهجمات السيبرانية بدلا من المواجهة المباشرة، لأنها أكثر إقتصادية وأقل خطورة .

**ج- الحرب السيبرانية كأداة للصراع الطويل الأمد:** تستخدم الدول الكبرى العمليات السيبرانية لتقويض إقتصادات الدول المنافسة، والتأثير على إستقرارها السياسي بدون إعلان حرب صريح.

[1]. الحروب الهجينة هي مزيج بين الحرب التقليدية والحرب السيبرانية.

## المبحث الثاني: الإطار النظري للقانون الدولي الإنساني

يعدّ القانون الدولي الإنساني أحد الفروع الأساسية للقانون الدولي العام، وقد تطور ليشكل الإطار القانوني الذي ينظم سلوك الأفراد المتنازعة أثناء النزاعات المسلحة، بهدف الحد من آثار الحرب على الإنسان والبيئة، ويكتسي هذا الفرع من القانون طابعا إنسانيا فريدا من نوعه، إذ يرتكز على حماية الأشخاص الذين لا يشاركون مباشرة في العمليات القتالية، وكذلك على تنظيم الوسائل والأساليب المستخدمة في النزاعات.

يستمد القانون الدولي الإنساني مشروعيته من مجموعة من الإتفاقيات والأعراف الدولية وقد شهد مسار تطوره ونشأته تفاعلا مستمرا مع التحولات التي عرفها المجتمع الدولي، وهو يرتكزعلى مجموعة من الخصائص والمبادئ التي تميزه عن غيره من فروع القانون الدولي العام.

على ضوء ما سبق سنتناول في هذا المبحث ثلاثة مطالب؛ حيث نتطرق في المطلب الأول لمفهوم القانون الدولي الإنساني وفي المطلب الثاني لمصادرالقانون الدولي الإنساني وفي المطلب الثالث لخصائص ومبادئ القانون الدولي الإنساني .

### المطلب الأول: مفهوم القانون الدولي الإنساني

نتناول في هذا المطلب التعاريف المختلفة التي وردت بشأن القانون الدولي الإنساني في الفرع الأول، وبعدها نتطرق لنشأته وتطوره التاريخي في الفرع الثاني .

#### الفرع الأول: تعريف القانون الدولي الإنساني

يعرف القانون الدولي الإنساني بـأنه: "مجموعة القواعد القانونية الإنسانية التي تطبق في النزاعات المسلحة وتهدف إلى حماية الأشخاص والأموال"[1].

كما أنه يوجد إتجاهان في تحديد ماهية القانون الدولي الإنساني، حيث يتسم الإتجاه الأول بأنه واسع، بينما يتسم الإتجاه الثاني بأنه ضيّق كثيرا من مفهوم القانون الدولي الإنساني :

[1]. سهيل حسين الفتلاوي وعماد محمد ربيع، **موسوعة القانون الدولي 5، القانون الدولي الإنساني**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص 20.

**أولا: الإتجاه الواسع في تعريف القانون الدولي الإنساني**

يذهب جانب من الفقه إلى تعريف القانون الدولي الإنساني تعريفا موسعا بأنه: "ذلك القسم من القانون الذي تسوده المشاعر الإنسانية ويهدف لحماية الإنسان"[1]. وهذا التعريف شامل وواسع ضم القواعد القانونية الدولية المكتوبة والعرفية، والتي تهدف إلى إحترام الإنسان والحفاظ عليه، وعلى سلامته الجسدية والنفسية. هذا التعريف وجهت له العديد من الإنتقادات منها :

أ- هذا التعريف الواسع أدى إلى التداخل بين القانون الدولي الإنساني وحقوق الإنسان، وبالتالي الوقوع في خلط بين هذا القانون والنظم القانونية الوطنية للدول،و لم يحدد زمن تطبيقه، كما قصر الحماية على الأفراد دون الممتلكات مع العلم أن هذه لأخيرة عرضة للإعتداء أيضا[2].

ب- هذا التعريف يدمج قواعد وقوانين الحرب داخل القانون الدولي الإنساني وهذا غير صحيح، لأن هناك العديد من القواعد لا تتصل بحماية الإنسان، ولكن تنظم العمليات الحربية.

**ثانيا: الإتجاه الضيق في تعريف القانون الدولي الإنساني**

أنصار هذا الاتجاه يضيّقون من مفهوم القانون الدولي الإنساني، حيث يرون أنه عبارة عن " قوانين أو لوائح جنيف التي تهتم بحماية العسكريين من غير المقاتلين، أو من خارج العمليات العسكرية مثل الجرحى والمرضى وأسرى الحرب، والتي تهتم كذلك بالمدنيين وإبقائهم خارج حدود العمليات العسكرية"[3].

وجهت أيضا العديد من الانتقادات لهذا التعريف الضيق للقانون الدولي الإنساني منها :

أ ـ هذا التعريف أغفل جانبا مهما من القانون، والمتمثل في تنظيم وسائل وأساليب القتال، وهي الوظيفة التي تجسدها بوضوح "قوانين لاهاي"، والتي تعدّ مكملة لإتفاقيات جنيف، حيث تنظم إستخدام الأسلحة وتكتيكات الهجوم، ومبدأ التمييز بين الأهداف العسكرية والمدنية، وبهذا التعريف يفقد القانون الدولي الإنساني توازنه بين الحماية الإنسانية من جهة والقيود المفروضة على أطراف النزاع من جهة أخرى .

ب ـ التعريف المذكور لا يراعي تطور القانون الدولي الإنساني بعد إتفاقيات جنيف لعام 1949، خاصة في ظل البروتوكولين الإضافيين لعام 1977، واللذين وسعا نطاق الحماية لتشمل النزاعات غير الدولية،

---

[1]. منتصر سعيد حمودة، **القانون الدولي الإنساني مع الإشارة إلى أهم مبادئه في الفقه الإسلامي**، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 54.

[2]. فاطمة بابا، **القانون الدولي الإنساني بين النص و الواقع**، رسالة ماجستير، العلوم القانونية و الإدارية ،كلية الحقوق، جامعة يحي فارس بالمدية، الجزائر،2009/2008، ص 7.

[3]. منتصر سعيد حمودة،مرجع سابق، ص 55.

حيث غطيا فئات جديدة كحركات التحرر الوطني والمقاتلين غير النظاميين، وبالتالي هذا التعريف لا يمكّن من الإلمام الكامل بطبيعة القانون الدولي الإنساني، ولا يراعي عناصره الثلاثة الأساسية وهي حماية الأشخاص، تنظيم أساليب ووسائل القتال، تطبيقه في النزاعات الدولية وغير الدولية[1].

هذا وقد عرفت اللجنة الدولية للصليب الأحمر القانون الدولي الإنساني بأنه: "مجموعة القواعد الإتفاقية أو العرفية المنشأة، التي تستهدف على وجه التحديد تسوية المشكلات الإنسانية المترتبة مباشرة عن النزاعات المسلحة الدولية أو غير الدولية، والتي تقيد لأسباب إنسانية حق أطراف النزاع في إستخدام سبل ووسائل الحرب محل إختيارها، والتي تحمي الممتلكات والأشخاص المتضررين أو المحتمل تضررهم من النزاع"[2].

وبالتالي فإنّ اللجنة الدولية للصليب الأحمر حددت مجالين رئيسيين يتناولهما القانون الدولي الإنساني هما؛ حماية الأشخاص الذين لم يشاركوا في الأعمال العدائية، وكذلك القيود المفروضة على أساليب ووسائل الحرب، وهو ما يعني أنّ هذا التعريف جمع ما بين قانون جنيف وقانون لاهاي.

محكمة العدل الدولية أيضا عرفت القانون الدولي الإنساني معتمدة على قانون لاهاي من جهة والقوانين الواردة في إتفاقيات جنيف الأربعة والبروتوكولين من جهة أخرى، حيث أكدت أنّ العلاقة بين القانونين المذكورين تطورت إلى درجة الإتحاد، وشكّلا نظاما واحدا يعرف بـ"القانون الدولي الإنساني"، وهذا ما أكدته في رأيها الإستشاري المتعلق بمسألة التعرف إذا ما كان اللجوء إلى الأسلحة النووية يعتبر غير شرعي وفقا لمبادئ وقواعد القانون الدولي الإنساني المطبق في النزاعات المسلحة أم لا[3].

إن الفتوى الصادرة عن محكمة العدل الدولية بتاريخ 1996/07/08 بشأن مشروعية التهديد بالأسلحة النووية أو إستخدامها، تعتبرالمرة الأولى التي يصل فيها قضاة المحكمة إلى تحليل قواعد القانون الدولي الإنساني بقدر من التفصيل، وهذا بسبب طلب الإفتاء الذي طرحته الجمعية العامة للأمم المتحدة على المحكمة في 1994/12/15 حول "هل يرخص وفقا للقانون الدولي التهديد بإستخدام الأسلحة النووية أو إستخدامها في جميع الأحوال"، ثم أصدرت المحكمة رأيها الإستشاري في

[1]. منتصر سعيد حمودة،مرجع سابق، ص 56.
[2]. رشيدة مصباح، **محاضرات في القانون الدولي الإنساني و مسؤولية الحماية**، قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم حقوق، جامعة الدكتوريحي فارس، المدية ،الجزائر، 2020/2019، ص16.
[3]. أمينة بن حوة ، **محاضرات في القانون الدولي الإنساني**، قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم حقوق، جامعة البليدة 2، 2024/2023، ص15.

1996/07/08، وذلك بعد فترة من المناقشات والدراسات، وقد رأت المحكمة أنّ قانون النزاعات المسلحة يقوم على مبدأين هما[1] :

1- حماية السكان المدنيين والأعيان المدنية.

2- حظر الإضرار بهم دون مبرر.بالنسبة للأمم المتحدة لم تقدم تعريفا موحدا رسميا للقانون الدولي الإنساني في صك قانوني واحد، لكنها تعتمد تعريفا عمليا متداولا في وثائقها الرسمية وتصريح هيئاتها، يمكن الإستناد إليه كتعريف معتمد، ورد في مصادر تابعة للأمم المتحدة ما يلي: "القانون الدولي الإنساني هو مجموعة القواعد التي تسعى لأسباب إنسانية إلى الحد من آثار النزاع المسلح، ويحمي الأشخاص الذين لا يشاركون أو لم يعودوا يشاركون في القتال، ويقيد وسائل وأساليب الحرب"[2].

مهما تعددت تعاريف القانون الدولي الإنساني، إلا أنها تجمع على أنه فرع من فروع القانون الدولي العام، هدفه حماية المدنيين والمقاتلين في الحالات المنصوص عليها قانونا، والحد من آثار الحرب على الإنسان والممتلكات من خلال تنظيم وسائل وأساليب الحرب مع الحفاظ على التوازن بين الضرورات العسكرية والمبادئ الانسانية .

**الفرع الثاني: نشأة وتطور القانون الدولي الإنساني**

ترجع الجذور الأولى للقانون الدولي الإنساني إلى العصور القديمة، حيث وجدت بعض الأعراف والقواعد التي تحكم سلوك المحاربين وتحمي الأسرى والجرحى و الممتلكات ،وهذا بهدف حفظ كرامة المدنيين و التقليل من الخسائر.

**أولا: نشأة القانون الدولي الإنساني**

مر القانون الدولي الإنساني بعدة مراحل تاريخية أثناء تطوره مواكبة لتطور حياة الإنسان فكريا و علميا، ومن الأمثلة على ذلك :

**أ ـ حضارات الشرق القديم:** مثل قانون حمورابي في بابل، الذي إحتوى على أحكام تتعلق بالأسرى.

**ب ـ القانون الروماني:** عرف بعض القواعد التي تحكم العلاقات مع العدو وتحد من إستعمال العنف غير المبرر.

---

[1]. أمينة بن حوة ، مرجع سابق، ص15.

[2]. الأمم المتحدة، مكتب تنسيق الشؤون الإنسانية، **ماهو القانون الإنساني الدولي؟**، على الرابط: https://www.unocha.org/story/what-international-humanitarian-law، تاريخ الاطلاع: 2025/03/04. وقت الإطلاع: 14:30.

**ج ـ الحضارة الإسلامية:** الإسلام قد عرف مفهوم القانون الدولي الإنساني منذ أكثر من ألف وأربعمائة سنة، وقد أسهم في إرساء قواعد إنسانية للحرب كتحريم قتل غير المقاتلين، وإحترام الأسرى، ومنع التنكيل بالجثث، وعدم تخريب الممتلكات، وتحريم حرق الزرع والحيوانات.

**د- عصر النهضة:** في عصر النهضة الأوربية نادى الكثير من المفكرين بضرورة التقليل من آثار الحرب وصاغوا مذهبا إنسانيا أساسيا نادى بأن تقتصر الحرب على المقاتلين دون الإضرار بالمدنيين والممتلكات التي ليس لها طابع عسكري، وكان من أهم واضعي هذا المفهوم "جون جاك روسو" في فصل من فصول العقد الإجتماعي، و"ايمريك دي فاتيل" الذي تناول على نحو أكثر تحديدا لمشاكل قانون الحرب في كتابه "قانون الشعوب"، وكان الأول من سكان جنيف والثاني من سكان نوشاتيل، عاشا في عصر لم تكن منطقة المنشأ بالنسبة لهما جزءا من الإتحاد الفيدرالي السويسري، وقد انضمت إليه فيما بعد، وأسهمتا في إنشاء سويسرا الرومانديةـ وهكذا حدث أن صيغ القانون الدولي الإنساني في جنيف بصياغة خاصة، ومنها انتشر في بلدان العالم جميعها، مما أدى إلى تسميته بـ "قانون جنيف"، وهي التسمية المستخدمة بصورة عامة[1].

يلاحظ أنّ هذه الأفكار لا ترقى إلى مستوى الإلتزام الدولي، لأن العلاقات الدولية لا يحددها المفكرون، إنما تحددها تصرفات الدول، وهذا يعني أنّ المجتمع الأوروبي كان يستخدم الحرب التدميرية، التي تهدف إلى إبادة الطرف الآخر من العسكريين والمدنيين على حد سواء.

ظهر القانون الدولي الإنساني بصورته الحديثة خلال القرن التاسع عشر مع إعتماد إتفاقية جنيف الأولى لعام 1864 بفضل جهود الناشط الإنساني "هنري دونان"، الذي تأثر بفضائع معركة سولفرينو سنة 1859، ومنذ ذلك الحين تطور هذا القانون ليشمل حماية أوسع للأشخاص والأعيان خلال النزاعات المسلحة[2] .

**ثانيا: تطور القانون الدولي الإنساني**

لعبت اللجنة الدولية للصليب الأحمر دورا هاما في تطوير قواعد القانون الدولي الإنساني، بالإضافة إلى المنظمات المتخصصة في متابعة حقوق الإنسان، التي أصدرت العديد من البيانات عن إنتهاكات القانون الدولي الإنساني، ومن هذه المنظمات منظمة العفو الدولية ومنظمة هيومن رايتس ووتش، وغيرها من المنظمات الإنسانية .

تتمثّل أهم محطات تطور القانون الدولي الإنساني في إعتماد العديد من الاتفاقيات مثل :

[1]. سهيل حسين الفتلاوي وعماد محمد ربيع، مرجع سابق، ص 46.
[2]. نفس المرجع، نفس الصفحة.

1 ـ إتفاقية لاهاي لعامي 1899 و1907 .

2 ـ إتفاقيات جنيف الأربعة 1949 .

3 ـ البروتوكولين الإضافيين لاتفاقيات جنيف الأربعة لعام 1977 .

4 ـ البروتوكول الإضافي الثالث لعام 2005 .

5 ـ تطور القانون العرفي عبر الممارسة الدولية .

6 ـ إدراج قواعد القانون الدولي الإنساني ضمن أنظمة المحاكم الجنائية الدولية مثل: المحكمة الجنائية الدولية ليوغسلافيا سابقا ورواندا، وأخيرا في نظام المحكمة الجنائية الدولية .

خلاصة القول أنّ القانون الدولي الإنساني هو قانون يطبق وقت النزاعات المسلحة أو ما يسمى بـ "قانون جنيف"، وقواعده خاصة بأساليب القتال أوما يسمى بـ "قانون لاهاي"، وهما القانونان اللذان دمجا وتم تحديثهما بـ "البروتوكولين الإضافيين" لعام 1977 واللذان بدأ العمل بهما عام 1978، ولا يزال هذا القانون في تطور، يحتاج إلى قواعد جديدة وآليات لتضمن تطبيقه من طرف جميع الدول.

**المطلب الثاني: مصادر القانون الدولي الإنساني**

يقوم القانون الدولي الإنساني، كغيره من فروع القانون الدولي على جملة من المصادر التي يستمد منها قواعده ومبادئه. تنقسم هذه المصادر إلى مصادر أصلية نتناولها في الفرع الأول، وهي تتمثل أساسا في المعاهدات الدولية، العرف الدولي والمبادئ العامة للقانون، وأخرى إحتياطية نتناولها في الفرع الثاني كأحكام القضاء الدولي وقرارات المنظمات الدولية والفقه الدولي، هذه المصادر هي الإطار القانوني الذي يضبط سلوك أطراف النزاع.

**الفرع الأول: المصادر الأصلية للقانون الدولي الإنساني**

من خلال إستقراء نص المادة 38 من النظام الأساسي لمحكمة العدل الدولية[1]، نجد أنه حدد المصادر الأصلية للقانون الدولي والتي تعتبر ملزمة، وهي: المعاهدات الدولية، العرف الدولي، والمبادئ العامة للقانون. وبإعتبار أنّ القانون الدولي الإنساني فرع من فروع من القانون الدولي العام، فإنّ له نفس المصادر .

كما حددت المادة 21 من النظام الأساسي للمحكمة الجنائية الدولية[2] القانون الواجب التطبيق عند نظر المنازعات أمامها، فقط أن هذه المادة أوردت مصادر القانون الدولي الإنساني التي تطبقها المحكمة بشكل مختلف عن مصادر القانون الدولي العام الواردة في النظام الأساسي لمحكمة العدل الدولية، ولم

[1]. راجع المادة 38 من النظام الأساسي لمحكمة العدل الدولية.
[2]. راجع المادة 21 من النظام الأساسي للمحكمة الجنائية الدولية.

تنص على العرف كمصدر من مصادر القانون الدولي الإنساني، بإعتبار أنّ دول العالم توجب على المحاكم الجنائية عدم الحكم بالعرف .

على ضوء المادتين المذكورتين، نتناول فيما يلي المصادر الأصلية للقانون الدولي الإنساني:

**أولا: المعاهدات**

هناك العديد من الاتفاقيات التي يستمد منها القانون الدولي الإنساني أحكامه، نذكر أهمها :

**أ ـ اتفاقيات لاهاي لعامي 1899 و1907:** تعد هذه الاتفاقيات من أقدم الوثائق القانونية التي سعت إلى تقنين الحرب في إطار القانون الدولي، وقد مهدتا الطريق لتطوير لاحق أكثر عمقا وشمولية كما في إتفاقيات جنيف، فقد تناولتا الجوانب الأساسية لسير العمليات القتالية، وحقوق وواجبات المقاتلين، وحماية السكان المدنيين والدول المحايدة، هذه الإتفاقيات بدورها انطوت على العديد من الإتفاقيات نذكرها على النحو التالي:

**1ـ إتفاقيات لاهاي لعام 1899**: تم توقيعها في 1899/07/20، خلال مؤتمر السلام الأول في لاهاي بمشاركة 26 دولة، وكانت تهدف إلى وَضع قواعد إنسانية لحماية ضحايا النزاعات المسلحة، تضمنت ثلاث إتفاقيات رئيسية هي: إتفاقية تسوية المنازعات الدولية بالطرق السلمية، إتفاقية قوانين وأعراف الحرب البرية وإتفاقية حظر إستخدام بعض الأسلحة[1].

**2 ـ إتفاقيات لاهاي لعام 1907**: تم توقيعها في 1907/10/18 خلال مؤتمر السلام الثاني بمشاركة أوسع (44 دولة) ووسعت نطاق الإتفاقيات السابقة، ضمت 13 إتفاقية، أبرزها الإتفاقية الرابعة التي تناولت أعراف وقوانين الحرب البرية وهي تعتبر تطوير لإتفاقيات 1899[2].

**ب ـ إتفاقيات جنيف:** تمثلت اتفاقيات جنيف في عدة اتفاقيات، تتمثل فيما يلي:

**1ـ إتفاقية جنيف لعام 1864 المتعلقة بتحسين حالة الجرحى العسكريين في الميدان**: وقد أبرمت إتفاقية أخرى بغرض تعديلها وتطوير أحكامها في سنة 1906، خاصة بتحسين حال الجرحى والمرضى العسكريين في الميدان، وتكرس أحكامها تعديل وتطوير أحكام إتفاقية عام 1864، حيث شملت في مجال الحماية طائفة جديدة من ضحايا النزاعات المسلحة وهي طائفة المرضى[3].

[1]. فاطمة بابا، مرجع سابق، ص 44.
[2].نفس المرجع، ص 45.
[3]. نفس المرجع ، ص 46.

**2- إتفاقية جنيف لمعاملة أسرى الحرب لعام 1929**: تناولت هذه الإتفاقية كل ما يخص الأسير، وكان لها دورمهم في معالجة أسرى الحرب العالمية الثانية، تضم هذه الاتفاقية 39 مادة، وهي بمثابة صيغة جديدة لإتفاقية 1906 المذكورة سابقا[1].

**3- إتفاقيات جنيف الأربع لعام 1949**: أبرمت بتاريخ 1949/08/12، وقد دعت إلى تنظيمها سويسرا خلال الحرب العالمية الثانية، وهي الركيزة الأساسية للقانون الدولي الإنساني، تتكون من أربعة إتفاقيات، وثلاث بروتوكولات ملحقة بها، ومن خلالها تم التوصل إلى الإتفاقيات المعمول بها حاليا في النزاعات المسلحة والمتمثلة في :

**1-3. إتفاقية جنيف الأولى**: هي إتفاقية خاصة بتحسين حالة الجرحى والمرضى في القوات المسلحة، وقد تم من خلالها تعديل وتطوير أحكام إتفاقية جنيف لعام 1929[2] .

**2-3. إتفاقية جنيف الثانية**: تتعلق بحالة الجرحى والمرضى والغرقى من أفراد القوات المسلحة في البحار، وقد جاءت لتعديل وتطوير أحكام وقواعد إتفاقيات لاهاي لعام 1907[3].

**3-3. إتفاقية جنيف الثالثة**: وهي إتفاقية جاءت لتحسين حالة أسرى الحرب، وقد تضمنت تعديلا لأحكام إتفاقية جنيف الثانية لعام 1929[4].

**4-3. إتفاقية جنيف الرابعة**: المتعلقة بحماية المدنيين أثناء النزاعات المسلحة، وقد جاءت لحفظ الحد الأدنى من الحقوق لضحايا النزاعات المسلحة غير الدولية، ونظرا لكون هذه الإتفاقية غير كافية دعمت بالبروتوكول الإضافي الثاني لعام 1977[5].

**3-5- البروتوكول الإضافي الأول لعام 1977**: تم إعتماده في 1977/06/08، هدفه الحفاظ على حقوق ضحايا النزاعات المسلحة، واعتبر حروب التحرير نزاعات دولية مسلحة، كما وسع مجال الحماية القانونية للوحدات الصحية وأعوان الخدمات الطبية المدنية

**5- البروتوكول الإضافي الثاني لعام 1977**: اعتمد في 1977/06/08، هدفه حماية ضحايا النزاعات المسلحة غير الدولية، وقد أقر مبدأ عدم التدخل في الشؤون الداخلية للدولة، حتى لا يكون القانون الدولي الإنساني حجة للتدخل في الشؤون الداخلية للدولة.

---

[1]. فاطمة بابا، مرجع سابق، ص47

[2]. منتصر سعيد حمودة، نفس المرجع، ص 93 .

[3]. نفس المرجع، ص 97 .

[4]. راجع كتاب موسوعة القانون الدولي 5، القانون الدولي الإنساني، ص ص 259 -266

[5]. راجع كتاب القانون الدولي الإنساني مع الإشارة إلى أهم مبادئه في الفقه الإسلامي، ص ص 110 - 126 .

**6- البروتوكول الإضافي الثالث لعام 2005**: اعتمد في ديسمبر 2005، وقد عمل هذا البروتوكول على وضع شارة جديدية[1] تسمى شارة البروتوكول الثالث، كما أضافت المادة الثالثة من هذا البروتوكول بعدا جديدا، إذ يجوز للدول الأطراف أن تضع إحدى الشارات الدولية أو شارتها الوطنية داخل هذه الشارة، ولا تختلف شروط إستعمالها وإحترامها عن الشروط التي تطبق على الشارات الأخرى التي أقرتها الإتفاقيات السابقة والبروتوكولين الإضافيين[2].

**ثانيا: العرف الدولي**

إنّ المصدر الثاني من مصادر القانون الدولي الإنساني هو العرف الدولي، والعرف هو: "عبارة عن مجموعة من القواعد القانونية التي تنشأ في المجتمع الدولي بسبب تكرار الدول لها لمدة طويلة، وبسبب التزام الدول بها في تصرفاتها، وإعتقادها بأن هذه القواعد تتصف بالإلتزام القانوني"[3]، وهو ما يعني ضرورة توافر ركني العرف الدولي (المادي والمعنوي)، لكي تنشأ القاعدة القانونية الدولية العرفية.

يعتبر العرف الدولي مصدرا أساسيا للقانون الدولي الإنساني، ذلك أنّ معظم قواعده القانونية أنشأت عن طريق الأعراف الدولية، وهذا ما أكدته قاعدة مارتنز التي وضعها "فريدريك دي مارتينز" في إتفاقية لاهاي الثانية الخاصة بالحرب البرية لعام 1899 في الفقرة الثالثة من المقدمة، وذكرت نفس القاعدة في إتفاقية لاهاي الرابعة الخاصة بالحرب البرية لعام 1907 في الفقرة السابعة من المقدمة، مفاد هذه القاعدة هو أنه: "في الحالات التي لا تشملها أحكام الإتفاقية التي يتم عقدها، يظل السكان المدنيون والمقاتلون تحت حماية وسلطان مبادئ قانون الأمم المتحدة، كما جاء في الأعراف التي إستقر عليها الحال بين الشعوب المتمدنة والقوانين الإنسانية ومقتضيات الضمير العام"[4] .

إذن العرف الدولي مهم جدا فهو يسد الثغرات القانونية ويعوض عدم تطبيق بعض المعاهدات المكتوبة، كما أن قواعد لاهاي مصدرها العرف، وهي ملزمة لجميع الدول بغض النظر عن قبولها أو عدم قبولها، كما أن إتفاقيات جنيف والبروتوكولات الملحقة بها جزء من القانون الدولي العرفي وتطبق في أي نزاع مسلح.

---

[1]. هي الكريستالة الحمراء إلى جانب شارتي الصليب والهلال الأحمر، هذه الشارة عبارة عن مربع أحمر قائم على رقعة بيضاء.

[2]. اللجنة الدولية للصليب الأحمر،البروتوكول الإضافي الثالث، على الرابط:
https:llihl-databases.icrc.orglassetsl2023-10lapiii-AR .PDF ، تاريخ الاطلاع: 2025/03/10، وقت الإطلاع: 13:00.

[3]. عمر سعد الله، **قراءة حديثة للقانون الدولي الإنساني**، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص 165 - 166.

[4]. محمد المجذوب، القانون الدولي العام، الطبعة 5، منشورات الحلبي الحقوقية، بيروت، لبنان، 2004، ص 117. و ذات المبدأ ورد في البروتوكول الإضافي الأول لسنة 1977 في نص الفقرة الثانية من المادة الأولى، والذي سيتم التفصيل فيه نهاية هذا المبحث الثاني.

**ثالثا: المبادى العامة للقانون**

النظام الأساسي لمحكمة العدل الدولية استخدم عبارة "مبادئ القانون العامة" في الفقرة (ج) من المادة 38 كمصدر ثالث للقانون الدولي العام الذي تطبقه المحكمة للفصل في القضايا، كما أن البروتوكول الإضافي الأول لعام 1977 (اللائحة التمهيدية لإتفاقيات جنيف) أقر هذه المبادئ العامة في الفقرة الثانية من المادة الأولى التي تنص على أنه: "يظل المدنيون و المقاتلون في الحالات التي لا ينص عليها هذا اللحق "البروتوكول" أو أي إتفاق دولي آخر، تحت حماية و سلطان مبادئ القانون الدولي كما استقر بها العرف و مبادئ الإنسانية و ما يمليه الضمير العام"[1].

تعرف المبادئ العامة للقانون بـأنها: "مجموعة القواعد المشتركة في الأنظمة الدولية المتطورة، حيث يمكن لأي دولة في غياب الإتفاقيات والمعاهدات الدولية والأعراف الدولية أن تستند إلى المبادئ العامة لإيجاد حلول للخلافات الدولية المطروحة"[2].

المبادى العامة للقانون هي مجموعة من المبادئ الأساسية التي يقوم عليها القانون الدولي الإنساني، يمكن حصرها في مبادئ قانون لاهاي وقانون جنيف، هذه المبادئ يشترك فيها كل من القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان وهي تشمل: مبدأ التناسب، مبدأ الإنسانية، مبدأ التمييز بين الأهداف العسكرية والمدنية، مبدأ الإحتياط، مبدأ الضرورة العسكرية، مبدأ الحياد، مبدأ الحماية الخاصة.

المبادئ العامة للقانون يمكن أن تشكل مرجعا قانونيا لسد الثغرات في النظام القانوني الدولي ولاسيما في حالات الإنتهاكات الجسيمة التي تمس قواعد القانون الدولي الإنساني، حتى في غياب نصوص إتفاقية صريحة .

**الفرع الثاني: المصادر الإحتياطية للقانون الدولي الإنساني**

إحتياطيا يمكن أن يستمد القانون الدولي الإنساني أحكامه من أحكام القضاء الدولي أو من قرارات المنظمات الدولية أو من الفقه، وهو ما سيتم توضيحه فيما يلي :

[1]. المادة 2/1 من البروتوكول الإضافي الأول لعام 1977.
[2]. أمينة بن حوة ، مرجع سابق، ص 75.

**أولا: أحكام القضاء الدولي**

يقصد بأحكام القضاء الدولي مجموعة الأحكام والأوامر التي تصدر عن الجهات القضائية الدولية المتخصصة بالفصل في قضايا الجرائم الدولية[1].

يرى المختصون في القانون الدولي العام، أنّ أحكام محكمة العدل الدولية بمثابة إيضاح لقواعد القانون الدولي الإنساني، بسبب صدورها من أعلى هيئة قضائية دولية، تبين مدلول تلك القواعد وتحدد مدى تطبيقها في مسائل معينة[2].

وهناك العديد من المحاكم الجنائية الدولية التي ساهمت في تطوير بعض قواعد القانون الدولي الإنساني، عن طريق الأحكام التي أصدرتها، مثل: محكمتي نورمبورغ وطوكيو، المحكمة الجنائية الدولية الخاصة ليوغسلافيا سابقا والمحكمة المشكلة بموجب معاهدة روما عام 1998، وقد أرست هذه المحاكم قواعد مهمة في المسؤولية الجنائية الفردية الإنسانية، وأدخلت قواعد جديدة إلى القانون الدولي تقوم على أساس محاكمة الأفراد الطبيعيين[3].

**ثانيا: قرارات المنظمات الدولية**

إن المنظمات الدولية تعمل على إرساء قواعد القانون الدولي، وذلك عن طريق إتخاذ القرارات، وقد نشأ خلاف حول كون قرارات المنظمات الدولية مصدر للقانون الدولي، وذلك بإعتبار أنّ هذه القرارات لم يتضمنها نص المادة 38 السابق الذكر.

أغلب الفقهاء اعتبروا إغفال هذه المادة عن ذكر هذا المصدر لا يعني عدم إعتباره من المصادر الإحتياطية للقانون الدولي الإنساني، لأن المادة لم تحدد المصادر على وجه التخصيص، ولكن ليس كل ما تصدره المنظمات الدولية يساهم في إنشاء قاعدة قانونية، فالأمر يقتصر على القرارات التي تتمتع بطابع الإلزام على وجه عام، مثل قرارات منظمة الأمم المتحدة وقرارات منظمة الصحة العالمية[4].

هذا وتعمل المنظمات الدولية على إنشاء قواعد القانون الدولي الإنساني بعدة طرق؛ مثل إصدار قرارات متالية، مما يؤدي إلى تكوين العرف الدولي والذي يعتبر من المصادر الأساسية للقانون الدولي،

---

[1]. أمينة بن حوة ، المرجع سابق، ص 75.

[2]. سهيل حسين الفتلاوي وعماد محمد ربيع، مرجع سابق، ص 37. ومثال ذلك الحكم الصادر عن محكمة العدل الدولية عام 1949، بخصوص عدم شرعية المستوطنات الصهيونية في الأراضي الفلسطينية المحتلة، وذلك إستنادا وتفسيرا للمادة 4/49 من إتفاقية جنيف الرابعة التي منعت سلطة الإحتلال أن تنقل أجزاء من سكانها المدنيين إلى الإقليم الذي تحتله.

[3]. انظر سهيل حسين الفتلاوي وعماد محمد ربيع، نفس المرجع، نفس الصفحة.

[4]. أمينة بن حوة، مرجع سابق، ص 78.

كذلك العمل على عقد المؤتمرات الدولية والدبلوماسية بهدف إنماء وتطوير قواعد القانون الدولي الإنساني، خاصة إذا نتج عنها قرارات وإتفاقيات دولية ملزمة[1].

**ثالثا: الفقه الدولي**

مهمة الفقيه هو البحث في أصل القاعدة القانونية ومدى قوتها الملزمة ونطاق تطبيقها على الأشخاص القانونية، وسريانها من حيث الزمان والمكان، والآثار المترتبة عن مخالفتها أو تنفيذها، وعما إذا كانت تستمد قوتها من العرف الدولي أو المعاهدات، وتطبيقات القضاء للقاعدة وردود فعل هذه الدول على هذه التطبيقات، وبناءا عليه يقوم الفقيه بتقديم آراء وعمل علمي، ولكن لا يشكل قاعدة قانونية ملزمة للدول والقضاء الدولي، غير أنه يسهّل على المحاكم والدول الإستدلال على وجود قاعدة قانونية، أو تفسير هذه القاعدة أو إزالة الغموض عنها[2].

بهذا يساهم الفقه في تطوير القانون الدولي الإنساني، عن طريق الرجوع إلى آراء ومؤلفات الفقهاء، التي يقومون فيها بالشرح والتوضيح والدراسة المعمقة لمختلف الحالات الدولية.

**المطلب الثالث: خصائص ومبادئ القانون الدولي الإنساني**

إن الهدف الرئيسي والجوهري لإتفاقيات لاهاي وجنيف والبروتوكولات والأعراف الدولية هوتوفير حماية خاصة للمدنيين والعسكريين في زمن الحرب، وتخفيف آلامهم ومعاناتهم وتقديم المساعدة التي يحتاجونها.

هذا ويشكل فهم الخصائص والمبادئ التي يقوم عليها القانون الدولي الإنساني أساسا ضروريا لإستيعاب طبيعته ووظيفته الإنسانية أثناء النزاعات المسلحة. على ضوء ذلك نتناول في هذا المطلب فرعين؛ يتناول الفرع الأول الخصائص التي تميز القانون الدولي الإنساني عن غيره من فروع القانون الدولي، أما الفرع الثاني فيتناول المبادئ التي تعبر عن القيم الجوهرية التي توجه تطبيق قواعد هذا القانون .

**الفرع الأول: خصائص القانون الدولي الإنساني**

يتميز القانون الدولي الإنساني بجملة من الخصائص التي تجعله فرعا متميزا من فروع القانون الدولي العام، كما أنه يمثل الجانب الإنساني في السلوك البشري، فهو يهتم بحماية الإنسان وحقوقه

[1]. مثال ذلك الدراسات التي أجرتها اللجنة الدولية للصليب الأحمر بتاريخ 1969/09/13 في ظل المؤتمر الدولي العشرون المنعقد في فيينا تحت عنوان: "إنماء وتطويرالقوانين والأعراف المطبقة في النزاعات المسلحة". محمد طلعت الغنيمي، الوسيط في قانون السلام، منشأة المعارف، الإسكندرية، مصر، 1982، ص 130.
[2]. سهيل حسين الفتلاوي وعماد محمد ربيع، مرجع سابق، ص 38.

الأساسية في أشد الظروف صعوبة وقسوة، وقد تطورت هذه الخصائص نتيجة الخصوصية التي يتمتع بها هذا القانون في نطاق تطبيقه ومحتواه وغايته، ويمكن أن نوجز هذه الخصائص في النقاط التالية :

**أولا: القانون الدولي الإنساني أحد فروع القانون الدولي العام**

توصلنا من خلال التعاريف السابقة للقانون الدولي الإنساني (التي تناولناها في الفرع الأول من المطلب الأول)، أنه يعتبر أحد فروع القانون الدولي العام، ويترتب عن ذلك أنّ مصادر الأصل هي نفسها مصادر الفرع[1].

**ثانيا: القانون الدولي الإنساني يخاطب الأفراد مباشرة**

يفرض القانون الدولي الإنساني التزامات ويمنح حقوقا، وبهذا فالشخص الطبيعي يخاطب بالقواعد الدولية الإنسانية، حيث نجد أنّ إتفاقيات جنيف الأربعة لعام 1949 والبروتوكولان المكملان لها لعام 1977، والتي تعد الأساس القانوني للقانون الدولي الإنساني تتضمن الكثير من النصوص التي تمنح للأفراد حقوقا مباشرة كضحايا للنزاعات المسلحة[2].

**ثالثا: القانون الدولي الإنساني حديث النشأة**

إن أول إتفاقية دولية إعتنت بضحايا الحروب كانت إتفاقية جنيف لعام 1864، ثم جنيف لعام 1906، ثم جنيف لعام 1929 ، ثم إتفاقيات جنيف الأربعة لعام 1949 والبروتوكولين الإضافيين لعام 1977[3].

**رابعا: القانون الدولي الإنساني قانون رضائي**

القانون الدولي الإنساني قانون رضائي شأنه شأن القانون الدولي العام، حيث لا تلتزم به الدول (صاحبة السيادة) إلا بإرادتها الحرة وإنضمامها إلى الإتفاقيات ذات الصلة، باعتبارها دولا ذات سيادة.

**خامسا: الطابع الإنساني للقانون الدولي الإنساني**

يعد الطابع الإنساني أبرز خصائص القانون الدولي الإنساني، لأنّ هدفه الرئيسي هو حماية الحقوق الأساسية للإنسان أثناء النزاعات المسلحة، ويظهر ذلك خلال جملة من القواعد التي تضمن الكرامة

[1]. راجع مصادر القانون الدولي الإنساني السابق الإشارة إليها.
[2]. أمينة بن حوة ، مرجع سابق، ص 18 .
[3]. منتصر سعيد حمودة، مرجع سابق، ص 57 .

والسلامة البدنية والنفسية للجميع (المدنيين والمقاتلين في حالة العجزعلى حد السواء)، وقد أكدت على ذلك المادة الثالثة المشتركة بين إتفاقيات جنيف الأربعة لعام 1949[1].

**سادسا: الصفة الإلزامية (الطبيعة الآمرة) لقواعد القانون الدولي الإنساني**

إن قواعد القانون الدولي الإنساني ذات قوة إلزامية، وعلى الدول الإلتزام بها وإحترامها وإلا تعرضت للمسؤولية الدولية، حيث أصبح المنتهك لهذه القواعد يعد مرتكبا لجريمة دولية ويخضع للمحاكمة أمام المحكمة الجنائية الدولية.

أكدت إتفاقية فيينا لقانون المعاهدات لعام 1969 هذه الصفة[2]. وبالتالي فإنّ قواعد القانون الدولي الإنساني الواردة في إتفاقيات جنيف والبروتوكولين هي قواعد آمرة وملزمة للدول الأعضاء فيها، حتى مع حق هذه الدول في التحفظ على نصوص هذه الإتفاقيات التي لا تؤثر في أغراض و جوهر الإتفاقيات[3].

**سابعا: قواعد القانون الدولي الإنساني تتسم بالعالمية و العلانية**

مضمون هذه الخاصية هو أنّ معظم دول العالم منضمة إلى الاتفاقيات الدولية التي تعد مصدرا لهذا القانون، وبالتالي فالمجتمع الدولي كله قد تقبل هذه الإتفاقيات الدولية، فهو يخاطب جميع الدول والكيانات المنخرطة في النزاعات المسلحة الدولية وغير الدولية نظرا لأهمية دوره في حماية ضحايا النزاعات وحتى القوات المسلحة، وبالتالي إذا كان هناك تعارض بين القانون الدولي الإنساني وإتفاقيات أخرى فإن أولوية التطبيق تكون للقانون الدولي الإنساني[4]، وهذا ما أكدته المادة الأولى من البروتوكول الإضافي الثاني لعام 1977[5].

**ثامنا: الطابع المؤقت لقواعد القانون الدولي الإنساني**

يطبق القانون الدولي الإنساني فقط في أوقات النزاع المسلح، سواء كان دوليا أو غير دولي ويتوقف العمل به بعد إنتهاء النزاع أو الإحتلال، وقد نصت المادة الثانية المشتركة بين إتفاقيات جنيف الأربعة

---

[1]. المادة الثالثة المشتركة بين إتفاقيات جنيف الأربعة لعام 1949والتي نصت على: "في حالة نشوب نزاع ذو طابع دولي يعامل الأشخاص الذين لا يشتركون مباشرة في الأعمال العدائية معاملة إنسانية دون أي تمييز مجحف".

[2]. المادة 11 من إتفاقية فيينا نصت على أن: "المعاهدة المتعارضة مع قاعدة آمرة من قوعد القانون الدولي العام تعتبر باطلة بطلان مطلقا إذا كان وقت إبرامها يتعارض مع قاعدة آمرة من قواعد القانون الدولي".

[3]. منتصر سعيد حمودة، مرجع سابق، ص 59.

[4].رشيدة مصباح، مرجع سابق، ص 18.

[5]. المادة الأولى من البروتوكول الإضافي الثاني لعام 1977 نصت على أنه: "ينطبق هذا البروتوكول على جميع النزاعات المسلحة التي لا تشمل نزاعا دوليا... وتحدث في إقليم أحد الأطراف المتعاقدة".

لعام 1949 على أن تطبيق الإتفاقيات يبدأ في حالة الحرب المعلنة، أو أي نزاع مسلح ينشب بن طرفين أو أكثر[1].

**الفرع الثاني: مبادئ القانون الدولي الإنساني**

تعد المبادئ العامة التي يستند إليها القانون الدولي الإنساني جوهر قواعده -وهو ما تمت الإشارة إليه سابقا في المبادئ العامة للقانون كمصدر أصلي ثالث للقانون الدولي الإنساني- فهي الضمانة الأولى لتحقيق التوازن بين حماية الأفراد وضروريات الحرب[2]، من أبرز هذه المبادئ ما يلي :

**أولا: مبدأ الإنسانية**

ورد هذا المبدأ في المادة 27 من من إتفاقية جنيف الرابعة[3]، كما أن ديباجة إتفاقية لاهاي لسنة 1899 و1907 تناولته ضمنيا، وكذلك البروتوكول الإضافي الأول لسنة 1977 نص على المعاملة الإنسانية للأشخاص المحرومين من حريتهم في المادة 75 منه[4].

هذا المبدأ ورد أيضا في المادة 35 من البروتوكول الإضافي الأول لسنة 1977[5] وأعيد ذكره في مؤتمر سان ريمو بشأن القانون الدولي المطبق في النزاعات المسلحة في البحار سنة 1994، والذي جاء في الفقرة الثانية من المادة 38 من الجزء الثالث تحت عنوان: "القواعد الأساسية والتمييز بين الأعيان أو الأشخاص المحميين والأهداف العسكرية".

يتمثل مبدأ الإنسانية في ضرورة إحترام كرامة الإنسان أثناء النزاعات المسلحة، والتخفيف من معاناة الأشخاص الذين لا يشاركون في القتال أو توقفوا عن المشاركة فيه، كما أنّ هذا المبدأ يشكل الأساس الذي بنيت عليه الإتفاقيات الدولية (إتفاقيات جنيف 1949 والبروتوكولين الإضافين لعام 1977)، حيث تفرض هذه النصوص إلتزامات على أطراف النزاع بمعاملة الأفراد معاملة إنسانية دون تمييز، وحظر كافة الأفعال التي تمس كرامتهم كالقتل والتعذيب والمعاملة القاسية أو المهينة، ومبدأ الإنسانية لا يستمد فقد من النصوص المكتوبة بل من العرف الدولي أيضا، مما يعزز طابعه الإلزامي في النزاعات المسلحة الدولية وغير دولية على حد سواء[6].

---

[1]. انظر المادة الثانية المشتركة بين إتفاقيات جنيف الأربعة لعام 1949.
[2].أحمد أبو الوفا، النظرية العامة للقانون الدولي الإنساني (في القانون الدولي وفي الشريعة الإسلامية)، الطبعة الأولى، دار النهضة العربية، مصر، 2006، ص 116.
[3].راجع المادة 27 من اتفاقية جنيف الرابعة لعام 1949.
[4]. انظر المادة 75 من البروتوكول الإضافي الأول لسنة 1977.
[5]. انظر المادة 35 من البروتوكول الإضافي الأول لسنة 1977.
[6]. عمر سعد الله، **تطور تدوين القانون الدولي الإنساني**، دار الغرب الإسلامي، لبنان، 1997، ص 123 - 125.

**ثانيا: مبدأ عدم التمييز**

وفقا لمبدأ عدم التمييز فإن جميع الأفراد متساوون ويعاملون معاملة عادلة، أي المعاملة ليست على أساس الجنس أو اللغة أو المركز الإجتماعي أو الثروة أو الآراء الدينية أو السياسية أو الفلسفية أو أي معيار مشابه .

**ثالثا: مبدأ التمييز**

يعدّ هذا المبدأ أحد الركائز الأساسية في القانون الدولي الإنساني، وينص على ضرورة التمييز في جميع الأوقات بين المدنيين والعسكريين وكذلك بين الأهداف العسكرية والأعيان المدنية، ويحظر بموجبه إستهداف المدنيين أو الأعيان المدنية ما لم يشاركوا مباشرة في الأعمال العدائية.

ورد هذا المبدأ في المادة 48 من البروتوكول الإضافي الأول لعام 1977[1]، وكذلك في المادة 51 من نفس البروتوكول التي تحظر الهجمات العشوائية التي لا تميز بين المقاتلين والمدنيين[2].

أكد على هذا المبدأ القانون الدولي العرفي ومحكمة العدل الدولية وكذلك المحكمة الجنائية الدولية، كما أن إنتهاكه يعد جريمة حرب وفقا للمادة 8 من النظام الأساسي للمحكمة الجنائية الدولية.

**رابعا: مبدأ الضرورة**

عرف فقهاء القانون الدولي الضرورة الحربية بأنها "الحالة التي تكون ملحة إلى درجة أنها لا تترك وقتا كافيا من قبل الأطراف المتحاربة لإختيار الوسائل المستخدة في أعمالها العسكرية الفورية"[3]، هذا المبدأ يدل على أن إستخدام القوة يجب أن يكون مبررا بضرورة عسكرية، أي أن الأعمال العدائية لا تجوز إلا لتحقيق ميزة عسكرية محددة ومباشرة، ومع ذلك فهو يخضع لقيود إنسانية تتجلى في وجوب مراعاة القواعد الإنسانية في أساليب القتال[4].

وقد أشارت المادة 52 من البروتوكول الإضافي الأول إلى أن الهجوم لا بد أن يكون موجه فقط نحو الأهداف العسكرية[5]، كما أنّ المادتين 35 و51 من ذات البروتوكول جاء فيهما أن حق أطراف

---

[1]. تنص المادة 48 من البروتوكول الإضافي الأول لسنة 1977 على أنه: "يجب على أطراف النزاع أن تميز بين في جميع الأوقات بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية وأن توجه عملياتها فقط ضد الأهداف العسكرية".

[2]. راجع المادة 51 من البروتوكول الإضافي الأول.

[3]. أمينة بن حوة ، مرجع سابق، ص 84.

[4]. محمد المجذوب، طارق المجذوب، **القانون الدولي الأنساني** ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2009، ص38.

[5]. راجع نص المادة 52 من البروتوكول الإضافي الأول لعام 1977.

النزاع في إختيار وسائل القتال ليس غير محدود[1]. كذلك إتفاقيتا لاهاي لعام 1899 و1907 جاء فيهما أن الحرب يجب أن تقتصر على تحقيق الضرورات العسكرية المشروعة، كما أكد العرف الدولي على ضرورة الإلتزام بمبدأ الضرورة، وقد أخذت محكمة العدل الدولية بهذا المبدأ في حكمها في قضية نيكاراغوا، حيث تم مناقشة القوة في ضوء الضرورة العسكرية[2].

إن المفهوم القانوني للضرورة العسكرية في القانون الدولي الإنساني يستعمل كجزء من التبرير القانوني للهجمات على الأهداف العسكرية المشروعة وقد يكون لها نتائج معاكسة، وحتى رهيبة على الأعيان المدنية، ذلك أن القوات المسلحة وهي تخطط للأعمال العسكرية يسمح لها أن تأخذ بالحسبان المتطلبات العملية لوضع عسكري في أية لحظة .

وهكذا فإن مبدأ الضرورة يخضع لقيود إنسانية أي أن الضرورة لا تبيح إلحاق الأذى الكبير والمبالغ فيه بالمدنيين والأعيان المدنية، فالضرورة الحربية لا تعني التخلي عن الإنسانية (مبدأ الإنسانية) أو أخذها كمبرر لخرق القوانين الدولية كإستعمال الأسلحة الممنوعة لغرض تحقيق هدف عسكري إستراتيجي، لذلك فالكثير من الفقهاء قيدوا هذا المبدأ بمبادئ أخرى مثل مبدأ التناسب.

**خامسا: مبدأ التناسب**

يعد هذا المبدأ من المبادئ الأساسية في القانون الدولي الإنساني وله أهمية كبيرة في حماية المدنيين والأعيان المدنية، وهو يقتضي أن تكون الوسائل المستخدمة في الهجوم متناسبة مع الهدف العسكري المشروع.وطبقا لهذا المبدأ فأنه لا ينبغي على المتحاربين أن يلحقوا بخصومهم أضرارالا تتناسب مع الغرض من الحرب، و هو تدمير أو إضعاف القوة العسكرية للعدو[3].

تم إقرار مبدأ التناسب في شكل قاعدة ضمن إعلان سان بيترسبورغ عام 1869 بشأن حظر إستعمال بعض القذائف في وقت الحرب مفادها "أن الهدف المشروع الوحيد الذي يجب أن تسعى إليه الدول أثناء الحرب هو إضعاف قوة العدو"[4]، وقد نصت المادة 22 من لائحة لاهاي المتعلقة بقوانين وأعراف الحرب البرية لسنة 1907 على أنه: "ليس للمتحاربين حق مطلق في إختيار وسائل إلحاق

[1]. راجع نص المادتين 35 و51 من البروتوكول الإضافي الأول لعام 1977 .
[2]. راجع إتفاقيتي لاهاي لعام 1899 و1907.
[3].فاطمة بابا، مرجع سابق، ص 16.
[4]. أمينة بن حوة، مرجع سابق، ص 84.

الضر بالعدو"[1]. كما أن المادة 5/51- ب من البروتوكول الإضافي الأول السابق ذكرها تناولت فكرة الضرر المفرط مقارنة بالميزة العسكرية المتوقعة .

تكريسا لهذا المبدأ يفرض القانون الدولي الإنساني على الأطراف المتحاربة إتخاذ كافة الإحتياطات اللازمة قبل وأثناء العدوان لتفادي الإضرار بالمدنيين وزيادة معاناتهم، وهذا ما أكدته المادة 57 من البروتوكول الإضافي الأول[2].

**سادسا: مبدأ التقييد**

ينبثق هذ المبدأ عن المبدأ السابق، وهويقضي بأن حرية المتحاربين في إختيار وسائل الإضرار بالعدو ليست حرية مطلقة[3]، وأهم عناصر مبدأ التقييد: إختيار الوسائل والأساليب الأقل ضررا، وكذلك إتخاذ الإحتياطات قبل الهجوم وإصدار التحذيرات المسبقة، بالإضافة إلى تجنب الأضرار غير الضرورية .

تجدر الإشارة أنّ هناك مبادئ أخرى يقوم عليها القانون الدولي الإنساني مثل؛ مبدأ الفروسية، مبدأ الحيطة[4]، ومبدأ الحماية الخاصة[5]، وهكذا فإن مبادئ القانون الدولي الإنساني هي مبادئ متكاملة ومترابطة لحفظ السلم والأمن الدوليين وحماية المدنيين والعسكريين على حد سواء.

[1]. راجع المادة 22 من لائحة لاهاي المتعلقة بقوانين وأعراف الحرب البرية لسنة 1907.
[2]. راجع نص المادة 57 من البروتوكول الإضافي الأول لعام 1977.
[3]. فاطمة بابا، مرجع سابق، ص 16.
[4]. يفرض مبدأ الحيطة على الأطراف المتنازعة، اتخاذ جميع الإحتياطات الممكنة لتنجنب إصابة المدنيين وتقليل الأضرار الجانبية، راجع المادة 57 من البروتوكول الإضافي الأول لعام 1977.
[5]. نظم القانون الدولي الإنساني حماية خاصة لبعض الفئات الضعيفة والمعرضة للخطر مثل: الأطفال، الجرحى، المرضى، اللاجئين والنازحين، الصحفيين والأشخاص ذوي الإعاقة. للتفصيل أكثر راجع بعض المواد مثل: 27، 34، 50 و53 من اتفاقية جنيف الرابعة لعام 1949 .

**خلاصة الفصل الأول:**

تناولنا في هذا الفصل بالدراسة والتحليل الإطار النظري والمفاهيمي لكل من الحرب السيبرانية والقانون الدولي الإنساني، بهدف التمهيد لفهم التداخل القانوني بينهما، ففي المبحث الأول تم التعريف بالحرب السيبرانية كظاهرة حديثة في ميدان النزاع، لها عدة تعريفات لكن كلها تتفق على أنها حرب رقمية في الفضاء السيبراني، تناولنا نشأتها وتطورها وأنماطها المختلفة وخصائصها المتعددة التي تميزها عن باقي الحروب، أما بالنسبة لطبيعتها القانونية فهي غير محددة تماما، وذلك نظرا لخصائصها وصعوبة بلورة قوانينها التي لا زالت قيد الدراسة والتطور، وفي المبحث الثاني تناولنا القانون الدولي الإنساني بإعتباره الإطار القانوني الناظم لسير العمليات القتالية أثناء النزاعات المسلحة، وذلك من خلال تعريفه ونشأته وتطوره ومصادرالمتنوعة، خصائصه ومبادئه.

من خلال هذا العرض المزدوج يتضح أن الحرب السيبرانية تضع القانون الدولي الإنساني – لاسيما بالنسبة للمبادئ التي يقوم عليها- أمام تحديات جدية، تتمثل في مدى قابليتها للتطبيق على نمط من الحروب لا يخضع بالضرورة للمفاهيم الكلاسيكية للنزاع المسلح، وعليه فإن هذا الفصل يعد تمهيدا ضروريا لدراسة مدى توافق الهجمات السيبرانية مع مبادئ القانون الدولي الإنساني، وهذا ما سنتطرق إليه في الفصل الثاني.

# الفصل الثاني

## علاقة الحروب السيبرانية بمبادئ القانون الدولي الإنساني

## الفصل الثاني: علاقـــة الحروب السيبرانية بمبادئ القانون الدولي الإنساني

إنّ الحرب السيبرانية أصبحت أحد أبرز التحديات التي يواجهها العالم اليوم، فالهجمات السيبرانية وسيلة فعالة في التأثير على القدرات العسكرية الإقتصادية للدول، بل وتمتد في كثير من الأحيان إلى المساس بالأمن القومي والسلم الدولي، وإزاء هذا التطور المتسارع والخطير تثار تساؤلات قانونية وأخلاقية بشأن مدى إنطباق أحكام ومبادئ القانون الدولي الإنساني على هذا النوع من النزاعات غير التقليدية، ومدى إمكانية إرساء المسؤولية القانونية عن الإنتهاكات السيبرانية التي قد ترتكب أثناء النزاعات المسلحة.

على ضوء ما سبق قسمنا دراستنا في هذا الفصل (الثاني) إلى مبحثين؛ نتناول في المبحث الأول الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي الإنساني وإشكالات التطبيق، وفي المبحث الثاني نتناول الجهود الدولية لتنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني وتقرير المسؤولية الدولية عن الحرب السيبرانية.

## المبحث الأول: الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي الإنساني وإشكالات التطبيق

في ظل غياب إطار قانوني دولي خاص ينظم الحرب السيبرانية بشكل صريح، تثار إشكاليات جوهرية تتعلق بكيفية تكييف هذه العمليات وفق مفاهيم النزاع المسلح، المقاتل، الأهداف العسكرية، وما إذا كان بالإمكان تطبيق مبادئ القانون الدولي الإنساني الأساسية مثل التمييز، التناسب والضرورة العسكرية على الهجمات السيبرانية.

من هذا المنطلق سندرس في هذا المبحث الإطار القانوني الناظم للحرب السيبرانية في ضوء مبادئ قانون الدولي الإنساني، وتحليل أبرز الإشكاليات التي تعترض عملية تطبيق هذه القواعد على النزاعات السيبرانية، وذلك من خلال دراسة فقهية وقانونية مقارنة في مطلبين هما: المطلب الأول خصصناه لدراسة الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي الإنساني، والمطلب الثاني خصصناه لإشكالات تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية.

### المطلب الأول: الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي لإنساني

تعتبر الحرب السيبرانية من المواضيع التي ليس لها إطار قانوني محدد المعالم بدقة، فهي صراع جديد وقوانينها ما زالت في طور التبلور، وقد بذلت الكثير من الجهود للوصول إلى قانون ملائم لخصوصيات هذه الحرب ومدى إمكانية تطبيق أحكام ومبادئ القانون الدولي الإنساني عليها. لذلك قسمنا هذا المطلب إلى فرعين؛ خصصنا الفرع الأول لدراسة مفهوم دليل تالين الذي يعد من أهم الدراسات التي تناولت الإطار القانوني للحرب السيبرانية، أما الفرع الثاني فسنوضح فيه دور دليل تالين في تنظيم الحرب السيبرانية ضمن مبادئ القانون الدولي الإنساني.

#### الفرع الأول: مفهوم دليل تالين

يعتبر دليل تالين من أبرز الدراسات القانونية الحديثة التي حاولت تنظيم الحرب السيبرانية وفق قواعد القانون الدولي –لا سيما قواعد ومبادئ القانون الدولي الإنساني-، وفيما يلي سنقوم بدراسته من عدة نواحي؛ حيث سنقوم بتعريفه (أولا)، ونذكر إصداراته (ثانيا)، ونوضح دوره وأهميته في تنظيم الحرب السيبرانية (ثالثا)، كما سنعرض لبعض النقاط البارزة في محتواه (رابعا) وأخيرا نتطرق لبعض الانتقادات الموجهة إليه (خامسا).

**أولا: تعريف دليل تالين**

دليل تالين هو عبارة عن دراسة أكاديمية أعدتها مجموعة من الخبراء الدوليين بقيادة مركز التميز للدفاع السيبراني التابع لحلف شمال الأطلسي (NATO.ccdcoe) في مدينة تالين (استونيا)، يتناول الدليل كيفية تطبيق القانون الدولي خاصة القانون الدولي الإنساني على الفضاء السيبراني، حيث عرّف الحرب السيبرانية بأنها: "كل نشاط سيبراني سواء كان هجومي أو دفاعي، يهدف إلى جرح أو قتل الأشخاص أو تخريب أو تدمير الممتلكات"[1].

وقد ساهمت اللجنة الدولية للصليب الأحمر في إعداده، وذلك بسبب إهتمامها بمجال الأسلحة وتخوفها من التحديات التي أفرزتها التكنولوجيا العسكرية لا سيما الأسلحة الذاتية التشغيل، ومشاركتها كانت فعالة في إعداد دليل تالين لعام 2013[2] الذي يعد الصك الدولي الأول الذي ينظم هذه الهجمات[3].

يتمثل الهدف الرئيسي من دليل تالين في التحقيق في القضايا وتطبيق القانون الدولي في مجال الحرب السيبرانية، ويتكون دليل تالين من قسمين رئيسيين هما: قانون الأمن السيبراني الدولي وقانون النزاعات المسلحة السيبرانية، موزعين على 07 فصول، كما يتضمن 95 قاعدة قانونية صاغتها لجنة الخبراء في القانون الدولي في تالين بإستونيا، على نحو يحدد الخطوط الحمراء التي تستوجب التدخل العسكري وطرق مشاركة مختلف الأطراف[4].

في عام 2017 تم إصدار النسخة المحدثة لدليل تالين (القانون الدولي المطبق على عمليات الانترنت) ليشمل القواعد التي تضمنها الإصدار الأول، ويضم أربعة أجزاء رئيسية، وبلغت عدد القواعد التي يمكن تطبيقها على العمليات السيبرانية 154 قاعدة من القانون الدولي[5].

**ثانيا: إصدارات دليل تالين**

صدر دليل تالين في إصدارين، وذلك سنتي 2013 و2017، وفق ما سيتم توضيحه فيما يلي:

**أ- دليل تالين 1.0 (2013):** يركز على تطبيق القانون الدولي على النزاعات المسلحة السيبرانية، يشمل فقط العمليات السيبرانية التي ترتقي إلى مستوى النزاع المسلح، ويتناول العديد من المبادئ مثل[6]:

---

[1]. سعيد درويش ، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية، المجلد 54، العدد 5، جامعة الجزائر 1 بن يوسف بن خدة، 2017، ص 185.

[2]. صدرت النسخة الأولى من دليل تالين (Tallin manual) سنة 2013، أما النسخة الثانية له فصدرت سنة 2017.

[3]. سعيد درويش ، مرجع سابق، ص 185.

[4]. نفس المرجع، نفس الصفحة.

[5]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1272.

[6]. للإطلاع على دليل تالين، راجع الموقع الرسمي للجنة الدولة للصليب الأحمر:
https://lwww.icrc.org/ar/doc/resources/documments/faq/130628-cyber-warfar :q-and-a-eng.htm ، تاريخ الاطلاع: 11-04-2025، وقت الاطلاع: 02:00

1- السيادة.

1- حظر استخدام القوة.

2- حث الدفاع عن النفس.

3- المبادئ الأساسية للقانون الدولي الإنساني للتمييز التناسبي والضرورة الانسانية.

**ب - دليل تالين 2.0 (2017):** وهو أوسع نطاقا من سابقه، حيث يشمل جميع أنواع العمليات السيبرانية سواء في زمن السلم أو الحرب، يتناول الأحكام التالية[1]:

1- حقوق الإنسان في الفضاء السيبراني.

2- مسؤولية الدولة عن الأفعال السيبرانية.

3- النظام القانوني الدولي في العلاقات السيبرانية السلمية.

4- التنظيم القانوني للأفعال التي لا تصل إلى درجة النزاع المسلح.

**ثالثا: أهمية دليل تالين**

مما سبق إستنتجنا أن دليل تالين له أهمية بالغة في تنظيم الحرب السيبرانية و يمكن إبراز أهميته في النقاط التالية:

أ- لا يعد دليل تالين ملزما قانونيا، لكنه مرجع اجتهادي وأكاديمي مؤثر.

ب- يعكس اتفاق الخبراء حول كيفية تفسير وتطبيق القانون الدولي على الهجمات السيبرانية.

ج- يستخدم كمرجع من قبل الأكاديميين، واضعي السياسات، العسكريين والمحاميين الدوليين.

**رابعا: نقاط بـارزة في محتـوى دليل تالين**

دليل تالين هو أحد المحاولات الرئيسية لتوضيح كيفية تطبيق القانون الدولي على الهجمات السيبرانية، تناول ما يعرف بـ "النقاط الباردة" أو "الفجوات القانونية" التي لا تزال تشكل تحديات حقيقية في تفسير وتطبيق المبادئ التقليدية للقانون الدولي الإنساني في سياق الحروب السيبرانية. وتتمثل أهم النتائج التي توصل إليها هذا الدليل فيما يلي[2]:

أ- الهجمات السيبرانية ممكن أن ترقى إلى مستوى القوة المحظورة بموجب المادة 4/2 من ميثاق الأمم المتحدة.

---

[1]. راجع الموقع الرسمي للجنة الدولة للصليب الأحمر:
. https://lwww.icrc.org/ar/doc/resources/documments/faq/130628-cyber-warfar :q-and-a-eng.htm

[2]. نور أمير الموصلي، **الهجمات السيبرانية في ضوء القانون الدولي الإنساني**، رسالة ماجستير في التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الإفتراضية السورية، سوريا، 2024، ص 25.

ب- الدولة يمكن أن تكون مسؤولة عن الأعمال التي تقوم بها جهات غير حكومية إذا كانت تحت السيطرة الفعلية.

ج- يمكن الرد على الهجوم السيبراني باستخدام القوة إذا بلغت الهجمة مستوى "الهجوم المسلح".

د- أثناء النزاع المسلح يجب احترام قواعد التمييز بين الأهداف المدنية والأهداف العسكرية حتى في الهجمات السيبرانية.

**خامسا: انتقادات موجهة لدليل تالين**

على الرغم من أن دليل تالين تناول الكثير من المسائل القانونية المهمة، والتي كانت تشكل عائقا في تطبيق القانون الدولي العام بصفة عامة والقانون الدولي الإنساني بصفة خاصة، وجهت إليه العديد من الإنتقادات يمكن حصرها في النقاط التالية[1] :

أ- بعض قواعده محل خلاف ولم يتم تبنيها عالميا.

ب- بعض الدول الكبرى مثل الصين وروسيا لم توافق على الكثير من الافتراضات القانونية الواردة فيه.

ج- اعتماده على تفسيرات غربية قد لا تلقى قبولا عالميا.

د- هو اجتهاد غير ملزم قانونا.

هـ- لا يحسم الجدل حول المعايير الدقيقة لتطبيق القانون الدولي الإنساني على الفضاء السيبراني.

و- هناك تباين في المواقف الدولية بشأن مبادئ معينة، مما يحد من توحيد الممارسات.

**الفرع الثاني: دور دليل تالين في تأطير الحرب السيبرانية ضمن مبادئ القانون الدولي الانساني**

يعد دليل تالين أول محاولة منهجية لتفسير كيفية تطبيق القانون الدولي وخاصة القانون الدولي الإنساني على النزاعات السيبرانية، وقد وضع مجموعة من المبادئ التي تشكل أساسا قانونيا للتعامل مع الهجمات السيبرانية في زمن النزاع، بما ينسجم مع قواعد النزاعات المسلحة التقليدية، ومن أهم المبادئ الواردة في دليل تالين والمرتبطة بمبادئ القانون الدولي الإنساني نجد:

**أولا: دليل تالين ومبدأ السيادة**

جاء في دليل تالين أن لكل دولة الحق في ممارسة سيادتها على الفضاء السيبراني الموجود داخل إقليمها، ويعد أي تدخل خارجي غير مبرر في هذا الفضاء انتهاكا للقانون الدولي العام[2].

[1]. نور أمير الموصلي، مرجع سابق، ص 26.

[2]. راجع القاعدة الأولى و الثانية من دليل تالين 1.0 حول القانون الدولي المنطبق على الحرب السيبرانية.

ينسجم هذا المبدأ مع قاعدة احترام سيادة الدول، وهي قاعدة أساسية في العلاقات الدولية وفي القانون الدولي الإنساني، حيث يحظر استخدام أراضي دولة محايدة كمساحة للعمليات العسكرية من دون موافقتها، وهو ما ينطبق أيضا على البنية التحتية السيبرانية.

**ثانيا: دليل تالين ومبدأ حظر استخدام القوة**

جاء فيه أنّ أيّ هجوم سيبراني يسبب أضرارا جسمية مماثلة لاستخدام الأسلحة التقليدية (كخسائر في الأرواح أو دمار واسع للبنى التحتية) قد يعد إستخدام للقوة المحظورة بموجب الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة[1]، وقد نص هذا المبدأ على: "أن العمليات السيبرانية إن أسفرت على أضرار جسيمة ووفيات، يمكن الرد عليها بأسلحة الحرب الحقيقية"[2].

في حال وصول الهجوم السيبراني إلى هذا المستوى، يصبح من الممكن تطبيق مبدأ الدفاع الشرعي عن النفس الوارد في المادة 51 من ميثاق الأمم المتحدة[3]، مما يفتح الباب إلى إستخدام القوة بما فيها القوة التقليدية ردا على الهجوم السيبراني، كما أكد المبدأ الوارد في المادة 13 من دليل تالين على ذلك ونص على أنه: "إذا تجاوز النشاط السيبراني سقف أي هجوم مسلح بالمعنى المقصود في المادة 51 من ميثاق الأمم المتحدة، فينبغي أن يكون للدولة الحق في ممارسة حقها الأصيل في الدفاع عن النفس"[4].

**ثالثا: دليل تالين ومبدأ التمييز**

يقتضي مبدأ التمييز -كما سبقت الإشارة إليه في نهاية الفصل الأول- أن توجه الهجمات فقط ضد الأهداف العسكرية لا ضد الأعيان المدنية أو المدنيين، حتى ولو كانت الهجمات من طبيعة غير مادية كالهجمات السيبرانية[5]، وبهذا فإن استهداف نظم المستشفيات أو البنية التحتية للطاقة التي تخدم السكان المدنيين يعد انتهاكا للقانون الدولي الانساني، وهذا ما أكدته القاعدة 51 من دليل تالين التي تناولت حماية المدنيين، وهذا تطبيقا لمبدأ حماية المدنيين الوارد في القانون الدولي الإنساني[6] .

---

[1]. راجع المادة 4/2 من ميثاق الأمم المتحدة.
[2]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1272.
[3]. راجع المادة 51 من ميثاق الأمم المتحدة.
[4]. ناجي محمد أسامة الشاذلي مرجع سابق ،ص 1272.
[5]. اللجنة الدولية للصليب الأحمر، **قاعدة القانون الدولي الإنساني العرفي رقم 7، مبدأ التمييز بين الأعيان المدنية والأهداف العسكرية**.
[6]. تنص القاعدة 51 من دليل تالين 01. (2013) على أنه: "المدنيون يظلون تحت الحماية طالما لم يشاركوا في العمليات العدائية التي تتم في الفضاء السيبراني".

**رابعا: دليل تالين ومبدأ التناسب**

من المبادئ الأساسية التي أكدها دليل تالين، أن تكون الخسائر العرضية في صفوف المدنيين أو الأعيان المدنية الناتجة عن الهجوم السيبراني متناسبة مع الميزة العسكرية المتوقعة، أي أن الهجوم يجب أن يوازن بين الضرورة العسكرية والآثار الجانبية الإنسانية، وهذا ما نصت عليه القاعدة 14 من دليل تالين[1].

**خامسا: دليل تالين ومبدأ الضرورة العسكرية**

بمعنى أن يكون كل هجوم سيبراني مرتبط بهدف عسكري مشروع، ولا ينفذ لأغراض تعسفية أو دون هدف عسكري واضح، وهذا ما أكدته القاعدة 22 من دليل تالين، حيث نصت على أنه: "لا يجوز توجيه الهجمات إلا ضد الأهداف العسكرية"[2].

**سادسا: مبدأ الانسانية**

يقتضي مبدأ الإنسانية منع استخدام وسائل وأساليب تسبب معاناة غير ضرورية أو غير متناسبة، وهو ما قد ينطبق على بعض الأسلحة السيبرانية التي تعطل الخدمات الحيوية دون مبرر عسكري هادف، وقد أشار دليل تالين الثاني (2.0) إلى هذا المبدأ في القاعدتين 32 و 33[3].

فيما يتعلق بالدول المحايدة، أكد دليل تالين على تطبيق قواعد الحياد التي تمنع استخدام البنية التحتية السيبرانية التابعة لدولة محايدة لشن عمليات هجومية دون إذنها، وهي ذات القواعد المعتمدة في القانون الدولي الانساني بخصوص احترام حياد الدول غير المشاركة في النزاع[4].

هناك مبادئ أخرى تبناها دليل تالين مثل: المبدأ الخاص بالتجسس، والذي مفاده أنّ: "التجسس السيبراني الخالص لا يعد عملا حربيا، فهجمات التجسس يمكن إعتبارها تحضيرا لهجوم مدمر قد تتطلب الرد عليها بضربة وقائية، وقد تطالب الدول بحقها في الدفاع عن النفس إذا كان المهاجم دولة أو جماعة منظمة"[5].

---

[1]. تنص القاعدة 14 من دليل تالين 1.0 على أنه: "يحضر شن هجوم متوقع أن يسبب خسائر في أرواح المدنيين، أو إصابات بينهم، أو أضرارا في الأعيان المدنية، أو مزيجا من ذلك بشكل مفرط مقارنة بالميزة العسكرية المباشرة والملموسة المتوقعة من الهجوم" .

[2]. سعيد درويش، مرجع سابق، ص 195.

[3]. راجع القاعدتين 32 و 33 من دليل تالين 2.0 .

[4]. راجع المواد 1-5 من إتفاقية لاهاي الخامسة بشأن إحترام حقوق وواجبات الدول المحايدة في الحرب البرية 1907.

[5]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1272.

أما إذا كان المهاجم فردا فمبدأ تالين الخاص بالتجسس جاء فيه ما يلي: "إذا كان المهاجم فردا، فلا يحق للدولة المعتدى عليها اللجوء لضربة وقائية، وترتيبا على ذلك لا يمكن من حيث المبدأ الرد على التسريبات والأخبار المتداولة عن هجوم ما، قبل حدوثه من خلال أداة عسكرية، إلا إذا كانت الإصابات أو الخسائر المحتملة وشيكة الحدوث"[1].

نستنتج مما سبق وجود علاقة تربط دليل تالين بمبادئ القانون الدولي الإنساني، وهذا ما أكدته قواعده (دليل تالين 1.0 ودليل تالين 2.0)، حيث عالج إمكانية تصنيف الهجمات السيبرانية كاستخدام القوة أو الهجوم المسلح وغيرها من المسائل القانونية المرتبطة بمبادئ القانون الدولي الإنساني، مما يعني خضوعها لأحكام النزاع المسلح، وهذا يربط الحرب السيبرانية بالقانون الدولي الانساني بشكل مباشر، وكذلك بالقانون الدولي العام.

يمكنا تلخيص العلاقة التي تربط خصائص الحرب السيبرانية بمبادئ القانون الدولي الإنساني عبر دليل تالين، وطريقة معالجته لها من خلال الجدول التالي :

**جدول رقم(03): ربط خصائص الحرب السيبرانية بمبادئ القانون الدولي الانساني عبر دليل تالين**

| الخاصية السيبرانية | المبدأ القانوني الانساني | كيف عالجه دليل تالين |
|---|---|---|
| الطابع غير المادي للهجمات | مبدأ التمييز | طالب الخبراء في الدليل بوجوب التفريق بين الأهداف العسكرية والأهداف المدنية حتى عند استهداف الأنظمة المعلوماتية |
| صعوبة تحديد الفاعل | مبدأ المسؤولية | تناول الدليل مسؤولية الدول حتى عندما تنفذ الهجمات عبر أطراف غير حكومية إذا ثبتت السيطرة |
| الانتشار السريع للآثار | مبدأ التناسب | الدليل أكد على ضرورة تقسيم الآثار الجانبية للهجمات السيبرانية وعدم تجاوز الضرر المطلوب لتحقيق الأهداف العسكرية |
| ازدواجية استخدام البنى التحتية | مبدأ الإنسانية | يعتمد الدليل على ضرورة الحذر عند استهداف البنى التحتية ذات الاستخدام المزدوج كشبكات الكهرباء، الماء، الاتصالات |

**المصدر:** إعداد الطالبتين[2].

ما نستخلصه من دراستنا لدليل تالين أنه وبالرغم من طابعه غير الملزم، إلا أنه نجح في توجيه أنظار المجتمع الدولي إلى ضرورة تكييف قواعد القانون الدولي الإنساني مع طبيعة الفضاء السيبراني ومتغيراته، كما وفر أساسا نظريا وعمليا يمكن البناء عليه لتطوير أطر قانونية أكثر إلزاما وتنظيما لهذا

[1]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1272.
[2]. إعتمادا على القواعد الواردة في دليل تالين 1.0 ودليل تالين 2.0 .

النوع المستجد من الحروب، فهو يشكل خطوة متقدمة نحو تحقيق التوازن بين ضرورة حماية المدنيين والبنى التحتية الحيوية، وبين متطلبات الأمن السيبراني في زمن تتنامى فيه التهديدات الإلكترونية بشكل غير مسبوق.

**المطلب الثاني: إشكاليات تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية**

نظرا لطبيعة الحرب السيبرانية المرنة وغير التقليدية، برز خلاف فقهي حول مدى إمكانية تطبيق قواعد القانون الدولي الإنساني هذا النوع من الحروب، فمنهم من يرى إمكانية التطبيق ومنهم من عارض الفكرة، وكل منهما إعتمد على حجج واقعية وقانونية .

سنحاول دراسة وتحليل الإتجاهين في فرعين مختلفين، الفرع الأول نتناول فيه موقف الفقه المؤيد لتطبيق القانون الدولي الإنساني على الحرب السيبرانية، وفي الفرع الثاني نتناول موقف الفقه المعارض لتطبيق القانون الدولي الإنساني على الحرب السيبرانية، وفي الفرع الثالث نتناول الاتجاه الوسيط في تطبيق مبادئ القانون القانون الدولي الإنساني على الحرب السيبرانية.

**الفرع الأول: الاتجاه المؤيد لتطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية**

أصحاب هذا الإتجاه يرون أن القانون الدولي الإنساني يمكن أن يمتد ليشمل الهجمات السيبرانية استنادا إلى الطابع المرن والتطوري لهذا القانون، والذي يهدف بالأساس إلى حماية المدنيين وتنظيم وسائل وأساليب القتال بغض النظر عن طبيعتها؛ فالإتفاقيات الأساسية مثل اتفاقيات جنيف لعام 1949 والبروتوكول الإضافي الأول لعام 1977 تتحدث بعمومية في الوسائل والأساليب دون حصرها، مما يتسع تأويلا ليشمل التكنولوجيا السيبرانية الحديثة، كما يستند إلى ما يعرف بمبدأ الإنسانية ومبدأ الضرورة العسكرية، وهما مبدآن أساسيان في القانون الدولي الإنساني، يقتضيان أن تخضع أية وسيلة قتالية جديدة لهذين المعيارين عند تقييم مشروعيتهما[1].

هناك من الفقهاء من أيدوا هذا الموقف (القانون الدولي الإنساني ينطبق بجميع مبادئه وقواعده بصفة عامة على أي نزاع مسلح، بما فيها الحروب السيبرانية)، وقالوا أنه إذا كانت الإتفاقيات الواردة في القانون الدولي الإنساني لم تشر على وجه التحديد للهجمات السيبرانية، إلا أن هذه الحجة ليس لها أهمية[2].

[1]. نور أمير الموصلي، مرجع السابق، ص 54.
[2]. رمضان عبد الله عموري، **الحروب السيبرانية (الواقع – التحديات) في ضوء القانون الدولي الإنساني**، مجلة الحق للعلوم الشرعية والقانونية، العدد 14، جامعة بني وليد، ليبيا، 2024، ص 202 .

كما أنّ شرط (مبدأ) مارتنز –المشار إليه سابقا- هو من المسلمات الراسخة في القانون الدولي الإنساني، ويقرر صراحة أنه عند عدم وجود وضع لا تشمله الإتفاقيات الدولية يبقى المدنيون والمقاتلون تحت رعاية وسلطان مبادئ القانون الدولي الإنساني من التقاليد الثابتة ومن المبادئ الإنسانية[1] .

جاء في الفقرة الأولى من المادة 35 من البروتوكول الإضافي الأول -لإتفاقيات جنيف- لعام 1977 أن حق أطراف النزاع في إختيار وسائل وأساليب القتال ليس حقا مطلقا، بل يجب أن يكون مقيدا بالقواعد الأساسية للقانون الدولي الإنساني، وبالتالي حتى في حالة وجود غموض في بعض الأحكام الواردة في القانون الدولي الإنساني يمكننا الإستناد إلى المبادئ العامة للقانون الدولي وشروط مارتينز لتفسيرها، حيث توفر قاعدة عامة لتطبيق مبادئ القانون الدولي الإنساني على جميع النزاعات، مهما كان نوع السلاح المستخدم[2].

كذلك أشارت المادة 36 من البروتوكول الإضافي الأول إلى إلتزام كل طرف سام ومتعاقد عند دراسته أو تطويره أو إقتناءه لسلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب، بالتحقيق فيما إذا كان السلاح محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[3].

أما المادة 82 فقد استكملت ما قضت به المادة 36 بنصها على وجوب استشارة مستشارين قانونيين لتقديم المشورة للقاعدة العسكرية بالنسبة لهذا الموضوع[4]، وبهذا فإن لكل دولة الحق في اقتناء أسلحة أو تطويرها بشرط عدم الخروج عن التزاماتها القانونية فيما يخص الأمن والسلم الدوليين وإحترام القواعد الإنسانية الدولية[5].

بالرغم من أن الحروب السيبرانية يعتريها الغموض خاصة في جانب التفرقة بين الأهداف المدنية والعسكرية في حال هجوم أو اختراق إلكتروني، إلا أنها تخضع لضوابط القانون الدولي الإنساني من ناحية خطر المساس بالمدنيين والأعيان المدنية.

فئة من الفقهاء يرون أن بعض الهجمات السيبرانية قد تؤدي إلى أضرار مادية جسيمة مثل تعطيل شبكات الكهرباء، أو أنظمة المستشفيات أو خدمات النقل، مما يعرض أرواح المدنيين للخطر، ويجعلها

---

[1]. سهيل حسين الفتلاوي، **الطبيعة القانونية العرفية لقواعد القانون الدولي الإنساني**، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص 45.

[2]. راجع المادة 35 من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام 1977.

[3]. انظر المادة 36 من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام 1977.

[4]. شويرب جيلالي ومراد فائزة، **مفهوم الحروب السيبرانية والأمن السيبراني**، مجلة الحقوق والحريات، المجلد 11، العدد 1، جامعة محمد خيضر، الجزائر، 2023، ص 172.

[5]. راجع المادة 82 من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام 1977.

تقارن في آثارها بالحروب التقليدية، وهذا ما أكده دليل تالين، حيث اعتبر الهجوم السيبراني هجوما مسلحا إذا أدى إلى نتائج تماثل تلك الناتجة عبر استخدام الفكرة العسكرية، وبالتالي يكون خاضعا لأحكام القانون الدولي الإنساني إذا وقع في سياق نزاع مسلح، وهذا ما درسناه ووضحناه في الفرع الثاني من المطلب الأول في المبحث الأول (الفصل الثاني علاقة الحروب السيبرانية بمبادئ القانون الدولي الإنساني)، حيث أكد دليل تالين على إمكانية تطبيق قواعد القانون الدولي الإنساني ومبادئه على الحرب السيبرانية.

دعمت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة هذا الرأي وقالت أن الهجمات السيبرانية تخضع لقواعد القانون الدولي، وفي مقدمة هذه القواعد نصوص ميثاق الأمم المتحدة لا سيما الأحكام المتعلقة بخطر استخدام القوة في العلاقات الدولية وخطر اللجوء للعدوان، كما أن قواعد دليل تالين الخاصة بالحروب السيبرانية جاءت موافقة لما نص عليه ميثاق الأمم المتحدة، حيث أكدت الجمعية العامة أن حقوق الأشخاص خارج الفضاء السيبراني وداخله يجب أن تحظى بالحماية، وطالبت الجمعية العامة من المفوضية السامية لحقوق الإنسان إعداد تقرير عن الخصوصية في الحق الرقمي، إذ تناول التقرير حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للإتصالات الرقمية أو اعتراضها وجمع البيانات الشخصية[1].

أصدرت مجموعة الخبراء الحكوميين التابعة للأمم المتحدة عدة تقارير سنة 2013، أجمعت فيها الدول الأعضاء على أن قواعد القانون الدولي بما في ذلك القانون الدولي الإنساني ينطبق على الفضاء السيبراني لاسيما المتعلقة بإستخدام القوة والسيادة وعدم التدخل، على الرغم من استمرار الخلاف حول تفسير تواجده في هذا المجال[2].

فالهجمات السيبرانية سلاح حديث من أسلحة النزاعات الدولية، والبروتوكول الأول وفقا للمادة 36 السابق ذكرها أكد انطباق هذه الأحكام الآمرة على الهجمات السيبرانية، لأن لقانون الدولي قد تطور ليأخذ بعين الاعتبار تغيز الظروف ولا يقتصر تطبيقه على أسلحة الماضي وإنما تنطبق مع أسلحة الحاضر، وبالنسبة لإعتبار الهجمات السيبرانية ليست نزاعا مسلحا وحجة القائلين أنها لا تحمل عملا عدائيا تقليديا، فنجدها قد أصبحت مسألة نسبية في الوقت الراهن، لأنه حتى المعلومات لا تحمل معيار

[1]. مصطفى كامل قرطاس، **الأمن السيبراني وحقوق الإنسان الرقمية**، المفوضية العليا لحقوق الإنسان، العراق، 2023، ص 23.

[2]. راجع تقرير الفريق الحكومي المعني بالتطورات في ميدان المعلومات والإتصالات في سياق الأمن الدولي، الجمعية العامة للأمم المتحدة، 2015.

الفاعل فقط، وإنما تحمل معيار آثار الفعل بصفة أكبر، وعليه يمكن اخضاعها للقانون الدولي الإنساني مثل الحروب البيولوجية والكيميائية[1].

دعمت اللجنة الدولية للصليب الأحمر هذا الإتجاه، حيث أكدت على أن القانون الدولي الإنساني ينطبق على الهجمات السيبرانية عندما تقع في إطار نزاع مسلح، وشددت على ضرورة احترام المبادئ الأساسية للقانون الإنساني في الفضاء الرقمي كما هو الحال في الميدان العسكري التقليدي، مثل مبدأ التسيير ومبدأ التناسب ومبدأ الضرورة والاحتياطات في الهجمات السيبرانية تطبق حتى في البيئة الرقمية، لذلك على الجميع الالتزام باحترام القواعد الإنسانية.

جاء في تقرير اللجنة الدولية للصليب الأحمرعام 2011: "أن الهجمات السيبرانية في إطار النزاع المسلح يجب أن تتوافق مع جميع مبادئ القانون الدولي الإنساني وقواعده"، وهذا ما أشارت إليه محكمة العدل الدولية (مبادئ وقواعد القانون الدولي الإنساني المطبقة في النزاع المسلح تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك المستقبلية)[2].

في نفس السياق جاء في التقرير المعنون بـ "التكلفة البشرية المحتملة للعمليات السيبرانة" أن الهجوم على البنية التحتية المدنية قد يؤدي إلى حرمان المدنيين من الخدمات الأساسية، وهو ما شكل خرقا واضحا لأحكام القانون الدولي الإنساني[3]. كما أشارت اللجنة خلال مشاركتها في أعمال الفريق العامل المفتوح العضوية في الأمم المتحدة بشأن الأمن في الفضاء السيبراني، إلى أن القواعد القائمة في القانون الدولي الإنساني كافية ـمن حيث المبدأـ لتنظيم سلوك الدول والجهات الفاعلة أثناء النزاعات السيبرانية[4].

دعت اللجنة الدولية للصليب الأحمر إلى توخي الحذر الشديد في تطوير أو إستخدام أدوات سيبرانية يمكن أن تلحق ضررا واسع النطاق أو عشوائيا، خاصة إذا استهدفت القطاعات الحيوية التي

---

[1]. جيلالي شويرب ومراد فائزة، مرجع سابق، ص 175.
[2]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 47 .
[3]. اللجنة الدولية للصليب الأحمر، **التكلفة البشرية المحتملة للعمليات السيبرانية**، على الرابط:
https://www.icr .org/ar/document/potential-human-cost-cyber-operatios.، تاريخ الإطلاع:2025/05/10، وقت الإطلاع: 14:30 .
[4]. اللجنة الدولية للصليب الأحمر، **بيان اللجنة أمام فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والإتصالات في سياق الأمن الدولي**، على الرابط:
https://www.icr.org/ar/document/icrc-statement-oewg-cybersecurity-2021.، تاريخ الإطلاع: 2025/05/10، وقت الإطلاع: 18:00.

يعتمد عليها المدنيون، مثل الصحة والمياه والطاقة، نظرا لإحتمال تسببها في معاناة إنسانية كبيرة دون تمييز[1] .

على ضوء ما سبق يمكننا القول أنه إذا كان تكييف الهجمات السيبرانية بإعتبارها سلاحا أو أسلوبا من أساليب الحرب، فعلى الدول التحقق من مشروعية إستخدامها وفقا لقواعد القانون الدولي الإنساني، وهو ما يؤكد انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية[2].

**الفرع الثاني: الاتجاه المعارض لتطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية**

رغم التوجه المتزايد نحو التأكيد على قابلية تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية في إطار النزاعات المسلحة، إلا أن هذا الطرح لم يخل من الجدل، فقد ظهرت أصوات معارضة ترى أن خصوصية الفضاء السيبراني من حيث طبيعته غير المادية وغموض مصادر الهجمات السيبرانية وصعوبة التمييز بين الأهداف العسكرية والمدنية تجعل من الصعب، بل ومن غير الملائم أحيانا تطبيق قواعد وضعت أساسا لتنظيم الحروب التقليدية.

يرى فريق من الفقهاء أن القانون الدولي الإنساني غير مهيأ بعد للتعامل مع الحرب السيبرانية، نظرا لإختلاف طبيعتها عن النزاعات المسلحة التقليدية، ويؤكد هؤلاء أن معظم الهجمات السيبرانية لا تستوفي الشروط القانونية لتعريف النزاع المسلح وفقا لاتفاقيات جنيف، خصوصا في غياب الضرر المادي والمباشر أو استخدام القوة المسلحة[3]. حيث إعتمد هؤلاء الفقهاء على مجموعة من الحجج لدعم موقفهم، وهي عبارة عن حجج قانونية وتقنية تشكك في مدى فاعلية وجدوى القانون الدولي الإنساني في بيئة سيبرانية معقدة ومتطورة بسرعة. **وأهم هذه الحجج** نذكر ما يلي:

---

[1]. اللجنة الدولية للصليب الأحمر، **القانون الدولي الإنساني والعمليات السيبرانية أثناء النزاعات المسلحة**، على الرابط: https://www .icr.org/ar/document/international-humanitarian-law-and cyber-operatios-during-armed-conflicts.، تاريخ الإطلاع: 2025/05/10، وقت الإطلاع 20:00.

[2]. عبد الرحمان شامل عبد الرحمان، زيد لقمان، **الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني**، مجلة نور القانونية، المجلد 01، العدد02، جامعة النور، العراق، 2024، ص164.

[3]. محمد الزبيدي، **الفضاء السيبراني بين القانون الدولي الإنساني والقانون الدولي العام**، مجلة البحوث القانونية والإقتصادية، العدد 58، جامعة المنصور، العراق، 2021، ص 145.

**أولا: الطبيعة غير المادية للهجمات السيبرانية**

تقتصر أغلب الهجمات السيبرانية على التشويش أو سرقة المعلومات أو الإضرار بالبنية التحتية التقنية، دون أن تلحق دمارا ماديا مباشرا ما يجعلها من وجهة نظر المعارضين غير قابلة للتكييف كهجمات مسلحة[1].

**ثانيا: صعوبة تحديد الفاعل السيبراني وتحميله المسؤولية**

في الفضاء السيبراني يمكن بسهولة إخفاء الهوية أو تنفيذ الهجمات من خلال أطراف متعددة الأماكن، مما يجعل تطبيق المسؤولية الدولية وقواعد التمييز بين المقاتلين والمدنيين معقدا جدا[2].

**ثالثا: تعدد أهداف الهجمات السيبرانية**

غالبا ما تكون أهداف الهجمات السيبرانية ذات طابع اقتصادي أو استخباراتي ولا تصنف ضمن النزاعات المسلحة الدولية أو غيرالدولية، مما يبعدها حسب المعارضين عن نطاق تطبيق القانون الدولي الإنساني[3].

**رابعا: تطور الأسلحة المستخدمة**

إن الأسلحة ذات التشغيل الذاتي والتي تعمل في البر والبحر والجو بدورها تشكل تحدي أو صعوبة، هذه الأسلحة لا تستطيع التمييز بين المدنيين والأعيان المدنية والمقاتلين عند القتال، إذن فمبدأ التناسب، مبدأ الإحتياط ومبدأ التمييز مبادئ يصعب التقيد بها، وهي مبادئ مكرسة في القانون الدولي الإنساني وتخضع لرقابة البشر، وبالتالي يظهر جليا أن التكنولوجيا بعيدة عن الإمتثال التام لقواعد القانون الدولي الإنساني .

إن الحرب السيبرانية كما سبق وأن وضحنا لها خصائص مميزة، مثل الطبيعة غير المادية للهجمات وصعوبة تحديد مصدرها وإتساع نطاق تأثيرها، وهذه السمات تجعل من الصعب تطبيق مبدأ التمييز، الذي يقتضي الفصل بين الأهداف العسكرية والمدنية، حيث يمكن للهجمات السيبرانية أن تستهدف البنى التحتية المدنية ذات الإستخدام المزدوج دون تمييز واضح. بالإضافة إلى ذلك فإن تقييم الأضرار المحتملة للهجمات السيبرانية بدقة يمثل تحديا، مما يثير تساؤلا حول مدى إحترام مبدأ التناسب،

---

[1]. هشام عيسى، **التحديات القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني**، مجلة القانون والتكنولوجيا، جامعة القاهرة، مصر، 2019، ص 97.

[2]. خالد عبد الكريم خروب، **الجيل الخامس والقانون الدولي الإنساني**، المجلة الجزائرية للعلوم القانونية، بدون عدد، بدون دار النشر ،الجزائر، 2020، ص 211.

[3]. نفس المرجع، ص 213.

علاوة على ذلك فإن صعوبة إسناد الهجمات السيبرانية إلى جهات محددة تعقد مسألة إسناد المسؤولية[1]. والجدول التالي يلخص ما قلناه سابقا بطريقة بسيطة وواضحة:

**جدول رقم 04: العلاقة بين خاصية الحرب السيبرانية والمبدأ القانوني المتأثر ونوع الإشكال (التحدي)**

| خاصية الحرب السيبرانية | المبدأ القانوني المتأثر | نوع الإشكال (التحدي) |
|---|---|---|
| صعوبة التتبع | التمييز | صعوبة تحديد الطرف المهاجم |
| إستهداف بنى مدنية | التمييز والتناسب | صعوبة تحديد الهدف (مدني وعسكري) |
| السرعة والتأثيرغير مادي | التناسب والإنسانية | صعوبة تقرير الضرر مسبقا |
| هجمات تلقائية أو عشوائية | الضرورة والإنسانية | قرارات غير مدروسة قد تسبب معاناة |

**المصدر:** جدول من إعداد الطالبتين[2].

كما أن هناك آراء ومواقف مؤيدة لهذا الإتجاه (المعارض لتطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية) منها:

**أ-** يرى الفقيه "جاري سوليس" أن القانون الدولي الإنساني ليس معدا بعد للتعامل مع تعقيدات الحرب السيبرانية، ويجب تطويره قبل الشروع في تطبيقه على هذ النوع من العمليات[3].

**ب -** حذر مجلس الأمن السيبراني الدولي (ICCS) من أن تطبيق القانون الإنساني على الفضاء السيبراني يواجه تحديات قانونية وتقنية، بسبب غياب المعايير الدولية لتعريف الهجوم السيبراني أو تحديد نطاقه الجغرافي والزماني[4].

**ج-** أبدت المفوضية السامية لحقوق الإنسان إهتمامها بالأبعاد الإنسانية للهجمات السيبرانية، ولاسيما تلك التي تستهدف البنية التحتية التي يعتمد عليها السكان المدنيين، مؤكدة ضرورة إحترام حقوق الإنسان خلال النزاعات المسلحة بما في ذلك الفضاء السيبراني، لأنها تعتبر القانون الدولي الإنساني قاصرا وغير كافي لضمان الحماية اللازمة[5].

رغم الجدل القائم بين المؤيدين والمعارضين لتطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية، فإن الواقع العملي يظهر غياب إطار قانوني واضح وملزم ينظم هذا النوع من الأعمال

---

[1]. سلوى يوسف الأكيابي، **مدى إنطباق القانون الدولي الإنساني على الهجمات السيبرانية**، مجلة روح القوانين، العدد 101، جامعة طانطا، مصر، 2023، ص ص1417-1423.

[2]. إعتمادا على الدراسات السابقة.

[3]. سلوى يوسف الأكيابي، مرجع سابق، ص 1419.

[4]. مجلس الأمن السيبراني الدولي، **تحديات قانونية في نطبيق القانون الدولي الإنساني على الفضاء السيبراني**، تقرير 2020.

[5]. مكتب المفوض السامي لحقوق الإنسان، **تأثير العمليات السيبرانية على حقوق الإنسان أثناء النزاعات المسلحة**، تقرير سنوي 2022.

العدائية الحديثة، فالمبادئ التقليدية مثل التمييز والتناسب والإحتياط والإنسانية تواجه تحديات كبيرة عند إسقاطها على الفضاء السيبراني، الذي يتسم بالغموض والسرعة وعدم التمييز بين الأهداف العسكرية والمدنية، أو بين الفاعلين الحكوميين وغير الحكوميين .

من جهة أخرى، تبقى آليات المساءلة والردع القانونية ضعيفة في المجال السيبراني، الأمر الذي يكرس نوعا من الإفلات من العقاب ويقوض فاعلية القانون الدولي الإنساني ككل، نتيجة لكل هذا ظهر رأي آخر وهو الرأي الوسيط بين الاتجاهين السابقين (المؤيد والمعارض).

**الفرع الثالث: الاتجاه الوسيط في تطبيق مبادئ القانون القانون الدولي الإنساني على الحرب السيبرانية**

يعد الاتجاه الوسيط هو الأكثر واقعية، حيث لا يرفض تطبيق القانون الدولي الإنساني مطلقا ولا يقبله بشكل مطلق، بل يشترط أن ترقى الهجمات السيبرانية إلى مستوى الهجوم المسلح من حيث الآثار لكي تكون خاضعة لهذا القانون، وهذا ما جاء به دليل تالين مثلما سبقت الإشارة إليه بالتفصيل.

إن النصوص القانونية التقليدية (القانون الدولي الإنساني، القانون الدولي العام) هي نصوص قاصرة ولابدّ من تطويرها، فحتى المؤيدون يعترفون بوجود فراغ قانوني تشريعي يستدعي تطوير النصوص القانونية أو تفسيرها بشكل يواكب التطورات السيبرانية وهناك دعوات فقهية لإدراج البروتوكولات الجديدة ضمن اتفاقيات جنيف أو اصدار اتفاقية دولية خاصعة بالحرب السيبرانية[1].

جميع الفقهاء والمختصين القانونيين الدوليين يطالبون بضرورة تفعيل الجهود الدولية من أجل ضبط قواعد الاشتباك السيبراني وتحديد مسؤولية الأطراف الفاعلة، ووضع آليات للوقاية من الانتهاكات وحماية السكان المدنيين بما ينسجم مع أهداف ومبادئ القانون الدولي الإنساني، لذلك **إقترحوا الحلول التالية :**

**أولا:** اعتماد بروتوكول إضافي ضمن إتفاقيات جنيف خاص بالحرب السيبرانية، يحدد المبادئ والضوابط التي يجب إحترامها في هذا النوع من النزاعات[2].

[1]. نجلاء إسماعيل، **الحرب السيبرانية في ضوء القانون الدولي الإنساني**، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي،بدون عدد، مصر، 2022، ص 112.
[2]. انظر محمد أبو العينين، **الحرب السيبرانية وتحديات القانون الدولي الإنساني**، مجلة الحق، العدد 3، جامعة بني وليد، ليبيا، 2022، ص ص 45-47.

**ثانيا:** تعزيز التعاون الدولي من خلال إنشاء هيئة دولية متخصصة لرصد وتقييم الهجمات السيبرانية ذات الطابع العسكري، تكون تحت مظلة الأمم المتحدة أو اللجنة الدولية للصليب الأحمر[1].

**ثالثا:** وضع معايير فنية دولية لتحديد طبيعة الهجمات السيبرانية، وتقييم آثارها لتحديد ما إذا كانت ترقى إلى مستوى النزاع المسلح[2].

**رابعا:** بناء قدرات الدول الضعيفة سيبرانيا، وذلك من خلال مساعدتها على تطوير البنية التحتية الرقمية وتعزيز قدراتها على الإستجابة للأخطارالسيبرانية ضمن إطار قانوني دولي مشترك، يمكّن من تقليل الفجوة الرقمية وتعزيز الأمن السيبراني العالمي[3].

يتضح من خلال ما سبق أن مسألة تطبيق القانون الدولي الإنساني على الحرب السيبرانية، تمثل إحدى أبرز الإشكاليات القانونية المعاصرة، وبسبب الطابع المعقد لهذا النوع من النزاعات واختلافه الجوهري عن النزاعات التقليدية، ظهر تيار فقهي يرى في القانون الدولي الإنساني إطارا مرنا يمكنه استيعاب هذه التغيرات.

[1]. انظر سفيان شعلال، **الحرب السيبرانية وتحديات القانون الدولي الإنساني**، مجلة الآداب والعلوم الإنسانية والإجتماعية، بدون دارالنشر، الجزائر، العدد 28، 2023، ص ص 213-215.

[2]. انظر شيماء طه، **الفضاء السيبراني في القانون الدولي: الطبيعة القانونية وحدود التنظيم**، مجلة المستقبل القانوني، العدد 30، جامعة أسيوط، مصر، 2023، ص ص 87-89.

[3]. انظر عبد العزيز عرابي، **الهجمات السيبرانية في ضوء القانون الدولي الإنساني**، مجلة الدراسات القانونية والسياسية، العدد 15، جامعة القاهرة، مصر، 2022، ص ص 134- 136.

## المبحث الثاني: الجهود الدولية في تنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني وتقرير المسؤولية الدولية عن الحرب السيبرانية

مع تزايد الإعتماد على الفضاء السيبراني في المجالات العسكرية والمدنية على حد سواء، برزت تحديات قانونية وأمنية غير مسبوقة تتعلق بإستخدام القوة السيبرانية في النزاعات المسلحة، فالحرب السيبرانية بخصائصها الفريدة مثل عدم التحديد المكاني والجهة الفاعلة غير الحكومية... أثارت تساؤلات عميقة حول مدى كفاية الإطار القانوني الدولي الحالي، ولا سيما القانون الدولي الإنساني في مواجهة هذه التهديدات. من هذا السياق كثفت الدول والمنظمات الدولية جهودها لوضع معايير قانونية وأخلاقية تنظم استخدام القدرات السيبرانية في النزاعات، كما سعت إلى تطوير آليات فعالة لتحديد المسؤولية عن الأفعال السيبرانية الضارة، سواء ارتكبتها دول أو جهات فاعلة من غير الدولة .

على ضوء ذلك سنقسم هذا المبحث إلى مطلبين؛ نتناول في المطلب الأول الجهود الدولية المبذولة لتنظيم الحرب السيبرانية، وفي المطلب الثاني نتناول المسؤولية الدولية الناجمة عن الحرب السيبرانية .

**المطلب الأول: الجهود الدولية لتنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني**

سعت الدول والمنظمات الدولية الحكومية وغير الحكومية للتصدي لمخاطر الحرب السيبرانية وتنظيم الفضاء السيبراني، من خلال عقد إتفاقيات وإعداد دراسات وإبتكار تقنيات إلكترونية للسيطرة على هذا السلاح الشديد الخطورة والدائم التطور.

تناولنا مختلف هذه الجهود في فرعين متتاليين؛ الفرع الأول يتضمن الإعلانات والإتفاقيات الدولية الخاصة بتنظيم الحرب السيبرانية وفق مبادى القانون الدولي الإنساني، والفرع الثاني يتضمن المنظومات التقنية للحد من الحرب السيبرانية.

**الفرع الأول: الإعلانات والإتفاقيات الدولية الخاصة بتنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني**

قامت العديد من الدول بوضع قوانين لتحريم الجرائم السيبرانية وفرض عقوبات للحد منها، إلى جانب إبرام اتفاقيات ومعاهدات دولية، مساهمة بشكل كبير في تقنين هذه الجرائم والحد من الحروب السيبرانية، ولا تتصف عملية التشريع الخاصة بالهجمات في الفضاء السيبراني بالسهولة، بل تواجه تحديات كبيرة بسبب التطور السريع في هذا المجال وصعوبة كشف هوية المجرمين واسترجاع البيانات وفك تشفيرها.

بدأت الجهود الدولية مع نشر الجمعية العامة للأمم المتحدة للدليل المعروف باسم "دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها" عام 1994، حيث ركز على الجريمة الحاسوبية دون الاعتماد على مسميات أخرى (جرائم سيبرانية، جرائم إلكترونية)، ولم يتم التطرق لها بشكل شامل[1].

كما صدر إعلان فيينا بتاريخ: 17 أفريل 2000 عن مؤتمر الأمم المتحدة حول الجريمة و العدالة، حيث نصت الفقرة الثامنة عشر منه على ضرورة منع ومكافحة الجرائم المرتبطة بالحاسوب[2]، وقد دعا الإعلان لجنة منع الجريمة والعدالة الجنائية إلى الاضطلاع بالعمل في هذا الشأن، كما شدد على أهمية تعزيز التعاون الدولي في مواجهة الجرائم المرتبطة بالتكنولوجيا الرقمية، إلا أن هذه المادة تعاملت مع هجمات الفضاء الالكتروني على اعتبارها مسألة متعلقة بجرائم ذات طابع جنائي بالدرجة الأولى وليس شكلا جديدا مع المواجهات الدولية.

---

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 500 .

[2]. مؤتمرالأمم المتحدة بشأن الجريمة والعدالة، إعلان فيينا الصادر بتاريخ: 17 أفريل 2000، الفقرة 18 وجاء فيها: "نقرر صوغ توصيات سياسية ذات توجه عملي بشأن منع ومكافحة الجريمة المتعلقة بالحواسيب، وندعو لجنة منع الجريمة والعدالة الجنائية إلى الإضطلاع بعمل هذا الشأن، آخذة في الإعتبارالاعمال الجارية في المحافل أخرى، ونعلن رسميا إلتزامنا أيضا بالعمل على تعزيز قدرتنا على منع الجريمة المرتبطة بالتكنولوحيا الراقية والحواسيب والتحري عن تلك الجرائم وملاحقتها".

اعتمد البرلمان الأوروبي -أيضا- في أبريل 2001 الاتفاقية الأوروبية بشأن الجريمة السيبيرانية، والتي بدأت ملامحها من خلال لجنة الخبراء الأوروبيين (CDPC) التي تأسست في عام 1996 للعمل على معالجة الجرائم في الفضاء الالكتروني، وقد استمرت أعمال اللجنة من 1997 حتى 2000 لإعداد مشروع الاتفاقية، وتم اعتمادها رسميا عام 2001[1].

تهدف الاتفاقية المذكورة إلى توحيد التشريعات الجزائية المتعلقة بالجرائم الإلكترونية وتوفير الإجراءات القانونية اللازمة لمحاكمة مرتكبي الجرائم بواسطة أجهزة الكمبيوتر، كما أرست نظاما فعالا للتعاون الدولي يشمل تبادل المعلومات وحفظ الأدلة الالكترونية وتسليم المجرمين، هذه الإتفاقية هي اتفاقية بودابست لعام 2001، ويعاب على هذه الاتفاقية أنها تنفذ من قبل الأفراد وضد الأفراد دون التطرق إلى الهجمات السيبرانية التي تنفذها الدول ضد بعضها[2]، إذن فإتفاقية بودابست هي إتفاقية معنية بالجريمة السيبرانية وليست خاصة بالحرب الإلكترونية، لكن هذا لا يمنع من وجود تقاطعات من حيث إستخدام الفضاء الإلكتروني، وقد سبق وأن وضحنا الفرق بين الجريمة السيبرانية والهجمة السيبرانية والحرب السيبرانية والعلاقة التي تربطهم.

إضافة إلى اتفاقية بودابست لعام 2001، تم الإتفاق بين الدول على إصدار قانون "أونيسترال" النموذجي، والذي يتطلب استجابة ديناميكية في ضوء الطابع الدولي لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، وقد تم صياغة هذا القانون النموذجي بشأن التجارة الإلكترونية، وقانون آخر بشأن التوقعات الإلكترونية[3].

أصدرت الأمم المتحدة القرار رقم: 56/121 في 19 ديسمبر 2002 بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لقضية المعلومات، تضمن دعوة الدول الأعضاء إلى وضع تشريعات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات[4]، بعدها صدر القرار رقم: 58/32 بتاريخ: 18 ديسمبر 2003 الخاص بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي بشأن تعزيز التعاون الدولي لمكافحة إساءة استخدام تكنولوجيا المعلومات، وأكد على ضرورة استخدامها لأغراض سليمة للحفاظ على مستقبل مشترك للبشرية[5].

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق ، ص 500.
[2]. نور أمير موصلي، مرجع سابق، ص 168 .
[3]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 48.
[4]. نبيلة عبد الفتاح قشطى، مرجع سابق، ص 501.
[5]. نفس المرجع، نفس الصفحة.

في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة في تايلاندا بانكوك عام 2005 عقدت ورشة عمل بعنوان: "التدابير اللازمة لمكافحة الجريمة المرتبطة بالحاسوب"، وفي الثاني والعشرين من أبريل 2005، أصدر القرار رقم: 60/177 الذي دعا الحكومات لتنفيذ التوصيات التي خرجت بها الورشة[1].

وقد سعت الأمم المتحدة جاهدة ليكون لها دور في بناء الدبلوماسية السيبرانية سنة 2004، حيث كونت فريقا من الخبراء الحكوميين (Group of Government Experts) لتحقيق التعاون الدولي في دراسة قضايا الأمن السيبراني والحرب السيبرانية، وقدمت العديد من التوصيات بشأن التدابير الرامية إلى تقليل التهديدات والمخاطر السيبرانية وزيادة الاستقرار[2].

في عام 2013 نادى فريق الخبراء الحكوميين من خلال الجهود الدبلوماسية على أن مبدأ السيادة الوطنية ينطبق على الفضاء السيبراني بدرجة انطباقه على الأرض نفسها، كما تم الاتفاق على قائمة مطولة من القواعد والإجراءات لبناء الثقة في الفضاء السيبراني، ويعد دليل تالين الصادر في 2013 مرجعا فنيا وأكاديميا، غير أنه لا يشكل مصدرا رسميا من مصادر القانون الدولي، مثل المعاهدات والعرف لأنه غير ملزم قانونا، لكن رغم ذلك يكتسب أهمية عملية في مجال تنظيم الحرب السيبرانية، كونه يمثل إجتهادا فقهيا جماعيا من خبراء قانونيين دوليين، سعى إلى تفسير كيفية تطبيق قواعد القانون الدولي -لا سيما القانون الدولي الإنساني- على الفضاء السيبراني، وهو يستخدم من قبل العديد من الدول والجهات الفاعلة كمرشد لفهم وتطوير سياستها السيبرانية، إلا أن ما ورد فيه لا يعبر عن توافق دولي أو إلتزام قانوني، بل يظل في إطار التوجيه القانوني غير الملزم الذي قد يساهم في تطوير الأعراف الدولية مستقبلا[3].

في أبريل عام 2015 صدر تقرير عن مجموعة من الخبراء، شكلت من طرف مجلس الأمم المتحدة وأقرته مجموعة العشرين، يقضي بوضع معايير للحد من المواجهات في الفضاء الإلكتروني، وتضمن هذا التقرير معايير معالجة سلامة وأمن البيانات[4].

إن اللجنة الدولية للصليب الأحمر كان لها دور مهم في تأطير وتنظيم الحرب السيبرانية، فقد قدمت العديد من البيانات والتقارير تؤكد فيها أن مبادئ القانون الدولي الإنساني مثل التمييز بين الأهداف المدنية والعسكرية تنطبق على الهجمات السيبرانية في سياق النزاعات المسلحة، وشاركت في إعداد دليل تالين وقدمت العديد من الدراسات، ولا زالت لحد الساعة تدافع عن الإنسان وتظهر فظاعة وخطورة هذه

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص501.
[2].الأمم المتحدة ،تقرير الفريق الحكومي الدولي للخبراء في أمن المعلومات، الجمعية العامة، 2004.
[3]. راجع قاعدة 11 من دليل تالين لسنة 2013.
[4]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 502.

الحرب، فقد قدمت في سبتمبر 2024 تقريرا بعنوان: "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، هذا التقرير أعطى نظرة شاملة عن التحديات الرئيسية التي يواجهها القانون الدولي الإنساني في سياق النزاعات المسلحة الحديثة، وركز على موضوعات مثل الأسلحة النووية، الحروب الهجينة، حماية الأفراد المحتجزين والتقنيات الحديثة في الحروب[1].

من جانب آخر حاول الاتحاد الدولي للاتصالات (Itu) وضع معايير تقنية وأخلاقية للأمن السيبراني من خلال مبادرات مثل: الأجنحة العالمية للأمن السيبراني والتي تسعى لتعزيز التعاون الدولي لمواجهة الجريمة السيبرانية والهجمات ذات الطبيعة العسكرية[2].

غالبا ما تسفر الهجمات السيبرانية عن إحداث توتر واحتقان في العلاقات الدبلوماسية بين الدول، ولعل أهم هذه الهجمات هو تصاعد ذروة الحرب السيبرانية بين كل من روسيا والولايات المتحدة الأمريكية على خلفية اتهام وجّه إلى روسيا بالتدخل في الانتخابات الرئاسية الأمريكية لصالح دعم ترامب واختراق البريد الالكتروني لحملة المنافس، مما شكّك في شرعية الانتخابات الأمريكية[3].

غالبا ما تلجأ الدول لوسائل تنطوي على استخدام الأدوات الدبلوماسية التقليدية للاستفادة من الفضاء السيبراني، وبالشكل الذي يعمل على احتواء التهديدات والهجمات السيبرانية، وهناك العديد من الأمثلة التي أظهرت أهمية الدبلوماسية في احتواء الصراعات السيبرانية كإتفاق الأمن السيبراني بين الولايات المتحدة الأمريكية والصين عام 2015[4].

يتضح مما سبق أن هناك جهودا دولية مستمرة ومحاولات متواصلة من أجل وضع إطار تشريعي ينظم ويقيد عمليات الهجوم في الفضاء الإلكتروني، إلا أن هذه الجهود الدولية والمساعي ظلت دون توافق عالمي نظرا لغياب التوافق السياسي بين الدول لبلورة هذا الإطار التشريعي، وكذلك طابع التشكيك في النوايا.

**الفرع الثاني: المنظومات التقنية للحد من الحروب السيبرانية**

مع تزايد التهديدات السيبرانية وتطور أدوات الحرب الرقمية، برزت الحاجة الملحة إلى تطوير منظومات تقنية قادرة على الوقاية من هذه التهديدات أو الحد من آثارها، فقد أضحى الفضاء السيبراني ساحة معقدة للصراعات لا تقتصر على الفاعلين الحكوميين فحسب، بل تشتمل أيضا جهات غير رسمية

[1]. اللجنة الدولية للصليب الأحمر، **القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة،** على الرابط: https://www .icr.org/en/report/2024-icrc-report-ihl-challenges تاريخ الإطلاع:2025/05/10وقت الاطلاع:12:20
[2]. الإتحاد الدولي للإتصالات، الأجندة العالمية للأمن السيبراني، جنيف 2008 .
[3]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1295 .
[4]. نفس المرجع، نفس الصفحة

تملك قدرات تقنية متقدمة. في هذا السياق باتت المنظومات التقنية كأنظمة الحماية المتقدمة، تقنيات الذكاء الإصطناعي ونظم الإنذار المبكر تلعب دورا محوريا في التصدي للهجمات السيبرانية ورصدها وتحليلها والتقليل من أضرارها على البنية التحتية الحيوية والمصالح الوطنية للدول. هذا ويعد فهم كيفية توظيف هذه المنظومات وتطويرها عملا حاسما في تعزيز الأمن السيبراني، وفي بناء إستراتيجيات فعالة تواكب تسارع وتيرة الحروب السيبرانية وتعقيداتها.

يمكن تقسيم الأساليب التقنية الخاصة بالتصدي للهجمات الإلكترونية ومواجهتها إلى أساليب رئيسية (أولا)، أساليب احتياطية (ثانيا) وأساليب تعزيزية (ثالثا). وهو ما سيتم التفصيل فيه على النحو التالي:

**أولا: الأساليب الرئيسية لمواجهة الهجمات الإلترونية**

إنّ الأساليب التقنية الرئيسية الخاصة بالتصدي للهجمات الإلكترونية ومواجهتها تتمثل في ثلاث أنواع هي: الجدران النارية "Firewall"، البرامج المضادة للفيروسات "Antivirus program" وأنظمة كشف السلام "IDS"[1]:

**أ- الجدران النارية**: نظرا لانتشار اختراقات شبكة الانترنت المستجدة، ظهرت هذه التقنية في أواخر الثمانينات من القرن الماضي، وظهر منها عدة أجيال:

**1- الجيل الأول**: يعرف بمرشحات العبوة "Packet Filters" يقوم على فلترة الوحدة الأساسية المخصصة لنقل البيانات بين أجهزة الكمبيوتر على الانترنت، فإذا كانت العبوة تطابق شروط الجدار يسمح بمرورها، وإذا لم تكن مطابقة يرفضها ويتخلص منها ويقوم بإرسال إشارة خطأ (Error) للمصدر[2].

**2- الجيل الثاني**: يعرف بفلتر محدد الحالة "Stateful Filter"، يقوم بمراقبة حقول معينة في المعلومات المستقبلية ويقارنها بالحقول المناظرة لها في سلسلة كاملة من المعلومات الواردة ضمن السياق نفسه، ثم يرفض المعلومات التي لا تلتزم بقواعده، حيث تكون دليلا على أنها زرعت في السياق وليست جزءا منه، مما يثير الشك بأنها برامج خبيثة[3].

[1]. يحي الحياني وآخرون، مرجع سابق، ص 40.
[2]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 496 .
[3]. نفس المرجع، ص 497.

**3- الجيل الثالث**: يعرف باسم طبقات التطبيقات "Application Layer Firewall"، يتعامل مع التطبيقات والأنظمة المعقدة، بإمكانه اكتشاف إذا ما كان هناك نظام غير مرغوب فيه تم تسريبه أو إذا كان هناك نظام تم استخدامه بطريقة مؤذية[1].

هذا وتقوم تقنية "الجدران النارية" بمختلف أجيالها على مبدأ الفصل بين المناطق الموثوق بها والمناطق غير الموثوق بها في شبكات الكمبيوتر، وتقوم بمراقبة العمليات التي تمر بالشبكة ورفض أو السماح بالمرور، لهذا تعتبر من أهم وسائل الدفاع التقنية لصد الحرب الإلكترونية.

**ب- البرامج المضادة للفيروسات ( Antivirus program):** في أواخر الثمانينات من القرن الماضي تم تطوير برامج مضادة للفيروسات، نظرا لزيادة المخاطر التي تهدد أجهزة الكمبيوتر، فيقوم مضاد الفيروسات برصد نظام للاشتباه في تصرفات البرنامج، فإن اكتشف سلوكا مريبا يقوم بعمل فحص في البرنامج، ويمكن استخدام هذا الأسلوب لتحديد الفيروسات غيرالمعروفة أو نسخ أخرى من الفيروسات الموجودة، وتتصدى مضادات الفيروسات "للديدان الحاسوبية"، وهي برامج صغيرة تصنع للقيام بأعمال تدميرية أو سرقة البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للانترنت[2].

هناك أسلوب مضاهاة ملف "File Emulation"، ويتم فيه تنفيذ البرامج في بيئة افتراضية والاعتماد على الإجراءات التي تم تسجيلها، ويستطيع برنامج مضاد الفيروسات تحديد ما إذا كان البرنامج ضارا أم لا ويتخذ الإجراءات المناسبة[3].

تعد هذه التقنية الأكثر انتشارا في التصدي للهجمات الإلكترونية، وهو برنامج يتم استخدامه لاكتشاف البرامج الضارة، ومنعها من إلحاق الضرر بالكمبيوتر أو سرقة البيانات عن طريق إزالتها أو إجراء تعديلات عليها.

**ج- أنظمة كشف التسلل "Intrusion Détection Systemd"(IDS):** تتألف أنظمة كشف التسلل من عدة مكونات هي[4]:

1- جهاز استشعار ينبه على وقوع الأحداث.

2- لوحة تحكم لمراقبة الأحداث المتلقاة من خلال أجهزة الاستشعار.

3- محرك يسجل إدخالات الأحداث المتلقات من خلال أجهزة الاستشعار في قاعدة البيانات.

---

[1]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 497.
[2]. نفس المرجع، ص 498.
[3]. نفس المرجع، نفس الصفحة.
[4]. نفس المرجع، نفس الصفحة.

وهذه الأنظمة هي برامج مصممة للكشف عن محاولة الوصول إلى نظام أجهزة الكمبيوتر غير المرغوب بها أو محاولة تعطيل هذا النظام بشكل عام أو التلاعب به، ككسر الحماية أو استخدام البرامج الضارة.

**ثانيا: الأساليب الاحتياطية لمواجهة الهجمات الإلترونية**

بالإضافة إلى الأساليب والإجراءات الرئيسية لمواجهة الهجمات الإلكترونية (السابق ذكرها)، هناك إجراءات أخرى احتياطية تلجأ إليها الدول لحماية بياناتها خاصة المتعلقة بالأمن القومي نذكر منها: فصل وتقسيم الشبكات، التشديد على بيانات الدخول وعمل نسيج احتياطي"Back up"[1]:

**أ- التقسيم الشبكي (Subnetti) :** يتم فصل الشبكة إلى شبكات فرعية، بحيث تكون لكل منها قواعد دخول خاصة بها بهدف عزل الهجمات ومنع انتشارها في كامل النظام، إذا استهدفت شبكة فرعية فإن الضرر يظل محصورا فيها ولا يمتد إلى بقية الشبكة[2].

**ب- التشديد وعدم السماح للدخول إلى الشبكة:** أي التشديد على التحقق من هوية المستخدمين عند الدخول إلى الشبكات لاسيما الشبكات الحكومية، واستخدام وسائل مثل: كلمات مرور قوية، أرقام وطنية، الرسائل النصية لهواتف معتمدة، فهذا يساهم في الحد من التسلل والاختراق غير المصرح به[3].

**ج- النسخ الاحتياطي الدوري (Backup)**: وذلك بإنشاء نسخ احتياطية دورية ومنتظمة لكافة البيانات الحيوية والمعلومات المهمة، بجيث يتم النسخ على وسائل خارجية آمنة مثل أقراص صلبة غير متصلة بالشبكة بهدف استعادة البيانات بسرعة في مجال الهجوم أو الفقدان[4].

**د- تشفير الشبكات والبيانات:** يعني ذلك اعتماد تشفير قوي للبيانات المتبادلة داخل الشبكة والمخزنة عليها البيانات، وذلك يمنع المتسللين من استغلال البيانات حتى لو تم الوصول إليها، كما أنّ تخزين البيانات في أنظمة منفصلة وآمنة يزيد من مرونة النظام وأمنه[5].

**ثالثا: أساليب تعزيزية لمواجهة الهجمات الإلترونية**

بالإضافة إلى الأساليب والتقنيات المذكورة أعلاه، هناك إجراءات إضافية أخرى تساهم في تعزيز أمن المعلومات وتقليل الخسائر الناتجة عن الهجمات السيبرانية المحتملة.

---

[1]. يحي الحياني وآخرون، مرجع سابق، ص 40.
[2]. نبيلة عبد الفتاح قشطي، مرجع سابق، ص 499.
[3]. نفس المرجع، نفس الصفحة.
[4]. نفس المرجع، نفس الصفحة.
[5]. نفس المرجع، نفس الصفحة.

هناك العديد من التسميات لبرامج الحماية، وهي تختلف من دولة لأخرى لكن كلها تصب في قالب واحد هو الدفاع للتغلب على التحديات السيبرانية، وبموجبها يقع على عاتق الدول اتباع الخطوات التالية:

**أ- التدريب والتطوير المستمر:** يقع على الهيئات المعنية تلقي تدريبات مستمرا، لتعزيز مهاراتها ومعارفها، وحتى تتمكن من مواجهة التهديدات والتقنيات الناشئة ومواكبة التطورات.

**ب- الأتمتة والتنسيق:** يقصد بالأتمتة إستخدام التكنولوجيا (مثل الروبوتات والذكاء الإصطناعي والبرمجيات) لأداء مهام أو عمليات بطريقة تلقائية، بحيث تؤدي أدوات الأتمتة والتنسيق إلى تحسين كفاءة وفاعلية مركز عمليات الأمن، وتساعد على فهم التعقيدات التكنولوجية وإتخاذ القرار[1].

**ج- البحث الإستباقي في التهديدات:** وذلك بالبحث عن التهديدات المخفية والهجمات المبكرة[2]، وتجدر الإشارة في هذا الشأن أنّ مسألة الحماية والدفاع الرقمي تتمتع به الدول التكنولوجية المتطورة، أما الدول المصنفة كعالم ثالث فهي غير قادرة للوصول إلى هذا المستوى بسبب ضعف التكنولوجيا .

**المطلب الثاني: المسؤولية الدولية الناجمة عن الحرب السيبرانية**

في ظل تزايد الإعتماد على الفضاء السيبراني، ظهرت تحديات جديدة في مجال القانون الدولي، لاسيما فيما يتعلق بالمساءلة القانونية عن الأعمال العدائية التي تشن عبر الفضاء الرقمي، فقد أصبحت الهجمات السيبرانية وسيلة متاحة للدول والجماعات الفاعلة، مما يثير تساؤلات جدية حول كيفية تحديد المسؤولية في ظل الطبيعة غير التقليدية لهذا النوع من الحروب، خاصة عندما تكون الجهة المنفذة غير معروفة أو ليست كيانا دوليا، وبالتالي لا بد من تأصيل قانوني دقيق في ضوء قواعد القانون الدولي العام والقانون الدولي الإنساني.

على ضوء ما سبق نتناول هذا المطلب في ثلاثة فروع؛ حيث سنتطرق في الفرع الأول لأحكام المسؤولية الدولية عن الحرب السيبرانية، وفي الفرع الثاني للأساس القانوني لقيام المسؤولية الدولية عن الحرب السيبرانية، وفي الفرع الثالث لمسألة التعويض عن الأضرار الناجمة عن الحرب السيبرانية.

**الفرع الأول: أحكام المسؤولية الدولية عن الأفعال السيبرانية**

إن انتهاك القوانين والاعراف الدولية والإعتداء على المدنيين يرتبط بفكرة المسؤولية، وتتعلق المسؤولية هنا بالدولة والفرد. والأفعال السيبرانية تعدّ من الانتهاكات الدولية التي تنتج عنها مسؤولية تستوجب التعويض وإصلاح الضرر.

[1]. يحي الحياني وآخرون، مرجع سابق، ص 52.
[2]. نفس المرجع، نفس الصفحة.

في البداية لا بد من التطرق لتعريف المسؤولية الدولية (أولا)، حتى نتمكن من فهم العلاقة التي تربط عناصرها (ثانيا):

**أولا: تعريف المسؤولية الدولية**

تعرف المسؤولية الدولية بأنها: "ما ينشأ نتيجة عمل مخالف لالتزام قانوني دولي ارتكبه أحد أشخاص القانون الدولي وسبّب ضررا لشخص دولي آخر، وتكون غاية المسؤولية الدولية التعويض على هذا الضرر"[1]، وعرفها آخرون بأنها: "الإلتزام الذي يفرضه القانون الدولي على الشخص بإصلاح الضرر لصالح من كان ضحية، سواء كان تصرف أو إمتناع، وتحمل العقاب جزاء هذه المخالفة[2].

عرفت لجنة القانون الدولي المسؤولية الدولية بأنها: "إسناد فعل غير مشروع دوليا لأحد أشخاص القانون الدولي العام، مما يرتب إلزامه بدفع التعويض أو جبر الضرر الذي حدث نتيجة هذا الفعل غير المشروع دوليا"[3].

نستنتج من خلال التعريفات السابقة أنّ المسؤولية الدولية هي علاقة بين شخصين من أشخاص القانون الدولي، يلتزم أحدهما بتعويض الضرر الذي سببه للآخر. وقد ساهم كل من الفقه والقضاء الدوليين في تطوير قواعد المسؤولية الدولية على نحو يكفل ضمان المشروعية الدولية، لاسيما القواعد الآمرة التي تنظم المصالح الأساسية والضرورية للإنسانية، فالمسؤولية الدولية هي نظام قانوني يترتب بموجبه على الدولة التي ارتكبت عملا يجرمه القانون الدولي التعويض عن الضرر الذي لحق بالدولة المعتدى عليها.

إذن المسؤولية الدولية وفقا للمفهوم القديم مسؤولية ضيقة تقوم على ثلاثة ركائزهي: أشخاص القانون الدولي العام متمثلة في الدولة فقط، واقتصار المسؤولية الدولية التي تتحملها الدولة في صورة تعويضات، بالإضافة إلى أنّ حدود المسؤولية تقف عند أضرار الدولة الناجمة عن أعمال يعاقب عليها القانون الدولي.

**ثانيا: عناصر المسؤولية الدولية**

حتى تقوم المسؤولية الدولية يجب توافر ثلاثة عناصر نذكرها على النحو التالي:

---

[1]. فلك هاشم عبد الجليل المهيرات، **المسؤولية الدولية للمنظمات الدولية في القانون الدولي العام**، رسالة ماجستير في القانون، جامعة الشرق الأوسط، الأردن، 2016، ص 23.
[2]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1273 .
[3]. نفس المرجع، نفس الصفحة.

**أ- الفعل:** هو سلوك غير مشروع دوليا أو حتى تصرف مشروع لكنه يسبب ضررا لأي شخص من أشخاص القانون الدولي، ويشترط لوجود هذا الفعل أن ينتهك مبادئ القانون الدولي[1].

**ب - العلاقة السببية:** المقصود بها ضرورة إسناد أو نسبة الواقعة المنشئة للمسؤولية الدولية لأحد أشخاص القانون الدولي العام سواء كانت دولة أو منظمة دولية، أما الأعمال التي تنسب إلى أفراد عاديين فإن الدولة تكون مسؤولة عنها بشروط وضوابط وأحوال معينة، لأن القاعدة العامة هي عدم مسؤولية الدولة عن تصرفاتهم، والاستثناء أن تنعقد مسؤوليتها في حالتين[2]:

1- تتمثل الحالة الأولى في تصرف الفرد بناء على تعليمات من الدولة وبتوجيه منها وتحت رقابتها.

2- أما الحالة الثانية فهي عدم بذل الدولة العناية الواجبة لمنع هذه الأعمال التي يترتب عليها ضررا للآخرين.

ما تجدر الإشارة إليه أنه يمكن أن تشترك في المسؤولية الدولية أكثر دولة إذا تم الفعل غير المشروع بمساهمة مشتركة، كما تسأل الدولة إذا سمحت بالتصرف الضار أن يمر عبر الفضاء السيبراني لها أو ساعدت على ذلك، ومن ناحية أخرى يمكن أن تشترك المسؤولية بين الدولة والأفراد كما في جرائم الحرب السبيرانية، فيتحمل الأفراد المسؤولية الدولية الجنائية وتتحمل الدولة المسؤولية المدنية أو التعويض، كما تسأل المنظمات الدولية عن الأعمال غير المشروعة التي يرتكبها موظفوها والأجهزة التابعة لها والتي تتصرف باسمها[3].

**ج - الضرر:** يعرف الضرر بأنه: "كل ضرر يلحق مصلحة أو حق مشروع لأحد أشخاص القانون الدولي العام، وهذا الضرر قد يكون ماديا أو معنويا"[4].

يعد الضرر أهم عنصر من عناصر المسؤولية، لأنه إذا انعدم الضرر انعدمت المسؤولية، وللضرر أنواع؛ فبالنظر إلى مصلحة المعتدى عليه ينقسم إلى ضرر مادي وضرر معنوي، وبالنظر للجهة التي لحقها الضرر نجد هناك ضرر مباشر وضرر غير مباشر.

وقد عرّف الفقهاء الضرر المادي بأنه: "كل مساس بحق من حقوق الشخص القانوني الدولي المادية أو بحقوق رعاياه، مما يترتب عليه أثرا ملموسا ظاهرا للعيان ويكون مباشرا. أما الضرر المعنوي فهو

---

[1]. انظر فلك هاشم عبد الجليل المهيرات، مرجع سابق، ص 39.
[2]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1277.
[3]. وائل احمد علام، **مركز الفرد من النظام القانوني للمسؤولية الدولية**، بدون رقم الطبعة، دار النهضة العربية، مصر، 2001، ص 25.
[4]. فلك هاشم عبد الجليل المهيرات، مرجع سابق، ص 40.

كل مساس بشرف أو اعتبار الشخص الدولي أو بأحد رعاياه، أي أنّ الضرر المعنوي هو كل إعتداء على حق من حقوق الأشخاص الدوليين أو رعاياهم، وتترتب عنه آثار غير ملموسة"[1].

تطبيقا على الهجمات السيبرانية نجد بأن الضرر بكافة أشكاله يتحقق من تلك الهجمات سواء كان الفاعل دولا قومية، كما حصل في الهجوم الفيروسي على البرنامج النووي الإيراني، أو تقوم به منظمات إجرامية تلحق أضرارا فادحة بالآخرين، خاصة في الهجمات التي تهدف لسرقة المعلومات كاختراق حسابات بنكية وسرقة أرقام بطاقات الإئتمان[2]، أو تعطيل نظام البنى التحتية للدولة كشبكات الماء والكهرباء أو إختراق الأنظمة الأمنية للدولة وتعريضها للهجوم السيبراني (هجمات تعرض الأمن والسلم الدوليين للخطر).

على الرغم من تحقق كل أركان المسؤولية الدولية في الهجمات السيبرانية، إلّا أن تحديد نطاق الضرر ووقت بدايته ونهايته ومعرفة الفاعلين ومراقبتهم وتتبعهم من أجل محاكمتهم أمر بالغ الصعوبة، وأحيانا يكون معرفة الفاعل مستحيلا، نظرا لما يتمتع به هذا الفضاء من إتساع وقابلية التخفي.

**الفرع الثاني: الأساس القانوني لقيام المسؤولية الدولية عن الحرب السيبرانية**

المسؤولية الدولية من المواضيع المهمة، وهي أهم ضمانة لكفالة تطبيق القانون الدولي بسبب غياب سلطة عليا مستقلة عن الدول تملك القدرة على فرض إحترام هذا القانون بمختلف فروعه -لاسيما بالنسبة لقواعد القانون الدولي الإنساني-، وهي تقوم على نظريتين هما: نظرية الفعل غير مشروع (أولا) ونظرية المخاطر (ثانيا)، وهو ما سيتم توضيحه فيما يلي على ضوء الحرب السيبرانية:

**أولا: المسؤولية عن الهجمات السيبرانية على أساس الفعل غير المشروع**

نظرية الفعل غير المشروع تعني الإخلال بالتزام دولي من قبل دولة، مما يستوجب مسؤولية هذه الدولة، سواء كان هذا الإخلال صادرا عن سلطة تشريعية أو تنفيذية أو قضائية وإلحاق ضرر بأحد الأجانب في شخصه أو ماله[3].

[1]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 51.
[2]. سامية صديقي، **المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي**، مجلة البحوث القانونية والإقتصادية، المجلد 6، العدد الأول، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2023، ص 829 .
[3]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 52.

إنّ الإخلال بالإلتزامات الدولية هو صورة من صور العمل غير المشروع، فإنتهاك إلتزام دولي ينشئ علاقة قانونية جديدة بين دولة صاحبة التصرف والدولة التي وقع الإخلال في مواجهتها، نجد الفقيه "بول روتر" يعتبر العمل غير المشروع أساسا لقيام المسؤولية الدولية بل الشرط الأهم لقيامها[1].

تعتبر الهجمات السيبرانية الدولية عملا غير مشروع، ويخضع للمسؤولية الدولية على هذا الأساس إذا توافر معيار الصفة الدولية، كما أنّ الهجمات الإلكترونية الدولية التي تخرق معاهدة أو عرف أو ميثاق دولي تعتبر عن عملا غير مشروع، لأنّ هذه الهجمات يترتب عنها أضرار سياسية وإقتصادية وإجتماعية وإستراتيجية، وقد تمس بأحد المبادئ التي كرستها الأمم المتحدة من أجل الحفاظ على الأمن والسلم الدوليين[2] .

إنّ إسناد المسؤولية للدولة عن أضرار ناتجة عن الهجمات السيبرانية معقد وصعب، خاصة من جانب تحديد هوية الفاعل، فأحيانا الدولة المسؤولة عن الضرر تنفذ هجوما سيبرانيا من دولة أخرى وتعتمد على أفراد ينتمون لدولة ثالثة.

إنّ التحقيق بشأن الهجمات السيبرانية قد يجمع بين المبادئ الأساسية لعمل أجهزة المخابرات، بوصفها عملا ماديا طبيعيا وبين الاختراق الإلكتروني العابر للحدود الدولية والشبكات، كما أنّ المحققين لا يمكنهم الولوج لدولة أخرى بإعتبار ذلك إنتهاكا لمبدأ السيادة[3]، وبهذا فالعمل غير المشروع يمس السلم الدولي ككل أو يمس دولة واحدة.

**ثانيا: المسؤولية الدولية عن الهجمات السيبرانية على أساس نظرية المخاطر**

جاءت نظرية المخاطر كنظرية حديثة نتيجة الإنتقادات التي وجهت لنظرية الفعل غير المشروع، هذه النظرية تقوم على أساس مساءلة الشخص القانوني الدولي الذي يقوم بإرتكاب سلوك مخالف للقانون الدولي أو غير مخالف، ولكنه على درجة من الخطورة وينتج عنه ضرر بدولة أخرى، إذن العبرة بحصول الضرر، ويؤكد أنصار هذه النظرية على أن المخاطر تقوم على فكرة تحمل النتائج المترتبة عن النشاطات الخطيرة وليس على أساس الخطأ[4].

من أهم الإتفاقيات التي أخذت بهذه النظرية نجد الإتفاقيات الخاصة بالطاقة الذرية مثل؛ إتفاقية باريس المتعلقة بالمسؤولية الدولية من قبل الغير في ميدان الطاقة النووية 1960[5].

---

[1]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 52..
[2]. نفس المرجع، نفس الصفحة.
[3]. سامية صديقي، مرجع سابق، ص 831.
[4]. نفس المرجع، ص 832.
[5]. راجع إتفاقية باريس المتعلقة بالمسؤولية الدولية من قبل الغير في ميدان الطاقة النووية، 1960.

هذه النظرية تقوم على شرطين هما: شرط الضرر وشرط الخطر. وبالنظر إلى الهجمات السيبرانية فهي أنشطة ضارة وخطرة في الفضاء السيبراني، وتسبب ضررا عابرا للحدود يمس البنية التحتية والأمن والسلم الدوليين[1].

ومنه نستخلص أن المسؤولية الدولية عن الهجمات السيبرانية في مجال قواعد القانون الدولي الإنساني قد لا تحقق أهدافها وأغراضها، ويرجع ذلك إلى صعوبة تحديد هوية المهاجم السيبراني وصعوبة ملاحقته قضائيا، حتى الضرر الناتج لا يمكن تحديده بدقة.

**الفرع الثالث: التعويض عن الضرر الناجم عن الحرب السيبرانية**

إنّ تحقق العناصر الثلاثة للمسؤولية السابق ذكرها (الفعل، العلاقة السببية والضرر) ينتج عنه قيام المسؤولية الدولية، وبالتالي التعويض عن الضرر، وهو ما يستوجب دراسة أشكال التعويض عن الضرر (أولا)، أساس التعويض عن الضرر في القانون الدولي الإنساني (ثانيا)، وكذلك مسألة إسناد التصرف في الفضاء السيبراني لأغراض المسؤولية الدولية:

**أولا: أشكال التعويض عن الضرر**

يترتب على المسؤولية الدولية عدة آثار قانونية، يأتي في مقدمتها التزام الدولة المسؤولة بجبر الضرر الذي نشأ عن التصرف غير المشروع، وأكد ذلك القضاء الدولي في العديد من أحكامه. ويتخذ التعويض عدة أشكال منها التعويض العيني، ويقصد به إعادة الأمور إلى ما كانت عليه قبل صدور التصرف أو التعويض المالي عن الضرر الناتج، وهذا هو الغالب واقعيا، وأشارت للتعويض المالي محكمة التحكيم الدائمة بأنه: "ليس بين مختلف مسؤوليات الدول فروق أساسية ويمكن تسويتها جميعا بدفع مبلغ من المال"[2]، وقد يتخذ التعويض صورة الترضية، كأن تقوم الدولة بتقديم اعتذارها وأسفها ويتم بالطرق الدبلوماسية.

أما التعويض عن الهجمات السيبرانية فيقصد به، "التزام يلقى على عاتق دولة ما في أعقاب حرب بتقديم تعويضات كافية عن الأضرار التي أصابت دولة أخرى أو رعاياها بسبب الحرب"[3].

[1]. سهيلة غجاتي و أميرة راهم ، مرجع سابق، ص 54.
[2]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1280.
[3]. نفس المرجع، ص 1278 .

**ثانيا: أساس التعويض في القانون الدولي الإنساني**

ألزمت المبادئ العامة لاتفاقيات لاهاي الأربعة لعام 1958، احترام قوانين وأعراف الحرب البرية وأوجبت على المحارب الذي يخل بأحكامها دفع تعويضات إذا اقتضت الحاجة، كما يكون مسؤولا عن جميع الأعمال التي يرتكبها أشخاص ينتمون إلى قواته المسلحة[1].

تنص المادة 91 من البروتوكول الإضافي الأول لعام 1977 على أن "يسأل طرف النزاع الذي ينتهك احكام الاتفاقيات او هذا اللحق (البروتوكول) عن دفع تعويض إذا اقتضت الحال ذلك، ويكون مسؤولا عن كافة الأعمال التي يقترفها الأشخاص الذين يشكلون جزءا من قواتها المسلحة"[2].

ومن المستقر عليه في القضاء والفقه والعمل الدولي أن مسؤولية الدولة حتى الآن هي مسؤولية مدنية. فإذا ثبتت مسؤولية الدولة عن أعمال سيبرانية فهذا ينجر عنه أيضا مسؤولية مدنية تستوجب التعويض. كما تضمنت اتفاقيات جنيف الدولية الأربعة لعام 1949 لأول مرة تعدادا للجرائم الخطيرة (الانتهاكات الجسيمة) الموقعة بسن تشريع لمعاقبتها. كما أنه أوجبت على هذه الدول معاقبة أي جريمة أخرى من جرائم القانون الدولي ولو لم يرد لها ذكر في هذا التعداد[3].

نستنتج مما سبق أن الدولة مسؤولة عن الأفعال السيبرانية التي تقوم بها أجهزتها وكل من يندرج تحت اختصاصها القضائي.

**ثالثا: إسناد التصرف في الفضاء السيبراني لأغراض المسؤولية الدولية**

يتيح الفضاء السيبراني للجهات الفاعلة إمكانيات تقنية متنوعة لإخفاء هيبتهم أو تزويرها، مما يزيد من تعقيد إسناد التصرف ويخلق صعوبات كبيرة، فعلى سبيل المثال ينطبق القانون الدولي الإنساني حتى أثناء النزاع المسلح على العمليات المرتبطة بالنزاع فحسب، وإذا تعذر تحديد منفذ العملية السيبرانية -وبالتالي يتعذر تحديد الصلة بين العملية أو النزاع المسلح– فقد يكون من الصعب تحديد ما إذا كان القانون الدولي الانساني ينطبق حتى على العملية أم لا.

يعد إسناد التصرف في العمليات السبيرانية مهمّا أيضا لضمان مساءلة الجهات الفاعلة التي تنتهك القانون الدولي بما في ذلك القانون الدولي الإنساني، وقد يؤدي التصور بأنه من السهل إنكار المسؤولية

[1]. ناجي محمد أسامة الشاذلي، مرجع سابق، ص 1279.
[2]. محمد فهاد الشلالدة، **القانون الدولي الإنساني**، بدون رقم طبعة، منشأة المعارف، الاسكندرية، مصر، 2005، ص 342.
[3]. نفس المرجع، ص 344.

عن هذه الهجمات أيضا إلى إضعاف الحظر المفروض على استخدامها، وقد يجعل الجهات الفاعلة أقل تدقيقا بشأن مخالفة القانون الدولي باستخدامها[1].

**أ- الأفعال التي تثير المسؤولية الدولية عن الحرب السيبرانية:** إنّ الدولة مسؤولة بموجب القانون الدولي عن التصرفات المسندة إليها، بما في ذلك انتهاكات القانون الدولي الإنساني، والتي تشمل :

1- تصرف من قبل أجهزة الدولة بما في ذلك قواتها المسلحة أو أجهزتها الاستخبارية.

2- تصرف من قبل أشخاص أو كيانات فوضتها الدولة للقيام بقدر من السلطة الحكومية مثل: الشركات الخاصة.

3- تصرف من قبل أشخاص أو مجموعات تعمل في الواقع بناء على تعليمات الدولة أو تحت إشرافها أو سيطرتها.

4- تصرف من قبل أشخاص أو مجموعات خاصة، والتي تعترف بها الدولة وتتبناها كتصرفات صادرة عنها.

**ب- صعوبة إسناد الفعل لمرتكب الحرب السيبرانية:** إن إحدى الخصائص الفنية للعمليات السبيرانية هي صعوبة نسبة أية عملية إلى مرتكبها، وفي هذا السياق قد يكون لتعريف "المرتكب" أو الجاني معاني كثيرة هي[2] :

1- آلة الهجوم التي تكون مرتبطة ارتباطا مباشرا بالهدف، وهذه الآلة هي الأقرب إلى الهدف، قد تخص طرفا ثالثا بريئا لا علم له بالعملية التي يجري تنفيذها.

2- الآلة التي أطلقت أو بدأت العملية.

3- مستخدم لوحة مفاتيح الآلة التي بدأت العملية.

4- البلد الذي يندرج تحت اختصاصه القضائي الفرد المذكور، مثال ذلك أنّ آلة توجد في روسيا قد يسيطر عليها فرد في فرنسا يتصرف نيابة عن الحكومة الإيرانية.

5- الكيان الذي تصرف لفرد تحت رعايته إن وجد.

في التطبيق العملي يستند الحكم على من تنسب إليه العملية إلى كل مصادر المعلومات المتاحة، التي قد تشتمل على التوقيعات الفنية والأدلة الجنائية التي جمعت فيما يتعلق بالفعل المعني، ومعلومات

[1]. هربت لين، **النزاع السيبراني والقانون الدولي الإنساني**، المجلة الدولية للصليب الأحمر، مجلد 94، العدد 886، 2012، ص 8.
[2]. نفس المرجع، ص 10.

الاستخبارات (مثل: المكالمات الهاتفية، التي التقطت أثناء مراقبة محادثات كبار القادة ومعرفة أولئك الذين لديهم دوافع للقيام بمثل هذه العمليات).

يقال في العادة من المستحيل نسبة عمليات سيبرانية معادية إلى مسؤول عنها، وتتضمن هذه المقولة شيئا من الحقيقة، فلو أن الجاني لا يرتكب الأخطاء ويستخدم أساليب لم تلاحظ من قبل ولا يترك خلفه أية أدلة تشير إليه، ولا يتحدث عن العملية في مكان عام أو مراقب ولا يقوم بأفعاله أثناء فترة تكون فيها دوافعه لتنفيذ مثل هذه العمليات معروفة للجمهور، فإن تحديد هوية الجاني قد يكون مستحيلا.

والحقيقة أنه في بعض الأحيان تتحقق كل الشروط ويشعر صناع القرار باليأس لعدم قدرتهم على التصرف بالشكل المناسب في مثل هذه الظروف، ولكن في حالات أخرى لا تكون مشكلة تحديد المسؤولية بهذه الصعوبة بأن واحدا أو أكثر من الشروط لم يتحقق، وقد يكون من الممكن إصدار بعض الأحكام المفيدة (وإن كانت غير كاملة) بشأن إسناد المسؤولية عن العملية، على سبيل المثال لو لم يعرف مكان الآلة التي أطلقت هجوما معينا، فقد تتيح المؤشرات أو الاستخبارات البشرية تحديد هوية الكيان الذي أطلق الهجوم تحت رعايته، وقد يكون الأمر الأخير هو كل ما يلزم لاتخاذ مزيد من الإجراءات ضد الجاني .

**خلاصة الفصل الثاني :**

من خلال دراستنا للإطار القانوني الناظم للحرب السيبرانية وعلاقته بمبادى القانون الدولي الإنساني، نجد أن دليل تالين أفضل مرجع قانوني، وهو الأهم لحد الساعة بالرغم من أنه مجرد مشروع قانون ولايكتسب الصفة الإلزامية، لأنه حاول تقنين الحرب السيبرانية في إطار النزاع المسلح، وبخصوص إمكانية تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية ظهر اتجاهان مختلفان: اتجاه مؤيد أعطى حججا مقنعة، وإتجاه معارض حدد أسباب إعتراضه، ونتيجة لهذين الموقفين ظهر اتجاه ثالث وهو الأرجح، حيث يرى إمكانية تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية، مع ضرورة تطوير القواعد القانونية الموجودة وإعطاء دليل تالين القوة الإلزامية، وضرورة بذل جهود دولية أكثر لمواجهة خطر السيبرانية سواء عن طريق منظومات قانونية أو منظومات تقنية.

أما بخصوص مسألة المسؤولية الدولية الناجمة عن الحرب السيبرانية، فنجد أن قواعد المسؤولية التقليدية يصعب تطبيقها بسبب طبيعة وخصائص هذه الحرب، كتحديد الفاعل، والضرر، والعلاقة السببية، لذلك لا بد من تطويرها هي أيضا.

# الخـــاتمـــــة:

**الخـــاتمـــة :**

إنّ العالم اليوم يشهد نوعا جديدا من الحروب، وذلك بسبب التقدم التكنولوجي الذي فرض تحولات في طبيعة النزاعات المسلحة، وقد برزت الحرب السيبرانية كوجه جديد ومعاصر من الحروب متجاوزة بذلك الحدود التقليدية للمعارك .

من خلال هذه الدراسة قمنا بإعطاء مفهوم للحرب السيبرانية وإظهار طبيعتها القانونية وما تتميز به من خصائص، وذلك لغرض الوصول إلى الإطار القانوني الذي ينظمها وعلاقتها بمبادئ القانون الدولي الإنساني الذي يطبق في حالة النزاعات الدولية التقليدية، ومناقشة الخلافات القائمة بخصوص انطباقها أو عدم انطباقها على الحرب السيبرانية، كما تطرقنا للجهود الدولية المبذولة للتصدي لهذه الحرب ومعالجة فكرة المسؤولية الناجمة عن الحرب السيبرانية، حيث توصلنا إلى مجموعة من النتائج مرفوقة بجملة من الإقتراحات، نوردها على النحو التالي :

**أ- النتائج :**

1- الحرب السيبرانية هي استخدام متعمد وممنهج للوسائل التكنولوجية والقدرات الإلكترونية من قبل دول أو أطراف فاعلة غير حكومية، بهدف شن هجمات رقمية على البنى التحتية الحيوية أو الأنظمة المعلوماتية التابعة لجهات معادية، وذلك ضمن سياق نزاع مسلح فعلي أو كوسيلة لتحقيق أهداف عسكرية إستراتيجية، بحيث تحدث هذه الهجمات آثارا مماثلة أو تجاوز آثار الوسائل الحربية التقليدية.

2- تتميز الحرب السيبرانية بمجموعة من الخصائص أهمها: اللامادية، عابرة للحدود، تعدد الفاعلين، السرعة والخفاء، وصعوبة الإسناد. كما تتميز بطبيعة قانونية مرنة، مما يطرح إشكال صعوبة تطبيق القواعد القانونية الخاصة بالحروب الكلاسيكية، كما أنها تعد أكبر وأخطر تهديد للأمن والسلم الدوليين.

3- يكفل القانون الدولي العام بصفة عامة والقانون الدولي الإنساني بصفة خاصة -لاسيما بخصوص مبادئه الأساسية- الحماية القانونية للبنية التحتية وللمدنيين ضد الهجمات السيبرانية، مع تسجيل الثغرات القانونية التي تفرضها طبيعة الحرب السيبرانية .

4- هناك صعوبة في تطبيق مبادئ القانون الدولي الإنساني على الحروب السيبرانية، حيث –عمليا- نواجه صعوبات تقنية وقانونية، فالتمييز بين الأهداف العسكرية والمدنية في الفضاء السيبراني يظل معقدا، كما أنّ حساب التناسب بين الضرر العسكري المرجو والأضرار الجانبية يصعب تقديره في العمليات السيبرانية. نفس الأمر بالنسبة لتطبيق مبدأ الإنسانية وكذلك صعوبة تحديد الفاعل المسؤول، وبالتالي فمن الصعب مساءلة الدولة أو الكيان المسؤول عن الهجمات السيبرانية في ظل غياب أدلة تقنية.

5- مبدأ الإنسانية ومبدأ مارتينز من أهم المبادئ الدولية التي تحد من الهجمات السيبرانية، وهي أساس توقيع المسؤولية الدولية .

6- يعتبر دليل تالين الأول أهم وأول دراسة أكاديمية وقانونية، جاء بمجموعة من القواعد الناظمة للحرب السيبرانية معتمدا في ذلك على مبادئ القانون الدولي الإنساني، بعدها جاء دليل تالين الثاني كتكملة للدراسة السابقة وسد الثغرات القانونية، لكن كونه غير ملزم دوليا بقي الإشكال قائما .

7- هناك العديد من الجهود الدولية لمواجهة الحرب السيبرانية، أهمها إتفاقية بودابيست ودليل تالين والعديد من القرارات الصادرة عن الأمم المتحدة، وكذلك اللجنة الدولية للصليب الأحمر التي لا تنفك عن إعطاء التوصيات لمحاربة هذه الحرب التي تفتك بالإنسانية .

8- توجد صعوبة في إثبات المسؤولية وتوقيع العقاب وتحديد التعويض، نظرا للغموض الذي تتميز به هذه الحرب السيبرانية، ومع ذلك فإنّ الجهود الدولية تبقى مستمرة .

**ب- الإقتراحات :**

على ضوء النتائج المتوصل إليها أعلاه، توصلنا إلى مجموعة من الإقتراحات نوردها فيما يلي:

1- تطوير الإطار قانوني الدولي الخاص بالحرب السيبرانية، حيث ينبغي على المجتمع الدولي العمل على صياغة إتفاقية دولية جديدة أو تعديل الإتفاقيات القائمة، لتشمل القواعد التي تنظم إستخدام الفضاء السيبراني في النزاعات المسلحة، مع مراعاة خصوصيته وتعقيداته التقنية.

2- إدماج مبادئ القانون الدولي الإنساني في السياسات السيبرانية الوطنية والدولية، بحيث يجب أن تلتزم الدول عند تطوير قدراتها السيبرانية العسكرية بمبادئ: الضرورة، التناسب والتمييز، لضمان حماية المدنيين وعدم إستهداف الأعيان المدنية.

3- تعزيز دور المنظمات الدولية في تنظيم الفضاء السيبراني، إذ لا بد من دعم الجهود التي تبذلها الأمم المتحدة واللجنة الدولية للصليب الأحمر وغيرها من المنظمات، لتقنين إستخدام الوسائل السيبرانية خلال النزاعات المسلحة وتقديم الإرشادات القانونية والفنية للدول.

4- إنشاء آلية دولية للرصد والتوثيق السيبراني، عن طريق اقتراح تأسيس هيئة دولية مستقلة تقوم بتوثيق الهجمات السيبرانية، وتحليل مدى امتثالها لقواعد القانون الدولي الإنساني، مع إتاحة نتائج التحقيق للهيئات القضائية الدولية وذلك بغرض إقامة المسؤولية الدولية.

5- تعزيز التعاون الدولي في مجال الأمن السيبراني، وذلك من خلال تبادل المعلومات وتنسيق الجهود لمحاربة العمليات السيبرانية .

6- رفع الوعي والتدريب على القانون الدولي الإنساني في المجال السيبراني، وذلك بإدراج محتوى متخصص في القانون الدولي الإنساني ضمن برامج التدريب العسكرية وخبراء الأمن السيبراني.

**7-** حث الدول على تبني سياسات شفافة تجاه قدراتها السيبرانية العسكرية، لأن الشفافية تعزز الثقة بين الدول وتقلل من مخاطر سوء الفهم أو التصعيد، كما تمكّن المجتمع الدولي من مراقبة مدى إحترام القانون في هذا المجال.

# قائمة
# المصادر والمراجع

## قائمــة المصادر والمراجــع:

### أولاً: القواعد الدولية

**أ- المواثيق والاتفاقيات الدولية :**

1- إتفاقية لاهاي الثانية بشأن قوانين وأعراف الحرب البرية، 29/ 1899/07

2- اللائحة الملحقة بإتفاقية لاهاي الثانية بشأن حظر إستخدام بعض الأسلحة، 1899.

3- إتفاقية لاهاي الرابعة بشأن قوانين وأعراف الحرب البرية، المؤرخة في 18 أكتوبر 1907.

4- إتفاقية لاهاي الخامسة بشأن احترام حقوق وواجبات الدول المحايدة في الحرب البرية، 1907.

5- النظام الأساسي لمحكمة العدل الدولية، المعتمد في مؤتمر سان فرانسيسكو في 26 حزيران/ يونيو 1945 .

6- ميثاق الأمم المتحدة الموقع بتاريخ 26 جوان 1945 في سان فرانسيسكو، مؤتمر الأمم المتحدة الخاص بنظام الهيئة الدولية، نيويورك، دخل حيز النفاذ في 24 أكتوبر 1945 .

7- اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب المؤرخة في 12 آب/أغسطس 1949، اعتمدت وعرضت للتوقيع والتصديق والانضمام من قبل المؤتمر الدبلوماسي لوضع اتفاقيات دولية لحماية ضحايا الحروب، المعقود في جنيف من 21 أفريل إلى 12 أوت 1949، تاريخ بدء النفاذ 21 أكتوبر 1950 وفقا لأحكام المادة 53 .

8- اتفاقية فيينا لقانون المعاهدات، اعتمدت من قبل مؤتمر الأمم المتحدة بشأن قانون المعاهدات، اعتمدت الاتفاقية في ختام أعماله في 22 آيار/مايو 1969، وعرضت للتوقيع في 23 أيار/مايو 1969، ودخلت حيّز النفاذ في 27 كانون الثاني/ يناير 1980 وفقا لأحكام المادة 84 .

9- البروتوكول الإضافي الأول الملحق باتفاقيات جنيف المعقودة في 12 أوت 1949، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، اعتمد وعرض للتوقيع والتصديق والانضمام من قبل المؤتمر الدبلوماسي لإعادة تأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة وتطويره بتاريخ 08 جوان1977، تاريخ بدء النفاذ 7 ديسمبر 1978 وفقا لأحكام المادة 95 .

10- البروتوكول الإضافي الثاني الملحق باتفاقيات جنيف المعقودة في 12 أوت 1949، المتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، اعتمد وعرض للتوقيع والتصديق والانضمام من قبل المؤتمر

الدبلوماسي لإعادة تأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة وتطويره بتاريخ 08 جوان 1977، تاريخ بدء النفاذ 07 ديسمبر 1978، وفقا لأحكام المادة 23 .

11-نظام روما الأساسي للمحكمة الجنائية الدولية، الوثيقة A/CONF.183/9 المؤرخة في 17 تموز/يوليو 1998. تاريخ بدء النفاذ: 01 تموز/ يوليو 2002، بموجب المادة 126 .

**ب- الإعلانات، التقارير والوثائق الدولية :**

1-مؤتمر الأمم المتحدة بشأن الجريمة والعدالة، إعلان فيينا، 17 أفريل 2000.

2-لجنة القانون الدولي، مشروع مواد حول مسؤولية الدول عن الأفعال غير المشروعة دوليا مع التعليقات، الأمم المتحدة، الجمعية العامة، الدورة 56، الوثيقة 10، A/56/2001

3-الأمم المتحدة، تقرير الفريق الحكومي الدولي للخبراء في أمن المعلومات، الجمعية العامة، 2004.

4-الجمعية العامة للأمم المتحدة، تقرير الفريق الحكومي المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، 2015.

5-مجلس الأمن السيبراني الدولي، تحديات قانونية في تطبيق القانون الدولي الإنساني على الفضاء السيبراني، تقرير سنة 2020.

6-مكتب المفوض السامي لحقوق الإنسان، تأثير العمليات السيبرانية على حقوق الإنسان أثناء النزاعات المسلحة، تقرير سنوي، 2022.

7-اللجنة الدولية للصليب الأحمر، قاعدة القانون الدولي الإنساني العرفي رقم 7، مبدأ التمييز بين الأعيان المدنية والأهداف العسكرية، بدون سنة.

**ثانياً: الكتب**

1. الغنيمي محمد طلعت، الوسيط في قانون السلام، منشأة المعارف، بدون طبعة ،مصر، 1982.

2. سعد الله عمر، تطور تدوين القانون الدولي الإنساني، دار الغرب الإسلامي، بدون طبعة، لبنان، 1997.

3. علام وائل أحمد، مركز الفرد من النظام القانوني للمسؤولية الدولية، دار النهضة العربية، بدون طبعة، مصر، 2001.

4. المجذوب محمد، القانون الدولي العام، منشورات الحلبي الحقوقية، الطبعة الخامسة، بيروت، 2004.

5. الشلالدة محمد فهاد، القانون الدولي الإنساني،منشأة المعارف، بدون طبعة، مصر، 2005.

6. أبو الوفا أحمد، النظرية العامة للقانون الدولي الإنساني (في القانون الدولي وفي الشريعة الإسلامية)، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 2006.

7. المجذوب محمد، المجذوب طارق، القانون الدولي الإنساني، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2009.

8. الفتلاوي سهيل حسين، ربيع عماد محمد، موسوعة القانون الدولي 5، القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2009.

9. منتصر سعيد حمودة ، القانون الدولي الإنساني مع الإشارة إلى أهم مبادئه في الفقه الإسلامي، دار الفكر الجامعي، الطبعة الأولى، مصر، 2009.

10. الفتلاوي سهيل حسين، الطبيعة القانونية العرفية لقواعد القانون الدولي الإنساني، دار الثقافة للنشر والتوزيع، بدون طبعة، الأردن، 2012.

11. سعد الله عمر، قراءة حديثة للقانون الدولي الإنساني، دار هومة للطباعة والنشر والتوزيع، الطبعة الأولى، الجزائر، 2012.

12. الشاذلي مجدي عبد العزيز، الحروب السيبرانية، المفهوم- السيمات- الانماط- التحديات القانونية الدولية، دار النهضة العربية، مصر، 2021.

13. فرطاس مصطفى كامل، الأمن السيبراني وحقوق الإنسان الرقمية، المفوضية العليا لحقوق الإنسان، قسم النشر والتثقيف، شعبة البحوث والدراسات، جمهورية العراق، 2023.

14. الحياني يحي، نعمان مصطفى، الخمسان عبد الله و العزيري هاشم، الأمن السيبراني في كل ما يخص مركز عمليات المراقبة، نسخة PDF ، بدون رقم طبعة، بدون دار نشر، بدون بلد النشر،بدون سنة النشر.

**ثالثاً: الدراسات الأكاديمية**

**أ ـ رسائل الماجستير :**

1- بابا فاطمة، القانون الدولي الإنساني بين النص و الواقع، رسالة ماجستير في القانون الدولي لحقوق الإنسان ،جامعة يحي فارس المدية، الجزائر، 2009/2008.

2- هاشم عبد الجليل المهيرات فلك ، المسؤولية الدولية للمنظمات الدولية في القانون الدولي العام، رسالة ماجستير في القانون، جامعة الشرق الأوسط، الأردن، 2016.

3- الموصلي نور أمير، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير في التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، 2024.

**ب ـ مذكرات الماستر :**

1- بوطاطة أمينة، الحروب السيبرانية في العلاقات الدولية: المفهوم والظاهرة، مذكرة لنيل شهادة الماستر، علاقات دولية، كلية الحقوق والعلوم السياسية والعلاقات الدولية، جامعة 20 أوت 1955 بسكيكدة، الجزائر، 2022/2021.

2- غجاتي سهيلة، راهم أميرة، الهجمات السيبرانية وأثرها على تهديد السلم والأمن الدوليين، مذكرة لنيل شهادة الماستر في القانون، قانون عام، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945 قالمة، الجزائر، 2024/2023.

**رابعاً: المقالات العلمية**

1. هربت لين، النزاع السيبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مجلد 94، العدد 886، 2012.

2. درويش سعيد، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 54، العدد 5، جامعة الجزائر 1 بن يوسف بن خدة، الجزائر، 2017.

3. يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية (مجلة مختصة في الدراسات والبحوث القانونية)، المجلد 4، العدد 4، جامعة القاهرة، مصر، 2018.

4. عيسى هشام، التحديات القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني، مجلة القانون والتكنولوجيا، جامعة القاهرة، مصر، 2019.

5. خروب خالد عبد الكريم، الجيل الخامس والقانون الدولي الإنساني، المجلة الجزائرية للعلوم القانونية، بدون رقم الطبعةن بدون دار النشر، بدون بلد النشر، 2020.

6. الزبيدي محمد، الفضاء السيبراني بين القانون الدولي الإنساني والقانون الدولي العام، مجلة البحوث القانونية والاقتصادية، العدد 58، جامعة المنصور، العراق، 2021.

7. أبو العينيين محمد، الحرب السيبرانية وتحديات القانون الدولي الإنساني، مجلة الحق، العدد 3، جامعة بني وليد، ليبيا، 2022.

8. إسماعيل نجلاء، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، مصر، 2022.

9. حامد علي البلداوي محمد، مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني، مجلة الجامعة العراقية، العدد 57، الجزء الثاني، الجامعة العراقية، العراق، 2022.

10. عرابي عبد العزيز ، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مجلة الدراسات القانونية والسياسية، العدد 15، جامعة القاهرة، مصر، 2022.

11. شويرب جيلالي، مراد فائزة، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، المجلد 11، العدد الأول، جامعة محمد خيضر، بسكرة، الجزائر، 2023.

12. شعلال سفيان، الحرب السيبرانية وتحديات القانون الدولي الإنساني، مجلة الآداب والعلوم الإنسانية والاجتماعية، العدد 28، الجزائر، 2023.

13. صديقي سامية، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، المجلد 6، العدد الأول، جامعة محمد البشير الإبراهيمي، الجزائر، 2023.

14. يوسف الأكيابي سلوى، مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، مجلة روح القوانين، العدد 101، جامعة طنطا، مصر، 2023.

15. طه شيماء، الفضاء السيبراني في القانون الدولي: الطبيعة القانونية وحدود التنظيم، مجلة المستقبل القانوني، العدد 30، جامعة أسيوط، مصر، 2023.

16. ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية: دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، الجزء الثاني، العدد 103، مصر، جويلية 2023.

17. عموري رمضان عبد الله، الحروب السيبرانية (الواقع – التحديات) في ضوء القانون الدولي الإنساني، مجلة الحق للعلوم الشرعية والقانونية، العدد 14، جامعة بني وليد، ليبيا، 2024.

18. عبد الرحمان عبد الرحمان شامل ولقمان زيد، الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني، مجلة نور القانونية، المجلد 01، العدد 02، جامعة النور، العراق، 2024.

19. عبد الفتاح قشطي نبيلة، الحرب السيبرانية وسبل مواجهتها، مجلة شؤون استراتيجية، العدد 17، كلية الحقوق جامعة المنوفية، مصر، 2024.

**خامساً: المحاضرات**

1. مصباح رشيدة، محاضرات في القانون الدولي الإنساني ومسؤولية الحماية (مادة) قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم حقوق، جامعة يحي فارس المدية، الجزائر، 2020/2019.

2. بن حوة أمينة، محاضرات في القانون الدولي الإنساني، (مادة) قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم حقوق، جامعة البليدة 2، الجزائر، 2024/2023.

**سادساً: المواقع الإلكترونية**

1. الأمم المتحدة، مكتب تنسيق الشؤون الإنسانية، ما هو القانون الإنساني الدولي؟ على الرابط:

https://www.unocha.org/story/what-international-humanitarian-law

2. اللجنة الدولية للصليب الأحمر، الحرب السيبرانية والقانون الدولي الإنساني: التمييز بين الحروب السيبرانية وغيرها، على الرابط:

https://www.icrc.org/ar/document/cyber-and-international-humanitarian-law

3. اللجنة الدولية للصليب الأحمر، البروتوكول الإضافي الثالث، على الرابط:

https://ihl-databases.icrc.orglassetsl2023-10lapiii-AR .PDF

4. اللجنة الدولية للصليب الأحمر، التكلفة البشرية المحتملة للعمليات السيبرانية، على الرابط:

https://www.icr .org/ar/document/potential-human-cost-cyber-operatios

5. اللجنة الدولية للصليب الأحمر، بيان اللجنة أمام فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، على الرابط:

https://www.icr.org/ar/document/icrc-statement-oewg-cybersecurity-2021

6. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية أثناء النزاعات المسلحة، على الرابط:

https://www.icr.org/ar/document/international-humanitarian-law-and%20cyber-operatios-during-armed-conflicts

7. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، على الرابط:

https://www.icr.org/en/report/2024-icrc-report-ihl-challenges

8. دليل تالين على الموقع الرسمي للجنة الدولية للصليب الأحمر، على الرابط:

https://lwww.icrc.org/ar/doc/resources/documments/faq/130628-cyber-warfar%20:q-and-a-eng.htm

9. قناة الجزيرة، اختراقات الكترونية، البداية إشارة موريس، على الرابط:

https://2u.pw-mtkkj

10. ويكيبيديا، متى ظهرت الحرب السيبيرانية، على الرابط:

http://llar.m.WiKipedia.org/wiki/d8

# الفهرس

**الفهرس**

مقدمـــة : ..... ب
الفصل الأول: الإطـار المفاهيمي للحروب السيبراية والقـانون الدولي الإنساني..... 7
المبحث الأول: الإطار المفاهيمي للحروب السيبرانية..... 8
المطلب الأول: مفهوم الحرب السيبرانية..... 8
الفرع الأول: تعريف الحرب السيبرانية..... 8
الفرع الثاني: نشأة وتطور الحروب السيبرانية..... 12
المطلب الثاني: الطبيعة القانونية للحرب السيبرانية وخصائصها ..... 16
الفرع الأول: الطبيعة القانونية للحرب السيبرانية..... 16
الفرع الثاني: خصائص الحرب السيبرانية..... 20
المطلب الثالث: أنماط الحرب السيبرانية والتمييز بينها وبين الحرب التقليدية ..... 22
الفرع الأول: أنماط الحرب السيبرانية..... 22
الفرع الثاني: التمييز بين الحرب السيبرانية والحرب التقليدية ..... 28
المبحث الثاني: الإطار النظري للقانون الدولي الإنساني ..... 30
المطلب الأول: مفهوم القانون الدولي الإنساني..... 30
الفرع الأول: تعريف القانون الدولي الإنساني ..... 30
الفرع الثاني: نشأة وتطور القانون الدولي الإنساني..... 33
المطلب الثاني: مصادر القانون الدولي الإنساني..... 35
الفرع الأول: المصادر الأصلية للقانون الدولي الإنساني..... 35
الفرع الثاني: مبادئ القانون الدولي الإنساني ..... 44
خلاصة الفصل الأول:..... 48
الفصل الثاني: علاقـــة الحروب السيبرانية بمبادئ القانون الدولي الإنساني..... 50
المبحث الأول: الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي الإنساني وإشكالات التطبيق ..... 51
المطلب الأول: الأساس القانوني لعلاقة الحرب السيبرانية بمبادئ القانون الدولي لإنساني ..... 51
الفرع الأول: مفهوم دليل تالين..... 51
الفرع الثاني: دور دليل تالين في تأطير الحرب السيبرانية ضمن مبادئ القانون الدولي الانساني..... 54
المطلب الثاني: إشكاليات تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية ..... 58
الفرع الأول: الاتجاه المؤيد لتطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية..... 58

الفرع الثاني: الاتجاه المعارض لتطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية.....62
الفرع الثالث: الاتجاه الوسيط في تطبيق مبادئ القانون القانون الدولي الإنساني على الحرب السيبرانية
.....65
المبحث الثاني: الجهود الدولية في تنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني وتقرير المسؤولية الدولية عن الحرب السيبرانية .....67
المطلب الأول: الجهود الدولية لتنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني.....68
الفرع الأول: الإعلانات والإتفاقيات الدولية الخاصة بتنظيم الحرب السيبرانية وفق مبادئ القانون الدولي الإنساني .....68
الفرع الثاني: المنظومات التقنية للحد من الحروب السيبرانية.....71
المطلب الثاني: المسؤولية الدولية الناجمة عن الحرب السيبرانية.....75
الفرع الأول: أحكام المسؤولية الدولية عن الأفعال السيبرانية.....75
الفرع الثاني: الأساس القانوني لقيام المسؤولية الدولية عن الحرب السيبرانية .....78
الفرع الثالث: التعويض عن الضرر الناجم عن الحرب السيبرانية .....80
خلاصة الفصل الثاني : .....84
الخـــاتمـــة : .....83
المصادر والمراجع قائمــة المصادر والمراجــع:.....86
الفهرس.....87

# الحرب السيبرانية على ضوء مبادئ القانون الدولي الإنساني

# The Legal Status of Cyber Warfare Under the Principles of International Humanitarian Law

**الطـــالبتين :**

**– شيماء كاك**

**– زكية هتشان**

**ملخص المذكرة**

تعالج هذه المذكرة إشكالية مدى تطبيق مبادئ القانون الدولي الإنساني على الحرب السيبرانية، ذلك أن القانون الدولي الإنساني يطبق على النزاعات المسلحة التقليدية، مرتكزا على مبادئ أساسية أهمها مبدأ التمييز بين الأهداف المدنية و العسكرية ، مبدأ التناسب، مبدأ الضرورة العسكرية، مبدأ الإنسانية، وهذا من أجل حماية المدنيين و تقييد وسائل القتال، إلا أن الحرب السيبرانية بإعتبارها شكلا مستحدثا من النزاعات تتميز بخصائص فريدة منها الطبيعة غير المادية للهجمات و صعوبة التمييز بين الأهداف المدنية و العسكرية، كذلك صعوبة تطبيق مبدأي الضرورة و التناسب، كذلك مسألة تحديد المسؤولية التي تعتبر معقدة لصعوبة تحديدالفاعل والضرر، هذه السمات تعيق التطبيق الكامل للمبادئ التقليدية للقانون الدولي الإنساني، مايستدعي إعادة النظر في الإطار القانوني القائم، و تطوير القواعد الموجودة حتى تواكب التحديات التي تفرضها الحرب السيبرانية.

**الكلمات المفتاحية**: الحرب السيبرانية/ مبادى القانون الدولي الإنساني.

**Abstract**

This thesis addresses the issue of the extent to which the principles of international humanitarian law can be applied to cyber warfare. International humanitarian law traditionally applies to conventional armed conflicts and is based on fundamental principles, most notably the principles of distinction between civilian and military targets, proportionality, military necessity, and humanity. These principles aim to protect civilians and limit the means of warfare. However, cyber warfare, as a new form of conflict, presents unique characteristics, such as the non-material nature of attacks and the difficulty in distinguishing between civilian and military targets. It also complicates the application of the principles of necessity and proportionality, as well as the issue of responsibility due to the challenge of identifying the perpetrator and the damage caused. These characteristics hinder the full application of traditional international humanitarian law principles, necessitating a reassessment of the existing legal framework and the development of current rules to address the challenges posed by cyber warfare.

**Keywords:** Cyber warfare / Principles of international humanitarian law.

**Résumé**

Ce mémoire traite de la problématique de l'application des principes du droit international humanitaire à la guerre cybernétique. En effet, le droit international humanitaire s'applique traditionnellement aux conflits armés classiques, en se fondant sur des principes fondamentaux, notamment le principe de distinction entre les cibles civiles et militaires, le principe de proportionnalité, la nécessité militaire, et le principe d'humanité. Ces principes visent à protéger les civils et à limiter les moyens de combat. Toutefois, la guerre cybernétique, en tant que forme émergente de conflit, se caractérise par des spécificités uniques, telles que la nature immatérielle des attaques et la difficulté de distinguer entre cibles civiles et militaires. Elle rend également difficile l'application des principes de nécessité et de proportionnalité, ainsi que la détermination de la responsabilité, en raison de la complexité d'identifier l'auteur et les dommages causés. Ces éléments entravent l'application complète des principes traditionnels du droit international humanitaire, d'où la nécessité de repenser le cadre juridique existant et de développer les règles actuelles pour faire face aux défis posés par la guerre cybernétique.

**Mots-clés :** Guerre cybernétique / Principes du droit international humanitaire.