

الهجمات السيبرانية في ضوء القانون الدولي الإنساني

Cyber Attacks in Light of the International Humanitarian Law

عمر بوقريط

Ammar Bougrit

مخبر الدراسات القانونية التطبيقية

Applied Legal Studies Laboratory

جامعة الإخوة منتوري قسنطينة 1 - الجزائر-

University of Constantine 1-Algeria-

bougritammar@gmail.com

assia.sebti@doc.umc.edu.dz

تاريخ الاستلام: 2026/06/01 تاريخ القبول للنشر: 2026/09/12 تاريخ النشر: 2026/10/01

ملخص:

ان قواعد ومبادئ القانون الدولي الإنساني، بالرغم من كونها شاملة وعامة، تواجه صعوبات جمة في تطبيقها على الهجمات السيبرانية، وذلك نظرا للطابع الافتراضي للهجمات السيبرانية وارتباطها الوثيق بالبنية التحتية المدنية، مما يشكل تحديا أمام تطبيق مبدأي التمييز والتناسب بصفة دقيقة وفعالة. بالإضافة إلى ذلك، يعد "دليل تالين" خطوة هامة نحو تنظيم الهجمات السيبرانية في إطار القانون الدولي، إلا أنه غير ملزم ولا يغطي كل الجوانب المهمة. وبناءً عليه، تبرز حاجة ملحة لإنشاء نظام قانوني دولي خاص لتنظيم الحروب السيبرانية وتأثيراتها السلبية في ظل الاعتماد المتزايد على التكنولوجيا.

الكلمات المفتاحية: القانون الدولي الإنساني؛ الهجمات السيبرانية؛ الطابع الافتراضي؛ البنية التحتية؛ التمييز.

Abstract :

While the rules and principles of international humanitarian law are comprehensive and general, their application to cyberattacks presents significant challenges. This is due to the virtual nature of cyberattacks and their close connection to civilian infrastructure, which poses a challenge to the accurate and effective application of the principles of distinction and proportionality. Furthermore, the Tallinn Manual represents an important step towards regulating cyberattacks within the framework of international law, but it is non-binding and does not cover all relevant aspects. Therefore, there is an urgent need to establish a specific international legal framework to regulate cyber warfare and its negative impacts in light of increasing reliance on technology.

Keywords: International humanitarian law; cyberattacks; virtualisation; infrastructure; distinction.

* المؤلف المراسل.

مقدمة:

شهد العالم خلال العقدين الأخيرين تطورا هائلا في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي انعكس بشكل واضح على طبيعة ميادين القتال وأساليب إدارة النزاعات. ولم يعد استخدام التكنولوجيا مقتصرًا على المجالات المدنية، بل امتد إلى الفضاء السيبراني، حيث أصبحت معظم أنظمة الأسلحة الحديثة تعتمد بشكل كبير على البنية التحتية الرقمية، بما في ذلك أنظمة الحاسوب وشبكات الأنترنت. ونتيجة لذلك، غدا الفضاء السيبراني عنصرا أساسيا وميزة بارزة للنزاعات المعاصرة.

وبالنظر إلى أن معاهدات القانون الدولي الإنساني وُضعت في فترة لم تكن فيها الهجمات السيبرانية معروفة بالشكل الذي نشهده اليوم، يثور التساؤل حول مدى قدرة هذه القواعد التقليدية على مواكبة التحولات التكنولوجية الحديثة. فالتطور المتسارع في مجال الفضاء السيبراني أفرز أنماطا جديدة من الهجمات ووسائل القتال، الأمر الذي يطرح إشكالية مدى قابلية قواعد القانون الدولي الإنساني الحالية للتطبيق على الهجمات السيبرانية، أو ما إذا كانت الحاجة أصبحت قائمة لتطوير بعض هذه القواعد وتحسينها بما ينسجم مع طبيعة التهديدات الرقمية المعاصرة.

أهداف البحث:

أولا - التعرف على ماهية الهجمات السيبرانية من خلال تعريفها والتطرق إلى ما يتصل بها من مفاهيم.

ثانيا - التعرف على الهجمات السيبرانية الخاضعة إلى أحكام القانون الدولي الإنساني.

ثالثا - التعرف على الطبيعة القانونية للهجمات السيبرانية.

رابعا - دراسة مدى مواءمة المبادئ النازمة لسير العمليات العدائية مع الهجمات السيبرانية وموقف الفقه الدولي والمنظمات الدولية منها.

وانطلاقا مما سبق، تتمحور إشكالية هذا البحث حول التساؤل الآتي:

ما مدى انطباق القواعد التقليدية المنظمة للنزاعات المسلحة على الهجمات السيبرانية؟

للإجابة عن هذه الإشكالية، اعتمدنا على المنهج الوصفي التحليلي لوصف متغيرات الدراسة وتحليلها، واقترحنا خطة مكونة من مبحثين تناولنا في المبحث الأول ماهية الهجمات السيبرانية من خلال مطلبين، نتطرق في المطلب الأول إلى تعريف الهجمات السيبرانية وما يتعلق بها من مفاهيم، ونتطرق في المطلب الثاني إلى الهجمات السيبرانية الخاضعة إلى أحكام القانون الدولي الإنساني،

وفي المبحث الثاني تناولنا بالدراسة والتحليل مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية وفق مطلبين، نتناول في المطلب الأول الطبيعة القانونية للهجمات السيبرانية، وفي المطلب الثاني ندرس مدى موافقة المبادئ النازمة لسير العمليات العدائية مع الهجمات السيبرانية وموقف الفقه الدولي والمنظمات الدولية منها.

المبحث الأول:

ماهية الهجمات السيبرانية:

يتناول هذا المبحث بالدراسة محاولة إعطاء تعريف للهجمات السيبرانية ومختلف المفاهيم والمصطلحات التي ترتبط بها وصولاً إلى تحديد الهجمات السيبرانية التي تخضع لأحكام القانون الدولي الإنساني وذلك لتمييزها عن تلك التي تخضع لتنظيم القوانين الجنائية الوطنية المطلب الأول: تعريف الهجمات السيبرانية وما يتعلق بها من مفاهيم

نتطرق في هذا المطلب إلى مفهوم الهجمات السيبرانية من خلال بيان تعريفها، باعتبارها من أبرز التهديدات التي أفرزها التطور التكنولوجي في العصر الحديث، كما نتناول جملة من المفاهيم المرتبطة بها، بهدف الإحاطة بالإطار المفاهيمي لهذا النوع من الهجمات وتمييزه عن غيره من الأنشطة الإلكترونية المشابهة.

الفرع الأول: تعريف الهجمات السيبرانية:

أ- التعريف اللغوي والاصطلاحي:

* التعريف اللغوي:

إن مصطلح السيبرانية أو السايبر أو السيراني يعد ترجمة لكلمة (Cyber) المشتقة من مصطلح (Cybernetics)، وقد استخدم هذا المفهوم لأول مرة في المجال الأكاديمي من طرف عالم الرياضيات الأمريكي نوربرت وينر سنة 1948 في كتابه "علم التحكم الآلي: أو التحكم والاتصال في الحيوان والآلة"، حيث استعمله للدلالة على آليات التنظيم الذاتي والتحكم¹

أما من الناحية اللغوية، فإن أصل كلمة "سايبر" يعود إلى الكلمة اليونانية (Kybernetes) التي تعني القيادة أو التوجيه والتحكم عن بعد، وقد ظهر استعمالها بداية في أدب الخيال العلمي قبل أن ينتقل إلى المجالات العلمية والتقنية.

وبالرجوع إلى القواميس اللغوية، نجد أن أغلبها لم تتوسع في بيان الأصل الدقيق لكلمة السيبرانية، باستثناء ما أورده قاموس المورد الذي عرّف السيبرانية بأنها علم التحكم أو علم التحكم

الآلي² وهو تعريف ينسجم مع طبيعة الهجمات السيبرانية القائمة على التحكم عن بعد والسيطرة على الأنظمة والأجهزة الإلكترونية.

كما عرّفها أغلب القواميس العسكرية المتخصصة انطلاقاً من مجال استخدامها العملي والعسكري، ومن ذلك قاموس المصطلحات العسكرية الأمريكية الذي اعتبرها كل فعل يتم عبر الشبكات الإلكترونية بهدف التحكم في البرامج الإلكترونية الأخرى أو تعطيلها³ كما عرّف قاموس مصطلحات أمن المعلومات السيبرانية بأنها هجوم يُنفذ عبر الفضاء الإلكتروني بغرض السيطرة على المواقع الإلكترونية أو البنى المحمية إلكترونياً، بهدف تعطيلها أو تدميرها أو إلحاق الضرر بها.

وعلى مستوى الوثائق الدولية، اعتمدت الأمم المتحدة في نسخها العربية مصطلح "السيبرانية" بدل "الإلكترونية"، ويتضح ذلك من خلال القرار رقم 239/57 الصادر عن الجمعية العامة للأمم المتحدة والمتعلق بإنشاء ثقافة عالمية للأمن السيبراني، إضافة إلى القرار رقم 199/58 الذي دعا الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني⁴

* التعريف الاصطلاحي:

تباينت التعريفات الفقهية والعملية لمصطلح الهجمات السيبرانية تبعاً لاختلاف الزاوية التي يُنظر إليها من خلالها، سواء من الناحية التقنية أو العسكرية أو القانونية، ويستعمل هذا المصطلح للدلالة على جملة من العمليات التي تُنفذ عبر الفضاء الإلكتروني، وقد تصل في بعض الحالات إلى مستوى النزاع المسلح أو تتم في إطاره وفقاً لما يقصده القانون الدولي. كما يُقصد به أحياناً وسائل وأساليب القتال المعتمدة على التكنولوجيا الرقمية لاستهداف الأنظمة والشبكات المعلوماتية⁵ فنذكر بعض أقوال فقهاء القانون الدولي من تعريفاتهم للهجمات السيبرانية كمايلي:

وفي هذا السياق، قدّم عدد من فقهاء القانون الدولي تعريفات للهجمات السيبرانية، من أبرزها تعريف "فيورتس" (Fuertes) الذي اعتبرها هجوماً يتم عبر شبكة الأنترنت من خلال التسلسل غير المشروع إلى المواقع والأنظمة الإلكترونية بقصد تعطيل البيانات أو إتلافها أو الاستيلاء عليها، موضحاً أنها قد تأخذ شكل سلسلة من الهجمات الإلكترونية التي تشنها دولة ضد دولة أخرى⁶.

أما "مايكل شميت" (Schmitt) فقد عرّف الهجمات السيبرانية بأنها مجموعة من التدابير والإجراءات التي تعتمدها الدولة لاستهداف نظم المعلومات التابعة للخصم بهدف التأثير فيها أو

إلحاق الضرر بها، مع العمل في الوقت ذاته على حماية وتأمين نظم المعلومات الخاصة بالدولة المهاجمة⁷.

ومنهم من عرفها بأنها مجموعة من العمليات التي تجمع بين الحرب الإلكترونية وأساليب الخداع النفسي، فضلاً عن استهداف شبكات الاتصال العسكرية للخصم وأنظمتها الأمنية الإلكترونية بهدف التأثير في قدراته العملياتية.

أما الفقيه **روسيني (Roscini)** فيرى أن الهجوم السيبراني يتمثل في توظيف القدرات الإلكترونية العسكرية للتأثير في الأنظمة والشبكات الإلكترونية الأخرى وتعطيلها أو تدميرها، سواء كانت هذه الأنظمة مخصصة لأغراض مدنية أو عسكرية⁸.

كما ورد في معجم الاستخدامات العسكرية الصادر عن هيئة الأركان المشتركة الأمريكية سنة 2011، عقب إنشاء القيادة السيبرانية الأمريكية، أن الهجوم السيبراني هو نشاط عدائي يُنفَّذ بواسطة الحواسيب أو الشبكات أو الأنظمة المرتبطة بها، ويستهدف تعطيل أو تدمير الأنظمة السيبرانية الحيوية للخصم أو ممتلكاته أو وظائفه الأساسية، ويؤكد هذا التعريف أن آثار الهجوم السيبراني لا تقتصر على الأنظمة المعلوماتية أو البيانات المستهدفة ذاتها، بل قد تمتد إلى نتائج مادية أو وظيفية أخرى، كما أن تنفيذ الهجوم وآثاره قد يفصل بينها زمنياً أو مكانياً⁹.

ومن جانبها، عرفت القيادة الاستراتيجية الأمريكية سنة 2007 الهجوم السيبراني بأنه استخدام الوسائل الإلكترونية والتقنيات المعلوماتية لأغراض عسكرية بهدف حرمان الخصم من الاستفادة الفعالة من أنظمة الحاسوب الخاصة به، إلى جانب اختراق نظم المعلومات وشبكات الاتصالات بغرض الحصول على البيانات والمعلومات التي تحتويها وتحليلها واستغلالها¹⁰.

وقد عرّف **الفتلاوي** الهجوم السيبراني بأنه هجوم يُنفَّذ عبر شبكة الأنترنت من خلال التسلل غير المشروع إلى المواقع والأنظمة الإلكترونية بهدف تعطيلها أو تدميرها أو الاستيلاء على البيانات المخزنة فيها، وهو في جوهره سلسلة من العمليات الإلكترونية التي قد تنفذها دولة ضد دولة أخرى¹¹.

الفرع الثاني: تمييز الهجمات السيبرانية عن المصطلحات المشابهة لها

أ- الحرب السيبرانية: يُعد مفهوم الحرب السيبرانية (Cyber Warfare) من المفاهيم الحديثة المرتبطة بالنزاعات المسلحة في القرن الحادي والعشرين، إذ تقوم على استخدام وسائل وأساليب قتالية إلكترونية متطورة قد ترقى إلى مستوى النزاع المسلح أو تُستخدم في سياقه

ويكمن الفرق بين الهجمات السيبرانية والحرب السيبرانية في أن الأخيرة تمثل صورة خاصة من صور الهجمات السيبرانية، حيث تقع أثناء نزاع مسلح قائم أو تحدث آثاراً مادية تعادل في خطورتها آثار الهجمات العسكرية التقليدية، أما الهجمات السيبرانية فهي مفهوم أوسع يشمل مختلف الأنشطة الإلكترونية الضارة الموجهة ضد الدول، سواء ارتكبت في زمن السلم أو أثناء النزاعات المسلحة، وسواء ترتب عليها أضرار مادية جسيمة بالأرواح والممتلكات أم اقتصر أثرها على تعطيل الأنظمة المعلوماتية وإرباك مؤسسات الدولة وتحقيق أهداف أمنية أو عسكرية¹³

ب- الأمن السيبراني: ظهر مفهوم الأمن السيبراني في مرحلة ما بعد الحرب الباردة استجابةً للتطورات التكنولوجية المتسارعة والتحولات الجيوسياسية المصاحبة لها، وقد استخدم المصطلح لأول مرة من قبل المتخصصين في علوم الحاسوب خلال أوائل تسعينيات القرن الماضي للإشارة إلى المخاطر الأمنية المرتبطة باستخدام الحواسيب والشبكات. ومع مرور الوقت تجاوز المفهوم نطاقه التقني الضيق ليشمل الأبعاد الاجتماعية والاقتصادية والسياسية الناتجة عن التهديدات الرقمية، ويقصد بالأمن السيبراني مجموعة التدابير والإجراءات الرامية إلى حماية الموارد البشرية والمادية المرتبطة بتكنولوجيا المعلومات والاتصالات، والحد من الأضرار والخسائر المحتملة الناجمة عن المخاطر والتهديدات السيبرانية، مع ضمان استعادة الأنظمة لوضعها الطبيعي بأسرع وقت ممكن بما يحافظ على استمرارية النشاط والإنتاج¹⁴

ت- الفضاء السيبراني: يقصد بالفضاء السيبراني البيئة الافتراضية التي تتداخل بصورة وثيقة مع العالم المادي وتتفاعل معه بشكل مستمر، بحيث يؤثر كل منهما في الآخر. ويتميز هذا الفضاء بطابعه العابر للحدود الوطنية، الأمر الذي جعله مجالاً عالمياً تتشابك فيه المصالح والمخاطر. ومن ثم لم يعد الأمن السيبراني مسألة داخلية تخص دولة بعينها، بل أصبح جزءاً من منظومة الأمن الجماعي الدولي في ظل التهديدات المشتركة التي تواجه مختلف الفاعلين في مجتمع المعلومات العالمي¹⁵.

ج- القوة السيبرانية: تتمثل القوة السيبرانية في قدرة الدولة على توظيف الفضاء السيبراني لتحقيق مزايا استراتيجية والتأثير في مجريات الأحداث داخل مختلف البيئات التشغيلية، وتعتمد هذه القوة على مجموعة من الموارد والإمكانات المادية والبشرية والتقنية، بما في ذلك أنظمة الحاسوب والشبكات الإلكترونية والبنية التحتية المعلوماتية والكوادر المتخصصة، وتستخدم هذه المقومات كأداة من أدوات القوة الوطنية لتحقيق مصالح الدولة والتأثير في سلوك الفاعلين الآخرين على الساحة الدولية¹⁶

ح- الإرهاب السيبراني: يُعرف الإرهاب السيبراني بأنه استخدام الحواسيب أو الشبكات أو أنظمة المعلومات لتنفيذ هجمات أو التهديد بتنفيذها بدوافع سياسية، بهدف إلحاق الضرر بالبنية التحتية الحيوية أو بث الرعب بين الحكومات والمجتمعات وإجبارها على الاستجابة لمطالب أو أهداف سياسية واجتماعية معينة. كما يشمل استغلال شبكة الأنترنت ووسائل الاتصال الرقمية في الدعاية والتجنيد ونشر المعلومات المضللة من قبل التنظيمات الإرهابية.

خ- الإستراتيجية السيبرانية: تشير الاستراتيجية السيبرانية إلى عملية تطوير وتوظيف القدرات السيبرانية بصورة متكاملة ومنسجمة مع مختلف المجالات التشغيلية الأخرى، بما يسهم في تحقيق الأهداف الوطنية للدولة. وتركز هذه الاستراتيجية على إدارة التحديات المرتبطة بالفضاء السيبراني، ولا سيما بناء آليات ردع فعالة للتأثير في سلوك الجهات الفاعلة التي تستفيد من التطورات التقنية المتسارعة¹⁷

د- الصراع السيبراني: يقصد بالصراع السيبراني ذلك الخط من الصراعات الذي تُستخدم فيه الوسائل والتقنيات الرقمية كأدوات للتأثير والمواجهة بين الأطراف المتنازعة. ويُعد أحد أشكال الصراع الدولي المعاصر، حيث يمكن من خلاله إلحاق أضرار كبيرة بالبنية التحتية المعلوماتية والاتصالية للطرف الآخر، سواء عبر تعطيل شبكات الاتصال العسكرية، أو تضليل المعلومات، أو الاستيلاء على البيانات السرية، الأمر الذي قد يترتب عليه خسائر عسكرية واقتصادية بالغة¹⁸.

المطلب الثاني: الهجمات السيبرانية الخاضعة لأحكام القانون الدولي الإنساني

يشير تحديد الهجمات السيبرانية الخاضعة لأحكام القانون الدولي الإنساني أهمية بالغة في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصالات وتزايد استخدامها في النزاعات المسلحة. لذلك يقتضي الأمر بيان المعايير القانونية التي تجعل من الهجوم السيبراني نشاطاً مشمولاً بقواعد القانون الدولي الإنساني، مع توضيح نطاق تطبيق هذه الأحكام على مختلف صور العمليات السيبرانية أثناء النزاعات المسلحة.

يرى فريق خبراء دليل تالين¹⁹ أن مفهوم النزاع المسلح لا يقتصر على الأعمال العدائية التقليدية، بل يشمل كذلك الأعمال التي تُنفذ عبر الوسائل السيبرانية، متى ارتبطت بحالة نزاع مسلح بين الأطراف المتحاربة. ومن ثم، تخضع العمليات السيبرانية للقواعد والمبادئ ذاتها التي تنظم الأعمال العدائية التقليدية في إطار القانون الدولي الإنساني²⁰

ويجد هذا التوجه سنده في المادة (36) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949، التي تلزم الدول الأطراف عند دراسة أو تطوير أو اقتناء أسلحة أو وسائل أو أساليب جديدة للقتال، بالتحقق من مدى توافقها مع أحكام القانون الدولي الإنساني والقواعد الدولية ذات الصلة²¹

الفرع الأول: مفهوم الهجوم بموجب القانون الدولي الإنساني والعمليات السيبرانية:

أصبحت البنى التحتية المدنية الحيوية تعتمد بصورة متزايدة على الأنظمة الرقمية والشبكات المعلوماتية، الأمر الذي جعل حمايتها ضرورة أساسية لضمان سلامة السكان المدنيين. ويمنح القانون الدولي الإنساني حماية خاصة لبعض المرافق والأعيان، مثل الوحدات الطبية والأشياء الضرورية لبقاء السكان المدنيين، بصرف النظر عن طبيعة الوسائل المستخدمة لاستهدافها.

غير أن معظم القواعد المستمدة من مبادئ التمييز والتناسب والاحتياط لا تنطبق إلا على العمليات العسكرية التي تندرج ضمن مفهوم "الهجوم" في القانون الدولي الإنساني. وقد عرفت المادة (49) من البروتوكول الإضافي الأول للهجمات بأنها «أعمال العنف الموجهة ضد الخصم، سواء كانت في إطار الهجوم أو الدفاع»²²

وتكتسب مسألة تحديد نطاق مفهوم الهجوم في البيئة السيبرانية أهمية بالغة، لما يترتب عليها من آثار تتعلق بحماية المدنيين والأعيان المدنية. ويُجمع الفقه الدولي إلى حد كبير على أن العمليات السيبرانية التي يُتوقع أن تؤدي إلى القتل أو الإصابة أو إحداث أضرار مادية تُعد هجمات بالمعنى المقصود في القانون الدولي الإنساني.

كما ترى اللجنة الدولية للصليب الأحمر أن هذا المفهوم يشمل الآثار المباشرة وغير المباشرة المتوقعة للعمليات السيبرانية. ومن الأمثلة على ذلك وفاة المرضى في أقسام العناية المركزة نتيجة انقطاع التيار الكهربائي عن المستشفى بسبب هجوم سيبراني استهدف شبكة الكهرباء.

ومن جهة أخرى، تمثل العمليات السيبرانية التي تؤدي إلى تعطيل الخدمات الأساسية دون إحداث أضرار مادية مباشرة أحد أبرز التهديدات التي قد يتعرض لها المدنيون. ومع ذلك، لا يزال هناك خلاف فقهي بشأن ما إذا كان مجرد فقدان الوظيفة التشغيلية للأنظمة أو الشبكات، دون وقوع ضرر مادي ملموس، يكفي لاعتبار العملية السيبرانية هجوماً بموجب القانون الدولي الإنساني.

وفي هذا السياق، تتبنى اللجنة الدولية للصليب الأحمر موقفاً موسعاً لمفهوم الهجوم، إذ ترى أن أي عملية تستهدف تعطيل حاسوب أو شبكة معلوماتية أثناء نزاع مسلح تُعد هجوماً،

سواء تحقق هذا التعطيل بوسائل مادية أو إلكترونية. أما إذا تم حصر مفهوم الهجوم في العمليات التي تُحدث وفاة أو إصابة أو ضرراً مادياً فقط، فإن العديد من العمليات السيبرانية الموجهة ضد شبكات مدنية حيوية، مثل شبكات الكهرباء والاتصالات والخدمات المصرفية، قد تخرج من نطاق الحماية التي توفرها القواعد الأساسية للقانون الدولي الإنساني، رغم ما قد تسببه من آثار خطيرة على السكان المدنيين.

الفرع الثاني: الأهداف المدنية والأهداف ذات الاستخدام المزدوج:

يقصد بالأهداف ذات الاستخدام المزدوج تلك الأعيان المدنية التي تُستخدم في الوقت نفسه لأغراض مدنية وعسكرية. ونتيجة لهذا الاستخدام العسكري، تكتسب هذه الأعيان صفة الهدف العسكري طوال الفترة التي تُسهم فيها بصورة فعالة في العمل العسكري، مما يجعلها عرضة للاستهداف المشروع وفقاً لقواعد القانون الدولي الإنساني.

وقد كرس البروتوكول الإضافي الأول هذا المبدأ في المادة (2/52)، كما أكدته القاعدة (39) من دليل تالين، اللتان تشيران إلى أن الأعيان التي تُسهم مساهمة فعالة في العمليات العسكرية وتوفر ميزة عسكرية أكيدة للطرف المستخدم لها يمكن اعتبارها أهدافاً عسكرية مشروعة، حتى وإن كانت تؤدي في الأصل وظائف مدنية.

تجدر الإشارة إلى أن الهجمات الموجهة ضد الأعيان ذات الاستخدام المزدوج تخضع لمبدأ التناسب والالتزام اتخاذ الاحتياطات اللازمة أثناء تنفيذ الهجوم. غير أن الهجمات السيبرانية تثير تحديات خاصة في هذا المجال، إذ يصعب في كثير من الأحيان التمييز داخل الشبكات الإلكترونية ذات الاستخدام المزدوج بين الأجزاء المخصصة للأغراض العسكرية وتلك المخصصة للاستعمالات المدنية. وفي مثل هذه الحالات قد تُصنف الشبكة بأكملها كهدف عسكري، الأمر الذي يزيد من احتمالية تعرض المكونات المدنية للأضرار.

ومن جهة أخرى، تمثل البيانات المدنية الأساسية، كالسجلات الطبية والبيانات البيومترية وبيانات الضمان الاجتماعي والسجلات الضريبية والحسابات المصرفية وملفات العملاء وقوائم الناهخين، عنصراً جوهرياً في المجتمعات الرقمية الحديثة، إذ يعتمد عليها سير العديد من المرافق والخدمات الأساسية التي تمس الحياة اليومية للأفراد.

وبصفة عامة، يوفر القانون الدولي الإنساني الحماية للمدنيين وللأعيان المدنية من آثار العمليات العدائية. ومع ذلك، لا تزال مسألة اعتبار البيانات المدنية أهدافاً مدنية تتمتع بالحماية القانونية ومدى نطاق هذه الحماية محل نقاش ولم تحسم بصورة نهائية على المستوى الدولي.

ولذلك، يتعين على الدول تكثيف جهودها لضمان حماية هذه البيانات نظراً لما قد يترتب على استهدافها من أضرار جسيمة تفوق في بعض الأحيان الأضرار الناجمة عن تدمير الأعيان المادية. فحذف البيانات المدنية الأساسية أو التلاعب بها قد يؤدي إلى شلل شبه كامل في عمل المؤسسات الحكومية والشركات الخاصة، الأمر الذي يجعل استبعادها من نطاق الحماية المقررة للأعيان المدنية في القانون الدولي الإنساني سبباً في إيجاد فجوة قانونية خطيرة في حماية المدنيين أثناء النزاعات المسلحة²³

المبحث الثاني:

انطباق القانون الدولي الإنساني على الهجمات السيبرانية

يُعدّ التأكيد على سريان قواعد القانون الدولي الإنساني على النزاعات المسلحة التي تُنفَّذ باستخدام الوسائل السيبرانية خطوةً أساسية للحد من الآثار الإنسانية السلبية التي قد تنجم عن هذه العمليات أو التخفيف منها. غير أن ذلك وحده لا يكفي، إذ تؤكد اللجنة الدولية للصليب الأحمر على أهمية تعاون الدول من أجل بلورة فهم مشترك لكيفية تطبيق مبادئ وقواعد القانون الدولي الإنساني على العمليات السيبرانية. وتبرز أهمية هذا المسعى في ظل الطبيعة المترابطة والمعقدة للفضاء السيبراني، والتي تثير العديد من الإشكالات المتعلقة بتفسير وتطبيق المبادئ والمفاهيم الأساسية للقانون الدولي الإنساني المنظمة لسير الأعمال العدائية²⁴

المطلب الأول: الطبيعة القانونية للهجمات السيبرانية

أثارت مسألة التكيف القانوني للهجمات السيبرانية ومدى خضوعها لقواعد القانون الدولي الإنساني نقاشاً فقهيّاً وقانونياً واسعاً، خاصة فيما يتعلق بتحديد طبيعتها القانونية، وما إذا كانت تُعد وسيلة من وسائل القتال أم أسلوباً من أساليبه، فضلاً عن التساؤل حول إمكانية اعتبارها من الأسلحة المحظورة التي لا يجوز استخدامها أثناء النزاعات المسلحة على غرار بعض الأسلحة التقليدية المحظورة دولياً.

الفرع الأول: الهجمات السيبرانية كوسيلة للقتال

عندما يُستخدم الهجوم السيبراني لاختراق الأنظمة الإلكترونية المسؤولة عن حماية أو إدارة أو تشغيل المنشآت الحيوية بهدف تعطيلها أو إتلافها أو السيطرة عليها، فإنه يُنظر إليه باعتباره وسيلة من وسائل القتال، أي أداة تُستخدم لإلحاق الضرر بالخصم وتحقيق أهداف عسكرية محددة.

ومن أبرز الأمثلة على ذلك فيروس "ستاكنست" (Stuxnet)، الذي استُخدم لاستهداف منشآت "نطنز" و"بوشهر" النوويتين في إيران، حيث تسبب في إحداث أضرار جزئية بعملية تخصيب اليورانيوم. ويُعد هذا الفيروس برنامجاً إلكترونياً بالغ التعقيد، صُمم لمهاجمة أنظمة التحكم الصناعية المستخدمة في تشغيل ومراقبة المنشآت الآلية. وتُميز "ستاكنست" عن غيره من البرمجيات الخبيثة بقدرته على استهداف أهداف محددة بدقة عالية؛ إذ كان يخترق الأجهزة والحواسيب بحثاً عن أنظمة معينة تمت برمجته للتعرف عليها، وعند العثور عليها يقوم بتفعيل نفسه والبدء في التلاعب بأنظمة التحكم الخاصة بالمنشأة المستهدفة، مما يؤدي إلى إلحاق أضرار مادية بها وتعطيل عملها²⁵

يُعدّ تحديد الطبيعة القانونية للأنشطة والهجمات السيبرانية من أبرز التحديات التي تواجه المجتمع الدولي في الوقت الراهن، خاصة فيما يتعلق بإمكانية اعتبارها نوعاً من الأسلحة غير التقليدية ومدى خضوعها للاتفاقيات الدولية الخاصة بالحد من التسلح. وفي هذا السياق، يرى بعض الخبراء أن الهجمات السيبرانية لا يمكن وصفها بأنها "سلاح" بالمعنى التقليدي، لأنها لا تعتمد على القوة أو الطاقة الحركية المباشرة كما هو الحال في الأسلحة التقليدية، ومن ثم لا تنطبق عليها القواعد الدولية المنظمة لاستخدام الأسلحة.

غير أن هذا الرأي لا ينسجم تماماً مع الواقع العملي؛ إذ إن مفهوم السلاح لا يقتصر بالضرورة على الوسائل التي تُحدث آثارها بواسطة القوة الحركية. وقد أكدت وزارة الدفاع الأمريكية في تقييمها للقضايا القانونية الدولية المرتبطة بالعمليات المعلوماتية سنة 1999 أن الأنشطة الإلكترونية، رغم كونها غير ملموسة ولا تُدرك بالحواس البشرية على غرار القنابل أو الذخائر أو الوحدات العسكرية، قد تُحدث آثاراً ونتائج خطيرة تستوجب اهتمام المجتمع الدولي، الأمر الذي يجعل تقييم نتائج الهجمات السيبرانية أكثر أهمية من التركيز على طبيعتها التقنية أو آلية تنفيذها.

الفرع الثاني: الهجمات السيبرانية كأسلوب للقتال

يقوم القانون الدولي الإنساني على مبدأ أساسي يتمثل في أن الغاية من الحرب هي إضعاف القدرات العسكرية للخصم، وليس القضاء عليه أو إبادته. ومن هذا المنطلق، وضع القانون الدولي الإنساني مجموعة من القيود والضوابط التي تهدف إلى الحد من آثار النزاعات المسلحة وتقليل حجم الدمار والمعاناة الإنسانية الناجمة عنها.

كما أن التفاوت في القدرات العسكرية بين أطراف النزاع لا يبرر اللجوء إلى وسائل أو أساليب قتال محظورة بموجب القانون الدولي الإنساني، لأن ذلك من شأنه أن يعرض المدنيين

لخاطر جسيمة ويُضعف إمكانية احترام المبادئ الأساسية التي تحكم سير الأعمال العدائية، وعلى رأسها مبدأ التمييز بين المدنيين والمقاتلين، ومبدأ التناسب، وواجب اتخاذ الاحتياطات اللازمة أثناء الهجوم، فضلاً عن الالتزام بقواعد اختيار الأهداف العسكرية المشروعة، وهي مبادئ تكتسب أهمية خاصة في النزاعات المسلحة الدولية²⁶

تحدد اتفاقيات لاهاي لعامي 1899 و1907، إلى جانب اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين الملحقين بها لعام 1977، الإطار القانوني المنظم لاستخدام القوة وأساليب القتال أثناء النزاعات المسلحة الدولية وغير الدولية. وقد وضعت هذه الاتفاقيات مجموعة من الضوابط والقيود التي تهدف إلى الحد من الآثار الإنسانية للحروب، إذ تحظر التسبب في آلام غير ضرورية أو إحداث دمار مفرط أو ممارسة العنف بصورة تتجاوز ما تقتضيه الضرورات العسكرية. كما تشترط أن تُوجَّه الوسائل المستخدمة في القتال نحو أهداف عسكرية مشروعة دون استهداف المدنيين أو الأعيان المدنية، وأن يكون استخدامها قائماً على ضرورة عسكرية حقيقية، مع مراعاة مبدأ التناسب بين الضرر المتوقع والميزة العسكرية المرجوة، واتخاذ جميع الاحتياطات الممكنة لتقليل الخسائر والأضرار التي قد تصيب المدنيين.

ومن بين أساليب الحرب التي يحظرها القانون الدولي الإنساني: الغدر، ونشر الذعر بين السكان المدنيين، وتجويع المدنيين كأسلوب من أساليب القتال، والأعمال الانتقامية الموجهة ضد الأهداف غير العسكرية، والإضرار الجسيم بالبيئة الطبيعية، ومهاجمة المنشآت التي تحتوي على قوى خطرة، واحتجاز الرهائن، واستخدام الدروع البشرية، أو ترحيل السكان المدنيين لخدمة الأغراض العسكرية.

وفي هذا السياق، تندرج الحرب السيبرانية ضمن أساليب القتال الحديثة التي تعتمد على تنفيذ عمليات إلكترونية قد تترقى، في ظروف معينة، إلى مستوى النزاع المسلح. وتُستخدم هذه العمليات لدعم وتحسين فعالية الأنشطة العسكرية، كما في حالة شن هجوم سيبراني يؤدي إلى تعطيل شبكات الاتصالات في المطارات العسكرية أو المدينة التابعة للخصم بهدف تحقيق أفضلية عسكرية أثناء العمليات القتالية. ومن ثم، يمكن اعتبار العمليات السيبرانية إحدى وسائل وأساليب القتال التي تدخل ضمن التخطيط العسكري وإدارة العمليات الحربية²⁷

المطلب الثاني: مدى موافقة المبادئ النازمة لسير العمليات العدائية مع الهجمات السيبرانية وموقف الفقه الدولي والمنظمات الدولية منها

إن تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية يثير تساؤلات مهمة حول مدى ملاءمة المبادئ التقليدية المنظمة لسير العمليات العدائية مع الطبيعة التقنية والاقتراضية لهذه الهجمات. لذلك يقتضي الأمر دراسة مدى إمكانية إخضاع الهجمات السيبرانية لمبادئ التمييز والتناسب والاحتياطات في الهجوم، مع بيان موقف الفقه الدولي والمنظمات الدولية من هذه المسألة ومدى إقرارها بانطباق تلك المبادئ على العمليات السيبرانية أثناء النزاعات المسلحة.

الفرع الأول: مدى مواءمة المبادئ النازمة لسير العمليات العدائية مع الهجمات السيبرانية

تسعى أطراف النزاعات المسلحة، عند استخدامها للقوة أو للعمليات السيبرانية على وجه الخصوص، إلى إضعاف القدرات العسكرية للخصم أو القضاء عليها قدر الإمكان بهدف تحقيق التفوق العسكري وحسم النزاع. غير أن القانون الدولي الإنساني، الذي لا يهدف إلى منع استخدام القوة بقدر ما يسعى إلى تنظيمها والحد من آثارها الإنسانية، قد أخضع هذا الاستخدام لمجلة من المبادئ الأساسية التي تلتزم بها جميع أطراف النزاع. وتظل هذه المبادئ، رغم التطورات التكنولوجية وظهور الهجمات السيبرانية، معياراً أساسياً لتقييم مشروعية العمليات العدائية ومدى توافقها مع قواعد القانون الدولي الإنساني.

أ- مبدأ التمييز:

يُعد مبدأ التمييز من المبادئ الأساسية التي يقوم عليها القانون الدولي الإنساني، وقد كرسه البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1977 في المادة 48، التي أوجبت على أطراف النزاع التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، بحيث تُوجّه العمليات العسكرية حصراً ضد الأهداف العسكرية المشروعة. كما يُعتبر هذا المبدأ قاعدة عرفية راسخة في القانون الدولي، وهو ما أكدته اللجنة الدولية للصليب الأحمر وأيدته محكمة العدل الدولية²⁸

ويتضمن مبدأ التمييز جانبين أساسيين:

أولهما، التمييز بين المقاتلين والمدنيين، فالمقاتلون يُعدّون أهدافاً عسكرية مشروعة يجوز استهدافهم أثناء النزاعات المسلحة، ويشمل ذلك أفراد القوات المسلحة، وأعضاء الجماعات المسلحة المنظمة، والمدنيين الذين يشاركون بصورة مباشرة أو مستمرة في الأعمال العدائية، إضافة إلى المشاركين في الانتفاضة الشعبية أو الهبة الجماعية في إطار النزاع المسلح الدولي. أما المدنيون فيتمتعون بالحماية القانونية ولا يجوز توجيه الهجمات ضدهم.

أما الجانب الثاني فيتعلق بالتمييز بين الأهداف العسكرية والأعيان المدنية، فقد نصت الفقرة الثانية من المادة 52 من البروتوكول الإضافي الأول على أن الهجمات يجب أن تقتصر على الأهداف العسكرية فقط، ويُقصد بهذه الأخيرة الأعيان التي تسهم إسهاماً فعالاً في العمل العسكري بطبيعتها أو موقعها أو غايتها أو طريقة استخدامها، والتي يؤدي تدميرها أو الاستيلاء عليها أو تعطيلها إلى تحقيق ميزة عسكرية أكيدة في الظروف السائدة وقت الهجوم.²⁹

وفي البيئة السيبرانية تزداد صعوبة تطبيق هذا المبدأ بسبب الطبيعة المشتركة للفضاء السيبراني الذي يستخدمه المدنيون والعسكريون معاً. فقد يثور الشك أحياناً حول الطبيعة المدنية أو العسكرية للهدف أو الشخص محل الاستهداف. فعلى سبيل المثال، إذا وُجدت مؤشرات على وجود عسكريين داخل مستشفى، يثور التساؤل حول مدى جواز استهداف هذا المرفق. وفي هذا الصدد، تنص الفقرة الأولى من المادة 50 من البروتوكول الإضافي الأول، وكذلك القاعدة السادسة من قواعد القانون الدولي الإنساني العرفي التي وضعتها اللجنة الدولية للصليب الأحمر، على أنه في حال وجود شك بشأن صفة الشخص، وما إذا كان مدنياً أم مقاتلاً، فإنه يجب اعتباره مدنياً.

غير أن مفهوم "الشك" ذاته كان محل نقاش فقهي وقانوني. فالمملكة المتحدة، عند تصديقها على البروتوكول الإضافي الأول، اعتبرت أن المقصود هو "الشك الجوهري" الذي يبقى قائماً بعد تقييم جميع المعلومات المتاحة بصورة معقولة. في المقابل، يعتمد القانون الدولي الجنائي معيار "الشك المعقول" عند بحث المسؤولية الجنائية الدولية. كما أشار دليل تالين إلى أن مجرد وجود شك بسيط لا يكفي لتطبيق هذه القاعدة، بل يجب أن يستند الشك إلى أسس موضوعية ومبررات معقولة. وعليه، فإن مجرد احتمال وجود عسكريين داخل مستشفى لا يبرر استهدافه بهجوم سيبراني ما لم تتوافر معلومات كافية ومؤكدة تدعم هذا الاحتمال.³⁰

وفيما يتعلق بالأعيان، فإن الأهداف السيبرانية المشروعة تقتصر على الأهداف العسكرية دون غيرها. ومن أمثلة ذلك الحواسيب أو الأنظمة المعلوماتية المستخدمة في دعم العمليات العسكرية أو المخصصة أساساً للأغراض العسكرية. لذلك يُعد الهجوم السيبراني الذي يستهدف نظاماً للتحكم في الحركة الجوية العسكرية ويؤدي إلى تعطيل الطائرات العسكرية هجوماً مشروعاً من حيث المبدأ. أما استهداف القطاعات المصرفية المدنية أو المستشفيات أو المتاحف أو دور العبادة بواسطة هجمات سيبرانية، فيُعد اعتداءً على أعيان مدنية محمية بموجب القانون الدولي الإنساني، ومن ثم يكون عملاً غير مشروع.³¹

ب- مبدأ الاحتياطات في الهجوم:

حتى في الحالات التي تُعد فيها العملية السيبرانية هجوماً مشروعاً موجهاً ضد هدف عسكري، وتم تنفيذها وفقاً لمبدأ التمييز، فإن ذلك لا يعني الطرف المهاجم من الالتزام باتخاذ الاحتياطات اللازمة أثناء الهجوم للحد من الأضرار التي قد تلحق بالمدنيين والأعيان المدنية، ما دامت هذه الاحتياطات لا تؤثر بصورة جوهرية على تحقيق الميزة العسكرية المرجوة³² وقد كرس البروتوكول الإضافي الأول هذا الالتزام من خلال المادة 57، التي أوجبت على أطراف النزاع بذل كل ما هو ممكن للتحقق من الطبيعة العسكرية للهدف المراد مهاجمته، فضلاً عن اتخاذ جميع التدابير والاحتياطات اللازمة عند اختيار وسائل وأساليب الهجوم بهدف تجنب أو تقليل الخسائر في أرواح المدنيين والأضرار التي قد تصيب الأعيان المدنية³³. كما تناول دليل تالين مجموعة من الاحتياطات والتدابير الواجب مراعاتها عند تنفيذ الهجمات السيبرانية، ومن أبرزها:

- 1- ممارسة عناية مستمرة أثناء العمليات السيبرانية لتجنب إلحاق الضرر بالسكان المدنيين والأعيان المدنية.
- 2- التحقق من طبيعة الأهداف المراد استهدافها للتأكد من أنها ليست من الأشخاص أو الأعيان المشمولة بالحماية بموجب القانون الدولي الإنساني.
- 3- اختيار الوسائل والأساليب السيبرانية التي من شأنها تقليل الإصابات العرضية في صفوف المدنيين أو الحد من الأضرار التي قد تصيب الممتلكات المدنية.
- 4- مراعاة مبدأ التناسب من خلال الموازنة بين الميزة العسكرية المتوقعة من الهجوم وبين الأضرار المحتملة التي قد تلحق بالمدنيين والأعيان المدنية.
- 5- تفضيل استهداف الأهداف العسكرية التي تحقق الغرض العسكري المطلوب مع إحداث أقل قدر ممكن من الأضرار الجانبية.
- 6- إلغاء الهجوم أو تعليقه متى تبين أن الهدف ليس هدفاً عسكرياً مشروعاً، أو أنه يتمتع بحماية خاصة، أو إذا اتضح أن الهجوم قد يؤدي إلى خسائر عرضية مفرطة في صفوف المدنيين أو الأعيان المدنية.
- 7- توجيه إنذار مسبق وفعال للسكان المدنيين بشأن الهجمات السيبرانية المتوقعة أن تؤثر عليهم، ما لم تحول الظروف العسكرية دون ذلك³⁴

ت- مبدأ التناسب بين الضرر والميزة العسكرية المباشرة

يُعد مبدأ التناسب من المبادئ الأساسية التي يقوم عليها القانون الدولي الإنساني، إذ يهدف إلى الحد من المعاناة الإنسانية الناجمة عن العمليات العسكرية، سواء تلك التي تصيب الأشخاص أو الأعيان المدنية. ويقوم هذا المبدأ على تحقيق توازن دقيق بين الميزة العسكرية المتوقعة من العملية العسكرية من جهة، والأضرار والخسائر المحتملة التي قد تلحق بالمدنيين والممتلكات المدنية من جهة أخرى.

وتبرز صعوبات تطبيق هذا المبدأ في مجال الهجمات السيبرانية بسبب الطبيعة المعقدة لهذه العمليات، إذ أن الأنظمة والبرامج المستخدمة في تنفيذ الهجمات السيبرانية لا تملك القدرة الذاتية على إجراء الموازنة الدقيقة التي يتطلبها مبدأ التناسب، كما أن تقدير العلاقة بين المكاسب العسكرية المتوقعة والخسائر المدنية المحتملة يعد من أكثر المسائل تعقيداً حتى في العمليات العسكرية التقليدية، حيث يتطلب خبرة وتقديراً من القادة العسكريين المختصين. وتزداد هذه الصعوبة في البيئة السيبرانية بسبب صعوبة التنبؤ بالآثار المباشرة وغير المباشرة للهجوم³⁵

وفي هذا السياق، يرى شين أن مبدأ التناسب يمكن أن ينطبق على الهجمات السيبرانية، غير أن تطبيقه لا يزال يكتنفه قدر كبير من الغموض، خاصة فيما يتعلق بكيفية ضمان احترام هذا المبدأ عند الرد على الهجمات السيبرانية. كما يؤكد ركس هذا الرأي، مشيراً إلى أن استهداف البنى التحتية ذات الاستخدام المزدوج، التي تخدم الأغراض المدنية والعسكرية في آن واحد، يجعل تقدير الميزة العسكرية المتوقعة أمراً بالغ الصعوبة، وهو ما ينعكس على إمكانية تطبيق مبدأ التناسب بصورة فعالة في مجال العمليات السيبرانية³⁶.

ث- مبدأ الضرورة العسكرية:

يُعد مبدأ الضرورة العسكرية أحد الركائز الأساسية للقانون الدولي الإنساني، ويقصد به حق أطراف النزاع في استخدام القدر اللازم من القوة لتحقيق الأهداف العسكرية المشروعة المتمثلة في إضعاف قدرات العدو وتحقيق النصر، شريطة ألا يتجاوز استخدام القوة ما تقتضيه هذه الأهداف. وعليه، فإن أي استخدام للقوة يتجاوز حدود الضرورة العسكرية يعد عملاً غير مشروع ومخالفاً لقواعد القانون الدولي الإنساني.

وتتجلى التحديات المرتبطة بتطبيق هذا المبدأ على الهجمات السيبرانية في صعوبة التمييز بين الأهداف العسكرية والأعيان المدنية داخل الفضاء السيبراني، خاصة عندما تكون البنى التحتية المستهدفة ذات استخدام مزدوج وتؤدي وظائف مدنية وعسكرية في الوقت نفسه. ففي

حين يكون التمييز بين هذه الأهداف أكثر وضوحاً في النزاعات المسلحة التقليدية، فإنه يصبح أكثر تعقيداً في البيئة الرقمية بسبب الترابط الكبير بين الأنظمة والشبكات³⁷. كما تواجه الضرورة العسكرية في المجال السيبراني إشكالات عملية أخرى تتعلق بطبيعة النتائج المترتبة على هذه الهجمات. ففي العمليات العسكرية التقليدية قد يكون من الممكن تحقيق الهدف العسكري من خلال أسر المقاتلين أو تعطيل قدراتهم القتالية دون اللجوء إلى قتلهم، وهو ما يتيح قدراً أكبر من التقدير والمرونة في تطبيق مبدأ الضرورة العسكرية. أما في الهجمات السيبرانية، فإن غياب المواجهة المباشرة وصعوبة تحديد الأشخاص المستهدفين أو تقييم درجة التهديد الذي يمثلونه يجعل تطبيق هذا المبدأ أكثر تعقيداً وإثارة للإشكالات القانونية والعملية³⁸.

الفرع الثاني: موقف الفقه الدولي والمنظمات الدولية بشأن الهجمات السيبرانية

يذهب جانب واسع من فقهاء القانون الدولي وخبراء القانون الدولي الإنساني إلى التأكيد على انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية التي تُنفذ أثناء النزاعات المسلحة المعاصرة. ويستند هذا الاتجاه إلى أن العمليات السيبرانية التي تستهدف المرافق الصحية أو أفراد الطواقم الطبية أو العاملين في المجال الإنساني، وإن كانت لا تُحدث في بعض الأحيان آثاراً مادية ماثلة للهجمات العسكرية التقليدية، فإنها تظل أعمالاً غير مشروعة متى ترتب عليها المساس بالحماية الخاصة التي يقرها القانون الدولي الإنساني لهذه الفئات والأعيان³⁹.

وفي هذا السياق، يرى الفقيه مايكل شميث أن المعيار الأساسي لتقييم مشروعية السلوك لا يتمثل في الوسيلة المستخدمة بقدر ما يتمثل في النتائج والآثار المترتبة عليها. فالوسائل التي تبدو مشروعة في ذاتها قد تُستخدم لتحقيق أغراض غير مشروعة إذا أدت إلى إلحاق معاناة إنسانية مفرطة أو إلى إحداث أضرار جسيمة بالمدنيين، سواء من خلال التأثير على القطاعات المالية والمصرفية التي يعتمدون عليها أو من خلال الإضرار بالبنية التحتية المدنية الحيوية كالجسور والسدود ومحطات إنتاج الطاقة الكهربائية⁴⁰، ومن جانبه، يؤكد ماركو روسيني أن العمليات السيبرانية قادرة على تعطيل الخدمات الأساسية وشل عمل البنى التحتية الحيوية دون أن تُحدث بالضرورة دماراً مادياً أو خسائر بشرية مباشرة، الأمر الذي يستوجب تفسير قواعد القانون الدولي الإنساني بما يتلاءم مع التطورات التكنولوجية الحديثة. ووفقاً لهذا التصور، لا ينبغي حصر مفهوم العنف في الأضرار المادية فحسب، بل يجب أن يمتد ليشمل حالات التعطيل أو الإعاقة الجسيمة للبنى التحتية والخدمات الأساسية.

كما يرى دينيز هاريتون هايتز أن قصر مفهوم الهجوم على الأفعال التي تؤدي مباشرة إلى القتل أو الإصابة أو التدمير المادي لم يعد مقنعاً في ظل التطور العلمي والتكنولوجي المتسارع وما أفرزه من وسائل جديدة للتأثير في الخصم⁴¹، وفي الاتجاه ذاته، اعتبر هارولد هونغجو كوه أن الأنشطة السيبرانية التي تؤدي إلى الوفاة أو الإصابة أو التعطيل الجسيم يمكن النظر إليها باعتبارها شكلاً من أشكال استخدام القوة، ومن ثم تخضع لأحكام القانون الدولي الإنساني⁴².

أما على مستوى المنظمات الدولية، فقد أكدت كوردولا دروغيه، المستشار القانوني للجنة الدولية للصليب الأحمر، أن الإطار القانوني القائم للقانون الدولي الإنساني قابل للتطبيق على النزاعات السيبرانية، وأنه يجب احترام قواعده والالتزام بها في هذا المجال. كما رفضت الادعاءات القائلة بأن الفضاء السيبراني يمثل منطقة خالية من القواعد القانونية، مشيرة إلى أن القانون الدولي الإنساني سبق له أن تعامل مع تطورات تكنولوجية متعددة، وهو قادر على استيعاب المستجدات المرتبطة بالعمليات السيبرانية دون الحاجة إلى وضع منظومة قانونية جديدة بالكامل⁴³.

وتبني اللجنة الدولية للصليب الأحمر الموقف ذاته، إذ تعتبر القانون الدولي الإنساني الإطار القانوني الرئيسي المنظم للعمليات السيبرانية أثناء النزاعات المسلحة، لما يفرضه من قيود على استخدام هذه الوسائل ولما يوفره من حماية للسكان المدنيين والأعيان المدنية من آثارها المباشرة وغير المباشرة. وتؤكد اللجنة أن الطبيعة التقنية المتطورة للعمليات السيبرانية لا تحول دون خضوعها للقواعد ذاتها التي تنطبق على غيرها من وسائل وأساليب القتال التقليدية والحديثة⁴⁴.

كذلك أشار دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية لعام 2013 إلى إمكانية تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية. واعتبر الدليل أن الهجوم السيبراني قد يرقى إلى مستوى استخدام القوة متى كانت آثاره ماثلة أو قريبة من آثار استخدام القوة العسكرية التقليدية. وبناءً على ذلك، أكد الخبراء المشاركون في إعداد الدليل ضرورة إخضاع الحرب السيبرانية لأحكام القانون الدولي الإنساني، مع اعتماد حجم الضرر وآثاره، ولا سيما ما يتعلق بحياة المدنيين وسلامتهم، معياراً أساسياً لتحديد نطاق تطبيق هذه القواعد⁴⁵.

أكدت تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة الصادرة عامي 2013 و2015 أن أحكام القانون الدولي، بما في ذلك القانون الدولي الإنساني وميثاق الأمم المتحدة، تظل قابلة للتطبيق في بيئة تكنولوجيا المعلومات والاتصالات. وقد لقي هذا الاستنتاج ترحيباً من الجمعية العامة للأمم المتحدة التي أكدت عليه لاحقاً، كما حظي بدعم عدد من الدول والمنظمات الدولية،

من بينها الاتحاد الأوروبي والاتحاد الإفريقي وحلف شمال الأطلسي، التي أعلنت صراحة أن قواعد القانون الدولي الإنساني تنطبق على الهجمات السيبرانية التي تُنفذ أثناء النزاعات المسلحة. وفي عام 2019، شدد الفريق العامل المعني بالقانون الدولي للفضاء السيبراني التابع للمنظمة الاستشارية القانونية الآسيوية الإفريقية على ضرورة تطبيق كل من قانون الحرب وقانون اللجوء إلى القوة المسلحة على العمليات السيبرانية، مع مراعاة الخصائص التقنية التي تميز هذا النوع من العمليات⁴⁶، كما أعاد "نداء باريس من أجل الثقة والأمن في الفضاء السيبراني"، الذي أيدته إحدى وسبعون دولة في أبريل 2020، التأكيد على انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية خلال النزاعات المسلحة⁴⁷.

ومن خلال استعراض مختلف الآراء والمواقف الفقهية والدولية بشأن هذه المسألة، يتبين أن غياب نصوص صريحة في القانون الدولي الإنساني تتناول الهجمات السيبرانية لا يعني استبعادها من نطاق تطبيقه. فالقواعد الأساسية لهذا القانون تقوم على حماية المدنيين والأعيان المدنية من آثار الأعمال العدائية، بغض النظر عن الوسيلة المستخدمة في تنفيذها.

وعليه، فإن الهجمات السيبرانية التي تستهدف المدنيين أو الأعيان المدنية، أو تؤدي إلى الإضرار بالبنى التحتية الحيوية كشبكات الكهرباء والمياه والاتصالات والأنظمة الصحية والمصرفية، يمكن أن تُحدث آثاراً إنسانية خطيرة لا تقل عن تلك الناجمة عن الهجمات التقليدية. ومن ثم، فإن إخضاع هذه العمليات لأحكام القانون الدولي الإنساني يعد نتيجة منطقية تنسجم مع أهدافه ومقاصده الأساسية، حتى وإن كانت هناك تحديات عملية وقانونية تثيرها طبيعة الفضاء السيبراني عند تطبيق تلك الأحكام.

الخاتمة

أصبح موضوع التكييف القانوني للهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني من القضايا التي تكتسي أهمية متزايدة في العصر الحديث، وذلك في ظل التطور التكنولوجي المتسارع وما صاحبه من استخدامات سلبية للفضاء السيبراني في النزاعات المسلحة. فلم تعد آثار الهجمات السيبرانية تقتصر على تعطيل الأنظمة والشبكات المعلوماتية، بل امتدت لتؤثر بشكل مباشر في الواقع المادي، مسببة أضراراً جسيمة قد تصل إلى إزهاق الأرواح وتدمير الممتلكات والبنى التحتية الحيوية. ومن هذا المنطلق، برزت تساؤلات قانونية عديدة حول مدى خضوع هذه الهجمات لأحكام القانون الدولي الإنساني وإمكانية تطبيق قواعده ومبادئه عليها أثناء النزاعات المسلحة.

وبعد دراسة هذا الموضوع وتحليل مختلف جوانبه القانونية والعملية، أمكن التوصل إلى جملة من النتائج أهمها:

- أفرزت الثورة الرقمية وتطور تكنولوجيا المعلومات واقعاً جديداً في العلاقات الدولية، صاحبه ظهور تهديدات وتحديات متزايدة تمثلت في الهجمات السيبرانية التي أصبحت إحدى الأدوات المستخدمة في النزاعات المسلحة الدولية وغير الدولية.

- تخضع الهجمات السيبرانية التي تُنفذ في إطار نزاع مسلح قائم لأحكام القانون الدولي الإنساني باعتبارها من الوسائل والأساليب الحديثة للقتال، شريطة وجود ارتباط وثيق بينها وبين النزاع المسلح القائم.

- يتطلب احترام مبدأ التمييز في الهجمات السيبرانية توافر شرطين أساسيين، يتمثل الأول في مساهمة الهدف مساهمة فعالة في العمل العسكري، بينما يتمثل الثاني في أن يؤدي تدميره أو تعطيله أو الاستيلاء عليه إلى تحقيق ميزة عسكرية مؤكدة في ظل الظروف السائدة.

- يواجه تطبيق مبدأ التمييز في الفضاء السيبراني صعوبات عملية كبيرة، نظراً للطبيعة المزدوجة لمعظم البنى التحتية والشبكات المعلوماتية التي يستخدمها المدنيون والعسكريون على حد سواء.

- يقوم مبدأ التناسب على ضرورة الموازنة بين الميزة العسكرية المتوقعة من الهجوم وبين الأضرار العرضية المحتملة التي قد تلحق بالمدنيين والأعيان المدنية، بما يضمن عدم تجاوز الحدود التي يقرها القانون الدولي الإنساني.

- تزداد صعوبة تطبيق مبدأ التناسب في العمليات السيبرانية بسبب الترابط المعقد بين الشبكات والأنظمة الرقمية، وصعوبة التنبؤ الدقيق بالآثار غير المباشرة للهجوم، وهو ما يجعل تقدير النتائج المحتملة أكثر تعقيداً مقارنة بالأسلحة التقليدية.

- يعد الالتزام باتخاذ الاحتياطات اللازمة أثناء تنفيذ الهجمات السيبرانية التزاماً ببذل العناية والجهد الممكنين وفقاً للظروف والإمكانات المتاحة، وليس التزاماً بتحقيق نتيجة محددة بصورة مطلقة.

- كما أن اتخاذ التدابير اللازمة لإبعاد المدنيين والأعيان المدنية عن نطاق العمليات السيبرانية يمثل أحد أهم الواجبات الاحتياطية الملقاة على عاتق أطراف النزاع، حتى وإن استلزم ذلك فرض قيود مؤقتة على الوصول إلى بعض الأنظمة والشبكات، متى كان الهدف من تلك القيود حماية المدنيين من الأخطار والأضرار المحتملة الناجمة عن الهجمات السيبرانية.

استنادًا إلى النتائج المتوصل إليها، يمكن تقديم مجموعة من التوصيات التي من شأنها تعزيز حماية المدنيين والأعيان المدنية من الآثار السلبية للهجمات السيبرانية أثناء النزاعات المسلحة، وذلك من خلال:

- العمل على إبرام اتفاقية دولية خاصة أو اعتماد بروتوكول إضافي لاتفاقيات القانون الدولي الإنساني يتناول تنظيم استخدام الهجمات السيبرانية أثناء النزاعات المسلحة، ويكرس التزامات واضحة على عاتق الدول لضمان عدم توجيه هذه الهجمات ضد السكان المدنيين والأعيان المدنية.

- إلزام أطراف النزاع باتخاذ جميع التدابير والاحتياطات الممكنة عند تنفيذ العمليات السيبرانية، بما يكفل الحد من الأضرار العرضية التي قد تلحق بالمدنيين أو بالبنية التحتية المدنية.

-حث الدول، في حدود إمكانياتها التقنية واللوجستية، على بذل العناية الواجبة لتعزيز أمنها السيبراني، والعمل على الفصل قدر الإمكان بين الشبكات والبنى التحتية ذات الاستخدام العسكري وتلك المخصصة للأغراض المدنية، بما يسهم في الحد من المخاطر الناجمة عن الهجمات السيبرانية.

وفي الختام، يبقى من الضروري أن تُوجّه التطورات التكنولوجية المتسارعة في مجال المعلومات والاتصالات نحو خدمة التنمية البشرية وتعزيز رفاهية الشعوب، وأن تُستثمر القدرات التقنية الحديثة في دعم الأمن والاستقرار والتعاون الدولي، بدلاً من توظيفها في تأجيج النزاعات وإلحاق المزيد من المعاناة بالإنسانية.

الهوامش:

- 1 - سلمونة محمد ياسين محمد، هماش عبد السلام أحمد إسماعيل: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، الأردن، 2024، ص 30.
- 2 - نفس المرجع، ص 15.
- 3 - نفس المرجع، ص 30.
- 4 - إسماعيل محمود الرزاز: الحماية القانونية من الهجمات والجرائم السيبرانية، الطبعة الأولى، مركز المحمود لتوزيع الكتب القانونية، القاهرة، مصر، 2023، ص 16.
- 5 - نفس المرجع ونفس الصفحة.
- 6 - نفس المرجع ونفس الصفحة
- 7 - نفس المرجع ونفس الصفحة
- 8 - نفس المرجع، الصفحة 17

- 9 - نفس المرجع، الصفحة 17
- 10 - نفس المرجع، 18.
- 11 - *faisal saleh alabbadi, emad mohammed al amaren, sultan ibrahim aleitein : international responsibility arising from cyberattacks in the light of the contemporary international law, international journal of cyber criminology, volume 16, issue 1, january-jaune 2022, p 160.*
- 12 - إسماعيل محمود الرزاز، المرجع السابق، ص 27
- 13 - إسماعيل محمود الرزاز: المرجع السابق، ص 27.
- 14 - منى الأشقر جبور: الأمن السيبراني- التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، اللقاء السنوي الأول للمختصين في امن وسلامة الفضاء السيبراني، بيروت 27، 28 أغسطس 2012، ص 03.
- 15 - منى الأشقر جبور، المرجع السابق، ص 04
- 16 - إيهاب خليفة: القوة الالكترونية- كيف يمكن أن تدير الدول شؤونها في عصر الانترنت، مطبعة العربي، القاهرة، 2017، ص 24.
- 17 - تغريد معين حسن: الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، بحث منشور في مجلة البحوث الجغرافية، العدد 30، ص 242.
- 18 - تغريد معين حسن، المرجع السابق، ص 243.
- 19 - دليل تالين (Tallinn Manual) هو مجموعة من القواعد والمبادئ القانونية التي أعدها خبراء في القانون الدولي وخبراء في الأمن السيبراني، تحت إشراف مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (NATO CCDCOE) في تالين، إستونيا، بهدف دراسة كيفية تطبيق قواعد القانون الدولي القائمة على الأنشطة السيبرانية، ولا سيما الهجمات السيبرانية. ومن المهم التأكيد على أن دليل تالين ليس معاهدة دولية ولا يمثل قانوناً ملزماً للدول، وإنما يُعد مرجعاً فقهيّاً وأكاديميّاً مهمّاً يساعد على تفسير وتطبيق قواعد القانون الدولي في البيئة السيبرانية.
- 20- *Mohammad Saidul Islam : Cyber Warfare and International Humanitarian Law : A Study, International Journal of Ethics in Social Sciences, Vol 05, N° 01, June 2017, p 105.*
- 21 - خلافي سفيان: تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 02، 2022، ص 318.
- يختلف مفهوم الهجوم بموجب هذه المادة عن مفهوم الهجوم المسلح بموجب المادة 51 من ميثاق الأمم المتحدة الذي يندرج في نطاق اللجوء للحرب، ويجب التمييز بينهما، ويجب التأكيد على أن أي عملية سيبرانية ترقى إلى حد الهجوم بموجب القانون الدولي الإنساني لا يعني بالضرورة إنها تصنف كهجوم مسلح بموجب ميثاق الأمم المتحدة.
- 23 - *ibid, p 489.*

24 - *ibid*, p 488.

25 - سلمونة محمد ياسين محمد، هماش عبد السلام أحمد إسماعيل: المرجع السابق، ص 69.

26 - فاضل عبد الزهرة فاضل: التكييف القانوني لدور المدنيين في الهجمات السيبرانية، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 17، العدد 59، 2024، ص 1456.

27 - نفس المرجع، ص 1457.

28 - سلوى يوسف الأكيلى: مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، مجلة روح القوانين، العدد 101، الجزء الثاني، جافى 2023، ص 1379.

29 -- نفس المرجع ونفس الصفحة.

30 - نفس المرجع، ص 1383

31 - نفس المرجع، ص 1396.

32 - Schmitt, M.N. ORCID : *op cit*, p 20.

33 - Schmitt, M.N. ORCID : *ibid*, p 21.

34 - نور أمير الموصلى: الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، 2021، ص 49.

35 - مايا شوكت صفطى: إشكالية التطبيق الفعلي لقواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية أثناء النزاعات المسلحة المعاصرة، مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الاقتصادية والقانونية، المجلد 46، العدد 03، 2024، ص 54.

36 - نفس المرجع، ص 55.

37 - نفس المرجع، ص 53.

38 - يحيى ياسين سعود: الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، العدد 04، مصر، جامعة القاهرة، كلية الحقوق فرع الخرطوم، 2018، ص 96.

39 - اسحاق العشعاش: الهجمات السيبرانية ضد المنشآت الصحية الحرجة في زمن الأوبئة والجوائح، مجلة القانون الدولي للدراسات البحثية، العدد 05، 2020، ص 117.

40 - Michael N Schmitt: *classification of cyber conflicts*, *journal of conflicts and security law*, 2012, vol 17, N° 03, p 257.

41 - Dinnes Harrison Heather: *cyber warfare and the law of war*, Cambridge University Press, 2012, Cambridge, p 198.

42 - Harold Hongiu Koh: *international law in cyber space*, *Harvard International law journal*, vol 54, n° 07, 2012, p 08.

43 - Cordula Drogeh : *get of my cloud- cyber warfare*, *international humanitarian law and the protection of civilians*, *international review of the red cross*, vol 94, N° 886, p 565.

44 - القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر المقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، نوفمبر 2019، ص 10.

45 - Michael N Schmitt, *Tallinn Manual on international law applicable to cyber warfare*, ed 01, Cambridge University Press, New York, 2013, p 125.

46 - AALCO: *Summary report of the fourth meeting of the open-ended working group on international law in cyber space*, September 2019, p 10.

47 - France, *Paris call for trust and security in cyber space*, France diplomacy, November 2018.