



جمهورية العراق
وزارة التعليم العالي والبحث العلمي
معهد العلمين للدراسات العليا
قسم القانون العام

أثر الهجمات السيبرانية على المناطق المحمية / دراسة في ضوء أحكام القانون الدولي الإنساني

أطروحة تقدم بها الطالب
عباس ثائر صاحب عمران الحسناوي
إلى مجلس معهد العلمين للدراسات العليا
وهي جزء من متطلبات نيل درجة الدكتوراه في
القانون العام

بإشراف
الأستاذ المساعد الدكتور
فاضل عبد الزهرة فاضل الغراوي
أستاذ القانون الدولي

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَقَاتِلُوا فِي سَبِيلِ اللَّهِ الَّذِينَ يُقَاتِلُونَكُمْ
وَلَا تَعْتَدُوا إِنَّ اللَّهَ لَا يُحِبُّ الْمُعْتَدِينَ﴾

صدق الله العلي العظيم

البقرة: الآية ١٩٠

اقرار المشرف

اشهد ان اعداد الاطروحة للطلاب محمد عبد السلام محمد عبد السلام محمد عبد السلام محمد عبد السلام الموسومة الدراسة التاريخية عن طينها من الجبل الدراسة التاريخية عن طينها من الجبل الدراسة التاريخية عن طينها من الجبل الدراسة التاريخية عن طينها من الجبل قد جرى تحت اشرافي في معهد العظمين للدراسات العليا , وانها صالحة للمناقشة



الامضاء :

اللقب العلمي : د. م. م.

الاسم : ضامن عبد السلام

العنوان : معهد العظمين للدراسات العليا

التاريخ : ١٦ / ٤ / ٢٠٢٥

اقرار المقوم اللغوي

إشارة الى كتابكم ذي العدد (ق ٤ / ٥٤٤) بتاريخ (٢٠٢٥/٤/٢٠) نوّد إعلامكم أنّه تمّ تقويم أطروحة الدكتوراه للطالب (عباس ثائر صاحب الموسومة: (اثر الهجمات السيبرانية على المناطق المحمية - دراسة في ضوء احكام القانون الدولي الإنساني) لغويّاً، وقد ثبتت التصويبات على الرسالة، وأخذ الباحث بها؛ لذا أرشحها للمناقشة.

الامضاء: 

اللقب العلمي: أستاذ دكتور

الاسم: حيدر كريم كاظم الجمالي

العنوان: جامعة الكوفة - كلية التربية الاساسية

التاريخ: ٢٠٢٥ / ٤ / ٢٢



مجمع الدراسات العليا

السراي - السجف الاشرف



إقرار لجنة المناقشة

نحن أعضاء لجنة المناقشة نشهد أننا قد اطلعنا على أطروحة الطالب (عباس ثائر صاحب) الموسومة (أثر الهجمات السيبرانية على المناطق المحمية-دراسة في ضوء احكام القانون الدولي الانساني) ناقشنا في محتوياتها وأقررنا أنها جديرة بالقبول لنيل درجة الدكتوراه في القانون (العام) بتقدير ()

أ.د. محمد ياس خضير

٢٠٢٥ / /

عضواً

أ.م.د. خالد خليل مطر

٢٠٢٥ / /

عضواً

أ.د. بشير جمعة عبد الجبار

٢٠٢٥ / /

رئيساً

التوقيع:
اللقب العلمي:
الاسم:
التاريخ:

أ.د. صوب ناجي عيود

٢٠٢٥ / /

عضواً

أ.م.د. خالد خضير محام

٢٠٢٥ / /

عضواً

أ.م.د. فاضل عبد الزهرة فاضل

٢٠٢٥ / /

عضواً ومشرفاً

التوقيع:
اللقب العلمي:
الاسم:
التاريخ:

التوقيع:
اللقب العلمي:
الاسم:
التاريخ:

التوقيع:
اللقب العلمي:
الاسم:
التاريخ:

التوقيع:
اللقب العلمي:
الاسم:
التاريخ:

صدقت من قبل مجلس معهد المعلمين للدراسات العليا في جلسته المرقمة () المتعلقة في ٢٠٢٥ / /

أ.د. زيد عثمان محسن

عميد معهد المعلمين للدراسات العليا

الإهداء

الكريمان، من المهدِ حتّى الضُّوء الَّذي اشْرأَبَ في رأسي، والدَيَّ العزيزان،
أُهدي لكما عرقاً من جبين الحروف، تجدونه هنا.

أساتذتي الذين زَكَّوْا علمهم إذ منحوه لنا، ونحن نقفُ على أبوابهم المعرفيّة،
وأخصّ بالذكرِ أستاذي ومشرفي الأستاذ المساعد الدكتور فاضل عبد الزهرة
الغراوي، المُعطاء حدَّ انتهاء الوصفِ، مدينٌ له بشُكرٍ عظيمٍ لا يسُدُّه سدٌّ.

إخوتي وأصدقائي، الذين ساندوني مُذْ لحظة شُرُوعي في رحلتي مع الدكتوراه.
الكوفةُ بلدةُ الطوفانِ الكبير، بلدةُ إمام السَّلام والجمال عليّ بن أبي طالب (عليه
السَّلام)، ومسقطُ رأسِ المُتنبّي، شُكراً لماءِ الفرات الَّذي فاضَ في معرفةٍ وجمالاً.
شهداءُ غزّة ولبنان، هل يفي الشُّكرُ حقَّ من يموتُ دفاعاً عن كرامة أُمّةٍ كاملة؟

الباحث

شكر و عرفان

أتقدم بخالص الشكر وعظيم الامتنان إلى عمادة معهد العلمين للدراسات العليا، لما وفّرت من بيئة علمية محفزة ودعم متواصل خلال مسيرتي البحثية. وإلى اساتذتي في قسم القانون و أتوجه بوافر التقدير والعرفان إلى أستاذي المشرف، الأستاذ المساعد الدكتور فاضل عبد الزهرة الغراوي، على ما بذله من جهد كبير وتوجيهات سديدة كان لها الأثر البالغ في إخراج هذه الأطروحة إلى النور. ولا يفوتني أن أعبر عن شكري الجزيل إلى السادة أعضاء لجنة المناقشة الكرام، لما بذلوه من وقت وجهد في مناقشة هذه الأطروحة وتقديم ملاحظاتهم العلمية القيمة. و أتقدم بالشكر إلى مكتبة معهد العلمين للدراسات العليا، لما وفّرت من مصادر علمية وخدمات بحثية متميزة. وإلى كل من قدم لي العون والإسناد، ودعمي بكلمة أو نصيحة أو دعاء، أرفع أسمى آيات الشكر والعرفان.

الباحث

المستخلص

تتناول هذه الأطروحة دراسة "أثر الهجمات السيبرانية على المناطق المحمية" في ضوء أحكام القانون الدولي الإنساني، في سياق تصاعد الاعتماد على الفضاء السيبراني كساحة جديدة للنزاعات المسلحة المعاصرة. ومع ازدياد الهجمات التي تستهدف بنى تحتية حيوية مدنية، برزت تساؤلات قانونية جوهرية حول مدى كفاية القواعد التقليدية للقانون الدولي الإنساني لضمان حماية فعالة للمناطق المحمية من أخطار العمليات السيبرانية، وما إذا كان الإطار القائم قادراً على استيعاب التحديات الناشئة عن الطابع اللامادي وغير التقليدي لهذه الهجمات.

تسعى الدراسة إلى تأصيل المفاهيم المتعلقة بالهجمات السيبرانية، من حيث طبيعتها القانونية، وخصائصها المميزة عن العمليات العسكرية التقليدية، بما في ذلك خفاء مصدر الهجوم، وصعوبة تحديد المسؤولية، واتساع نطاق الأثر عبر الحدود دون استعمال وسائل القوة الفيزيائية التقليدية. وتُعنى بتحليل مفهوم "المناطق المحمية" على وفق ما حدده القانون الدولي الإنساني، التي تشمل المستشفيات والمرافق الصحية، والأعيان الثقافية، والبنى التحتية المدنية الحيوية، وما يترتب على هذه الحماية من التزامات قانونية في أثناء النزاعات المسلحة.

تناقش الأطروحة الإشكاليات التي تطرحها الهجمات السيبرانية المعاصرة، لاسيما في ضوء أمثلة عملية مثل الهجوم السيبراني الذي استهدف شبكة الكهرباء في أوكرانيا عام ٢٠١٥، والهجمات التي تعرضت لها أنظمة المستشفيات خلال جائحة كوفيد-١٩، والتي أدت إلى تعطيل الوصول إلى الرعاية الصحية في أوقات حرجية. ومن خلال تحليل هذه الحالات، يتم الوقوف على مدى توافر شروط اعتبار الهجوم السيبراني "هجومًا" بالمعنى المنصوص عليه في اتفاقيات جنيف والبروتوكولات الإضافية، مع ما يستتبع ذلك من انطباق لقواعد الحماية والالتزامات المفروضة على أطراف النزاع.

تركز الأطروحة على التحديات المرتبطة بتطبيق مبدأي التمييز والتناسب في البيئة السيبرانية، في ظل صعوبة الفصل بين الأهداف العسكرية والأعيان المدنية عندما تُستخدم الشبكات والأنظمة المعلوماتية المشتركة لكلا الغرضين، فضلاً عن ذلك مشكلة الآثار غير المادية للهجمات، التي قد تؤدي إلى حرمان السكان المدنيين من خدمات أساسية دون أن تُخلف دماراً مادياً ظاهراً، مما يثير تساؤلات حول تفسير مصطلحات "الضرر" و"الهجوم" و"الأثر العسكري المباشر" في البيئة الرقمية.

وتتناول الأطروحة إشكالية تحديد المسؤولية القانونية عن الهجمات السيبرانية، بالنظر إلى ما توفره التقنيات الحديثة من إمكانيات لإخفاء مصدر الهجوم أو استخدام جماعات غير حكومية كأذرع إلكترونية للدول المتنازعة، مما يعقد مسألة الإسناد القانوني، ومن ثم المحاسبة على فق قواعد القانون الدولي الإنساني. ويبرز من خلال ذلك مدى الحاجة إلى تطوير آليات تحقيق وتحليل للأدلة الرقمية بما يتلاءم مع طبيعة الفضاء السيبراني.

تخلص الأطروحة إلى أن الهجمات السيبرانية تفرض تحديات جدية على المفاهيم التقليدية للحماية الإنسانية في النزاعات المسلحة، إذ تقوض بعض الأسس التي يقوم عليها القانون الدولي الإنساني، لاسيما فيما يتعلق بحماية السكان المدنيين والمناطق المحمية من الأعمال العدائية. ويتبين أن هناك حاجة ملحة لمزيد من التفسير والتطوير لمفاهيم القانون الدولي الإنساني بما يستوعب التغيرات التكنولوجية، ويحافظ في الوقت نفسه على المبادئ الأساسية لهذا النظام القانوني، ولا سيما في ظل الطبيعة المتسارعة لتطور القدرات السيبرانية، واتساع استخدامها في النزاعات المسلحة الحديثة.

قائمة المحتويات

ت	الموضوع	رقم الصفحة
١.	الآية القرآنية	ب
٢.	الاهداء	ح
٣.	شكر وامتنان	خ
٤.	المستخلص	د
٥.	المقدمة	٦-١
٦.	الفصل الأول مفهوم الهجمات السيبرانية	٦٦ - ٧
٧.	المبحث الاول تعريف الهجمات السيبرانية	٨
٨.	المطلب الأول التعريف اللغوي والاصطلاحي للهجمات السيبرانية	٦٨
٩.	الفرع الاول التعريف بالهجمات السيبرانية لغة واصطلاحاً	٩
١٠.	الفرع الثاني اقسام وأنواع الهجمات السيبرانية	١٥
١١.	المطلب الثاني مفهوم المناطق المحمية	١٩
١٢.	الفرع الأول تعريف المناطق المحمية	٢٠
١٣.	الفرع الثاني الطبيعة القانونية للمناطق المحمية	٢٥
١٤.	المبحث الثاني الجهود الفقهية والدولية لمواجهة مخاطر الهجمات السيبرانية	٣٩

٤٠	المطلب الأول الجهود الفقهية لمواجهة المخاطر السيبرانية	١٥.
٤١	الفرع الأول دليل تالين والمخاطر السيبرانية	١٦.
٤٨	الفرع الثاني إعلان إبرايتشي لمبدأ الاستقرار السيبراني والسلام السيبراني.	١٧.
٥١	المطلب الثاني الجهود الدولية في مواجهة خطر الهجمات السيبرانية	١٨.
٥٢	الفرع الأول موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية	١٩.
٥٩	الفرع الثاني قرارات المنظمات الدولية لمواجهة الهجمات السيبرانية	٢٠.
١٣٤-٦٧	الفصل الثاني حماية المناطق المحمية من الهجمات السيبرانية	٢١.
٦٨	المبحث الأول المبادئ الدولية المنظمة للمناطق المحمية في القانون الدولي الإنساني	٢٢.
٦٨	المطلب الأول تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية	٢٣.
٦٩	الفرع الأول مبادئ القانون الدولي الإنساني وحظر الهجمات العشوائية	٢٤.
٨٣	الفرع الثاني معايير تحديد الأهداف العسكرية المشروعة في أثناء الهجمات السيبرانية	٢٥.
٩٤	المطلب الثاني تحديد انطباق القانون الدولي الإنساني على الهجمات السيبرانية	٢٦.
٩٥	الفرع الأول انطباق القانون الدولي الإنساني على الهجمات السيبرانية في سياق النزاع المسلح	٢٧.

١٠٠	الفرع الثاني انطباق القانون الدول الإنساني على الهجمات السيبرانية خارج سياق النزاع المسلح	٢٨.
١٠٣	المبحث الثاني آثار الهجمات السيبرانية على المناطق المحمية	٢٩.
١٠٤	المطلب الأول : مخاطر الهجمات السيبرانية على المناطق المحمية	٣٠.
١٠٥	الفرع الأول مخاطر الهجمات السيبرانية على المناطق المحمية والأفراد	٣١.
١١٥	الفرع الثاني الآثار الإيجابية والسلبية للهجمات السيبرانية	٣٢.
١٢٣	المطلب الثاني دور القانون الدولي الإنساني في مواجهة آثار الهجمات السيبرانية	٣٣.
١٢٣	الفرع الأول :الجهود الدولية والوطنية لمواجهة الهجمات السيبرانية	٣٤.
١٢٧	الفرع الثاني الجهود الإقليمية والدولية لتعزيز الأمن السيبراني للمناطق المحمية	٣٥.
٢١٦-١٣٧	الفصل الثالث المسؤولية الدولية الناشئة عن الهجمات السيبرانية على المناطق المحمية وفق القانون الدولي الإنساني	٣٦.
١٣٨	المبحث الأول المسؤولية الدولية عن أضرار الهجمات السيبرانية تجاه المناطق المحمية	٣٧.
١٣٩	المطلب الأول مفهوم المسؤولية وأركان أو عناصر المسؤولية الدولية	٣٨.
١٣٩	الفرع الأول : تعريف المسؤولية الدولية	٣٩.
١٤٥	الفرع الثاني أركان المسؤولية الدولية عن الهجمات السيبرانية على المناطق المحمية .	٤٠.

١٥٢	المطلب الثاني التكليف القانوني للهجمات السيبرانية والتعويض عنها	٤١.
١٥٣	الفرع الأول التكليف القانوني للهجمات السيبرانية	٤٢.
١٦٠	الفرع الثاني التعويض عن ضرر الهجمات السيبرانية على المناطق المحمية	٤٣.
١٧٧	المبحث الثاني الوسائل الدولية لتعزيز الحماية للمناطق المحمية في الهجمات السيبرانية	٤٤.
١٧٨	المطلب الأول دور الاتفاقيات الدولية في تعزيز الحماية للمناطق المحمية في الهجمات السيبرانية	٤٥.
١٧٩	الفرع الأول دور اتفاقيات جنيف الرابع لعام ١٩٤٩ في تعزيز الحماية للمناطق المحمية	٤٦.
١٨٩	الفرع الثاني البروتوكولان الإضافيان لعام ١٩٧٧	٤٧.
١٩٦	المطلب الثاني دور القضاء الجنائي الدولي في تعزيز الحماية للمناطق المحمية	٤٨.
١٩٧	الفرع الأول دور المحاكم الدولية المؤقتة	٤٩.
٢٠٣	الفرع الثاني دور المحاكم الدولية في تعزيز الحماية للمواقع المحمية في الهجمات السيبرانية	٥٠.
٢١٧	الخاتمة	٥١.
٢٢٣	المصــــادر والمراجع	٥٢.

المقدمة

أولاً : موضوع الدراسة

شهدت السنوات الأخيرة تطوراً هائلاً في المجالات الفكرية والصناعية والتجارية، والتي أدت بدورها إلى قيام ثورة كبيرة في وسائل القتال أيضاً سعياً في ميدان سباق التسليح، إذ دخلت وسائل الاتصال الإلكتروني والحاسوب الآلي والشبكات العنكبوتية ساحة الصراع، مما أدى إلى خلق متغيرات جديدة وحدث تغيير فعال وكبير في مفهوم الصراعات الحديثة، صفاً إلى صف وسائل القتال التقليدية، فقد حلت وسائل الاتصال والتكنولوجيا المعلوماتية ضيفاً جديداً في ساحة القتال، لتصبح نوعاً جديداً مهماً وخطراً من وسائل الصراع الإنساني، وهو حرب الفضاء السيبراني، أو الحروب السيبرانية أو الهجمات السيبرانية أو النزاعات السيبرانية. وأن الآثار المترتبة على الفهم القائم على العواقب لمفهوم الهجوم هو أن معظم الأحكام الموضوعية التي تحمي المدنيين وأعيانهم بموجب البروتوكول الإضافي الأول لعام ١٩٧٧ لا تنطبق و العمليات السيبرانية، وعلى الرغم من أن القانون الدولي الإنساني حاول حماية الأشخاص المتضررين والأعيان المدنية والمناطق المحمية من النزاع المسلح عبر اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين الملحقين لعام ١٩٧٧ واتفاقية لاهاي وغيرها، فقد تنص اتفاقيات جنيف الأربع على حماية المدنيين وغيرهم ممن توقفوا عن المشاركة في الحرب والجرحى وسواهم والأعيان المدنية، والمناطق المحمية، إلا أنها لم تستطع تغطية النزاعات الجديدة لقدم القانون الدولي ولحدثة الآلة الجديدة المستخدمة في هذه النزاعات، ولكن فرضت قيود على استخدام التكنولوجيا العسكرية في النزاعات المسلحة، و أن القانون الدولي الإنساني ما فتئ ساعياً إلى الحيلولة دون تعرض الأشخاص وممتلكاتهم في حالات النزاعات المسلحة إلى الأهوال والأخطار مما حدى به إلى حمايتهم عبر إنشاء واقامة مناطق محمية يحظر مهاجمتها لأي سبب كان ما دامت محميةً إلا أن هناك نهج متساهل يسمح بتوجيه مجموعة واسعة من العمليات السيبرانية ضد المدنيين والمناطق المحمية، وفي هذا الإطار وفيما يتعلق بأثر الهجمات السيبرانية على المناطق المحمية على وفق اتفاقيات جنيف الأربع، يمكن القول أن هذه الهجمات قد تنتهك وتخرق عدداً من المبادئ الأساسية للقانون الدولي الإنساني. ومن ثم فإن العمليات السيبرانية واسعة النطاق بما أنها غير مادية فقد توجه عمداً وبشكل قانوني ضد

المدنيين أو ضد البنى التحتية لأعيان مدنية أو لمناطق محمية. وقد تؤدي إلى توسيع تأثير الحرب على المدنيين، أو على الأعيان أو المناطق المحمية، التي يحظر شمولها بالنزاعات المسلحة إذا ما بقيت ملتزمة بشروط المنطقة المحمية على وفق ما يشترطه القانون الدولي الإنساني ومستوفاة لها. من المرجح أن تتفاقم هذه التأثيرات مع تزايد اعتماد المجتمعات الحديثة على التقنيات السيبرانية في البنية التحتية الأساسية مثل النفط والغاز وشبكات النقل، وأنظمة توليد الكهرباء ومرافق معالجة المياه وخدمات الاستجابة للطوارئ ويمثل الواقع السلبي للنهج المتساهل حجة قوية لإعادة تفسير الإطار القانوني الحالي من أجل التكيف مع الخصائص الخاصة للحرب السيبرانية.

أهمية الدراسة:

تتمثل أهمية الدراسة في أن الهجمات السيبرانية التي تستهدف المناطق المحمية من أبرز التحديات التي تواجهها المجتمعات الدولية في العصر الحديث، إذ إن هذه الهجمات تنطوي على تأثيرات سلبية جسيمة على المناطق المحمية بموجب اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين لعام ١٩٧٧، ومن ثم يجب دراسة مدى إمكانية انطباق القانون الدولي الإنساني على هذه الهجمات، ومدى إقامة المسؤولية الدولية، وذلك لما تشكله من اختراق لمبادئ وقواعد القانون الدولي في المناطق المحمية، وكذلك لحدثة هذه النزاعات وتقدمها ولا سيما أنها هجمات تخترق قواعد القانون الإنساني، الذي سبق ظهورها بكثير فلم نجد لها ذكراً في التشريعات الدولية الإنسانية السابقة له. واهتمت الدراسة في إمكانية تحديد الجهود الدولية لتقييد أو حظر استعمال الهجمات السيبرانية في المناطق المحمية في إطار مبادئ القانون الدولي الإنساني من خلال تطبيق المبادئ الدولية على الهجمات السيبرانية، من خلال بيان الإطار القانوني للهجمات السيبرانية، في اتفاقية الأمم المتحدة، وكذلك من خلال اتفاقيات جنيف الأربعة، والأحكام التي تضمنها في سبيل توضيح مدى شرعية هذا الاستخدام وللوقوف على جدية المجتمع الدولي في حماية المدنيين في المناطق المحمية، وما يترتب على استخدام تلك الهجمات على تلك المناطق، وبما يتوافق مع قواعد القانون الدولي الإنساني.

أهداف الدراسة:

تهدف هذا الدراسة إلى بيان كيفية تنظيم العمليات السيبرانية التي تتم في سياق النزاعات المسلحة الدولية في القانون الدولي الإنساني، وسيركز على تصنيف العمليات السيبرانية على أنها هجمات وإمكانية تطبيق القواعد الموضوعية التي تقيد سير الأعمال العدائية بموجب البروتوكول الإضافي الأول لاتفاقيات جنيف. وعلى وجه الخصوص، تهدف هذه الدراسة إلى بيان إلى أي مدى يتم تنظيم العمليات السيبرانية التي لا ترقى إلى مستوى الهجمات بموجب قواعد البروتوكول الإضافي الأول، فضلاً عن ذلك الآثار العملية لعدم تصنيفها كهجمات، ومن ثم يمكن تطبيق الطريقة التقليدية القانونية لتحديد كيفية تطبيق الإطار القانوني للقانون الدولي الإنساني على الحرب السيبرانية على المناطق المحمية.

إشكالية الدراسة:

يشكل الأمن السيبراني جزء من السياسات الوطنية في العالم، وذلك على اعتبار أنه يصنف كأولوية من أولويات الدفاع الوطني، إذ يمكن أن يتعرض الأمن الوطني والإقليمي والدولي بكافة أقسامه إلى الخطر، فيمكن أن يقع الأفراد والمؤسسات والأنظمة السياسية والعسكرية ضحايا للابتزاز والخطر الأمني ضمن مساحة الفضاء السيبراني، مما يستوجب التطلع على هذا الخطر على أنه حرب حقيقية مستحدثة، وبوسائل غير تقليدية، ويبدو أن التحدي الأكبر يتمثل في حدوث مثل هذه الحرب على المناطق المحمية، ومن الممكن أن تؤثر الهجمات السيبرانية على الجهود الدولية لحماية هذه المناطق وتقديم المساعدة الإنسانية للمتضررين. وعليه، فإن الإشكالية تتمثل في الإجابة على التساؤل الرئيسي وهو: الأثر الذي تتركه الهجمات السيبرانية على المناطق المحمية، بالنظر إلى أحكام القانون الإنساني الدولي، ويتفرع عن هذه الإشكالية العديد من الأسئلة الفرعية الآتية:

١. ما هو مفهوم الهجمات السيبرانية وخصائصها؟
٢. ما هو مفهوم المناطق المحمية وأنواعها؟
٣. هل هناك آليات فعالة وقانونية لمواجهة الحرب السيبرانية؟
٤. هل يمكن عد الهجمات السيبرانية أسلوب من أساليب القتال أو هي سلاح جديدة متطور؟
٥. هل هناك تنظيم قانوني ينظم هذه النزاعات؟

٦. هل يخضع مهاجمو المناطق المحمية سيبرانية إلى الجزاءات الدولية على اعتبارها جرائم دولية ضد الانسانية؟

٧. ما مدى إمكانية تطبيق القانون الدولي على الهجمات السيبرانية في المناطق المحمية؟

٨. هل بالإمكان تكيف الهجمات السيبرانية على وفق مبادئ القانون الدولي الإنساني، مثل مبدأ السيادة ومبدأ حظر استخدام القوة أو التهديد باستخدامها؟

فرضية الدراسة:

تفترض هذه الدراسة أن الهجمات السيبرانية، على الرغم من طبيعتها غير المادية، قد تحدث آثاراً مادية وإنسانية جسيمة على المناطق المحمية بموجب القانون الدولي الإنساني، الأمر الذي يوجب إخضاعها لأحكام الحماية الواردة في اتفاقيات جنيف الأربع وبروتوكولاتها الإضافية، أسوةً بالهجمات التقليدية، ولا سيما من حيث مبادئ التمييز والتناسب والضرورة العسكرية. كذلك تفترض الدراسة أن المناطق المحمية (مثل المستشفيات، ومراكز الإيواء، وشبكات المياه والكهرباء المخصصة للمدنيين) يمكن أن تكون عرضة لهجمات، كذلك تطرح سؤالاً: هل تُشكّل الهجمات السيبرانية التي تستهدف المناطق المحمية خرقاً لأحكام القانون الدولي الإنساني، بما يستدعي إخضاعها لنفس القواعد التي تنطبق على الهجمات العسكرية التقليدية، وبخاصة من حيث مبادئ التمييز والتناسب والاحتياطات الواجب اتخاذها.

نطاق الدراسة :

تقتصر هذه الدراسة على بحث الأثر القانوني للهجمات السيبرانية التي تُشن أثناء النزاعات المسلحة، حين تستهدف أو تؤثر على المناطق المحمية بموجب أحكام القانون الدولي الإنساني، كالمستشفيات، ومرافق الإيواء، والمنشآت المدنية الحيوية ذات الطابع الإنساني أو غير العسكري. ويغطي نطاق الدراسة تحليل مدى انطباق قواعد الحماية الواردة في اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين لعام ١٩٧٧، مع الاستناد إلى السوابق القضائية والمواقف الدولية الحديثة ذات الصلة، دون التوسع في أبعاد القانون الدولي العام أو قانون الأمن السيبراني الداخلي للدول، إلا بالقدر الذي يخدم فهم الوضع القانوني للمناطق المحمية ضمن النزاعات المسلحة ذات البعد السيبراني.

منهج الدراسة:

اعتمادنا المنهج الوصفي، وذلك من خلال شرح النصوص القانونية، التي تتعلق بالهجمات السيبرانية على المناطق المحمية، كذلك اعتمدنا على المنهج التحليلي من خلال تحليل النصوص القانونية التي تعنى بالهجمات السيبرانية في التشريعات الوطنية والدولية، وتحليل هذه النصوص والاتفاقيات الدولية التي تضمنها القانون الدولي الإنساني.

الدراسات السابقة:

تعد الدراسات السابقة لهذا الموضوع قليلاً نوعاً ما نظراً لحدثة المصطلح والاهتمام المتأخر به لا تأثير الهجمات السيبرانية على المناطق المحمية. وقد تنوعت هذه الدراسات من حيث المنهج والمجال، ويمكن تلخيص أبرزها على النحو الآتي:

1. Patrick Schubert (2022) "Protection of Civilian Data from Cyber Attacks in Armed Conflicts".

وقد ركزت على حماية البيانات المدنية كامتداد لحماية الأشخاص المدنيين بموجب اتفاقيات جنيف، وأكدت أن استهداف قواعد البيانات أو البنية التحتية الرقمية يمكن أن يُعد خرقاً لمبدأ التمييز في القانون الدولي الإنساني.

٢. رسالة منشورة عبر (DIVA Portal (2024) تناولت (أثر الهجمات السيبرانية على البنى التحتية المدنية)، مع تحليل واقعي لهجمات مثل Kyivstar ، وبيّنت تداخل الاستخدام المدني والعسكري لتلك المنشآت، ما يثير إشكاليات قانونية بشأن مشروعية استهدافها.

٣. رسالة ماجستير بجامعة ليدن بعنوان "The Principle of Proportionality in Military Cyber Operations"، درست تطبيق مبدأ التناسب في الهجمات السيبرانية، واقتрحت أدوات تقييم قانونية لمشروعية استهداف البنية المدنية الرقمية.

٤. رسالة دكتوراه بعنوان "Humanizing the Law of Cyber Targeting"، ناقشت إدخال مفهوم الكرامة الإنسانية كمعيار إضافي لضبط العمليات السيبرانية، خصوصاً تلك التي تمس بحقوق المدنيين في النزاعات المسلحة.

٥. رسالة من TalTech Institute حول مدى قابلية البروتوكولات الإضافية لاتفاقيات جنيف للتطبيق على الهجمات السيبرانية، واستعرضت حالات عملية مثل هجمات (2010) Stuxnet وهجمات إستونيا (٢٠٠٧) كنماذج أولية.

٧. رسالة ماجستير بجامعة القدس بعنوان "الحرب السيبرانية في القانون الدولي الإنساني"، خلصت إلى أن البيئة الرقمية لا تُخرج العمليات العدائية من نطاق القانون الدولي الإنساني، وإن كانت تفرض تحديات تفسيرية تستدعي تطوير أدوات قانونية ملائمة على الرغم من القيمة العلمية لهذه الدراسات، إلا أنها ركزت غالباً على الجانب العام للعمليات السيبرانية في أثناء النزاعات المسلحة، دون تخصيص الدراسة على المناطق المحمية بموجب اتفاقيات جنيف تحديداً، كما أنها لم تُفرد تحليلاً معمقاً لمسألة التكيف القانوني للهجوم السيبراني في ضوء المبادئ الأساسية للقانون الإنساني (كالتمييز، التناسب، الضرورة العسكرية). من هنا، تسعى هذه الأطروحة إلى سدّ هذا الفراغ البحثي عبر دراسة مركزة على الأثر القانوني للهجمات السيبرانية ضد المناطق المحمية، في ضوء نصوص القانون الدولي الإنساني وتطبيقاته العملية

هيكلية الدراسة:

قُسمت هذه الأطروحة إلى ثلاثة فصول رئيسية. تتأول الفصل الأول: مفهوم الهجمات السيبرانية، إذ استعرض تعريفها اللغوي والاصطلاحي ومفهوم المناطق المحمية، فضلاً عن ذلك الجهود الفقهية والدولية المبذولة لمواجهة مخاطر هذه الهجمات. أما الفصل الثاني: فقد خُصص لبحث حماية المناطق المحمية من الهجمات السيبرانية، وذلك من خلال دراسة المبادئ الدولية المنظمة لهذه المناطق في القانون الدولي الإنساني وتحديد إمكانية انطباقه على الهجمات السيبرانية، فضلاً عن استعراض آثار هذه الهجمات ودور القانون الدولي الإنساني في مواجهتها. وأخيراً، ناقش الفصل الثالث: المسؤولية الدولية الناشئة عن الهجمات السيبرانية على وفق القانون الدولي الإنساني، متتأولاً مفهوم المسؤولية وأركانها والتكيف القانوني لهذه الهجمات والتعويض عنها، فضلاً عن بحث الآلية الدولية لتعزيز الحماية للمناطق المحمية.

الفصل الأول

مفهوم الهجمات السيبرانية

إن تطور التكنولوجيا واستخدامهما سلباً كان له الأثر البالغ في ظهور نوع جديد من الأسلحة، لم يكن القانون الدولي الإنساني قد عرفها من قبل لحدثة ما يعرف بالهجمات السيبرانية، وقد ظهرت هذه الهجمات في الفضاء السيبراني، والتي كان لها الأثر البالغ في الاضرار بالبنى التحتية والاعيان.

وما يُميز الهجمات السيبرانية أنها غنية عن الاحتياج لموارد ومعدات كبيرة، إذ كل ما تتطلبه شخصاً يجد استخدامها ليحدث الضرر في الأجهزة المهاجمة. ومثلما الهجمات السيبرانية أصبحت ضرورية في استخدامها في الحروب صار من الضروري أن تتمتع كل دولة بالأمن السيبراني إذ إنه يتعلق بالحماية من مخاطر الهجمات المحتملة أو المتوقعة عن طريق مصادر خارجية من خلال الانترنت. فهو يمكن أن يكون حمايةً للحواشيب التابعة لمؤسسات الدولة وأجهزتها المدنية والعسكرية منها أو حتى الأفراد العاديين من أي نوع من الهجمات السيبرانية والاختراقات والتهديدات، التي تحدث عن طريق السيرفرات والحواشيب الأخرى وشبكة الإنترنت بشكل عام، ويعمل مختصو الأمن السيبراني في أجهزة الدولة وغيرها على ضمان عدم السماح للمهاجمين بالوصول إلى المعلومات العسكرية وغير العسكرية بحسب غاية المهاجم من هجومه السيبراني.

وتُعد الهجمات السيبرانية من أبرز التحديات، التي تواجه العالم اليوم، فهي تشكل تهديداً حقيقياً للأفراد والشركات والمؤسسات على حد سواء. ومع تطور التكنولوجيا، أصبحت هذه الهجمات أكثر تنوعاً وتعقيداً، مما يتطلب فهماً عميقاً لطبيعتها وآلياتها وتأثيراتها.

وسنبحث هذا الموضوع عبر مبحثين، سنتناول في المبحث الأول: تعريف الهجمات السيبرانية، وفي المبحث الثاني: الجهود الفقهية والدولية لمواجهة مخاطر الهجمات السيبرانية.

المبحث الأول

تعريف الهجمات السيبرانية

لقد شهد العالم أجيالاً مختلفة من النزاعات، جيل الواحد خصوصيته، التي امتاز بها على غيره من أجيال النزاعات الأخرى من حيث اختلاف وتنوع الأسلحة، التي تستخدم في أثناء النزاع، ومن حيث طبيعة الخطة والتكتيك والاستراتيجيات وساحات المعارك، وغيرها، ابتداءً من الجيل الأول، الذي كان التقليد الأقدم في تجيش الجيوش، واستخدام الأسلحة البدائية، وحتى الجيل الثاني، الذي غذى نزاعاته المسلحة بالقوة النارية، كذلك من خلال جمع أكبر عدد من المقاتلين الجنود واستخدام المدرعات والأسلحة الآلية. ثم جاء الجيل الثالث خلال الحروب الحرب العالمية الثانية (١٩٣٩-١٩٤٥)، الذي امتاز بتطور مدرعاته، واعتماده الكبير بالتطور الكبير القوة الجوية والحركة السريعة المباغتة. أما الجيل الرابع من أجيال النزاعات المسلحة، فقد اختلف عن سابقه من أجيال النزاعات المسلحة إذ اعتمد في نزاعاته على تأجيج الفتن وتشجيع الناس على الحرب الأهلية، ودعم التمردات الداخلية، بمعنى: إن سلاحه اختراق الخصم من الداخل، إذ يجعله يضرب نفسه بنفسه. أما الجيل الخامس، فقد كان الجامع بين أسلوب الحرب، الأسلوب التقليدي، الذي أدواته الآلة المادية والبشر، والأسلوب الحديث، الذي أدواته لا مادية، إذ تُستخدم من خلال أوامر، يرسلها أناس وراء الحاسب الآلي، وعبر الشبكة العنكبوتية، مثل ما يعرف اليوم بالهجمات السيبرانية. وإن الهجمات السيبرانية هذه قد تحولت بشكل ملحوظ إلى عينة جديدة عن النزاعات الحديثة، فقد استُخدمت في كثير من النزاعات، وعادة، تسبق الهجمات السيبرانية الهجوم العسكري التقليدي، أو ترافقه أحياناً. وقد استُخدمت الهجمات السيبرانية في نزاعاتٍ مسلحةٍ دوليةٍ مختلفة، وسنبين في هذا المبحث تعريف الهجمات السيبرانية من خلال مطلبين إذ سنبين في المطلب الأول التعريف اللغوي والاصطلاحي للهجمات السيبرانية، وفي المطلب الثاني مفهوم المناطق المحمية.

المطلب الأول

التعريف اللغوي والاصطلاحي للهجمات السيبرانية

بعد ما لجأ العالم في سنواته الماضية لاستخدام الأسلحة الحديثة غير التقليدية، مستغلاً العلم متكاملاً على التطور التكنولوجي، و بعد أن طورَ برامجاً إلكترونية ذكية بغية استخدامها عسكرياً، وقد وقع ما سعى إليه إذا إنه استطاع الوصل، لأن يعسكر البرامج التقنية لاستخدامها لأغراض عسكرية تُستخدم في فضاء إلكتروني عُرف اصطلاحاً فيما بعد بفضاء السايبر، أو الفضاء السيبراني، وقد تميز هذا الفضاء

بأنه قد يستخدم الإلكترونيات لتخزين المعلومات أو تعديلها. وقد يمنح هذا الفضاء الدولة التي تلجأ إلى استخدامه خصائصاً مهمة، ولا سيما إذا ما استخدم في الحروب، كذلك يمنح الأفراد المهاجمين ما يمنحه للدولة إذ إن غايته إيقاع الضرر وتحقيق الانتصارات عبر تعطيل واختراق أجهزة الحواسيب المراد مهاجمتها من قبل المهاجم إن كان دولة أو فرد بسرعة قصوى توجه نحو أشخاص أو دول خارج الحدود، وللغموض الذي يشوب أو يحيط الهجمات السيبرانية واجه فقهاء القانون الدولي الإنساني صعوبات جمة لحصرها بتعريف جامع مانع، ويرجع ذلك لحدثة الهجمات السيبرانية ولقدّم القانون الدولي الإنساني الذي سبق ظهور الهجمات السيبرانية. وإن الهجوم السيبراني هو محاولة متعمدة تقوم بها فرد أو منظمة لاختراق نظام المعلومات الخاص بفرد آخر أو مؤسسة لغرض الحصول على مكاسب أو تعطيل الشبكة. لذا تُعد الهجمات السيبرانية أخطر ما يواجهه الجيش العسكري، إذ تتخطى فاعليتها المجالات العسكرية لتشمل بإضرارها البنى التحتية الحيوية وتلحق أضراراً كبيرة إذا ما استهدفت القطاعات الاقتصادية والمالية و يمكن أن توجه نحو المجتمع أو تستخدم لأغراض سياسية بغية زعزعة المجتمع من الداخل^(١).

سنبحث هذا الموضوع عبر فرعين، سنتناول في الفرع الأول التعريف بالهجمات السيبرانية لغة واصطلاحاً، وفي الفرع الثاني نتناول أنواع الهجمات السيبرانية.

الفرع الأول

التعريف بالهجمات السيبرانية لغة واصطلاحاً

لأهمية التعرف على الهجمات السيبرانية، لابد من تعريفها لغة واصطلاحاً.

أولاً: التأصيل اللغوي للهجمات السيبرانية.

عند العودة إلى المعاجم اللغوية بحثاً عن مصدر كلمة سايبير "cyber" يتبين أنها يونانية الجذر أو الأصل إذ ترجع إلى المصطلح "kybernetes"، الذي ورد -أول مرة- في مؤلفات الخيال العلمي، الذي يعني: القيادة والتحكم عن بُعد. وأن السباق إلى هذه التسمية هو العالم في الرياضيات نوربرت وينر

١ سفاح كريم، الحروب الإلكترونية وأثرها على الأمن القومي، متاح على الرابط:

<https://www.alnahrain.iq/post/1031> آخر زيارة بتاريخ ٢٠٢٣/٥/٢

"Norbert Weiner" عندما شرع بدراسة القيادة والسيطرة والاتصال في عالم الخاص بالحيوان، فضلاً عن حقل الهندسة الميكانيكية^(١). وبالعودة إلى القواميس اللغوية فقد كادت أن تخلو من الإشارة إلى كلمة سايبير "cyber" لو لا ما أورده قاموس "المورد" من تعريف لها إذ عرفها بالقول: "السيبرانية هي علم الضبط" ومصدرها "kybernetes" وقد يتوافق هذا التعريف مع مفهوم الهجمات السيبرانية، أي: إنها ضبط الأشياء عن بعد والتحكم فيها. كذلك تعني علم التحكم الأتوماتيكي، مثلما تعني علم الضبط، وتعني أيضاً القيادة والتوجه فهو علم الاتصالات وانظمة التحكم الآلي في كل من الآلات والأشياء الحية، كذلك وردت بمعنى "كمبيوتر" و"عصري أو حديث جداً"^(٢). ولم تتوصل التعريفات العربية إلى مصطلح واضح يُعرف الهجمات السيبرانية ما خلا التي اقتصر على الاصطلاحات الواردة في القواميس الأجنبية. أما قاموس مصطلحات الأمن المعلوماتي فعرّفها: "هجوم من عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنية محمية الكترونياً لتعطيلها أو تدميرها والسيطرة عليها"^(٣). وإن غالبية المعاجم التي اختصت في المصطلحات العسكرية لم تذهب بتعريفها بكلمة سايبير إلى جذرها الأساس بل أوضحت في نطاق استخدامها العسكري -على سبيل المثال- عرفها قاموس المصطلحات العسكرية الأمريكية: الفعل الذي يستخدم عبر الشبكات الالكترونية بغية السيطرة أو تعطيل برامج الكترونية أخرى. وقد واجه المختصون العرب صعوبات كبيرة في اختيار مصطلحات عربية تقترب من مصطلح (cyber) بالإنكليزية، مثلما حدث مع الترجمة العربية لعنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية إذ لم تكن الترجمة صحيحة فقد تُرجم العنوان (Convention on Cybercrime) على أنه (الاتفاقية المتعلقة بالجريمة الإلكترونية)، وقد يكون السبب من هذه الترجمة هو غياب مصطلح يقابلها بالعربية^(٤).

١ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط ١، مكتبة زين الحقوقية والأدبية، لبنان، بيروت، ٢٠١٨، ص ١١.

٢ منير البعلبكي، المورد الحديث: قاموس إنكليزي-عربي، دار العلم للملايين، ط ٣، بيروت، ٢٠١٣، ص ٣٠٧.

٣ أحمد عبيس نعمة الفتلاوي، المصدر السابق، ص ١٢.

٤ مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوروبية رقم ١٨٥ بودابست، عام ٢٠٠٠.

ثانياً: التعريف الاصطلاحي للهجمات السيبرانية.

هي أنشطة الإلكترونية توجه من شخص أو جماعات تابعة إلى دولة ما، أو يعملون لصالحها، وباستقلال عنها، بالضد من أنظمة إلكترونية عائدة إلى دولة أخرى، غايتها الوصول إلى تلك الأنظمة بغية اختراقها أو السيطرة عليها، لتتحكم عن بعد بها، بغرض تحقيق الضرر الأكبر عند الطرف المهاجم. وقد عرف دليل تالين، الذي أُعدّ من قبل مجموعة خبراء في القانون الدولي الإنساني، الذي طُبّق على الحرب السيبرانية في العام ٢٠١٣، وقد كان "مايكل شيمت" أبرز الخبراء الذين أسهموا في اعدادها، وقد تعاون على اعداد مع "حلف شمال الأطلسي"، وبمساندة مجموعة تتألف من خبراء سيبرانيين، و"اللجنة الدولية للصليب الأحمر" و"القيادة السيبرانية الأميركية"، عرّف الهجمات السيبرانية بأنها: «عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، التي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان الأهداف». وعلى وفق تعريف الدليل في أعلاه، فقد رأى كثير من خبراء القانون الدولي الإنساني: إن توقف أحد الأعيان عن عملها الطبيعي، يعني: إن الضرر قد وقع وتحقق فعلاً، زيادة على تحقق ضرر مادي، ولا ضرورة من معرفة كيف الأمر قد حدث. و عرّف شيمت الهجمات السيبرانية: إنها «مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة» واختار بعض المختصين مصطلح الهجمات السيبرانية "cyber attack" بدلاً من الحرب السيبرانية كوصف واقعي، إذ إنه تصرف ويجول في عالم افتراضي منطلقاً من استخدام البيانات الرقمية وسائل اتصال تعمل إلكترونياً، ومن ثم تطور ليشمل مفهوماً أوسع قائماً على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة من خلال اختراق مواقع إلكترونية حساسة عادة ما يقوم بوظائف تصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى.

وبناءً على ما تقدم من تعريفات مسبقة، فهناك مقاييس عديدة اجتمعت لتشكّل نواة معيار الضرر:

- ١- أن يكون الضرر واسعاً في نطاقه.
- ٢- أن تكون ذات أمدٍ طويل، أي: أن تكون آثارها مستغرقة مدة زمنية.^(١)

١ حسن فياض، الهجمات السيبرانية في منظور القانون الدولي الإنساني، مجلة الدفاع الوطني اللبناني، عدد ١٢٤، بيروت، لبنان، ٢٠٢٠، ص ٨-١٠.

٣- أن تكون ذات هدف معين، أي: أن عملية استخدام سلاح أو وسيلة كهذه بقصد أن تكون واسعة النطاق وطويلة الأمد.

واستحوذت الهجمات السيبرانية على مفاهيم ودلالات عديدة فمن الفقهاء من اصطلح عليها "الحرب الافتراضية" و"الحرب الإلكترونية" ومنهم من اصطلح عليها "بالحرب المعلوماتية" ومنهم كذلك من فضل أن يصطلح عليها "الهجمات السيبرانية"، ويذهب الباحث مع الرأي الأخير أيضاً. ويمكن عدّ ما أورده مجموعة من فقهاء الناتو بالاستناد إلى المادة (٣٠) من دليل تالين إذ نصت الحرب السيبرانية على شمول: " كل العمليات السيبرانية سواء كانت دفاعية أو هجومية التي يعتقد أنها قد سببت إصابات أو وفيات للبشر، أو أضرار للأشياء المادية ". وينبغي التمييز بين هجمة سيبرانية في سياق نزاع مسلحة بوصفها عدوانية تلتفت أنظار القانون الدولي الإنساني، ويمكن أن تُكَيّف قواعده عليه، و بين هجمة سيبرانية أخرى بذات الفعل والتأثير تشنها جماعات أو أفراد خارجين عن القانون إذ لا يمكن أن ينطبق عليها مصطلح الحرب السيبرانية لأن الحرب السيبرانية تعني الهجمات السيبرانية في سياق النزاعات المسلحة. وقد وجد بعض الفقهاء تعريفاً للهجمات السيبرانية مبسطاً إذ اعتبروها الأعمال العدائية، التي تشنها دولة ما ضد معطيات الدولة الإلكترونية المُخزّنة أو المُعالجة أو المرسل من حاسوب لآخر بقصد سرقتها أو اتلافها وحتى تعديلها ونسخها.^(١) وعرفت الهجمات السيبرانية بأنها هجمة إلكترونية معلوماتية حديثة ومتطورة توجهها دولة عبر الشبكات العنكبوتية تجاه دولة أخرى معتديةً عليها بغية أن تسيطر على شبكات ومحتوى الكمبيوتر التابع لمرفق عسكري أو حيوي للدولة المُستهدفة فقد يؤدي الهجوم إلى تحكم وسيطرة الدولة المهاجمة على أجهزة الدولة الخصم أو الدولة المستهدفة والتشويش عليها. وقد يسبق الهجوم السيبراني الهجوم العسكري التقليدي أو يرافقه أحياناً، وتجري أحياناً أخرى بشكل منفصل، إذ يُشن الهجوم بغية دون علم الدول المُستهدفة أو الخصم^(٢) ويمكن تعريف الهجمات السيبرانية تعريفاً لفقهاء وقانونياً وقضائياً.

١ درويش سعيد، الحرب السيبرانية وأثرها على حقوق الإنسان: دراسة في ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤، عدد ٥، الجزائر، ٢٠١٧، ص ١٨٢.

٢ صابر محمد محمود المزعل و ياسمين محمد حسن يونس، القانون الدولي والنزاعات المسلحة، المجلة الدولية لنشر البحوث والدراسات، المجلد ٦ العدد ٦٢، ٢٠٢٤، عمان، الأردن، ص ٣٨ - ٣٩.

التعريف الفقهي للهجمات السيبرانية

كل سلوك عدائي يتم عبر الفضاء الرقمي، يُستخدم فيه نظام معلوماتي أو شبكة حاسوبية كوسيلة أو كهدف، ويهدف إلى تعطيل أو إتلاف أو تقييد أو التأثير في بنية تحتية أو وظيفة حيوية لدولة أو جهة محمية، سواء أثناء السلم أو زمن النزاعات، متى ما ترتب عليه أثر قانوني يُوجب المسؤولية الدولية^(١). ويستند هذا التعريف إلى اتجاهات فقهاء القانون الدولي الإنساني الذين يرون أن الفضاء السيبراني لا يخرج عن نطاق أعمال القوة إذا ترتب عليه أثر مادي أو إنساني جسيم.

التعريف القانوني:

من الزاوية القانونية، يمكن تعريف الهجمات السيبرانية بأنها: أي عمل أو سلسلة أعمال تتم باستخدام أدوات تكنولوجية عبر الفضاء السيبراني، تستهدف معلومات أو أنظمة رقمية بطريقة غير مشروعة أو غير مبررة دوليًا، تؤدي إلى تهديد أو إضرار بأمن الدولة أو الأفراد، أو تعيق تقديم الخدمات الأساسية، وتعدّ مخالفة للقواعد العامة للقانون الدولي، وبخاصة مبدأ عدم استخدام القوة ومبدأ التمييز في النزاعات المسلحة^(٢). يُستمد هذا التعريف من الممارسة الدولية وتكييفات لجنة القانون الدولي التي تنظر للهجوم السيبراني ضمن أعمال القوة الخاضعة للضبط بموجب ميثاق الأمم المتحدة

التعريف القضائي

في السياق القضائي، لا يوجد تعريف صريح ملزم للهجمات السيبرانية في السوابق الدولية، لكن يُمكن استخلاص تعريف عملي استنادًا إلى أحكام وتدابير محكمة العدل الدولية:

“الهجوم السيبراني هو كل فعل تقوم به دولة أو جهة فاعلة غير حكومية عبر وسيط إلكتروني يستهدف المساس بالبنية المدنية أو الوظيفة الحيوية المحمية دوليًا، ويحدث أثرًا قابلاً للتقويم وفق قواعد القانون

1 Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), Rule 9

٢ اللجنة القانونية الدولية، تقرير عن أعمال دورتها الثانية والسبعين، وثيقة الأمم المتحدة (A/75/10 (2021)، الصفحات ١٨٧-١٩٠. International Law Commission (ILC), Report on the Work of Its Seventy-

Second Session, UN Doc A/75/10 (2021), pp. 187-190

متاح على الرابط: <https://legal.un.org/ilc/reports/2021>

الدولي، ويُنظر إليه كعمل عدائي عندما يخرق الالتزامات الدولية المستقرة، كما في المادة ٤/٢ من ميثاق الأمم المتحدة أو اتفاقيات جنيف^(١).

وقد استخدمت محكمة العدل الدولية، ضمن أوامرها المؤقتة في قضية أوكرانيا ضد روسيا، توصيفات لعمليات رقمية تهدد البنية التحتية المدنية، واعتبرتها خاضعة لمعيار الحماية من "أعمال عدائية غير مشروعة

يعرف الباحث الهجمات السيبرانية بأنها: أنشطة عدائية مُنظمة تُمارس عبر الفضاء الإلكتروني، تستهدف الأنظمة التقنية وشبكات المعلومات، والبنى التحتية الرقمية للدول أو المؤسسات أو الأفراد، باستخدام وسائل تكنولوجية تهدف إلى التدمير أو التعطيل أو التجسس أو التأثير النفسي والمعلوماتي. فمن البعد العسكري، فإن الهجمات السيبرانية تُعد أحد أشكال الحروب غير التقليدية، إذ تُستخدم لتحقيق أهداف استراتيجية دون اشتباك مادي مباشر، وغالباً ما تكون جزءاً من عمليات عسكرية هجينة تهدف إلى إضعاف الخصم أو شل قدراته الدفاعية والاقتصادية. ومن ناحية البعد القانوني، تطرح الهجمات السيبرانية تحدياً للقواعد التقليدية للقانون الدولي، ولا سيما فيما يتعلق بمبدأ السيادة، وعدم التدخل، واستخدام القوة، وتثير أسئلة حول تطبيق قواعد القانون الدولي الإنساني، لا سيما ما يتعلق بحماية المدنيين والبنية التحتية الحيوية. أما من ناحية البعد الإنساني، فالهجمات السيبرانية قد تؤثر بشكل مباشر أو غير مباشر على حقوق الإنسان الأساسية، مثل الحق في الحياة، والخصوصية، وحرية التعبير، بل وقد تؤدي إلى حرمان السكان من خدمات أساسية مثل الكهرباء والمياه والصحة، ما يجعل لها أثراً إنسانياً تتجاوز البعد التقني الصرف.

ويرى الباحث: إن الهجمات السيبرانية هي محاولات غير مصرح بها لاختراق أنظمة الحاسوب، الشبكات، الأجهزة الذكية، أو البنية التحتية لتكنولوجيا المعلومات بهدف الحصول على معلومات سرية، تعطيل الخدمات، أو التسبب في أضرار مادية أو معنوية. تتنوع هذه الهجمات في طرقها وأهدافها، وقد تشمل اختراق الأنظمة، وانتشار البرمجيات الخبيثة (مثل الفيروسات، والديدان، وبرامج التجسس)، والاحتيايل الإلكتروني، والهجمات الموجهة للخدمات (مثل هجمات DDoS التي تستهدف تعطيل خدمات الشبكة عن طريق إرسال كميات هائلة من الطلبات)، والتصيد الاحتيالي (Phishing)، والتصيد بواسطة الترويج لملفات ضارة (Malware)، والهجمات الهجينة، التي تجمع بين عدة تقنيات مختلفة. تُعد الهجمات

1 on Provisional Measures, Ukraine v. Russian Federation, ICJ Reports 2022, para. 86c .

: متاح عبر الرابط <https://www.icj-cij.org/case/182>

السيبرانية تهديدًا خطيرًا على الأمن الإلكتروني للأفراد، والشركات، والمؤسسات، والحكومات، وتستدعي تبني استراتيجيات دفاعية فعالة وتحسين التوعية الأمنية للمستخدمين.

الفرع الثاني

أقسام وأنواع الهجمات السيبرانية

بعد أن تعدد أبعاد النظام الدولي واتسع مدى تأثيره مما زاد من تعقيد ظاهرة الهجمات السيبرانية التي قد تحاط بصعوبات كثيرة وتحديات ترتبط بإلزامية التي تُستخدم فيها القوة بشكلها المرن في فضاء ألكتروني ضمن الإطار القانوني، الذي تعامل مع القوة الصلبة ضمن العلاقات الدولية وما ورد في "ميثاق الأمم المتحدة" في المادة (٢) الفقرة (٤)، التي قضت أن يتمتع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة.. الخ وتنقسم الهجمات السيبرانية إلى عدة أنواع :

• أقسام الهجمات السيبرانية

أولاً: حرب المعلومات الشخصية (التجسس الإلكتروني):

التجسس الإلكتروني "cyber espionage" هو عملية قرصنة وسرقة معلومات محفوظة في جهاز إلكتروني عبر اختراقه أو حتى من خلال اختراق الشبكة، وغالباً ما تكون المعلومات المستهدفة بالغة الأهمية سواء أكانت معلومات عسكرية، أم أمنية، أم صناعية، أم تجارية أم غير ذلك، و يخلف آثار استراتيجية كبيرة في الخصم المستهدف. يتخطى هذا النوع الخصوصية الإلكترونية الفردية؛ وهذا ما يعد تعدياً على الحقوق الشخصية للإنسان واعتداءً على حرمة الحياة الخاصة، ومنها التسلل إلى البيانات المالية فسرقتها ثم نشرها وافشائها عبر الشبكة العنكبوتية، أو أن يقوم شخص ما بإنشاء ملف عبر الحاسوب، يضم معلومات شخص آخر دون علمه أو دون أن يأذن له بتكوين الملف، أو العبث بسجلات رقمية وتغيير مدخلاتها المخزنة في قواعد البيانات. وبما أن هذه الهجمات قادرة على تحقيق أضراراً كبيرة في وقت قياسي معين صارت كثير من الدول تلجأ إلى استخدامها إما في الأوقات تشدد فيها الخلافات أو النزاعات السياسية بين دولة وأخرى وإما وقت الحرب متزامنة مع العمليات العسكرية التقليدية. ومن الأمثلة على التجسس الإلكتروني، الذي تتجسسه دولة ضد أخرى ما قامت به أمريكا في العام (٢٠٠١) إذ اتهمتها لجنة التحقيقات -على وفق تقريرها- التي شكلها البرلمان الأوروبي باستخدامها لشبكة التجسس الإلكترونية المسماة (echelon network)، التي اتُهمت بسرقة المعلومات الصناعية الخاصة بالصناعات الأوروبية. ولمناسبة القول إن الدول لم تكن وحدها المستهدفة من قبل الهجمات السيبرانية بل حتى الشركات التجارية و الشركات الاعلانية والمنظمات غير الحكومية، التي صارت تتعرض أيضاً للكثير من عمليات التجسس الإلكتروني^(١).

١ طلال ياسين العيسى، عدي محمد عدنان، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد ١٩، العدد الأول، عمان، ٢٠١٩، ص ٨٥.

ثانياً: حرب المعلومات بين الشركات والمؤسسات.

يدخل هذا النوع من الهجمات السيبرانية ضمن سباق بين شركة و أخرى أو شركة وشركات أخرى غايته الأساسية تعطيل الشركة المنافس وتهديد واخللت أسواقه، إذ تقوم شركة ما منافسة لشركة أخرى باختراق نظام الشركة المنافسة المعلوماتي لتسرق ما توصلت إليه من نتائج وتفاصيل أبحاث أعدتها، أو تدمير بياناتها، أو محوها وإضافة محلها بيانات غير صحيحة^(١).

ثالثاً: حرب المعلومات العالمية (الحرب السيبرانية).

إن الحرب السيبرانية أو الإلكترونية هي التي تستخدم ضمن فضاء الكتروني يستخدم فيها الآلة و السلاح الإلكتروني عند ما يُشن هجوم، فيوجه الهجوم السيبراني أساساً إلى أجهزة الكمبيوتر أو الحاسوب الآلي خاصة العدو أو أنظمتها وبرامجه الإلكترونية، التي تُعد المحرك الرئيس للدولة الكترونياً والتي دائماً ما تكون محتوية على معلومات بغرض حرمان الخصم المستهدف استخدام انظمتها وأجهزته وشبكاته الإلكترونية أو حتى تدميرها وتحطيمها كاملة. وإن المستوى هذا من الحروب يحدث أو يقوم عادة بين بعض الدول أو ما قد تبدأه قوة عالمية اقتصادية على دول معينة لمعرفة وسرقة أسرار الخصم المستهدف إذا توجه المعلومات المسروقة عكسياً مضاداً لمصالحهم إذ إن من يمتلك التكنولوجيا من الدول غالباً يتفوق في المعركة أيضاً وذلك عبر استخبارات فعالة ونوعية وقدرة هجومية عالية خاطفة، وقدرة دفاعية تمكنها من الدفاع عن البنى التحتية الحيوية زيادة على ذلك قدرتها العالية على السيطرة والتحكم وما إلى ذلك. وأسهم التطور في مجال التكنولوجيا المعلوماتية خاصة الحاسوب ووسائل الاتصالات والشبكات العنكبوتية والإلكترونية في إمكانية استهداف الخصم إن كان من الأفراد أو الدول أو المؤسسات عبر استخدام أساليب جديدة توازي طبيعة التطور، ويمكن أن تكون الحرب السيبرانية على ثلاثة مستويات:

١- المستوى الأول ينسحب على العمليات التي تصاحب الحرب التقليدية، وهو ما يحقق التفوق في المعركة، مثل مهاجمة نظام الدفاع الجوي التابع للدولة الخصم، الذي يخلفه استهدافه خسائر استراتيجية كبيرة، وذلك لما للدفاع الجوي من أهمية كبيرة لدى الدول.

٢- المستوى الثاني يكون هذا المستوى في الحرب الإلكترونية أو السيبرانية المحدودة، فقد يقصد الهجوم السيبراني في هذا المستوى البنى التحتية وحتى الأهداف المدنية.

٣- المستوى الثالث، وهذا المستوى هو أيضاً من الحروب الإلكترونية أو السيبرانية غير المحدودة

إذ يبتغي المهاجم من خلالها تعظيم الدمار للبنى التحتية، مما يؤثر سلباً في البنية الاجتماعية للدولة مثل الهجوم الذي يُشن على دولة قاصداً أسواق رأس المال وخدمة الطوارئ والتنظيم الإلكتروني التابعة لمولدات الطاقة وغير ذلك من الأهداف التي ترتب عليها آثار تدميرية ذات نطاق واسع وأن الهدف من هذا النوع في هذه الحروب هو توسيع نطاق الخسائر المادية بالقدر الممكن. لذا فالهجمات السيبرانية تستهدف معلومات أو نظم معينة محددة تفيد الطرف المهاجم زيادةً لقيمة المعلومات أو أنظمتها بالنسبة للمهاجمين لتقليل وتقليص قيمتها بالنسبة للمهاجم المدافع أو بهما معاً. وذلك لأن قيمة المعلومات ونظامها هو المعيار لمقدار استحواذ المهاجم أو المدافع للمعلومات ونظامها على أن تشكل ضمن أهدافه المادية الهدف الذي يرتجي المهاجم تحقيقه عند شنه للهجمات كأن يكون سرقة وبيع سجلات لحسابات مصرفية أو حتى لمجرد الاثارة وإظهار القدرات مثلما في سرقة المعلومات^(١).

أنواع الهجمات السيبرانية

أولاً: هجوم الحرمان من الخدمة.

ويفهم هذا الهجوم من اسمه، غايته منع المستخدمين من الخدمة والتأثير عليها، ويطلق على أخطر أنواعه اسم (DDOS Distributed Denial of service) إذ إن المهاجم يستخدم في هجومه مجموعة من أجهزة الحاسوب لأفراد مجهولين إلا أنه استغل بعض الثغرات في أجهزتهم في أماكن مختلفة فيقوم باستهداف سيرفر محدد أو شبكة ما من خلال استخدام هذه الأجهزة دون أن يعلم أصحابها^(٢).

ثانياً: الفيروسات (البرامج الخبيثة).

الفايروس (virus) برنامج كأحد البرنامج التطبيقية، يصمم مخرب ما؛ لإضرار النظام بشكل كبير بعد ربطه بالبرامج الأخرى ويمتلك القدرة على تكرار نفسه ليبدو، وكأنه يتوالد تلقائياً، وهذا ما يجعله قادراً على استهداف البرامج الأخرى في الكمبيوتر ومواقع أخرى في ذاكرة الكمبيوتر لغرض تدميرها^(٣)، والفايروسات و حددها التقرير الصادر عن المركز القومي للحاسبات في الولايات المتحدة الأمريكية، هي برامج تهاجم وتصيب أنظمة الكمبيوتر بأسلوب مماثل إلى حد كبير الفايروسات الحيوية، التي تصيب البشر، والفضل يعود أولاً، في وضع فكرة لفايروس معلوماتي إلى الدكتور فريد كوهن في حلقة الدراسية

١ طلال ياسين العيسى، عدي محمد عدنان، مصدر سابق، ص ٨٥-٨٦.

٢ نور امير الموصل، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير، الجامعة الافتراضية السورية، سوريا، ٢٠٢١، ص ١٦.

٣ المصدر نفسه، ص ١٧.

الملقاء في جامعة كاليفورنيا، في أمريكا، عن أمن الحاسوب الآلي عام ١٩٨٣. و أبرز صفات الفايروسات بشكل عام هي قدرتها على الاختفاء، الانتشار، الاختراق والتدمير^(١).

ثالثاً: القنابل المعلوماتية.

القنبلة المعلوماتية معروفة باسم "الشفرة الموقوتة"، وهي نوع خبيث من البرامج صغيرة الحجم تُدخل بطرائق غير مشروعة وتُخفى مع برامج أخرى، وهذه البرامج شكلياً ليست ملفاً متكاملًا بل هي شفرة توضع بين مجموعة من الملفات لغرض تقسيمها على أجزاء متعددة هنا، وهناك حتى لا يمكن معرفتها بحيث تتجمع فيما بينها على وفق الأمر المعطى لها ضمن زمان ومكان معينين أو حين تحدث واقعة معينة، لذا لا يمكن اكتشافها لمدة طويلة، وهذه البرامج تُستخدم لغاية تدمير المعلومات والبيانات وتغيير برامج ومعلومات النظام، زيادةً على ذلك أن هدفها حماية بعض برامج الملكية من القرصنة. ويتجلى ظهورها في الحملات الإعلانية و هو الحال في بعض المجالات، التي يوزع معها أقراص هدية تحتوي على بعض البرامج، فضلاً عن ذلك وجود هذه البرامج الخبيثة في مواقع الانترنت المتضمنة البرامج هذه، ويمكن إظهار بعض البرامج المؤجرة مع الاحتفاظ بحقوق الملكية للمالك الأصلي، ففي مثل هذه الحالات حين لا يدفع المستأجر القيمة الإيجارية المحددة مسبقاً يُعد إخلالاً بالعقد المبرم بينهما، وهذا ما يحفز المالك على إرسال قنبلة موقوتة أو قد تكون القنبلة أساساً في البرنامج المستأجر موجودة، وحينها المالك لا يرسل ما يمنع انفجارها^(٢).

رابعاً: برامج الدودة.

هي برامج تستفيد من الثغرات الموجودة في نظام تشغيل الحاسب لغرض الانتقال من حاسب إلى آخر، مما يقود إلى اختراق الشبكة بالكامل والتسبب أخيراً بآثار محطمة، وبفضل الوصلات، التي تقوم بترابط الشبكات بعضاً ببعض، ما يسمح لهم بالانتقال من شبكة إلى ثانية اذ يتكاثرون كالبكتيريا في عمليات النقل، ومن غايات تلك البرامج الفايروسية أن تشغل قدرًا أكبر من سعة الشبكة مما يؤدي إلى تقليص أو خفض قدرتها ، وقد تتخطى غاياتها لتتكاثر وتنتشر بادئةً بالتخريب الفعلي للملفات والبرامج وأنظمة التشغيل وبروتوكولات الاتصال. وقد تكون أكثر الوسائل وضوحاً لبث وإرسال هذه الديدان هي مرفقات البريد الالكتروني التي أصابها الفيروس وكذلك التنزيلات التلقائية عند الدخول لمواقع انترنت

١ عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، ط١، منشورات زين الحقوقية، لبنان،

٢٠١٧، ص١٤٠-١٤١.

٢ عمار عباس الحسيني، مصدر سابق، ص١٤٣-١٤٤.

معينة والتسلل عبر ثغرة أمنية في نظام تشغيل ما أو برنامج حماية، ومن جهة أخرى تظهر أضرار هذه الديدان في إتاحتها للمهاجم استخدام الحاسب المصاب لمهاجمة مواقع في الشبكة العنكبوتية أو إرسال بريد إلكتروني أو تحميل برامج غير آمنة إليه^(١).

وأن الهجمات السيبرانية متعددة الأنواع وأنها متجددة ولا تقتصر على نوع واحد، ويبدو أن المستقبل ستظهر أنواع أخرى أكثر تطوراً وخطورة، لذا ينبغي تدارك الأمر للحد منها^(٢).

يرى الباحث: أن خطورة الهجمات السيبرانية لا تكمن في تنوعها وأساليبها المتطورة فحسب، بل في تجاوزها للحدود الجغرافية والقانونية التقليدية، بما يجعل التصدي لها يتطلب نهجاً تكاملياً يشمل البعد التقني والقانوني والسياسي. وأن اعتماد الدول المتزايد على الفضاء السيبراني في إدارة شؤونها الحيوية جعل من هذه الهجمات أداة فاعلة في الصراعات الدولية، الأمر الذي يستدعي تطوير قواعد القانون الدولي لتواكب هذه التهديدات، وتعزيز التعاون الدولي لرصدها ومنعها والحد من آثارها وأن الهجمات السيبرانية تمثل تحولاً نوعياً في مفاهيم الصراع والأمن، إذ لم تعد المواجهات محصورة في الميدان العسكري التقليدي، بل أصبحت تُخاض عبر لوحات المفاتيح والخوارزميات. وتكمن خطورتها في قدرتها على تحقيق تأثير استراتيجي كبير دون إراقة دماء أو تحريك جيوش. ومن ثم فقد أصبحت الحاجة ملحة لتطوير منظومة قانونية دولية متخصصة تنظم هذا النوع من الهجمات، وتحدد المسؤولية القانونية، إلى جانب تعزيز قدرات الدفاع السيبراني الوطني، ولا سيما في الدول النامية، التي غالباً ما تكون هدفاً سهلاً في هذا النوع من الحروب غير المتكافئة.

المطلب الثاني

مفهوم المناطق المحمية

على الرغم من أن القانون الدولي المعاصر يحرم استعمال القوة، بل يحرم حتى التهديد بما بها في العلاقات الدولية، ووضعها خارج دائرة القانون والشرعية الدولية، فإن الحرب لا تزال حقيقة واقعية من حقائق الحياة وظاهرة اجتماعية وإنسانية صاحبت الإنسان منذ ظهوره على وجه الأرض، ولما كان القانون الإنساني يرمي إلى حماية الأشخاص والأعيان غير المشاركة في العمليات العسكرية، فإن إحدى وسائل توفير هذه الحماية هي إنشاء أماكن للحماية في أثناء النزاعات المسلحة التي لا تمتد

١ عمار عباس الحسيني، مصدر سابق، ص ١٤٥-١٤٦.

٢ نور امير الموصلي، مصدر سابق، ص ١٨.

إليها السنة النيران ولا العمليات العسكرية من قبل الأطراف المتنازعة، لتوفير الحماية والاحترام للفئات المتضررة من الأشخاص والأعيان ذات الطابع المدني، وعليه فإن هذه الدراسة سعت إلى التعريف بالمناطق المحمية في ضوء قواعد القانون الدولي الإنساني، إبراز مكانتها، وبيان وتحديد المبررات القانونية لإنشاء المناطق المحمية في أثناء النزاعات المسلحة، لذلك سنبيين في هذا المطلب مفهوم المناطق المحمية وطبيعتها من خلال فرعين نناقش في الفرع الأول تعريف المناطق المحمية، ونناقش في الفرع الثاني الطبيعة القانونية للمناطق المحمية.

الفرع الأول

تعريف المناطق المحمية

لأهمية التعرف على الهجمات المناطق المحمية ، لابد من تعريفها لغة واصطلاحاً.

أولاً: المناطق المحمية لغةً.

الحمى لغةً: هي قطعة الأرض الفسيحة وما فيها من عيون وينابيع تُحمى من الناس، ويُمنعون أن يرعوا فيها بأغنامهم ومواشيهم وأنعامهم. وحمى الشيء حمياً وحمى وحمايةً ومحميةً: منعه ودفعه عنه. ويُقال حمى أهله في القتال حماية. وحماه الناس يحميه إياهم حمى وحمايةً: منعه. والحماية: الرجل يحمي أصحابه في الحرب، وهم أيضاً الجماعة يحمون أنفسهم. و أحمى المكان: جعله حمى لا يُقرب. و أحماه: وجده حمى. ويقال حمى فلان الأرض يحميها حمى لا يُقرب. ويقال: أحميتُ المكان فهو محمى إذا جعله حمى. ويقال: تحماه الناس، أي: توقوه واجتنبوه. وحمى من الشيء حميةً ومحميةً^(١). وللحمى جذور تاريخية في الجزيرة العربية قبل الإسلام فكانت هذه تقاليد معروفة على مستوى المعابد والمزارات، إذ كانت هناك أراضٍ مخصصة لها أو شبه موقوفة عليها. وهناك شكل آخر للحمى في الجاهلية تذكرها كتب التاريخ، مفادها أن الشريف من العرب وكبير قومه في الجاهلية كان إذا نزل مع عشيرته وأهله أرضاً استعوى كلباً، فكان يحمي لنفسه ولأهله مدى عواء الكلب لا يُشرك فيه غيره، ولا يسمح لغيره أن يرعى فيه^(٢). وقال الأصمعي: يُقال حمى فلان الأرض يحميها حمى لا يُقرب. وحمى: المكان الممنوع، يقال أحميتُ المكان فهو محمي، إذ جعلته حمى، فأما حميته فهو بمعنى حفظته. وجاء في معجم البلدان: الحمى

١ ابن منظور، لسان العرب، باب حما، دار المعارف، القاهرة، ج١٧، المجلد الثاني ص ١٠٤-١٠.

٢ محمد عدنان البخت، الحمى والمحميات ودورها في الإسلام، الصحيفة الاقتصادية، ٢ تشرين الثاني/نوفمبر ٢٠٠٩

مقال منشور على الرابط https://www.aleqt.com/2009/11/02/article_296139.html تاريخ الزيارة

بالكسر والقصر؛ وأصله في اللغة الموضع، الذي فيه كلاً يُحمى من الناس أن يروعوا فيه أي أن يمنعونهم، يقال حميت الموضع وذلك إذا حميت منه. والحمى جمعها أحمية، وهو تنظيم عرفي لصيانة وحسن استغلال المراعي الطبيعية والمحافظة عليها، نشأ في الجزيرة العربية قبل الإسلام، وتستند حمايتها إلى تقاليد وأعراف تتضمن جزاءات للمخالفين. ويرجع تاريخ نشأت أغلب أنواع المناطق المحمية إلى ما يزيد على ألفي عام في عصر ما قبل الإسلام (العصر الجاهلي)، وقد تطورت تماشياً مع الظروف البيئية الطبيعية آنذاك، ولشحة الموارد الطبيعية المتجددة أو لعدم اكتشافها، وللحاجة صونها واستغلالها إلا كانت تدخل ضمن السياق القبلي وأنها ذات مفهوم قبلي وتخضع إلى موازين القرى. استند مفهوم الحمى بالإسلام على إدارة المراعي الطبيعية بطريقة تتلاءم و الظروف الطبيعية السائدة والممارسات المحلية مع الخضوع لتعليمات معينة. فقد وضع النبي إرشادات عامة حول الحمى إذ أصبح أحد الأدوات الأساسية للمحافظة على الطبيعة في الشريعة الإسلامية. سمح الإسلام للدولة فقط أن تقوم بحماية مساحات معينة لأغراض الصالح العام وأوقف الحمى القبلي وممارسة التسلط والإقطاع والحروب بين القبائل طلباً لاحتلال مرعى أو مورد ماء أو غيره كالسلب والنهب. ولقد نهى الرسول صلى الله عليه وآله وسلم أن يحمى على الناس حمى و كانوا في الجاهلية يفعلون وسمح بما يحمى لخیل المسلمين وإبل الزكاة وركابهم التي تُعدُّ للجهاد، ويحمل عليها في سبيل الله، ومن هنا جاء قول الرسول صلى الله عليه وآله وسلم: «لا حمى إلا لله ورسوله». وأجاز الرسول صلى الله عليه وآله وسلم الحمى لأغراض المصلحة العامة بما يخدم مصالح المسلمين، ومن منطلق المصلحة العامة، وحمى الرسول عليه وعلى آله الصلاة والسلام النقيع، وقد حمى سرف وضرية وجُرش، وكتب لأهالي الأخيرة: «فمن رعاه من الناس فماله سُحت». ونلاحظ أن بعض الوفود التي كانت تؤمُّ المدينة المنورة كانت تطلب من الرسول صلى الله عليه وآله وسلم أن يحمي لها، فمنها من طلب حمى جبل لصاحب نحل، وهذا عنزة العذري يطلب من الرسول صلى الله عليه وآله وسلم أن يحمي لبني عذرة واديهم، وبالإجمال أقر الرسول بشكل عام حمى من دخل الإسلام وحماه له^(١).

ثانياً: المناطق المحمية اصطلاحاً.

١ محي الدين محمود قواس، الإدارة المستدامة للمراعي الطبيعية عند العرب (نظام الحمى)، مجلة بحوث جامعة حلب، العدد ١٢، دمشق، سوريا ٢٠١٧، ص ٦-٨.

إن فكرة تشكيل وتأسيس المناطق المحمية جاءت على وفق متطلبات القانون الدولي الإنساني، الذي يرتكز على مجموعة من القواعد القانونية والاتفاقيات، التي تسعى أساساً إلى إيجاد الحماية لفئات معينة من الأفراد و الممتلكات والأعيان ذات الطابع المدني، كذلك لحرمة أن يتعرض الأفراد والأعيان ذات الطابع المدني إلى كافة الهجمات خلال النزاعات المسلحة الدولية منها و غير الدولية. فقد نصت اتفاقية جنيف الأولى و الرابعة لعام ١٩٤٩ على " إمكانية تأسيس مناطق ومواقع استشفاء وأمان"، فقد نُظِمت بطريقة تمنحها حماية فئات محددة، كذلك إنشاء مناطق محايدة. فضلاً عن ذلك فقد أورد البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩ على إمكانية الاعلان عن مناطق خالية من وسائل الدفاع. وكذلك أورد البروتوكول الإضافي الأول على حظر، وتخطي العمليات العسكرية إلى مناطق اتفقت أطراف النزاع على اعتبارها مناطق منزوعة السلاح. مضافاً إلى ذلك فإن جهاز مجلس الأمن في الأمم المتحدة وضع مناطق أخرى تحت الحماية الدولية متمثلة بالمناطق الآمنة ومناطق حظر الطيران إذ كانت الغاية من إنشائها توفير الحماية للفئات التي أصابها الضرر من الأشخاص والأعيان ذات الطابع المدني جراء النزاعات المسلحة^(١).

يشمل مصطلح «المنطقة المحمية» أيضاً المناطق البحرية المحمية، التي تشمل حدودها بعض المناطق المحيطية، والمناطق المحمية عبر الحدود، التي تتداخل مع العديد من البلدان التي تزيل الحدود داخل المنطقة لأغراض الحفظ والاقتصاد^(٢). وكان الهدف الرئيس من إقرار قواعد القانون الدولي هو توفير حماية قانونية للمدنيين والأعيان بغية درء ما تتعرض له من انتهاكات جسيمة لذا كان من أهم آليات توفير الحماية هي فكرة إنشاء المناطق المحمية بحيث لا تصلها النزاعات المسلحة^(٣). وإن القانون الدولي الإنساني قد أوجد نوعين من الحماية، حماية عامة، وأخرى خاصة للأعيان المدنية تجلت في اتفاقية جنيف الرابعة لعام ١٩٤٩ والبروتوكولين الإضافيين لعام ١٩٧٧ الملحقين باتفاقيات جنيف الأربع لعام ١٩٤٩ واتفاقية لاهاي المعنية بحماية الأعيان الثقافية في خضم النزاعات المسلحة لعام ١٩٥٤ فيما يخص الحماية

١ إسرائ صباح الياسري، التنظيم الدولي للمناطق المحمية دراسة في ضوء القانون الدولي الإنساني، المركز العربي للدراسات والبحوث العلمية، ط١ القاهرة، مصر، ٢٠١٨ ص ١٧-١٩.

٢ محمد صابر، المحميات في الوطن العربي إدارة التنوع الأحيائي وتنميتها، مؤسسة زايد الدولية للبيئة، ط١، الإمارات العربية المتحدة، ٢٠٢٠، ص ٢٥.

٣ سوداني نور الدين، المناطق المحمية بموجب القانون الدولي الإنساني، وآليات محاكمة منتهكها أمام القضاء الدولي الجنائي، مجلة أبحاث، المجلد ٦، العدد الأول، الجزائر، ٢٠٢١، ص ٥٠٠.

العامّة فهو ما قد يشكل الاعتداء المباشر على الأعيان المدنية والتي تكون مأهولة بالمدنيين الذين سيصبحون عرضة للهجمات فصار لزاماً توفير الحماية للأعيان التي لا استغناء عنها لضمان الحماية القادرة على حفظ حياة السكان المدنيين^(١). ونصت المادة (٢٥) من لائحة لاهاي المعنية بالحرب البرية لعام ١٩٠٧ على حظر أو قصف المساكن أنى كانت الوسيلة و بينت اللجنة الدولية للصليب الأحمر أماكن النزاع المباشر من المباني المدنية إذ ينبغي أن تُجَنَّب الاعتداءات وعلى الرغم من كلّ ما أوردته الاتفاقيات من نصوص تحظر المساس بالأعيان والمدنيين إلّا أن الدول المتنازعة والنزاعات المسلحة لم تمتنع تماماً عن المساس بالمدنيين والأعيان مما حدى بالمجتمع الدولي إلى تجريم وحظر أي اعتداء على هذه الأعيان إذ إن تدمير الممتلكات والاعتداء عليها من غير ضرورة عسكرية يعد انتهاكاً جسيماً لأحكام الاتفاقية على وفق نص المادة (١٤٧) كذلك أوجبت المادة (٢٧) من البروتوكول الإضافي الأول باتخاذ التدابير اللازمة كافة لتفادي أي هجوم قدر المستطاع على المباني التابعة لدور العبادة والفنون، وسواها و حظرت القواعد العرفية (٣٥ و ٣٦ و ٣٧) توجيه الهجوم نحو منطقة منشأة لإيواء الجرحى، كذلك توجيه الهجوم إلى منطقة منزوعة السلاح، وحظرت أيضاً شن الهجوم على الأماكن المجردة من وسائل الدفاع^(٢).

ويمكن تعريف المناطق المحمية تعريفاً فقهيّاً وقانونياً وقضائياً أما التعريف الفقهي للمناطق المحمية: تُعرّف المناطق المحمية بأنها مساحات جغرافية يُعترف بها قانوناً خلال فترات النزاع المسلح، ويُتفق بين أطراف النزاع على استثنائها من العمليات العسكرية. وتُمنح هذه المناطق وضعاً قانونياً خاصاً يكفل لها الحماية بموجب اتفاقات دولية أو ترتيبات متبادلة، بما يضمن تحييدها عن القتال، وتوفير الأمان للفئات غير المشاركة في الأعمال العدائية، مثل المدنيين والمرضى والجرحى والأطفال.

وقد بيّن فقهاء القانون الدولي الإنساني أن هذه المناطق تتخذ أشكالاً متعددة تختلف بحسب الغرض من إنشائها وطبيعة الحماية الممنوحة لها، ومنها: مناطق الأمان، والمناطق المحايدة، ومناطق الاستشفاء،

١ ماريّا عبد الرؤوف الدباس، حماية الأعيان المدنية وفقاً للقانون الدولي الإنساني (المناطق المحمية - المنشآت ذات الطاقة الخطرة - المرافق الإعلامية - البيئة الطبيعية)، مجلة الحكمة، المجلد ٤١، العدد ٧٤، سوريا، ٢٠١٠، ص ٨٣-٨٤.

٢ ماريّا عبد الرؤوف الدباس، مصدر سابق، ص ٨٥-٨٦.

والمناطق المنزوعة السلاح، على أن يُراعى في كل منها التزام الحياد الكامل وعدم استخدامها في الأغراض العسكرية^(١).

التعريف القانوني للمناطق المحمية:

تُعرف المناطق المحمية، في إطار القانون الدولي الإنساني، بأنها تلك المساحات التي تُنشأ استناداً إلى أحكام اتفاقيات جنيف لعام ١٩٤٩ والبروتوكولين الإضافيين لعام ١٩٧٧، وتُخصص لحماية فئات معينة لا تشارك في الأعمال القتالية، مثل الجرحى، والمرضى، والمدنيين.

ويُشترط لإنشائها اتفاق صريح بين أطراف النزاع، وتخضع لضوابط قانونية صارمة تضمن تحييدها الكامل عن العمليات العسكرية، وتمنع استخدامها لأي غرض عسكري مباشر أو غير مباشر. وقد نص البروتوكول الإضافي الأول في المادة (٥٩) على مفهوم "المدن المفتوحة"، بينما أفردت المادة (٦٠) أحكاماً لـ "المناطق المنزوعة السلاح". أما اتفاقية جنيف الرابعة، فقد عالجت في المواد (١٤ إلى ٢٤) إنشاء "مناطق الاستشفاء" و"المناطق الآمنة"، موضحةً شروطها ومتطلبات احترامها من قبل أطراف النزاع^(٢).

التعريف القضائي للمناطق المحمية:

في الاجتهادات القضائية للمحاكم الدولية، لا يوجد تعريف محدّد صريح للمناطق المحمية، ولكن ثمة إجماع قضائي على أن استمرار الحماية مشروط بعدم استخدام هذه المناطق لتحقيق أغراض عسكرية. فإذا استُغلت كخنادق أو مستودعات للأسلحة أو مواقع تخفي وجود وحدات مسلّحة، فإنها تفقد وضعها القانوني كمحمية، وتعلن أهدافاً مشروعة تستوجب المحاسبة الجنائية. وقد بيّنت المحكمة في قضية تاديتش أنه عندما تُستخدم منطقة محمية كغطاء لنشاطات عسكرية، فإن هذا يلغي وضعها المحمي، ويستوجب ملاحقة المسؤولين عنها بموجب قانون الجرائم الدولية^(٣).

١ حسين محمد الصادق، الحماية الدولية للمدنيين أثناء النزاعات المسلحة في القانون الدولي الإنساني الإسكندرية،

مصر: دار الفكر الجامعي، (٢٠١٦)، ١٢٢

٢ إسراء صباح الياسري، التنظيم الدولي للمناطق المحمية: دراسة في ضوء القانون الدولي الإنساني (الإسكندرية،

مصر: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، (٢٠١٨)، ٤٥-٤٧

٣ إبراهيم عبد الحميد عمر، مسؤولية الأفراد أمام القضاء الجنائي الدولي: دراسة قانونية في ضوء أحكام المحكمة الجنائية الدولية والإقليمية (القاهرة: دار النهضة العربية للطباعة والنشر، (٢٠٢٠)، ١٨٢-١٨٣؛ بالاستناد إلى ICTY،

Prosecutor v. Duško Tadić، قضية IT-94-1-T، الحكم الصادر في ٧ مايو ١٩٩٧، الفقرة ٥٨٦

ويعرف الباحث: المناطق المحمية بأنها مساحات جغرافية محددة تُنشأ بموجب اتفاقات صريحة أو قواعد عرفية في سياق النزاعات المسلحة، بهدف تأمين الحماية للأشخاص أو الممتلكات أو المواقع التي تتأثر بشدة من آثار الأعمال العدائية. ويمنع داخل هذه المناطق أي نشاط عسكري، هجومي أو دفاعي، مع احترام مبدأ الحياد التام، وتخضع هذه المناطق لضوابط قانونية صارمة ومراقبة إنسانية أو دولية عند توفر الإمكانيات. ويمثل هذا المفهوم أداة تنفيذية رئيسية من أدوات القانون الدولي الإنساني، الغاية منها تقليل الأذى الناتج عن الحرب على الفئات الضعيفة أو الممتلكات الحيوية ذات الأهمية الإنسانية أو الثقافية أو البيئية.

الفرع الثاني

الطبيعة القانونية للمناطق المحمية

إن القانون الدولي الإنساني أورد تعريفات مختلفة للمناطق المحمية، التي تمنح السكان المدنيين الذين قد يتعرضون للخطر أو أنهم تعرضوا للخطر، حماية خاصة إذ إن لا قتال قد يقع فيها. وحددت اتفاقيات جنيف الأربع لعام ١٩٤٩ وبروتوكولاتها الإضافيان لعام ١٩٧٧ المناطق المحمية وبينت طبيعتها القانونية لما لها من أهمية خاصة في توفير الملاذ الآمن على وفق ما أوردته من نصوص قانونية. بينما شهد واقع العمل الدولي صوراً أخرى للمناطق المحمية، التي بينها القانون الدولي الإنساني، وكان لإنشائها ضرورة لا تستوجب اتفاق كل أو بعض الأطراف المتنازعة وإنما تلتزم هذه الحالة استصدار قراراً من قبل مجلس الأمن على وفق أحكام الفصل السابع من ميثاق الأمم المتحدة، حمايةً للفئات الأكثر تضرراً، إذ أضاف مجلس الأمن مناطق أخرى إلى المناطق الآمنة، التي تستخدم من أجل منح الحماية للمدنيين، وتعرف باسم "المنطقة الآمنة ومنطقة حظر الطيران". وتعتمد هذه المناطق على قواعد اتفاقيات جنيف الأربع. وقد يؤدي أحياناً وضع المدنيين من السكان الضعفاء وجمعهم في منطقة محمية -واقعاً- إلى احتمال تعرضهم إلى مخاطر كبيرة قد يواجهونها. فمثلاً، قد يصبحون عرضة - وهم عزّل - إلى هجوم عسكري، لذا ينبغي تعيين الجهة التي تقع على عاتقها مسؤولية قانونية وعسكرية في حماية المناطق والأشخاص بدقة وحزم. ولم تتوافق المناطق الآمنة التي أُقيمت من قبل الأمم المتحدة في يوغسلافيا السابقة في ١٩٩٣ والمناطق الإنسانية الآمنة في رواندا في ١٩٩٤ بمقاييس القانون الإنساني الخاصة بالمناطق الآمنة، وعوضاً عن ذلك، كانت هذه المناطق خلاصة الحلول الدبلوماسية والعسكرية التي

تفاوض مجلس الأمن عليها. ففي هذه المناطق ضرورة الدراسة الدقيقة لمفهوم مثل مفهوم المناطق المحمية^(١).

وتقسم المناطق المحمية على:

- مناطق الاستشفاء والأمان.
- المناطق المحايدة.
- المناطق المجردة من وسائل الدفاع.
- المناطق منزوعة السلاح.
- المناطق الآمنة.
- مناطق حظر الطيران^(٢).

أولاً: المناطق والمواقع المحمية بموجب اتفاقيات جنيف الأربع وبروتوكولها الإضافيين لعام ١٩٧٧.

١- مناطق الاستشفاء والأمان:

يمكن تعريف مناطق الاستشفاء بأنها مناطق ومواقع تقام على أراضي طرف من أطراف النزاع أو على أرض محتلة بغية حماية الجرحى والمرضى من أفراد القوات المسلحة، فضلاً عن أفراد الخدمات والطواقم الطبية المعينين فيها، وينبغي على أطراف النزاع عدم الهجوم أو الاعتداء عليها. وترى اتفاقية جنيف الأولى عام ١٩٤٩ يمكن تقوم الدولة بإنشاء منطقة أو موقع مثل هذه المناطق أو المواقع حتى في أثناء السلم، وعقد اتفاقيات خاصة مع الطرف الخصم في أثناء النزاع المسلح. وقد توفر المعاهدة "مشروع اتفاق بشأن مناطق ومواقع الاستشفاء"^(٣). وعرفت مناطق الاستشفاء أيضاً إنها الأماكن المنشأة بصورة دائمة بعيداً عن مناطق النزاع المسلح كملجأ للجرحى والمرضى من المقاتلين وفئات أخرى كالأطفال وكبار السن الذين تمكن منهم الضعف أو المرض فاقترضى حمايتهم من الأسلحة ذات المدى البعيد، ولا سيما القصف الجوي^(٤). ويُنتقد هذا التعريف، لأنه قصر حماية المناطق المحمية على فئات

١ منظمة أطباء بلا حدود، القاموس العملي للقانون الإنساني، تقرير منشور على الرابط <https://ar.guide-humanitarian-law.org/content/article/5/mntq-wmq-mhmyw/> تاريخ الزيارة ٢٠٢٤/١٢/٢٥. الساعة ١٠:٠٠.

٢ إسرائ صباح الياسري، مصدر سابق، ص ٢٣.

٣ يُنظر: اتفاقية جنيف الأولى لعام ١٩٤٩، المادة ٢٣.

٤ شريف عتلم، دور اللجنة الدولية للصليب الأحمر في إنماء وتطوير قواعد القانون الدولي الإنساني، منشورات اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠١٥، ص ١٤١-١٤٢.

محددة من المدنيين بينما من الممكن أن تشمل حماية المناطق المحمية فئات أخرى كالنساء والنازحين^(١). وعُرفت أيضاً: إنها مناطق أنشأت بطريقة منظمة يمكن من خلالها حماية السكان المدنيين من مخاطر الحروب وآثارها. ويأخذ على هذا التعريف أنه جعل هذه المناطق معنيةً بالمدنيين فحسب بينما من الممكن أن تشمل الحماية الجرحى والمرضى من المقاتلين أيضاً^(٢). أما مناطق الأمان: هي المناطق التي تعنى بحماية كبار السن والأطفال الذين أعمارهم دون سن الخمس عشرة سنة والنساء الحوامل، وأمّهات الأطفال ممن أعمارهم دون سن السبع سنوات. وتعريف مناطق الاستشفاء بأنها المناطق المحددة، التي تنشأ في وقت السلم أو عند نشوب النزاعات المسلحة، غايتها أن توفر الحماية لنسبة كبيرة من الأفراد الذين، لم يشتركوا في الحرب أو الذين توقفوا عن الاشتراك في النزاعات المسلحة^(٣)، وجاء باتفاقيتي جنيف الأولى و الرابعة لعام ١٩٤٩ (يجوز للأطراف السامية أن تنشأ على أراضيها أو الأراضي المحتلة إذا دعت الحاجة إليها مناطق ومواقع استشفاء وأمان. الخ). وكى تتمتع هذه المناطق بالحماية الممنوحة لها من أي استهداف أو هجوم من قبل أطراف النزاع ينبغي أن تستوفي الشروط الآتية:

- ١- ألا تأخذ مكاناً كبيراً من الإقليم الذي أُقيمت عليه.
- ٢- أن تساوي الكثافة السكانية إمكانيات الإقامة أو أن تكون أقل منها.
- ٣- ألا تكون قريبة من النقاط الحربية والعسكرية والمنشآت كالإدارية والصناعية، التي من الممكن أن تُستهدف.
- ٤- ألا تقع في المناطق التي من المحتمل أن تكون لها أهمية في العمليات الحربية.
- ٥- ألا تستخدم الطرق ووسائل النقل لنقل العسكريين أو لأداء مهمات عسكرية.
- ٦- ألا تحمى بالوسائل العسكرية إطلاقاً^(٤).

و ينبغي على المعنيين توقيع اتفاقيات معنية بالتمييز المشترك لمناطق ومواقع المستشفيات، التي أنشأوها. كررت اتفاقية جنيف الرابعة تأكيدها على فكرة مناطق ومواقع المستشفيات، التي عينتها اتفاقية

١ إسرائ صباح الياسري، مصدر سابق، ص ٢٣.

٢ مالك منسي صالح الحسيني، الحماية الدولية للأهداف المدنية- دراسة في ضوء القانون المدني، رسالة ماجستير، المعهد العالي للدراسات السياسية الدولية، جامعة المستنصرية، بغداد، ٢٠٠٥، ص ٩٧.

٣ إسرائ صباح الياسري، المصدر السابق، ص ٢٤.

٤ المادتان (٤،٥) المشتركة من الملحق الأول لاتفاقيات جنيف الأولى لعام ١٩٤٩ والملحق الأول لاتفاقية جنيف الرابعة لعام ١٩٤٩.

جنيف الأولى "الخاصة بالمرضى والجرحى من أفراد القوات المسلحة". وبمثل هذه الحالة، ينبغي إنشاء مواقع كهذه، بغرض حماية المدنيين من آثار النزاع المسلح. وينبغي تنظيم وتهيئة مناطق الأمان والمستشفيات - التي يقيمونها على أرض أحد الأطراف في النزاع أو في منطقة قد احتلت - بقصد حماية الجرحى والمرضى والعجزة، والأطفال الذي تقل أعمارهم عن الخامسة عشرة، والحوامل، وأمهات الأطفال ممن أعمارهم أقل من سبع سنوات، فضلاً عن الذين وجبت حمايتهم في مناطق ومواقع المستشفيات، المشار إليها آنفاً، وثانيةً، ينبغي تعيين مواقع كهذه، في أثناء السلم وينبغي الاتفاق بشأنها بين الأطراف المتنازعة في أثناء النزاع المسلح^(١). وتؤكد الاتفاقية على أن الدول المعنية بالحماية - بصفتها دولة حامية - توفير الحماية، وكذلك أن اللجنة الدولية للصليب الأحمر هي مدعوة إلى أن تقدم مساعيها الحميدة لتمكين وتسهيل إنشاء مناطق ومواقع الاستشفاء والأمان^(٢). ولكي تُميّز مناطق المستشفيات والمناطق الآمنة توضع أشرطة ذات لون أحمر على أرضية بيضاء تحيط الحدود الخارجية للمنطقة وأيضاً توضع فوق مبانيها ولتميز ليلاً تستخدم وسائل ضوئية ملائمة، وكذلك تميز المناطق المخصصة للجرحى والمرضى، ويحق لكل دولة أن تعترف بمنطقة استشفاء وأمان، التي انشأها الخصم وأن تشترط فرض رقابة عليا عبر لجنة معينة أو أكثر بغرض التحقق من استيفاء الشروط الواردة بالاتفاق ويكون لأعضاء هذه اللجنة حرية الدخول في جميع الأوقات إلى هذه المنطقة. وهذا الشعار المميز تكفل قواعد اتفاقيات جنيف حمايته وأن استغلاله بطريقة مشينة أو عدم احترامه يُعدّ خرقاً فاضحاً للمعاهدات، وبذلك تُعدّ جرائم حرب^(٣). وقد أصدرت الجمعية العامة للأمم المتحدة عام ١٩٩٧ قرارها المتضمن المبادئ الأساسية لحماية المدنيين في أثناء النزاعات المسلحة^(٤). وقد أشارت إلى المناطق المخصصة لحماية المدنيين كمناطق الاستشفاء أو أي ملاذ مشابه ينبغي ألا يكون مسرحاً للعمليات العسكرية، ومن الأمثلة على مناطق الاستشفاء والأمان التي أنشأت في حرب التحرير في بنغلادش، وحرب جنوب الأطلسي، والنزاعات في كمبوديا وتشاد، وقبرص، نيكاراغوا ولبنان والعراق ويوغوسلافيا السابقة وسواها، إذ أُ

١ يُنظر المادة ١٤ الملحق الإضافي الأول.

٢ يُنظر المادة (١٤) اتفاقية جنيف الرابعة لعام ١٩٤٩.

٣ يُنظر المواد (٦٠، ٨، ٩)، الملحق الأول لعام ١٩٧٧، لاتفاقية جنيف الأربع لعام ١٩٤٩.

٤ يُنظر قرار (٢٥/٢٦٧٥) الصادر عن الجمعية العامة للأمم المتحدة، لعام ١٩٧٠.

نشأت معظمها بناءً على اتفاقيات مكتوبة، واستندت هذه الاتفاقيات إلى المبدأ الذي يوجب عدم الهجوم على المناطق، التي تنشأ لتكون ملاذاً للجرحى والمرضى^(١).

٢- المناطق المحايدة:

إذا أثرت النزاعات المسلحة على الأشخاص المحميين، فقد سمحت قواعد القانون الدولي الإنساني لأطراف النزاع بإنشاء مناطق محايدة لحماية هؤلاء من ويلات الحرب وتجنبهم آثار النزاع لذلك، تُعرف المنطقة المحايدة بأنها المنطقة، التي تُنشأ باتفاق أطراف النزاع في مناطق القتال لإيواء الجرحى والمرضى من المقاتلين وغير المقاتلين، وكذلك المدنيين، الذين لا يشاركون في الأعمال العسكرية. هذه المناطق مؤقتة، يُعدونتماشي مع الظروف الراهنة^(٢). وقد يمتد مفهوم المناطق المحايدة ليشمل مناطق ذات أهمية كبيرة للمجتمع الدولي بشكل عام. عُرِفَت هذه المناطق بأنها تلك التي تخص جميع الدول والتي يُحدد موقعها المحايد بموجب معاهدات دولية. تشمل هذه المناطق الممرات الدولية، مثل القنوات الدولية (مثل قناة السويس وبنما وكيل)، والمضايق الدولية (مثل مضيق هرمز وباب المندب). حددت الاتفاقيات الدولية أن هذه الممرات والمضايق تتمتع بالحماية، ولا يجوز لأطراف النزاعات عرض لها^(٣). بناءً على ما سبق، يمكن تعريف المناطق المحايدة بأنها: أماكن تنشأ في منطقة القتال بهدف توفير الحماية من مخاطر الحرب دون أي تمييز ضار لجميع الأشخاص الذين لم يشاركوا أو توقفوا عن المشاركة في الأعمال العسكرية ولا يقومون بأي عمل ذي طبيعة عسكرية في أثناء إقامتهم في تلك المناطق. تُنشأ هذه المناطق بناءً على اتفاق بين الأطراف المتحاربة، على وفق اقتراح الطرف الذي ينشأ المنطقة. أشارت اتفاقية جنيف الرابعة لعام ١٩٤٩ إلى هذه المناطق، ونصت على أنه "يجوز لأي طرف في النزاع أن يقترح على الطرف المعادي، إما مباشرة وأما عن طريق دولة محايدة أو هيئة إنسانية، إنشاء مناطق محايدة في الأقاليم، التي يجري فيها القتال لحماية الأشخاص " المذكورين في أدناه من مخاطر القتال دون أي تمييز:

أ. الجرحى والمرضى من المقاتلين وغير المقاتلين.

١ جون -ماري هنكرتس، لويز دوزوالد- بك، القانون الدولي الإنساني العرفي، المجلد الأول: القواعد اللجنة الدولية للصليب الأحمر، ص ١٠٨.

٢ شريف عتلم، وخالد غازي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني ط ١، القاهرة، مصر، ٢٠٠٩، ص ٣٧.

٣ سهيل حسين الفتلاوي، مصدر سابق، ص ٨٩.

ب. الأفراد من المدنيين الذين لا يشاركون في الأعمال ذات الطابع العسكري خلال إقامتهم في المناطق المعنية^(١). مع ذلك فغالباً ينبغي على أطراف أو طرفي النزاع المسلح عقد اتفاق مكتوب يُعين بداية ووقت تحديد أو تعيين المنطقة المحايدة، زيادةً على تفاصيل أو جزئيات موقعها الجغرافي وإيراداتها وطريقة تمويلها ومراقبتها، ولكن أن بعض المناطق المحايدة قد أُقيمت على وفق اتفاق ضمني أو عُرف اصطلاحاً (باتفاق السلوك) مثل المنطقة التي أنشأت في الجنوب الأطلسي التي تعرف (كوخ الصليب الأحمر)^(٢). وقد يبدو أن الهدف من إنشاء المناطق المحايدة هو حماية الأشخاص العاجزين عن القتال والأشخاص غير المشاركين في الأعمال العسكرية من ويلات النزاع عن طريق تجميعهم في منطقة معينة. تختلف المناطق المحايدة عن مواقع ومناطق الاستشفاء والأمان، فهي تُنشأ في مناطق القتال، وليست بعيدة عنها، وغالباً ما تكون ذات طابع مؤقت تقتضيه تكتيكات الأعمال العسكرية في وقت معين. بينما مناطق الاستشفاء والأمان تُنشأ غالباً بصفة دائمة وبعيدة عن مناطق القتال، و أنها تُنشأ في وقت السلم وفي أثناء النزاع المسلح. شهد تاريخ النزاعات المسلحة إنشاء العديد من المناطق المحايدة. من بين هذه الأماكن: منطقة شونقاي (Sohanghai) في عام ١٩٣٧ في منطقة جاكينو (Zone Jocquint) في الصين، وفي القدس عام ١٩٤٨، وفي دكا عام ١٩٧١^(٣).

٣- المناطق منزوعة السلاح:

جاء في القاعدة العرفية (٣٦) أنه: يُحظر أن يوجه الهجوم إلى منطقة منزوعة السلاح، اتفقَ عليها بين الأطراف المتنازعة. تجسد ممارسات الدول هذه القاعدة كواحدة من قواعد القانون الدولي العرفي السارية في النزاعات المسلحة الدولية وغير الدولية. تُعرّف المناطق منزوعة السلاح بأنها: (المناطق التي يحظر فيها على أطراف النزاع القيام بعمليات عسكرية، أو استخدامها لأي غرض يتعلق بسير العمليات العسكرية)^(٤). يُعد اتخاذ المناطق المنزوعة السلاح هدفاً للهجوم انتهاكاً جسيماً بحسب البرتوكول الإضافي الأول. ويُفهم من المنطقة منزوعة السلاح بشكل عام أنها منطقة متفق عليها بين أطراف النزاع، ولا يجوز لأي طرف فيها احتلالها أو استخدامها لأغراض عسكرية. ويمكن إنشاء مثل هذه المناطق في

١ يُنظر المادة (١٥) اتفاقية جنيف الرابعة لعام ١٩٤٩.

٢ جون -ماري هنكرتس، لويز دوزوالد- بك، مصدر سابق، ص ١٠٨.

٣ غسان الجندي، حق التدخل الإنساني، ط١، بدون دار نشر، عمان، الأردن، ٢٠٠٢. ص ٣٤.

٤ إسراء صباح الياسري، مصدر سابق، ص ٣٧.

السلم مثلما في النزاع المسلح. على وفق المادة (٦٠) من البروتوكول الإضافي الأول، و لكي تكون منطقة ما منزوعة السلاح فينبغي أن تحترم الشروط التالية:

- ١- ألا تستعمل المنشآت والمؤسسات العسكرية الثابتة بشكل عدائي.
- ٢- ألا ترتكب أي عمل عدائي من قبل السلطات أو السكان.
- ٣- أن يُجلى كل المقاتلين وجميع الأسلحة المستخدمة في النزاعات المسلحة.
- ٤- ألا تمتنع عن أي نشاط أو دعم للمجهود الحربي. غير أن الشروط المذكورة لا تتعارض مع وجود أشخاص في هذه المناطق مشمولين بحماية خاصة بموجب الاتفاقيات الدولية والبروتوكول ذاته، و لا مع وجود قوات شرطة يقتصر هدفها على الحفاظ على القانون والنظام. لذلك إذا تم الاتفاق على تحديد منطقة معينة كمنطقة منزوعة السلاح فلا يجوز لأي طرف من أطراف النزاع أن يلغي الاتفاق من طرف واحد أو يستخدم المنطقة لأغراض عسكرية، لأن ذلك يعد إخلالاً بالتزاماته وتتوقف الحماية الممنوحة للمنطقة المنزوعة السلاح إذا ارتكب أحد الأطراف انتهاكاً جسيماً للاتفاق الذي أنشئت بموجبه هذه المنطقة^(١). وتشير الممارسات إلى أن الإشراف الدولي يُعد أسلوباً مناسباً للتحقق من احترام الشروط المتفق عليها، و يمكن للاتفاق أن يسمح بوجود قوات حفظ السلام، أو أفراد شرطة يكون الغرض الوحيد من وجودهم هو الحفاظ على القانون والنظام، دون أن تفقد المنطقة طابعها المنزوع السلاح. بموجب تشريعات العديد من الدول، تُعد الهجمات على المناطق المنزوعة السلاح جريمة. وقد أنشئت مناطق منزوعة السلاح في نزاعات مسلحة دولية وغير دولية؛ على سبيل المثال، في النزاعات بين الهند وباكستان، وكوريا الشمالية والجنوبية، والجمهورية العربية السورية وسلطة الاحتلال الصهيوني، والعراق والكويت، والنزاعات في البوسنة والهرسك، وكولومبيا ونيكاراغوا^(٢).

٤- المناطق المجردة من وسائل الدفاع:

يرتكز مفهوم المناطق المجردة من وسائل الدفاع دائماً على المبدأ التقليدي للمدينة المفتوحة، التي تُعرّف بأنها مدينة خالية تماماً من وسائل الدفاع، سواء في الداخل أو الخارج، بحيث يمكن لقوات الخصم دخولها والاستيلاء عليها دون قتال أو إلحاق أضرار بالبنية التحتية أو السكان. ومن ثم، فإن أي مدينة تقع خلف خطوط الجبهة تُعدّ مدينة مدافع عنها، وتصبح هدفاً مشروعاً للهجمات العسكرية، ما لم يثبت خلوها

١ يُنظر الفقرة (٣-٤) من المادة (٦٠) البروتوكول الإضافي الأول لعام ١٩٧٧.

٢ فرانسواز بوشيه سولنييه، القاموس العلمي للقانون الإنساني، ترجمة محمد سعود، مراجعة عامر الزمالي ومديحة مسعود، ط١، دار العلم للملايين، لبنان، ٢٠٠٦، ص ٦٠٤.

من الأهداف العسكرية. وعليه، يمكن عدّ أي مدينة تقع على خط الجبهة وتفتقر إلى وسائل الدفاع الخارجية، وقابلة للاحتلال دون قتال أو إصابات، منطقة مجردة من وسائل الدفاع، وإن احتوت على منشآت عسكرية، كالمصانع الحربية، بشرط عدم استخدامها لأغراض دفاعية^(١) تعرف المناطق المجردة من وسائل الدفاع بأنها:

المناطق السكانية التي تقع عادة قرب مواقع عسكرية أو داخل نطاقها، التي تُحمى حمايةً خاصة لمجرد إعلانها مناطق مجردة من وسائل الدفاع العسكري. و عُرِفَتْ أيضاً أنها مناطق مأهولة بالسكان، تكون بالقرب من المواقع التابعة للقوات المسلحة، أو التي تخضع لقوات الاحتلال الخصم، بغية الابتعاد عن القتال والتدمير^(٢). وقد أشار البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩ إلى أن أي منطقة مأهولة بالسكان تقع قرب مناطق الاشتباك أو داخلها، وتترك مفتوحة أمام احتلال الخصم، تُعدّ منطقة مجردة من وسائل الدفاع^(٣). وتعمل الدول على تطبيق هذه القاعدة كإحدى قواعد القانون الدولي العرفي، التي تسري في المنازعات المسلحة الدولية وغير الدولية:

أ: الأماكن المجردة من وسائل الدفاع في أثناء المنازعات المسلحة الدولية:

إن مفهوم المواقع التي خلت من وسائل الدفاع يرجع إلى مفهوم المدينة المفتوحة التقليدي، وقد تضمن إعلان بروكسيل ودليل أكسفورد حظر مهاجمة الأماكن التي خلت من وسائل الدفاع، وقد تمّ تقنين ذلك في المادة ٢٥ من لائحة لاهاي، التي نصت على " حظر مهاجمة أو قصف المدن والقرى والمساكن والمباني غير المحمية، بأي وسيلة مستخدمة ". ويعد التقرير المقدم من لجنة المسؤولين التي انشئت عند انتهاء الحرب العالمية الأولى أن قصف الأماكن المجردة من وسائل الدفاع عمداً يعدّ خرقاً لقوانين وأعراف الحروب، وينبغي أن يخضع للمحاكمة الجنائية، وبمقتضى البروتوكول الإضافي الأول عام ١٩٧٧ تم حظر اتخاذ المناطق المجردة من وسائل الدفاع أهدافاً لمهاجمتها، ويُعدّ هذا الهجوم خرقاً كبيراً للبروتوكول، وتضمنت عديد من كتيبات الدليل العسكري حظر مهاجمة المواقع المجردة من وسائل الدفاع ويُعدّ دليل القانون الدولي الانساني في السويد أن القاعدة الرئيسية في ما يتعلق بالمواقع المجردة من وسائل

١ جون -ماري هنكرتس، لويز دوزوالد- بك، مصدر سابق، ص ١١١-١١٢.

٢ كامران الصالحي، قواعد القانون الدولي الانساني والتعامل الدولي، دون دار طبع، أربيل، العراق، ٢٠٠٨، ص ١٤٢.

٣ يُنظر المادة (٥٩) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩.

الدفاع في المادة ٥٩ من البروتوكول الإضافي الأول كتقنين لقانون دولي عرفي موجود سابقاً. وبموجب كثير من القوانين الوطنية التي اعتبرت الهجوم على المواقع المجردة من وسائل الدفاع جرمًا^(١).

ب: الأماكن المجردة من وسائل الدفاع في أثناء النزاعات المسلحة غير الدولية.

وإن حظر الهجمات على المواقع المجردة من وسائل الدفاع جاء نصاً في المادة (٣) من النظام الأساسي للمحكمة الجنائية الدولية، الذي ينمّح المحكمة اختصاصاً بمقاضاة منتهكي قانون الحرب واعرافها، كذلك قصف ومهاجمة المدن أو القرى أو المساكن أو المباني المجردة من أعمال الدفاع مهما كانت الوسيلة. وبموجب التشريعات الداخلية للدول يحظر مهاجمة المواقع الخالية من وسائل الدفاع مهما كان النزاع المسلح، ومن الشواهد على ذلك ما حدث في عام ١٩٩٧ في قضية بيريستيتش وآخرين، حُكم فيها على مجموعة أشخاص لاعطائهم الأوامر بالقصف على مدينة (زادار) الكرواتية ومحيطها، وقد طبقت محكمة مقاطعة زادار المادة (٢٥) من اتفاقية لاهاي إلى جانب المادة (٣) المشتركة في اتفاقيات جنيف والمادتين (١٣ و ١٤) من البروتوكول الإضافي الثاني لعام ١٩٧٧.

بما أن مفهوم المناطق المجردة من وسائل الدفاع أُسس لكي يحدد في النزاعات المسلحة الدولية لكنه من الممكن انطباقه أيضاً على النزاعات المسلحة غير الدولية؛ لأن حظر الهجوم على المواقع الخالية من وسائل الدفاع استند إلى فكرة الضرورة العسكرية الأكثر اتساعاً إذ لا ضرورة من مهاجمة مدينة أو قرية أو مسكن أو بناية مفتوحة للاحتلال وهذه القاعدة هي تكييف للمبدأ العرفي القائل بمنع الحاق ضرر كبير بالعدو أكبر من اللازم وبموجب القانون الدولي الانساني فإنه يمنع قصف المواقع المجردة من وسائل الدفاع التي من السهولة احتلالها^(٢).

تضمن الدليل العسكري لبريطانيا وصفاً واضحاً حدد من خلاله المدينة المفتوحة أو الخالية من وسائل الدفاع، إذ إنها مدينة مجردة من وسائل الدفاع تماماً داخلاً وخارجاً وبإمكان العدو دخولها والاستيلاء عليها دون قتال، وبدون التسبب بإصابات نفهم من هذا أن لا وجود لمدينة مفتوحة أو مجردة من وسائل الدفاع بالخلف من خط الجبهة القائم، وإن المدينة الكائنة خلف خط جبهة العدو هي مدينة يدافع عنها ومعرضة للقصف الأرضي أو غيره من أنواع القصف وتخضع للقيود الواجبة على كل نوع من القصف، أي ينبغي أن يكون القصف ضمن دائرة الاهداف العسكرية. وعرفت المادة (٢/٥٩) من

١ فرانسواز بوشيه سولنييه، مصدر سابق، ص ٦٠٢.

٢ فاوستو بوكار - رئيس المحكمة الدولية الجنائية ليوغسلافيا السابقة - النظام الأساسي للمحكمة الجنائية ليوغسلافيا

السابقة، مقال منشور على الرابط www.un.org/law/laval

البروتوكول الإضافي الأول عام ١٩٧٧ مفهوم المواقع المجردة من وسائل الدفاع هي أي مكان مأهول بالسكان واقع قرب منطقة تماس القوات المسلحة أو ضمنها، إذ من السهل احتلالها من قبل الخصم. وهذا التعريف جاء نفسه في القانون الدولي العرفي التقليدي بالنسبة للمدينة المفتوحة أو المنطقة المجردة من وسائل الدفاع. ووضحت المادة (٢/٥٩) من البروتوكول نفسه وكيفية طريقة الاعلان عن المواقع المجردة من وسائل الدفاع. وهذه الطريقة والكيفية جاءت بخلاف الطريقة المتعلقة بالمناطق التي انشأت على وفق اتفاق بين طرفين أو أكثر، إذ يسمح لأطراف النزاع أو احد اطرافه أن يعلن ومن جانب واحد منطقة مجردة من وسائل الدفاع شرط أن يجلى جميع المقاتلين، والأسلحة المتحركة تجلى والمعدات العسكرية عنها. وأن "يمنع استخدام المنشآت أو المؤسسات العسكرية الثابتة لأغراض عدائية". كذلك يمنع ارتكاب الأعمال العدائية من لدن السلطات أو السكان. ويمنع أيضاً النشاطات الداعمة للعمليات العسكرية. بالمقابل فإن الطرف الآخر يقر باستلامه هذا الإعلان، فتعامل المنطقة أو الموقع على أنه مجرد وخال من الوسائل الدفاعية. وقد ورد في المادة (٥/٥٩) من البروتوكول الإضافي الأول عام ١٩٧٧ "تتمكن أطراف النزاع من إنشاء مواقع مجردة من وسائل الدفاع".

وتفقد هذه المنطقة الحماية من الهجمات عندما تصبح غير مستوفاة للشروط المطلوبة، بحسب نص المادة (٥٩) من البروتوكول الإضافي الأول عام ١٩٧٧^(١).

ثانياً: المناطق الآمنة الجديدة، التي أقامها مجلس الأمن التابع للأمم المتحدة

١- المناطق الآمنة

إذا لم يتوصل أطرافُ نزاع مسلح ما إلى اتفاق بخصوص وقف أو إنهاء العمليات العسكرية، وقد يؤدي دوامها إلى إزهاق أرواح أكثر من المدنيين، فقد يصدر مجلس الأمن قراراً يقتضي إقامة مناطق تحمي وتحفظ السكان المدنيين من القتل أو الأذى الناتج عن النزاعات المسلحة، وقد اصطلح عليها اصطلاحات عديدة "كالمناطق الآمنة، ومراكز الإغاثة المفتوحة والملاذات الآمنة وسواها". وأن ميثاق الأمم المتحدة لم يدعُ صراحةً بإحدى نصوصه إلى إقامة هذه المناطق، لكن التأصيل القانوني لهذه المناطق نجده في مجلس الأمن بوصفه الجهاز الأهم في الأمم المتحدة. وعليه فإن فكرة المنطقة الآمنة تتمثل بتعيين أو إنشاء إقليم في دولة ما تعاني أزمات عادة تكون إنسانية وغالباً يكون موقعها حدودياً لتحمي من قبل قوات الأمم المتحدة بصفقتها منطقة محمية يقطنون فيها الذين لا يشاركون في العمليات العسكرية،

١ يُنظر الفقرة (٣) المادة (٥٩) - البروتوكول الإضافي الأول لعام ١٩٧٧.

حماية لهم ولتسهيل وصول المساعدات الإنسانية^(١). وعُرفت المناطق الآمنة: إنها المناطق البعيدة عن الهجمات المسلحة أو تكون بعيدة عن أي عمل عدائي، فغايتها حماية ومساعدة المدنيين من السكان من آثار النزاعات المسلحة وضمان وصول المساعدات الإنسانية إليها والقيام بعمليات الإغاثة بمنأى عن المخاطر والاعتداءات والسلب^(٢). ولإنشاء منطقة آمنة ينبغي أن يتوفر شرطان: الأول، أن المنطقة تنشأ بناءً على قرار يصدر من الأمم المتحدة، وأن تبقى ضمن رقابتها وإشرافها. أما الشرط الثاني، أن لا يؤدي أنشاؤها إلى خرق السيادة وانتهاكها للدولة، التي اقيمت عليها المنطقة الآمنة^(٣).

ومن الأمثلة على المناطق الآمنة ما أنشأت في شمال العراق بغرض حماية اللاجئين والنازحين واستقبالهم على وفق القرار الصادر عن مجلس الأمن (٦٨٨) بتاريخ ١٩٩١/٤/٥. والمناطق التي أُقيمت في العراق على شكل مخيمات بالاتفاق مع الأمم المتحدة بعد احتلال داعش لبعض محافظات العراق فأقيم مخيم في "حركة" في أربيل، ومخيم "داودية وكبر" في دهوك، ومخيم "تاسولية" في السليمانية، ومخيم "السوق العصري" في البصرة. وإن مصطلح المنطقة الآمنة لهو مصطلح أطلق على المناطق المنشأة بواسطة الأمم المتحدة في جمهورية البوسنة والهرسك، وقد اجترح مجلس الأمن -المرّة الأولى- مفهوم المنطقة الآمنة في "سربرنيتشا" والمناطق المحيطة بها. وكان غاية هذه القرارات حظر النشاطات العسكرية في هذه المناطق بقصد السماح للأمم المتحدة نشر قواتها حماية للمنطقة وضماناً لوصول المساعدات الإنسانية، واعتمد القراران على وفق الفصل السابع من ميثاق الأمم المتحدة، وإن القرارين ألزما جميع الدول، ولم يخضعا لاتفاقية خاصة بين أطراف النزاع. فضلاً عن ذلك، فإن مجلس الأمن في قراره ذي الرقم ٨٣٦ الصادر في ٤ حزيران/يونيو ١٩٩٣، والذي اعتمد بموجب الفصل السابع قد فوض القوات التابعة للأمم المتحدة باستعمال القوة لصد أي هجمة كانت على المناطق الآمنة^(٤). نرى أن

1 Chimni, Incarceration of victims Deconstructing safety zones. In, N. Al. Nauimi and R. Meese, international legal issues Arsing under the United Nations decade of international law, Netherlands, 1995, p. 825.

٢ صلاح الدين بوجلال، الحق في المساعدات الإنسانية، ط١، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٨، ص ٣١٦.

٣ محمد غازي ناصر الجناي، التدخل الإنساني في ضوء القانون الدولي العام، ط١، منشورات الحلبي الحقوقية، ٢٠١٠، ص ٨٦.

٤ فرانسواز بوشيه سولنييه، مصدر سابق ص ٦٠٥ - ٦٠٦.

المناطق الآمنة هي مناطق آنية لم تكن دائمة قامت جراء ظرف طارئ وعلى عجلة، لذا ينبغي تجنبها الوحدات العسكرية وإبعادها عنها، التي قد تشكل خطراً على القاطنين فيها.

٢- مناطق حظر الطيران

بعد أن أصبح مجلس الأمن الدولي مخولاً بإصدار قرارات تعنى في الحالات التي تُنتهك فيها حقوق الإنسان، ومنها التي تحدث في اثناء النزاعات المسلحة، إذ إن نشوب النزاع المسلح غالباً ما يرافقه انتهاك جسيم لحقوق الإنسان ما يوجب على مجلس الأمن إتخاذ القرارات المعنية بإستهداف المدنيين والأعيان المحمية والسماح بوصول المساعدات الإنسانية للمتضررين السكان نتيجة النزاعات المسلحة^(١). وقد أشار مجلس الأمن في مرات عديدة إلى رفضه التهاون مع الانتهاكات، التي صار التعامل معها من منطلق أنها تشكل تهديداً و خطورة على السلم والأمن الدوليين، ما يستدعي مجلس الأمن أن يوليها اهتماماً جاداً وأن يتخذ إجراءات بشأنها إذا ما لزم الأمر^(٢).

وعُرفت مناطق حظر الطيران: أنها مناطق يحظر أو يمنع فيها الطيران الحربي لأجل طرف نزاع ما ولكي يُفرض الحظر فقد يستوجب الأمر إقامة دوريات في المجال الجوي، لحساب أحد اطراف النزاع، أو يكون الحظر عن طريق تدمير منظومات مقاومة الطائرات لذلك الطرف، بعبارة أدق منع الطائرات الحربية من التحليق في مجال جوي لدولة ما^(٣). ومن الأمثلة على حظر الطيران عندما أقام التحالف الدولي عقب إنقضاء حرب الخليج الثانية عام ١٩٩١ منطقة حظر جوي شمال وجنوب العراق حمايةً للمدنيين وضماناً لعودة النازحين واللاجئين، فقد امتدّت منطقة الحظر من شمال العراق حتى كادت أن تكون اقرب إلى حدود بغداد، وبعد احتلال العراق عام ٢٠٠٣، انتفتت الضرورة من العمل بهذا القرار فأُلغي^(٤). وأصدر مجلس الأمن قراره ذي الرقم (٧٨١) في ٩ أكتوبر عام ١٩٩٢، الذي منع فيه الطيران الحربي ما خلا الطائرات الحربية التابعة للأمم المتحدة لتقديم المساعدات الإنسانية، في المجال الجوي لجمهورية البوسنة والهرسك، وطلب القرار إيكال امر مراقبة الحظر الى الأمم المتحدة، الذي فرضته

١ نادية محتالي، حماية حقوق الإنسان تحت الاحتلال، رسالة ماجستير، كلية الحقوق، جامعة باجي مختار، الجزائر ٢٠١٢، ص ١٢٩.

٢ القرارين الصادرين عن مجلس الأمن رقم (١٦٧٤، و١٧٣٨) لعام ٢٠٠٦.

٣ سوداني نور الدين، مصدر سابق، ص ٥٠٧.

٤ محمد غنايم، الحظر الجوي على شمال العراق، موقع إلكتروني www.aliazeera.net/specialcoverage تاريخ الزيارة: ٢٠٢٥/٢/٢ الساعة: ٨:٠٧ صباحاً.

وعلى الأمين العام للأمم المتحدة إعداد تقريراً حول تطبيق القرار وعضد مجلس الأمن قراره السابق بقرار آخر ذي الرقم (٧٨٦) في ١٠ نوفمبر لعام ١٩٩٢، إذ عدّ حظر تحليق الطائرات الحربية في المجال الجوي للبوسنة والهرسك من الأعمال الرئيسية لوصول المساعدات الإنسانية وحماية المدنيين. وفي العام ٢٠١١ أقام مجلس الأمن منطقة حظر جوي في ليبيا على وفق قراره رقم (١٩٧٣) بسبب انتهاكات الحكومة الليبية بحق المدنيين^(١).

نستخلص مما تقدم: أن المناطق المحمية تمثل إحدى الأدوات المهمة للمجتمع الدولي في الحفاظ على البيئة والتنوع البيولوجي، وأنها تكتسب طابعاً خاصاً من الحماية القانونية يركز على مصادر متعددة في القانون الدولي، تشمل الاتفاقيات الدولية البيئية، الأعراف، المبادئ العامة للقانون، وأحكام القضاء الدولي. إن النظام القانوني للمناطق المحمية قد تطور وتخطى الحماية في أوقات السلم، إذ إنه امتد ليغطي أيضاً بعض أشكال الحماية في أثناء النزاعات المسلحة، على وفق ما نص عليه القانون الدولي الإنساني. ومن خلال التحليل القانوني للنصوص الدولية والإقليمية، يتضح أن الطبيعة القانونية للمناطق المحمية لم تعد محصورة في مجرد تصنيفات بيئية أو إدارية، بل أصبحت تمثل التزاماً قانونياً دولياً يفرض على الدول احترام هذه المناطق وصيانتها، ويمنحها طابعاً قانونياً خاصاً قد يرقى في بعض الأحوال إلى مرتبة قواعد القانون الدولي العرفي أو حتى الآمرة، إذا ما ارتبطت بحماية حقوق الإنسان والموارد المشتركة للبشرية.

وفي ضوء ما تقدم، فإن الباحث يرى: إن الطبيعة القانونية للمناطق المحمية تشهد تطوراً نوعياً في القانون الدولي، يُظهر التفاعل المتزايد بين القانون الدولي البيئي والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ويؤكد أن هذه الطبيعة القانونية لا تقتصر على البعد البيئي فحسب، بل تشمل أبعاداً سيادية، إنسانية، وتنموية، تفرض على الدول والمجتمع الدولي التزامات متزايدة لا تقف عند حدود التراضي أو الإرادة المنفردة. فمن حيث المصدر القانوني، يرى الباحث أن الطبيعة القانونية للمناطق المحمية تتأسس على مزيج من الاتفاقيات الدولية: (مثل اتفاقية التنوع البيولوجي لعام ١٩٩٢، واتفاقية التراث العالمي لعام ١٩٧٢)، فضلاً عن الاتفاقيات الإقليمية (مثل اتفاقية برشلونة لحماية البحر المتوسط)، إلى جانب المبادئ العامة للقانون، والعرف الدولي المتنامي، الذي يُظهر وعياً متزايداً بضرورة حماية البيئة لصالح الأجيال القادمة. ومن حيث الوظيفة القانونية، يرى الباحث أن المناطق المحمية لم تعد فقط

١ سوداني نور الدين، مصدر سابق، ص ٥٠٧.

وسيلة إدارية لحماية الموارد، بل أصبحت تمثل مراكز قانونية خاصة ذات حماية دولية، فإن أي اعتداء عليها أو تقصير في حمايتها قد يرتب مسؤولية دولية للدولة، سواء أمام هيئات دولية أم بموجب مبدأ المسؤولية البيئية. وهذا التوجه يتعزز بفكرة الأمانة البيئية العالمية التي تجعل بعض المناطق -كالمواقع الطبيعية المصنفة ضمن التراث العالمي- خاضعة لنظام قانوني دولي يتجاوز السيادة الوطنية التقليدية. ومن حيث التطور التاريخي والوظيفي، يرى الباحث أن القانون الدولي شهد تحولاً من التركيز على سيادة الدولة المطلقة على الموارد الطبيعية إلى الاعتراف بمبدأ السيادة المقيدة، الذي يلزم الدول باستخدام أراضيها ومواردها بطريقة لا تضر بالبيئة العالمية أو بمصالح الدول الأخرى. وهذا التوجه له انعكاسات مباشرة على إدارة المناطق المحمية، إذ يُحتم على الدول أن تدير هذه المناطق على وفق معايير دولية صارمة تأخذ في الاعتبار البعد الإيكولوجي والإنساني والحقوق. ومن حيث العلاقة مع النزاعات المسلحة، يرى الباحث أن القانون الدولي الإنساني لا يغفل أهمية حماية المناطق ذات القيمة البيئية الخاصة في أثناء النزاع، إذ تنص اتفاقية لاهاي ١٩٥٤ على حماية الممتلكات الثقافية، ويمكن استنباط حماية المناطق المحمية من مبدأ التمييز ومبدأ التناسب، مما يضع عبئاً على الأطراف المتنازعة بتفادي الإضرار بتلك المناطق، ولا سيما إذا كانت تحتوي على نظم بيئية نادرة أو تهدد حياة السكان المدنيين. ويوصي الباحث بضرورة تطوير بروتوكولات تكميلية لاتفاقيات جنيف تأخذ في الحسبان الحماية الخاصة للمناطق المحمية خلال النزاعات المسلحة، على غرار الحماية التي تُمنح للمستشفيات أو المواقع الدينية. ومن حيث الأثر القانوني المترتب على مخالفة نظام المناطق المحمية، يرى الباحث أن الدولة التي تخل بالتزاماتها الدولية في حماية المناطق المحمية قد تتعرض للمساءلة الدولية أمام محاكم وهيئات دولية مثل محكمة العدل الدولية، أو قد تُفرض عليها عقوبات بيئية على وفق نظام المسؤولية الدولية للدول، لا سيما إذا نتج عن ذلك ضرر عابر للحدود أو أثر على حقوق الشعوب الأصلية أو الحقوق الجماعية للأجيال القادمة. وعليه، يخلص الباحث إلى أن الطبيعة القانونية للمناطق المحمية هي طبيعة مركبة ومتعددة الأبعاد، تتجاوز حدود القانون البيئي لتشمل أطراً متشابكة من القانون الدولي العام، مما يفرض إعادة النظر في السياسات الوطنية والآليات الدولية ذات الصلة لضمان حماية فعالة ومستدامة لهذه المناطق.

المبحث الثاني

الجهود الفقهية والدولية لمواجهة مخاطر الهجمات السيبرانية

في ظل ما يشهده العالم من تقدم تكنولوجي وثورة تقنية متسارعة في كافة المجالات، أصبحت الدول تتجه للاعتماد كلياً على ما يوفره الفضاء السيبراني من خدمات أسهمت في خلق النقلة النوعية التي تأملها الدول في جميع مجالات التنمية، لا سيما أن الفضاء السيبراني أدى دوراً مهماً في إزاحة العوائق الحدودية بين الدول وأصبح عاملاً في تقريب المسافات بين الشعوب، وعلى الرغم من أن هذا الفضاء - الذي يعد الطفرة التكنولوجية الأهم في القرن الحادي والعشرين - إلا أنه شهد العديد من الهجمات والجرائم السيبرانية، التي تعتمد على تقنيات متقدمة كـ (الحوسبة السحابية، والذكاء الاصطناعي، وأجهزة تصنت على شبكات الاتصال، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات)؛ لتسخيرها في القيام بعمليات إجرامية وتعاملات مشبوهة دون علم أصحابها، إذ يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين الحواسيب أو الأجهزة المتصلة بالإنترنت، التي يمكن استخدامها لتنش هجمات سيبرانية متنوعة، لأغراض إجرامية كـ (التخريب، والإرهاب، والتهديد، والابتزاز). إذ إن التنظيمات والجماعات الإرهابية قد استغلت جيداً المزايا التكنولوجية كعنصر حيوي لدعم وتحقيق أهدافها، ومنفذ لوجستي داعم وحاضن للنشاط الإعلامي لها في مناطق مختلفة من العالم، فمن خلال شبكات الإنترنت تستطيع تلك التنظيمات والجماعات تصوير أنفسهم وأعمالهم في السياق الذي يريدونه للتأثير على الرأي العام وتجنيد أعضاء جدد وجمع الأموال، ونظراً لأن الدول العربية كغيرها من دول العالم تسعى لاستغلال الطفرة التكنولوجية، والتقدم المتسارع لتدعيم عمليات التنمية لديها، فقد اتجهت هذه الدول نحو الفضاء الإلكتروني على جميع المستويات، ما جعلها عرضة للاستهداف من قبل الجماعات الإرهابية، التي أصبحت أكبر مهدد لأمنها القومي. إذ أصبحت الحماية السيبرانية أصبحت في العصر الحديث أحد أهم التحديات التي تواجه المجتمع الدولي، إذ أصبحت الهجمات السيبرانية تهديداً متزايداً الخطورة على الأمن القومي والاقتصادي للدول، سواء كانت هذه الهجمات تستهدف مؤسسات حكومية، شركات كبرى، أم حتى الأفراد. وفي هذا السياق، أصبح من الضروري بذل الجهود المشتركة على الصعيدين الفقهي والدولي لمواجهة ومكافحة هذه المخاطر السيبرانية المتزايدة.

إن الجهود الفقهية تؤدي دوراً بارزاً في فهم وتحليل التحديات القانونية والأخلاقية المتعلقة بالهجمات السيبرانية. فمن خلال الفقه السيبراني، يسعى الخبراء إلى وضع إطار قانوني وأخلاقي ينظم استخدام التكنولوجيا الرقمية، ويحد من تأثير الهجمات السيبرانية على الأفراد والمؤسسات. وتشمل هذه الجهود إثارة الوعي بأهمية حماية البيانات الشخصية، وتطوير سياسات وإجراءات للحفاظ على الأمن السيبراني، وتقديم التوجيهات القانونية للتعامل مع الهجمات السيبرانية وتحديد المسؤوليات القانونية في حال وقوعها. على الصعيد الدولي، تشهد المنظمات الدولية والحكومات جهوداً متعددة لمواجهة التحديات السيبرانية والحد من تأثيرها.

وسنبحث هذا الموضوع عبر مطلبين، نناقش في المطلب الأول الجهود الفقهية لمواجهة المخاطر السيبرانية، وفي الثاني الهجمات السيبرانية وأثرها على تهديد السلم والأمن الدوليين.

المطلب الأول

الجهود الفقهية لمواجهة المخاطر السيبرانية

تطورت التكنولوجيا بشكل هائل خلال العقود الأخيرة، مما أدى إلى تغييرات جذرية في شتى جوانب الحياة اليومية، بما في ذلك الاقتصاد والتعليم والترفيه والاتصالات. ومع ذلك، جاء هذا التقدم التكنولوجي بثمن، فظهرت معه مخاطر جديدة تتعلق بالأمن السيبراني. وهنا يأتي دور الجهود الفقهية التي تسعى لمواجهة ومواجهة هذه المخاطر بكل جدية وفعالية.

تمثل المخاطر السيبرانية تحدياً كبيراً للمجتمعات اليوم، إذ يمكن أن تؤثر بشكل كبير على الأفراد والمؤسسات والدول بشكل عام. فهي تشمل تهديدات متعددة تتراوح بين الاختراقات الإلكترونية وسرقة البيانات والاحتيال الإلكتروني والتجسس الصناعي والهجمات السيبرانية الضارة، التي يمكن أن تتسبب في أضرار جسيمة على المستوى الشخصي والاقتصادي والسياسي.

في مواجهة هذه التحديات، تعمل الجهود الفقهية على وضع الإطار القانوني والأخلاقي اللازم لتنظيم ومعالجة الأنشطة السيبرانية وتحديد الحدود والمسؤوليات والعقوبات المناسبة لمن ينتهكها. وتتنوع هذه الجهود بين المستويات الوطنية والدولية، إذ تسعى المؤسسات القانونية والفقهية في مختلف الدول إلى إقامة نظم تشريعية تظهر تطلعات المجتمع وتحقق العدالة والأمن السيبراني.

ترتكز الجهود الفقهية لمواجهة المخاطر السيبرانية على عدة مبادئ أساسية، من بينها الحفاظ على الخصوصية والأمان الإلكتروني للأفراد والمؤسسات، وضمان توافر البيانات والمعلومات بشكل آمن

وسليم، وتحقيق التوازن بين الاستفادة من التكنولوجيا وحقوق الأفراد والمجتمعات، وتعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية وتبادل المعلومات والخبرات.

زيادةً على ذلك، فإن الجهود الفقهية تسعى لتعزيز الوعي العام بشأن خطورة التهديدات السيبرانية وكيفية الوقاية منها، وتشجيع التدابير الوقائية والتقنيات الأمنية الحديثة للحد من المخاطر السيبرانية، وتعزيز الأمان الرقمي، وسننن الجهود الدولية لمواجهة المخاطر السيبرانية عبر فرعين نناقش في الفرع الأول دليل تالين والمخاطر السيبرانية، ونناقش في الفرع الثاني إعلان إيرايتشي لمبدأ الاستقرار السيبراني والسلام السيبراني.

الفرع الأول

دليل تالين والمخاطر السيبرانية

في خضم التطور التكنولوجي الحديث حطم الفضاء الإلكتروني الحواجز الجغرافية بين الدول والمنظمات والأفراد. فقد أصبح الناس جميعهم متصلين بشبكات واسعة تسمح بتبادل المعلومات بسرعة كبيرة، مما يحقق فوائد عظيمة^(١).

يتفق على أن الفضاء الإلكتروني غيّر شكل الصراعات بين الدول بشكل كبير. فإن تطور التكنولوجيا قد منح الدول وجماعات أخرى، مثل الإرهابيين، أدوات هجومية جديدة لتنفيذ وتحقيق هجمات إلكترونية. فهذه الهجمات يمكن أن تحطم أنظمة حيوية عسكرية أو مدنية عن بعد، وتعطل شبكات الدفاع والقطاع الخاص والبنية التحتية، وتؤثر على البيانات المالية والعسكرية بقصد إضعاف الدولة. على الرغم من خطورة هذه الهجمات التي تحدث باستمرار وتهدد الأمن العالمي، لم تصدر حتى الآن قوانين واضحة من الأمم المتحدة أو مجلس الأمن أو محكمة العدل الدولية للتعامل معها^(٢).

وإن المعهد الدولي للدراسات الاستراتيجية في لندن رأى أن الفضاء الإلكتروني سيصبح ميداناً مهماً من ميادي القتال في النزاعات المستقبلية، إذ إن أقوى الدول والمؤسسات ذات الاقتصاديات الكبيرة ليست في أمان من خطر الهجمات الإلكترونية.

1 Miranda Grange, Cyber Warfare and the Law of Armed Conflict, Research Paper, Faculty of Law, Victoria University of Wellington, 2014, P1.

2 Priyanka R. Dev, Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response, Texas International Law Journal, Vol. 50, Issue 2, 2015, P380.

وإن قاعدة مهمة هناك في العلاقات الدولية وهي منع استخدام القوة أو التهديد بها. وإن هذه القاعدة ذكرت في المادة الثانية، الفقرة الرابعة من ميثاق الأمم المتحدة، تؤكد على أن الدول الأعضاء ينبغي أن تتجنب تهديد أو استخدام القوة ضد سلامة أراضي أي دولة أخرى أو استقلالها السياسي أو بأي طريقة تتعارض مع أهداف الأمم المتحدة^(١).

لم يُعين ميثاق الأمم المتحدة بوضوح ما المقصود بـ "استخدام القوة" أو "الهجوم المسلح"، إلا أنه من خلال استقراء التاريخ، فقد تعارف العالم على أن أعمالاً غير ودية مثل: الضغوط الاقتصادية والسياسية والتجسس والمقاطعة والعقوبات التجارية قد لا تُعدّ استخداماً للقوة، مهما خلفت من آثار. أما "الهجوم المسلح" فيشمل عادةً إعلان الحرب، واحتلال الأراضي، والحصار البحري، واستخدام الجيش ضد أراضي دولة أخرى أو قواتها أو المدنيين. بعبارة أضيق، قد يشمل أي عمل عسكري تقليدي (بري، بحري وجوي)، ويسبب أضراراً مادية أو بشرية كبيرة، كي يُعدّ استخداماً للقوة أو هجوماً مسلحاً^(٢). وهذا الأمر يقودنا إلى سؤال: هل استخدام القوة الإلكترونية أو التهديد بها يُعدّ نوعاً من أنواع القوة العسكرية المحظورة بموجب ميثاق الأمم المتحدة؟ إذا كان الأمر كذلك، فهل يستدعي ذلك تطبيق العقوبات المنصوص عليها في الفصل السابع من الميثاق؟ أم أن هذه الأفعال الإلكترونية لا تقع ضمن نطاق الحظر الذي عناه الميثاق؟

أول ما يُلاحظ في نصوص ميثاق الأمم المتحدة المتعلقة بتجريم العنف في العلاقات الدولية هو تجنب استخدام عبارة "اللجوء إلى الحرب" بسبب المشاكل في تفسيرها. عوضاً عن ذلك، فقد استخدم الميثاق عبارة "استعمال القوة" لأنها أشمل، مع ذلك، قد نشأ نقاش حول معنى كلمة "القوة" الواردة في المادة الثانية، الفقرة الرابع^(٣)، لقد استخدمت المادة الثانية في فقرتها الرابعة مصطلح "القوة" دون أن توضح أو تحدد معناه. إذ إن للمصطلح هذا معانٍ كثيرة، ومجالات واسعة: فقد يشير إلى استخدام الجيش في العلاقات بين الدول، أو إلى استخدام الضغوط السياسية أو الاقتصادية، أو حتى إلى استخدام القوة داخل

١ محمد عبد الرحمن الدسوقي، قانون المنظمات الدولية: منظمة الأمم المتحدة ووكالاتها المتخصصة، الجزء الثاني، دار النهضة العربية، القاهرة، ٢٠٠٢، ص ٤٧-٤٨.

2 Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal of National Security Law and Policy, Vol.4, 2010, P71.

٣ عبد القادر مرزق، استخدام القوة في إطار القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، الجزائر، ٢٠١٢، ص ١٥.

الدولة ضد المعارضين^(١). مع ذلك أن جانباً كبيراً من فقهاء القانون الدولي قد رأى أن المقصود "بالقوة"، الواردة في المادة الثانية هو القوة العسكرية، وبحسب الفقيه رونزيتي فقد رأى أن التفسير الأكثر منطقية ودقة لنص المادة قد قصر مفهوم "القوة" على استخدام القوة العسكرية والمسلحة أو التهديد بها ما يعني: إن الضغوط الاقتصادية لم تُشمل بهذا الحظر^(٢). إن لفظ أو عبارة "القوة" الواردة في الميثاق كانت تأتي مصحوبة بمصطلح "المسلحة" في كثير من الحالات، مثلما جاء في ديباجة الميثاق والمادة (٤٤)، لكن اصطلاح "القوة" ورد في المادة (٢) في الفقر (٤) منه، وحده دون أن يتبعه مصطلح "القوة"، ما عفاً الأمر ووسع دائرة الاختلاف بين فقهاء القانون الدولي، حول المراد بمعنى "القوة": أي القوة العسكرية فحسب أم يتسع معنى "القوة" ليشتمل كذلك على الضغوطات الاقتصادية والسياسية؟، فانقسموا على اتجاهات عديدة:

الاتجاه الأول: ذهب أصحابه إلى تفسير المادة الثانية، الفقرة الرابعة، تفسيراً ضيقاً، فقد قالوا: بالقوة العسكرية فحسب، مسندين رأيهم إلى المادة في أعلاه، التي أوردت: إن استخدام القوة ينبغي أن يكون ضمن ديباجة الميثاق، وعلى وفق مواده الأخرى. وقد دلت أعمال المادة (٢ الفقرة ٤) التحضيرية جميعها على أن المراد بمعنى القوة التحضيرية هو القوة العسكرية فقط. وقد قدمت البرازيل مقترحاً في "مؤتمر سان فرانسيسكو" لعدّ الضغط الاقتصادي على الدول استخداماً للقوة غير مشروع المقترح قد جوبه بالرفض.

أما الاتجاه الثاني، فقد قال أنصاره: ليس ثمة أساس قانوني يُرسخ مفهوم القوة على أنه القوة العسكرية فحسب، إنما يسيراً توسيع المفهوم هذا، ليشتمل على الضغوط الاقتصادية والنفسية وأفعالاً أخرى. ويدعمون فكرتهم بأن الإكراه أو الإرغام السياسي والاقتصادي قد يشكل تهديداً للاستقلال السياسي للدولة، وهذا ما لا يقل خطورة عن التهديد العسكري^(٣).

الاتجاه الثالث: إن هذا الرأي قد رأى مفهوم القوة هو ليس الإكراه غير العسكري، الذي يمارس في نطاق معين ومحدود، ويقصدون بذلك ممارسة الإكراه بالقدر الكافي لتقييد أو تقليص حرية تصرف الدولة

١ صلاح الدين بودربالة، استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، اطروحة دكتوراه، كلية الحقوق، جامعة الجزائر، الجزائر، ٢٠١٠، ص ٤٧.

٢ عبد القادر مرزق، المصدر السابق، ص ١٥.

٣ زقار منية العمري، الدفاع الشرعي في القانون الدولي العام، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، الجزائر، ٢٠١١، ص ٣٥ - ٣٦.

المقصودة أو المستهدفة، دون أن يُمس أمنها القومي. ويعتقدون أن هذا الأمر ضروري لسير الحياة الدولية العملية، ومن ثم يعد استخد القوة أو الإكراه استخداماً مشروعاً للقوة.

ويثور خلاف ثانٍ وقد تعلق هذا الخلاف بحظر استخدام القوة الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة، إذ إنها حظرت على الدول استخدام القوة أو التهديد ضد السلامة الإقليمية أو الاستقلال السياسي لدولة ما، بالوسائل التي تتعارض و غايات الأمم المتحدة، وما خلا ذلك فقد يعد استخداماً مشروعاً للقوة. ورأى أصحاب التفسير الضيق للمادة (٤/٢) أن هذا الشرط أو القيد ما كان ليهدف قط إلى تضيق أو تقليص نطاق حضر ومنع استخدام القوة، إنما على خلاف ذلك، إذ يسعى إلى منح ضمانات محددة إلى الدول الصغيرة. وقد أخذت محكمة العدل الدولية بالتفسير الضيق للمادة المذكورة آنفاً، في قضية مضيق كورفو، إذ عُدت ما قامت به بريطانيا عندما إزالة الألغام البحرية في المياه الإقليمية الألبانية مظاهراً لاستخدام القوة، ومن ثم، يعد انتهاكاً لمبدأ السيادة الإقليمية^(١).

لكن، فريق آخر من الفقه قد رأى: إن حظر استخدام القوة يتحتم أن يكون قاطعاً، وحظراً شاملاً. فقد عدوا وضع استثناءات أو فرض بعض القيود المحددة على هذا الحظر قد يفتح باب التأويل و التبرير لكثير من الأعمال والانتهاكات الأخرى، كأن تتدخل دولة في إحدى الدول بذريعة فرض أو نشر الديمقراطية، مدعية أن هذا ليس من ضمن حظر استخدام القوة. وكان رأيهم هذا استناداً إلى الأعمال التحضيرية لمؤتمر فرانكيسكو، الذي وضع فيه ميثاق الأمم المتحدة، إذ إنها جاءت لتؤكد على أن تحديد صور استخدام القوة المنصوص عليها في المادة (٤/٢) جاء بقصد التوضيح ولم يأت إلى تضيق نطاق الحظر^(٢).

محصلة القول: إن العرف الدولي قد استقر على أن المراد من القوة الواردة في المادة (٤/٢) هو القوة المسلحة أو العسكرية فحسب، بمعنى أن تحشد دولة قواتها العسكرية للاعتداء على دولة أخرى أو على أراضيها. وقد أشارت محكمة العدل الدولية في الفتوى التي أفتتها بشأن مشروعية التهديد أو استخدام الأسلحة النووية إلى أن المادة (٤/٢) من الميثاق قد نصت على حظر استخدام القوة دون النظر إلى أنواع

١ محمد وليد سكاف، حق استخدام القوة ودوره في العلاقات الدولية، دار النهضة العربية، القاهرة، ٢٠٠٥، ص ١٢.

2 Rene Vark, The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force, Baltic Defence Review, No.10. Vol.2, 2003, P30.

وأشكال الأسلحة المستخدمة. على الرغم من ذلك، فحتى الآن لا وجود لأي اتفاق عالمي يحدد بشكل دقيق، أن استخدام الهجمات السيبرانية يُعد استخداماً للقوة على وفق المادة (٤/٢) من الميثاق^(١). ويتنازع اتجاهان رئيسيان بشأن تكييف الهجمات الإلكترونية كاستخدام للقوة على وفق المادة (٢ فقرة ٤) من الميثاق:

الاتجاه الأول: وهو "الاقتراب المقيد"، تبنى أنصاره تفسيراً حرفياً لنص المادة (٤/٢) من ميثاق الأمم المتحدة. وركزوا على فكرة إحداث تأثيرات مادية وبشرية كبيرة لتصنيف الهجمات السيبرانية كاستخدام للقوة على وفق المادة المذكورة آنفاً. وبناءً على ذلك، فقد رأوا أن الهجمات السيبرانية تشبه في تأثيراتها إلى حد كبير الإكراه السياسي أو الاقتصادي، أي: إنها لا تُخلف أضراراً مادية جسيمة، وقد لا تقع ضمن نطاق تلك المادة، بصرف النظر عن آثارها السلبية على الأمن الدولي. وأستند أصحاب هذا الاتجاه إلى هجوم "ستاكنست" السيبراني، الذي تعرضت له المنشآت النووية الإيرانية في العام ٢٠١٠ كعينة واضحة على أن الهجوم السيبراني يُعد استخداماً للقوة، إذ تسبب في تدمير جزء من أجهزة الطرد المركزي^(٢).

أما الاتجاه الثاني: "الاقتراب الموسع"، فيُعد نقيض الاتجاه الأول. وتبنى أنصاره تفسيراً واسعاً للمادة (٤/٢)، إذ إنهم رأوا ليس ضرورياً أن تحدث الهجمات السيبرانية أضراراً مادية جسيمة لعددها استخداماً للقوة. فإن أي هجمة سيبرانية تؤدي إلى تعطيل الأنظمة الحاسوبية الرئيسية للدولة وتشل مفاصلها الحيوية أو تحدث أضراراً اقتصادية كبيرة، فليس ثمة ما يمنع من عددها استخداماً للقوة على وفق المادة المذكورة سلفاً^(٣). وقد حاول (مايكل شميت) التوفيق بين هذين الاتجاهين، مؤكداً على أن الهجمات السيبرانية ينبغي أن تتواءم مع النهج التقليدي، الذي يعد أن إحداث الضرر الجسيم هو المعيار الحقيقي لمعنى استخدام القوة. ولكنه وسّع المفهوم ليشتمل على الأضرار الاقتصادية الكبيرة، إلى جانب الأضرار العسكرية. ومن ثم، يرى شميت أن الهجمات السيبرانية، التي تنجم عنها خسائر اقتصادية كبيرة تُعد استخداماً للقوة أو

1 Abel S. Knottnerus, International Law and the Use of Armed Force by States, Global Perspective, Springer Fachmedien Wiesbaden, 2016, P14.

2 Kriangsak Kittichaisaree, Op. Cit, PP 153. 154.

3 Sophie Barnett, Applying Jus Ad Bellum in Cyberspace, (Septmber 1, 2016), E-International Relations Studies, <http://www.e-ir.info/2016/09/01/applying-jus-ad-bellum-in-cyberspace/>.

بمثابتها.^(١) وقد حدد مايكل شميت، معايير أو مقاييس خمسة رئيسية لعد الهجوم السيبراني بمثابة استخدام للقوة :

١. شدة وقوة الضرر.

٢. الضرر المباشر واللاحق.

٣. وجود الاتصال المباشر بين القوة العسكرية وعواقبها.

٤. تخطي الهجوم السيبراني للحدود الجغرافية للدولة.

٥. إمكانية تقييم وتحديد الفعل المادي^(٢).

ونرى إن جهود فقهاء القانون الدولي لصد خطورة الاعتداءات السيبرانية هي الجزء الجوهرى والرئيس من التلبية الشاملة لتحديات الحداثة، إذ إنها تسعى جاهدة إلى إيجاد توازن حقيقي بين التطور التكنولوجي وحفظ الأفراد والمجتمعات من التهديدات والمخاطر السيبرانية المتفاقمة.

نظراً إلى أن لا موقف أو توجه رسمي من الأمم المتحدة، فقد ظهرت كثير من الاتجاهات الفقهية للتصدي إلى مخاطر الهجمات السيبرانية. وقد تمثلت الاستجابة الدولية الأبرز لحل اشكالية الهجمات السيبرانية فيما يُعرف بـ "دليل تالين للقانون الدولي المنطبق على الحرب السيبرانية"، والذي أعدته نخبة من أهم فقهاء القانون الدولي. نُشرت النسخة الأولى من هذا الدليل في عام ٢٠١٣، وتضمنت (٩٥) قاعدة قانونية إرشادية لتنظيم عمل أو سلوك الدول في سياق الحرب الإلكترونية. وفي عام ٢٠١٧، صدرت النسخة الثانية، محتويةً على (١٥٤) قاعدة، ما وفرَّ معالجة أشمل للعمليات السيبرانية ومراجعة وتسوية نقاط الخلاف التي وردت في النسخة الأولى من الدليل^(٣).

عرفت المادة (٣٠) من دليل تالين بسختها الأولى الهجمات السيبرانية بأنها عملية إلكترونية، سواء أكانت دفاعية أو هجومية، يُحتمل أن تؤدي إلى إصابة أو وفاة أفراد، أو إتلاف أو تدمير منشآت. يتضح من خلال التعريف في أعلاه أن فقهاء تالين اتفقوا على أن الفرق بين هجومات إلكترونية وغيره من أنشطة

1 Junaidu Bello Marshall and Mua'zu Abdullahi, Cyber- Attack: The Legal Response, International Journal of International Law, Vol.1, Issue 2, 2011, P3.

2 Titiriga Remus, Cyber-Attacks and International law of Armed Conflicts; a Jus ad Bellum perspective, Journal of International Commercial Law and Technology, Issue 8, No. 3, 2013, P 179.

1 ابراهيم السيد أحمد رمضان، مصدر سابق، ص ١٨١.

إلكترونية مثل التجسس أو الحرب النفسية، يكمن في أن الأولى يمكن عدها أعمالاً عنيفة تحدث أضراراً بالهدف المقصود، سواء أكانت أفراداً أو منشآت. ويراد من حجم الضرر هنا هو الضرر الجسيم، أي: حدوث خسائر فظيعة في المنشآت أو بين الأفراد، أو أن يحدث الهجوم على منشأة ما ضرراً بالغاً مثل أن يعطل أو يدمر أنظمة سد ما فيؤدي إلى فيضانات. أما الخسائر المحدودة فهي الناتجة عن هجوم سيبراني، سواء للأفراد أو المنشآت، فلا تصل إلى مستويات الأضرار الجسيمة. وقد أكد الخبراء في دليل تالين أن الضرر المراد هنا لا يجب حده ضمن أعمال العنف أو الهجوم بالقوة الحركية، وهو مفهوم راسخ في قانون الدولي الذ يطبق في أثناء النزاعات المسلحة، بل يتخطى الحد ليشتمل على الآثار العنيفة التي تسببها الأسلحة غير الحركية مثل الأسلحة البيولوجية والكيميائية، وكذلك الهجمات الإلكترونية أو السيبرانية..^(١) فالتأثيرات العنيفة المضرة التي تسببها الأخيرة، سواء ألى منشآت مدنية أم عسكرية، أم تتسبب في إصابة أم موت مدنيين أم عسكريين، تعد على وفق رأي خبراء تالين هجوماً مسلحاً^(٢). استند خبراء دليل تالين، على وفق المادة (١١)، إلى معيار "النطاق والأثر" لمعرفة الحد، الذي ينبغي أن يصله الهجوم الإلكتروني ليُعد استخداماً للقوة أو هجوماً مسلحاً. وعليه، من الممكن عد الهجوم السيبراني هجوماً مسلحاً إذا خلف أضراراً تبلغ إلى "عتبة الشدة"، وإن المراد من هذا هو إحداث الضرر المادي جسيم. واستند خبراء الدليل في اعتماد هذا المعيار إلى حكم أو رأي محكمة العدل الدولية في قضية نيكاراغوا، بوصفها الأنسب لفض الإشكال المتعلق بالعتبة المناسبة للأعمال التي تبلغ إلى حد استخدام القوة والهجمات المسلحة. واستناداً إلى هذا الحكم، أقرّ الخبراء بأن الأعمال التي قد لا تنجم عنها أضراراً مادية جسيمة قد تصل كذلك إلى عتبة استخدام القوة. فمثلاً، وعلى وفق حكم نيكاراغوا، فإن تسليح أمركيا وتدريب قوات الكونترا لتقاتل الحكومة الشرعية في نيكاراغوا يُعد استخداماً غير مشروع للقوة. وبالقياص على الهجمات الإلكترونية، اتفق خبراء دليل تالين في نسخته الثانية على أن قيام إحدى الدول بمد قوات أو أفراد بأجهزة وتدريبهم عليها، لشن هجمات سيبرانية ضد دولة أخرى يُعد استخداماً غير مشروع للقوة. وعرف خبراء

1 Titiriga Remus, Cyber- 2013, P 179.

2 Michael N. Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, Iss, 37, No.

3, 1999, PP 914.915.

تالين التهديد باستخدام القوة بأنه "التهديد بالهجمات يشكل تهديداً غير مشروع للقوة، فمن الممكن أن يكون هذا التهديد استخداماً غير شرعي للقوة إذا حدث فعلاً" (١).

يرى الباحث: أن دليل تالين يشكل خطوة أساسية نحو تقنين الفضاء السيبراني واحتواء مخاطره ضمن الإطار القانوني الدولي، إلا أنه ما يزال بحاجة إلى تطوير وتوسيع ليواكب التطورات التكنولوجية المتسارعة وتعدد الفاعلين في هذا المجال، ولا سيما الجهات غير الحكومية التي تقوم بعمليات معقدة ومؤثرة. ويؤكد الباحث أن التحدي الأكبر لا يكمن فقط في تطوير القواعد القانونية، بل في إيجاد آليات تنفيذ فعالة تضمن مساءلة مرتكبي الهجمات السيبرانية، ولا سيما في ظل الطبيعة العابرة للحدود لهذه الهجمات، وصعوبة التحقق من الجهة الفاعلة بدقة.

الفرع الثاني

إعلان إيريتشي لمبدأ الاستقرار السيبراني والسلام السيبراني.

أعد فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي لعلماء (wfs) اعلان (إيريتشي) بغرض تعيين وترسيخ مبادئ الاستقرار السيبراني والسلام السيبراني، فقد اعتدت الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية للحلقات الدراسية الدولية المعنية بشأن الطوارئ العالمية، إيريتشي (صقلية) في العام ٢٠٠٩. وأكد الاعلان ضرورة تحقيق الاستقرار والسلام السيبراني، أنهما مرتبطا ارتباطاً وثيقاً، وامتاز الاعلان بإيجازه، وتركيزه الدقيق على المبادئ الآتية المحققة للاستقرار والسلام السيبراني:

١- على الحكومات جميعها أن تعترف بضمان القانون الدولي حرية المعلومة والفكر كذلك تنطبق هذه الضمانات على الفضاء السيبراني (٢).

٢- ينبغي أن تعمل جميع الدول على معاً بغرض تشريع مدونة مشتركة للسلوك أو الفعل السيبراني ضمن اطار قانوني عالمي منسق تتعلق بالتعاون بما يكفل احترام خصوصية الإنسان وحقوقه، واقتراح أمين عام الاتحاد الدولي للاتصالات يجب على الأمم عدم شن العدوان أو الهجوم السيبراني ضد أمة أخرى (عدم المبادأة) و ألا تمنح الارهابيين السبرانيين حماية في بلدانها.

١ عبد القادر مرزوق، مصدر سابق، ص ١٥.

٢ هاني محمد خليل الغزاوي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والاحصاء والتشريع، العدد ٥٤٩، القاهرة، مصر، ٢٠٢٣، ص ٥١٩ - ٥٢٠.

- ٣- على الدول والمنظمات حتى الأفراد تنفيذ برامج شاملة للأمن وتحديثها على وفق المعايير المطلوبة دولياً والاستخدام المتقدم لتكنولوجيا حماية الأمن والخصوصية.
- ٤- على مطوري ومحدثي البرامج والمعدات السعي والبحث عن طرق حديثة لتطوير تكنولوجيا آمنة تدعم قدرة التصدي والدفاع ومقاومة نقاط الضعف.
- ٥- أن تسهم الدول مساهمة فعالة في جهود الأمم المتحدة الهادفة إلى النهوض بالأمن والسلام السيبراني.^(١)

لما تقدم فإن ينبغي حث الخطى نحو السلام السيبراني، وذلك لما تظهره الجماعات أو الدول من قدرات هائلة للهجمات السيبرانية العدوانية، ووجه الاتحاد العالمي للعلماء الدول إلى العمل لأجل وضع قانون عالمي للفضاء السيبراني تحت رعاية الأمم المتحدة ولا سيما ما يستخدم منها في المجالات العسكرية والعدوانية للفضاء السيبراني إذ إن إثارة السؤال حول إمكانية إيجاد السلام في عالم رقمي في وقت تزداد فيه الهجمات الإلكترونية بشكل أكبر قوة وتعقيداً وخطورة، تجعل تعريف السلام السيبراني أكثر صعوبة للباحثين والمهتمين.^(٢)

ويرى الباحث: إن العالم يتجه بسرعة نحو الاتصال في كل مكان، الذي من شأنه أن يغيّر بشكل أكبر كيفية الحصول على المعلومات وجمعها ومشاركتها واستهلاكها. و إن البشرية تعيش اللحظة الأكثر تطوراً وحدثة في خط الزمن البشري، التي تبدو فيها البيانات المتصلة بالفضاء السيبراني أثمن من أي وقت مضى. وأنه في ظل هذا المشهد تجري جهود دولية متواضعة أو خجولة، ولنقل أقل بكثير من الاستراتيجيات الوطنية التي وضعتها دول متقدمة للتصدي لتهديدات الهجمات السيبرانية، ولتحسين الأمن وضمان السلام السيبراني. فدعت بعض البلدان والأطراف ذات العلاقة إلى وضع معاهدة للحد من استعمال الأسلحة السيبرانية، في حين أصرت دول أخرى على أن هذه المعاهدة غير ضرورية أو سابقة لأوانها بمبررات تتصل بالسادة الوطنية. في ظل التحديات المتزايدة التي تواجه العالم اليوم في مجال الأمن السيبراني، وبناءً على الإيمان بأهمية تعزيز الاستقرار والسلام السيبراني للحفاظ على الأمن الرقمي العالمي، و إطلاق مبدأ الاستقرار السيبراني والسلام السيبراني، إذ إن الأمن السيبراني أصبح

١ أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة البحوث الفقهية والقانونية، العدد الخامس والثلاثون، الجزء الثالث، مصر، ٢٠٢٠، ص ٥١٧.

٢ سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي، العدد ٧٩، القاهرة، مصر، ٢٠٢٣، ص ٨١-٨٢.

جزءاً لا يتجزأ من الأمن الدولي والسلام العالمي، وأن الاستقرار السيبراني يشكل ركيزة أساسية لتعزيز التعاون والتفاهم بين الدول والمجتمعات الدولية.

يتضمن مبدأ الاستقرار السيبراني والسلام السيبراني مجموعة من المبادئ الأساسية، التي تهدف إلى تحقيق الأمن السيبراني والحد من التوترات والصراعات السيبرانية، وتشجيع التعاون الدولي في مجال الأمن السيبراني، ومن هذه المبادئ:

١. احترام السيادة الوطنية الرقمية: تؤكد على حق كل دولة في تحديد وتطبيق سياسات الأمن السيبراني داخل حدودها الوطنية، ولنلتزم بعدم التدخل في شؤون الدول الأخرى في هذا الصدد.
٢. التعاون الدولي وتبادل المعلومات: نؤمن بأهمية تعزيز التعاون بين الدول في مجال مكافحة الجرائم السيبرانية، وتبادل المعلومات ذات الصلة، مع احترام حقوق الخصوصية والسرية.
٣. الوساطة وحل النزاعات السيبرانية بالطرق السلمية: ندعو إلى استخدام وسائل الحوار والتفاوض لحل النزاعات السيبرانية، مع تجنب التصعيد واستخدام القوة الرقمية.
٤. تعزيز الوعي والتثقيف السيبراني: نسعى إلى تعزيز الوعي بمخاطر الأمن السيبراني وتثقيف الجمهور بشأن السلوكيات الآمنة على الإنترنت، وكيفية التعامل مع التهديدات السيبرانية.
٥. تنمية القدرات الفنية والتقنية: نحث على تعزيز القدرات الفنية والتقنية للدول والمؤسسات لمواجهة التحديات السيبرانية وتعزيز الأمن الرقمي^(١).

نستخلص مما تقدم: أن إعلان أبريتشي يمثل أحد الجهود القانونية والسياسية الدولية الحديثة لمواجهة التحديات المتنامية للهجمات السيبرانية، وذلك من خلال التأكيد على مسؤولية الدول عن أفعالها في الفضاء السيبراني، ودعوتها إلى احترام قواعد القانون الدولي، لا سيما مبدأ السيادة وعدم التدخل في الشؤون الداخلية، ومبدأ حظر استخدام القوة. ويعد هذا الإعلان تطوراً نوعياً في إطار بناء سلوك دولي مسؤول في الفضاء السيبراني، ويؤكد على أهمية تعزيز الشفافية، وتبادل المعلومات، وبناء الثقة بين الدول، بهدف تجنب النزاعات السيبرانية والحد من آثارها. ويظهر الإعلان توجهاً دولياً متزايداً نحو إنشاء بيئة سيبرانية آمنة تقوم على مبادئ التعاون والالتزام بالقانون الدولي.

وعليه يرى الباحث: إن إعلان أبريتشي يمثل خطوة إيجابية نحو تنظيم السلوك الدولي في الفضاء السيبراني، إلا أنه ما يزال في نطاق المبادئ غير الملزمة، ما يحد من فاعليته في ردع أو محاسبة

١ إبراهيم السيد أحمد رمضان، مصدر سابق، ص ١٨١٣-١٨١٥.

الجهات المنفذة للهجمات السيبرانية، سواء كانت دولاً أم جهات غير حكومية. ويؤكد الباحث أن أهمية الإعلان تكمن في أنه يسهم في بلورة فهم مشترك بين الدول حول القواعد الواجب اتباعها في الفضاء السيبراني، لكنه بحاجة إلى دعم دولي أوسع، وتطوير آليات تنفيذية تضمن الامتثال والردع، ولا سيما في ظل غياب إطار قانوني ملزم يوازي الاتفاقيات الدولية الخاصة بالقانون الدولي الإنساني أو قانون النزاعات المسلحة.

وأن الهجمات السيبرانية تمثل تهديداً فعلياً للأمن الوطني والدولي، ومن ثم فإن الإعلان، وإن كان خطوة توجيهية، يجب أن يتطور إلى اتفاقية دولية ملزمة تنص على آليات الاستجابة، وتحدد مسؤوليات الدول، وتُعزز من الشفافية والرقابة التقنية والقانونية. و يدعو الباحث إلى ضرورة إشراك الدول النامية في هذه النقاشات، لتجنب فرض معايير تقنية أو قانونية لا تراعي خصوصياتها السيادية والتكنولوجية. أن إعلان أبرائتشي يشكل نواة مهمة يجب البناء عليها، مع ضرورة مراعاة التطور السريع في أدوات الهجمات السيبرانية وأساليبها، بما يضمن مواكبة التحديات المستقبلية بحلول قانونية وواقعية متوازنة.

المطلب الثاني

الجهود الدولية في مواجهة خطر الهجمات السيبرانية

تصاعد الاهتمام الدولي بالعلاقة بين الأمن والتكنولوجيا نتيجة بعدين مهمين أما الأول فيتعلق بالتقدم التكنولوجي والانتشار السريع لتكنولوجيا الاتصال والمعلومات عالمياً ودخولها في كافة مجالات الحياة، وفي عمل المرافق الحيوية من خلال تطبيقاتها المتعددة، وأما الثاني فيتعلق بإمكانية استخدام ذلك التقدم وما نتج عنه من أدوات وآليات جديدة كوسيلة وكوسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وذلك من جراء تخطيها للحدود السيادية للدول ما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعلين على تنوعاتهم المختلفة والذين ترأّسوا ما بين استخدام الدول إلى الفاعلين من غير الدول، وظهر ذلك في استخدام الفضاء الإلكتروني كساحة للحرب الباردة والحرب النفسية وحرب الأفكار أو من خلال استخدامه لشن الحروب والإرهاب بين الدول أو استخدام الأفراد أو الجماعات الإرهابية أو القراصنة أو الجريمة المنظمة وذلك على نحو يؤثر في الطبيعة المدنية أو السلمية للفضاء الإلكتروني. ومع تحول الفضاء الإلكتروني إلى مجال جديد للتفاعلات الدولية وهو ما جعل منه ساحة يُظف في الاستخدامات المدنية والعسكرية على حد سواء، وقد ظهرت الهجمات السيبرانية عبر نمطين الأول يتعلق بالقوة الناعمة في الصراع عبر الفضاء الإلكتروني باستخدام حروب الأفكار والعمليات النفسية. أما النمط الآخر فهو مرتبط بالقوة الصلبة باستخدام الفيروسات والهجمات الإلكترونية

كنشاط عدائي. وفي هذا السياق أصبح الفضاء الإلكتروني مجالاً للصراعات بين كل أنواع اللاعبين سواء من الدول أم من غير الدول. وتبلورت الحروب السيبرانية في خصائص مغايرة للحروب التقليدية، من حيث طبيعة الأنشطة والفواعل والانعكاسات علي بنية الأمن العالمي، وكذلك في فرص الاستجابة لتلك التهديدات الجديدة. فضلاً عن أن تلك الهجمات أصبحت تمثل تهديداً حرجاً لعمل منظمات المجتمع المدني والمدافعين عن حقوق الإنسان. ومن ثم تخضع تهديدات الأمن السيبراني في ضوء التطورات التكنولوجية الأخيرة وتحديات الأمن السيبراني لضوابط وقواعد القانون الدولي، إذ يُعد الأمن السيبراني من أهم الأسلحة الأساسية، التي تسعى الدول لامتلاكها وحمايتها من أي اختراق لضمان المعلومات العسكرية. و أنه على الرغم من تطور وسائل الحرب وأساليبها عما كانت عليه عند صياغة اتفاقيات جنيف عام ١٩٤٩، ولكن ما يزال القانون الدولي الإنساني مُطبّقاً على الأنشطة جميعها، التي تقوم بها الأطراف في أثناء النزاع المسلح وينبغي احترامه. ولا يمكن مع ذلك استبعاد حقيقة مؤداها أنه قد تكون ثمة حاجة إلى تطوير القانون لضمان توفيره الحماية الكافية للسكان المدنيين لمواكبة تطور التكنولوجيا السيبرانية أو كلما اتضح تأثيرها الإنساني بشكل أفضل. وينبغي للدول أن تقرر هذا الأمر بنفسها. وسنتناول في هذا المطلب الهجمات السيبرانية وأثرها على السلم والأمن الدولي من خلال فرعين نناقش في الفرع الأول موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية، ونناقش في الفرع الثاني قرارات المنظمات الدولية لمواجهة الهجمات السيبرانية.

الفرع الأول

موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية

القوة السيبرانية، مفهوم يتزايد في أهميته وتعقيداته بسرعة مع تطور التكنولوجيا الرقمية. وفي ظل هذا التطور المتسارع، تواجه المجتمع الدولي تحديات جديدة تتعلق بسلامة وأمان الأنظمة الإلكترونية والمعلوماتية، ومن ثم تأثيراتها على السلم والأمن الدوليين. تحت مظلة ميثاق الأمم المتحدة، الذي يُعد الهيكل الأساسي لتنظيم العلاقات الدولية، يتم التعامل مع هذه التحديات بموضوعية على وفق مجموعة من المبادئ والأسس^(١).

منح ميثاق الأمم المتحدة الصادر عام ١٩٤٥ وعلى وجه التحديد في نص المادة (٥١) الحق للدول في رد العدوان دفاعاً عن النفس، ل ابل قَد عُدَّ هذا الحق بأنه حق طبيعي لا يجوز حرمان الدولة التي

١ أميرة عبد العظيم محمد عبد الجواد، مصدر سابق، ص ٣٧٧.

تتعرض للعدوان منه أو حتى الانتقاص منه، وهذا الحق يمكن أن تتخذه الدولة للدفاع عن نفسها بمفردها أو تتخذه مجموعة من الدول يجمعها هدف معين وهذا ما يسمى بالدفاع الشرعي الجماعي. وإذا ما كان هذا الحق قد منح الدول الأعضاء في الميثاق الدولي، فإن واضعي النص قد وضعوا قيداً للحد منه، وهو أن لا يكون هناك تعسف في استعماله أو التجاوز في مده ليلحق ضرراً بالدولة الأخرى وشعبها، بل ينبغي أن يكون مبدأ التناسب والضرورة حاضرين بين فعل العدوان الحاصل على الدولة، وبين الدفاع من أجل صد الاعتداء أو الحد منه، على أنه فيما لو تم التجاوز فأن حق الدفاع الشرعي سينقلب إلى عدوان صارخ تتحقق بإزائه مسؤولية الدولة القائمة بالدفاع طبقاً لقواعد المسؤولية الدولية بنوعيتها المدنية والجنائية الفردية^(١).

أولاً: الهجمات السيبرانية وحق الدفاع الشرعي.

يكثّر التوجه العسكري نحو الاستفادة من البنية التحتية الإلكترونية المدنية، بغية المحافظة على جاهزية القوات وقدراتها العسكرية في ظل تقلص الميزانيات، إذ سيصير صعباً تحمل تكاليف صيانة شبكات إلكترونية مستقلة أو اقتناء تقنيات مُصممة -فقط- للاستخدامات العسكرية. إن هذا الأمر سيضع الدول أمام مفارقة صعبة. من جهة، ستسعى إلى حرمان خصومها من استغلال البنية التحتية الإلكترونية صاحبة الاستخدام المزدوج، ومن جهة أخرى، سوف ترغب في تأمين البنية التحتية الإلكترونية، التي يلجئ إليها مواطنوها وأنشطتهم المختلفة^(٢).

في إطار هذا التحليل، سنتناول مبدأ الضرورة العسكرية الذي يرتبط ارتباطاً وثيقاً بمبدأ التناسب. فالجيوش تخوض المعارك بناءً على خطط مُعدة ومُجازة من القيادات العسكرية العليا. لكن في بعض الظروف الطارئة التي قد تظهر في أثناء النزاع المسلح، وقد يُضطر القائد إلى اتخاذ وإصدار قرار فوري في أثناء وقت محدود، وقد يصطدم بضرورات عسكرية حربية قد تؤثر في قراره. هذه الضرورات قد تفرضها على القائد ظروف القتال ومتطلبات اتمام مهمته، فهل يمضي في تنفيذ قراره أم يمتنع عنه؟ لقد أباحَت اتفاقيات جنيف ذات الصلة اللجوء لاستخدام مثل هذه الضرورات الحربية التي قد تفرضها ظروف القتال، وجعلت منها مسوّغاً لبعض الانتهاكات لأحكامها. فقد نصت المواد (٥١) و(٥٠) و(١٧) من الاتفاقيات الأولى والثانية والثالثة والرابعة على التوالي على أن تدمير الممتلكات أو الاستيلاء عليها على نطاق

١ يُنظر: المادة (٥١) من ميثاق الأمم المتحدة.

٢ سفاح كريم، مصدر سابق، متاح على الرابط: <https://www.alnahrain.iq/post/1031> آخر زيارة بتاريخ.

واسع يُعد انتهاكاً جسيماً لهذه الاتفاقيات ما لم تبرره الضرورات الحربية.^(١) على الرغم من عدم وضوح مفهوم الضرورة بشكل كامل، إلا أنه حظي بأهمية كبرى في القانون عموماً وفي القانون الدولي الإنساني على وجه الخصوص. والهدف الأساسي هو تقدير هذه الضرورة حق قدرها، ومن ثم لا يجوز مطلقاً اتخاذها غطاءً لانتهاك قوانين وأعراف الحرب. فإذا استُخدمت بهذه الطريقة، فإنها تخرج عن نطاقها الصحيح. لذا، لا ينبغي مهاجمة الأهداف المدنية، سواء كانت مدناً يقطنها سكان أو ممتلكات مدنية، إذ لا ضرورة ملحة لفعل ذلك. ويُقصد بفكرة الضرورة هنا عدم تجاوز تخطي ضرورات ومقتضيات النزاع، أي: تحقيق النصر وإضعاف قدرة العدو بالوسائل والأساليب، التي لا تتعارض و أحكام قوانين الحرب، سواء كانت هذه الأحكام تستند إلى قواعد عرفية أو اتفاقيات دولية، وذلك في إطار حق الدولة في رد العدوان أو الحفاظ على وجودها^(٢).

استناداً إلى ما سبق، يُستنتج أن مبدأ الضرورة العسكرية يسمح بمهاجمة الأهداف العسكرية كخيار أساسي وأولي. ومع ذلك، فإنه ليس من المستبعد، كضرورة قصوى، أن تُهاجم الأعيان المدنية إذا ما كانت تسهم مباشرة في تحقيق المكاسب العسكرية الحاسمة. إن الافتقار لوجود معايير واضحة كي تنظم استخدام التكنولوجيا المعلوماتية للأغراض العسكرية الهجومية، قد يعني في أحيان كثيرة إلى إمكانية تبرير استخدام هذه الهجمات بذريعة الضرورة العسكرية، وهو ما اتضح في التصريحات المتبادلة بين أمريكا وروسيا.

وفيما يتعلق بمبدأ الضرورة العسكرية، بين دليل تالين أنه في الحالات التي تتواجد فيها أهداف عسكرية عديدة لتحقيق ميزة عسكرية مماثلة، ينبغي اختيار الهدف، الذي من المتوقع أن يلحق أقل قدر من الخطر بالمدنيين والأعيان المدنية للهجوم السيبراني^(٣).

١ مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص ١٠٥.

٢ أشرف عبد العزيز الزيات، المسؤولية الدولية لرؤساء الدول، ط١، دار النهضة العربية، القاهرة، مصر، ٢٠١٠ ص ٢.

٣ يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، جامعة القاهرة، كلية الحقوق، المجلد ٤، العدد ٤، القاهرة، مصر، ٢٠١٨، ص ٩٤.

من الأمور البديهية أن القائمين على إدارة نظام الهجمات السيبرانية الحديث يناون عن ميادين القتال الفعلية، ويعملون تحت قيادة مسؤولة تدخل ضمن تسلسل هرمي عسكري، ابتداءً من وضع خطة الهجوم وصولاً إلى إصدار الأمر وتنفيذه.

من هذا المنطلق، يثور السؤال الآتي: من الذي يُحمل المسؤولية الجنائية عن الانتهاكات الخطيرة لقوانين الحرب؟

إن البشر وحدهم هم المخاطبون بالقواعد القانونية، فمهما تطورت أدوات وأساليب القتال، يظل الإنسان المسؤول الأول والأخير عن توجيهها واستخدامها. دون النظر إلى مدى تطور الذكاء الاصطناعي في المستقبل، سيبقى هناك -أبداً- إنسان في نقطة البداية، فالإنسان يخاطبه القانون وحده، أما الآلة أو الوسيلة فهي لا تُخاطب. سابقاً، إن الدولة كانت وحدها تُساءل دولياً عن الجرائم، التي يقتربها الأفراد بصفتهن ممثلين سلطة الدولة. و نظراً لفضاعة الجرائم، التي يقتربها هؤلاء باسم الدولة ضد الإنسان وكرامته، وصار الشخص الطبيعي أحد أشخاص القانون الدولي الإنساني، له حقوق يتمتع بها، وعليه التزامات يتحملها، وفي مقدمتها المسؤولية الجنائية الدولية الفردية^(١). وعلى وفق هذا التطور، تُوجت الجهود الفقهية في أواخر القرن الماضي بإنشاء المحكمة الجنائية الدولية، التي أُنشئت على وجه الخصوص لتتظر في الجرائم التي يقتربها الأفراد الطبيعيون.

إن المقصود بالمسؤولية هنا هو مساءلة الرؤساء والقادة عن الأفعال التي تخالف قوانين الحرب بشكل عام واتفاقيات جنيف بشكل خاص. وقد قسم الفقه هذا النوع من المسؤولية على قسمين: مسؤولية القائد عن أفعال مرؤوسيه والمسؤولية الفردية، ووقد وردا بالتعاقب في المادتين (٢٥) و(٢٨) من نظام روما الأساسي للمحكمة الجنائية الدولية. وفيما يتعلق بالمسؤولية الجنائية الناتجة عن تعطيل وسائل الاتصال المدنية في أثناء نزاع مسلح، فإنها تخضع مبدئياً إلى الأحكام العامة للمسؤولية الجنائية والقانون الدولي الإنساني، الذي يهدف إلى تنظيم سلوك المقاتلين وتقييد وسائل وأساليب القتال. إلا أن إبرام اتفاقية دولية في هذا المجال مستقبلاً سيُفعّل المسؤولية الجنائية الفردية عن الدعم المقدم للجماعات المسلحة التي قد تستخدم الوسائل الإلكترونية لأهداف غير عسكرية موجهة ضد دول أخرى، سواء كان هذا الدعم يتمثل في التدريب أو التمويل^(٢).

١ حسن فياض، مصدر سابق، ص ٢٨.

٢ المصدر نفسه ، ص ٢٨-٢٩.

في رأينا، نظراً للدور المحوري المتزايد للأنشطة السيبرانية في تنظيم المجتمعات المعاصرة، فمن المرجح أن تخضع هذه الأنشطة للقانون من خلال إدراجها في اتفاقية خاصة تمنحها حماية أكبر لهذه المجتمعات. ستفرض هذه الاتفاقية التزامات على الدول بالتصرف بمسؤولية لحماية الفضاء السيبراني وتقليل النقطة، التي تنتهك عندها العمليات الإلكترونية الحظر المفروض على استخدام القوة، و ستسمح أيضاً للدول بالرد بقوة على بعض العمليات السيبرانية غير المدمرة، وتعزيز حماية البنية التحتية السيبرانية والبيانات والأنشطة خلال النزاعات المسلحة. من الواضح أن هذه التحولات ستكون مصحوبة بتكاليف، فقد تكون باهظة وتؤثر على الخصوصية وتمتد إلى العمليات الميدانية وتحرم القادة الميدانيين من بعض الخيارات المتاحة سابقاً. ومع ذلك، نعتقد أن الاتفاقية ستعكس في نهاية المطاف المصالح الوطنية، وستدرك الدول أنه من مصلحتها اتخاذ مثل هذه التدابير لحماية وصولها الآمن إلى الفضاء السيبراني والخدمات التي يوفرها.

ثانياً: الهجمات السيبرانية وحقوق الإنسان الرقمية

إن التزايد في لجوء الدول إلى استخدام الفضاء الإلكتروني لشن هجمات سيبرانية أثناء النزاعات المسلحة يضع مبادئ وقواعد القانون الدولي الإنساني أمام اختبار حقيقي ومعقد حول إمكانية تطبيقها على هذا النوع الجديد من الحروب. فالفترة التي شهدت تقنين قواعد قانونية تتعلق بوسائل وأساليب القتال، وخاصة اتفاقيات لاهاي للأعوام ١٨٩٩-١٩٠٧ واتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولان الإضافيان لعام ١٩٧٧، لم يكن للهجمات السيبرانية فيها وجود يُذكر عند إبرامها، مما يعني أنها لم تُنظم بأحكام خاصة من الناحية القانونية. وعلى ضوء أحكام قانون الحرب، كان تطور وسائل وأساليب قتال جديدة أمراً متوقعاً. فقد نصت المادة (٣٦) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف على ما يلي: «يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي، التي يلتزم بها ذلك الطرف السامي المتعاقد. ومن ثم، تضع هذه المادة الإطار العام المنظم لاستخدام وسائل وأساليب قتال جديدة في النزاعات المسلحة. وتوضح أحكام هذه المادة أنه على ضوء قانون الحرب، يتعين على الدول التي تفتي أسلحة حديثة أو تطورها أو تتبع أسلوب قتال جديد، أن تحدد مشروعية استخدامها. ويفيد هذا النص ضمناً بأن جميع قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النص

الخاص يطبق النص العام، هذا من حيث المبدأ.^(١) في المقابل، لا تحظر المادة (٣٦) من البروتوكول الإضافي الأول تطوير أو اقتناء أسلحة حديثة، أو حتى حيازة أسلحة أو اعتماد أساليب جديدة لا تنظمها قواعد القانون الدولي الإنساني. وعليه، فإن أحكام هذه المادة لا توقف حق الدول في ذلك، بل تنص على ضرورة إجراء مراجعة قانونية عند اقتناء أسلحة جديدة أو تطويرها أو اعتماد أسلوب حديث، وهو ما يُعرف بالمطابقة القانونية مع قواعد القانون الدولي، وذلك قبل استخدامها. ومن ثم، لا يُعد هذا النص قانوناً جديداً، ولكنه يضيف طابعاً رسمياً على القاعدة القانونية العرفية التي تلزم الدول بتطبيق المعاهدات أو القواعد العرفية بحسن نية، ويُقصد بذلك هنا بشكل خاص القواعد الدولية التي تنظم العمليات العدائية (٢).

واستناداً إلى مبادئ القانون الدولي الإنساني، يُعد شرط مارتنز وسيلة فعالة لمواكبة التطورات التقنية التي تشهدها وسائل وأساليب القتال. وقد ظهر هذا الشرط للمرة الأولى في اتفاقية لاهاي الثانية لعام ١٨٩٩، وينص على أنه "في الحالات التي لا تنطبق فيها معاهدة أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون الدولي المستمدة من العرف المستقر، ومن مبادئ الإنسانية، وما يمليه الضمير العام". وبالمقاييس على هذا المفهوم، أمكن تحريم الأسلحة التي يرفضها الضمير الإنساني (٣). تنير وسائل وأساليب القتال الحديثة تحديات قانونية وعملية فيما يتعلق بضمان استخدامها بما يتفق مع قواعد القانون الدولي الإنساني القائمة وإيلاء الاعتبار اللازم للتداعيات الإنسانية المحتملة الناجمة عن استخدامها. فحق أطراف النزاع في اختيار وسائل وأساليب الحرب هو حق مقيد بضرورة احترام مبادئ وقوانين وأعراف النزاعات المسلحة. ويحظر القانون الدولي الإنساني استخدام وسائل وأساليب الحرب التي تتسم بالعشوائية في تأثيرها أو التي تسبب ضرراً مفرطاً أو آلاماً لا ضرورة لها. وبناءً على ذلك، تشكل هذه المنظومة القانونية المذكورة القيود والحدود المفروضة على استخدام وسائل وأساليب الحرب

١ حسن فياض، مصدر سابق، ص ٢٨.

2 Tallinn Mnnual on The International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), PP.106. 107.

٣ أحمد علو، مقال منشور على موقع الجيش اللبناني، آذار ٢٠١٩، العدد ٤٠٥. الساعة: ٢:٣٠ صباحاً، بتاريخ

٢٠٢٤ / ١٢ / ٢٥. على الرابط <https://www.lebarmy.gov.lb/ar/content/>

(١). مع دخولنا حقبة هذا النمط المستجد من الحروب، يكمن الخطر المرتبط بوسائل وأساليب القتال الحديثة في غياب المواجهة المباشرة والتقدير الإنساني المصاحب لها. يجب أن تظل الأعمال العدائية ضمن الهدف المنشود من الحرب، وهو إخضاع قوات الخصم وإرغامها على الاستسلام. وعليه، ينبغي ألا تتجاوز الوسائل والأساليب المستخدمة هذا الغرض لتصل إلى أعمال وحشية. فالهجمات السيبرانية يمكن أن تستهدف القطاعات الاقتصادية والأمنية والزراعية والصناعية وغيرها ضمن سياق نزاع مسلح. وقد نجحت بالفعل عدة هجمات في الماضي في قطع إمدادات خدمات أساسية للسكان المدنيين، حيث طالت هذه الهجمات السيبرانية قطاع الخدمات الصحية المحمي بموجب القانون الدولي الإنساني، فضلاً عن الأعيان المدنية كالممتلكات الضرورية لبقاء السكان المدنيين على قيد الحياة، والأعيان التي تضم قوى خطرة وغيرها المحمية أيضاً بموجب قانون الحرب (٢). ونرى: لقد خصص القانون الدولي الإنساني مجموعة من القواعد التي ترمي إلى تقليل آثار النزاعات المسلحة، سواء كانت دولية أو غير دولية. ويتضمن هذا القانون مبادئ وقواعد أساسية تنظم اختيار وسائل وأساليب القتال. وقد نشأت مبادئ القانون الدولي الإنساني من فكرة مفادها أنها لا تحظر الأعمال القتالية في النزاعات المسلحة، بل وضعت لتقييد وسائل وأساليب القتال في هذه النزاعات. ولهذه الأسباب، هناك اعتراف بضرورة قبول مستوى معين من العنف والخسائر في الأرواح والدمار من جميع الأطراف المتحاربة كنتيجة طبيعية للقيام بالأعمال العدائية. وتمثل هذه المبادئ أبسط الأسس الإنسانية التي تسري في كل زمان ومكان، وتقدم الحلول باستقراء الحالات غير المتوقعة وتساهم في سد الثغرات القانونية. وبناءً على ذلك، يقوم القانون الدولي الإنساني على المبادئ التي تحكم سير العمليات العدائية، وهي: التمييز، والتناسب، والاحتياطات.

١ القانون الدولي الإنساني وتحديات النزاعات المعاصرة، مقال منشور بتاريخ ٢٠١٣/٢/٥ على موقع اللجنة الدولية للصليب الأحمر، على الرابط <https://www.icrc.org/ar/document/contemporary-challenges-ihl>. تاريخ الزيارة: الساعة ١٢:٠٠، ٢٠٢٤/١٢/٤.

٢ قانون النزاعات المسلحة: عناصر أساسية، مقال منشور بتاريخ ٢٠١٧/١٠/٢٣ على موقع اللجنة الدولية للصليب الأحمر، على الرابط <https://www.icrc.org/ar/document/law-armed-conflict-essentials>. تاريخ الزيارة: الساعة ١٢:٠٠، ٢٠٢٤/١٢/٤.

الفرع الثاني

قرارات المنظمات الدولية لمواجهة الهجمات السيبرانية

تعد الهجمات السيبرانية من بين أخطر التحديات، التي تواجهها المنظمات الدولية في العصر الحديث. فهذه الهجمات ليست مقتصرة على الأفراد أو الشركات فحسب، بل تمتد تأثيراتها لتطال الهياكل الحكومية والمنظمات الدولية، مما يجعلها تشكل تهديداً جسيماً على الاستقرار الأمني والاقتصادي للدول والمجتمعات على حد سواء. تعتمد المنظمات الدولية على شبكات الاتصال والتكنولوجيا المتطورة لتحقيق أهدافها وتنفيذ مهامها، وهذا يجعلها أكثر عرضة للهجمات السيبرانية، التي تستهدف تعطيل عملياتها أو سرقة معلومات حساسة. إن التصدي لتلك الهجمات يتطلب تبني استراتيجيات متطورة وفعالة، وتنسيق جهود متعددة المستويات بين الدول والمنظمات الدولية. وفي هذا السياق، قامت المنظمات الدولية باتخاذ مجموعة من القرارات واتخاذ الإجراءات اللازمة لمواجهة هذا التحدي الأمني الخطير. تُعد الأمم المتحدة واحدة من أبرز المنظمات الدولية، التي تضطلع بدور رئيسي في مجال مكافحة الهجمات السيبرانية. فقد أدرجت الأمم المتحدة قضية الأمن السيبراني ضمن أجندتها الدولية، واتخذت عدة مبادرات لتعزيز التعاون الدولي في هذا المجال، وأن من أهم الجهود الدولية قرارات الأمم المتحدة المتنوعة لمنع ومكافحة الجرائم السيبرانية، كذلك مجهود الاتحاد الدولي للاتصالات بخصوص تطوير الاتصالات السلكية واللاسلكية، وأن أهم المبادرات تقدماً لتنظيم شبكة الانترنت الدولية ومكافحة الجرائم السيبرانية هي اتفاقية بودابست بخصوص الجرائم السيبرانية والاتصالات، وسنبحث أهم هذه المبادرات كما يأتي:^(١)

أولاً: قرارات الأمم المتحدة.

إن قرارات الأمم المتحدة بشأن الأمن السيبراني تمثل جزءاً حيوياً من جهود المجتمع الدولي لمواجهة التحديات المتعلقة بالتكنولوجيا الرقمية والتهديدات المتزايدة المرتبطة بها. تتعامل هذه القرارات مع مجموعة متنوعة من القضايا، التي تشمل الأمن السيبراني، مثل حماية البيانات، والتعاون الدولي لمكافحة الجريمة السيبرانية، وضمان الاستقرار السيبراني العالمي، وتعزيز القدرة على التحمل السيبراني

١- قرارات الجمعية العامة للأمم المتحدة:

إن من أهم قرارات الجمعية العامة في هذا الخصوص هو القرار الصادر عن الجمعية العامة في ٢٠/كانون الأول/ديسمبر من العام ٢٠٠٢ المرقم (٥٧/٢٣٩) المعني بإرساء ثقافة عالمية للأمن

١ أميرة عبد العظيم محمد عبد الجواد، مصدر سابق، ص ٤٨٢.

السيبراني، إذ إنها اعتمدت فيها قراراً بخصوص الأمن السيبراني، الذي أكد فيه على ضرورة دعم الجهود الوطنية لتبادل المعلومات والتعاون الوطني والدولي، ليتسنى التصدي لهذه الهجمات السيبرانية لما فيها من خطورة متزايدة عابرة لحدود الأوطان. وإن أهم ما جاء في القرار عدّة أن للبنية الأساسية للمعلومات مسؤولية تلقى على عاتق الحكومات فينبغي عليها أن تتصدر فيه وطنياً منسقةً مع ذوي الشأن من أصحاب المصلحة. كذلك القرار الصادر عن الجمعية العامة للأمم المتحدة في ٣٠ كانون الثاني/يناير من العام ٢٠٠٤ الذي عُنيَ بتدريس ثقافة عالمية للأمن السيبرانية حماية وصون البنى التحتية للمعلومات. وأيضاً ما جاء في القرارين الصادرين عن الجمعية العامة للأمم المتحدة القرار (٥٥/٦٣)، والقرار (٥٦/١٢٠)، الذين حددا الوضع والقانوني بخصوص مكافحة إساءة استخدام التكنولوجيا المعلوماتية لغيات إجرامية. كذلك القرار الذي أصدرته الجمعية العامة في كانون الأول/يناير من العام ٢٠١١ المرقم (٦٥/٤١) والتي صادقت فيه على التقرير الذي جاء عن فريق الخبراء الحكوميين في شأن المعلومات السلكية واللاسلكية في سياق الأمن الدولي. وما توصل إليه الخبراء أن هناك دولاً قد تستحدث وتطور تكنولوجيا المعلومات والاتصالات بغية استخدامها كوسائل حربية واستخبارية، و أن اللجنة الدولي نبهت الدول على ما ستخلفه الحرب السيبرانية من عواقب وخيمة، كمهاجمة شبكات الحاسوب في أثناء قيام النزاع المسلح، ومن عواقبها التشويش على أنظمة مراقبة ومتابعة الملاحة الجوية، وكذلك ما تسببه من تصادم أو تحطم الطائرات، أو قطع امدادات الكهرباء والماء على السكان المدنيين أو الحاق أضرار بالمرافق الكيميائية وحتى النووية. وتذكّر لجنة الخبراء الدولية أطراف النزاعات المسلحة بضرورة احترام قواعد القانون الدولي الإنساني، إذا ما استخدمت وسائل الحرب السيبرانية، ومن أمثال هذه القاعدة، مبدأ التمييز ومبدأ التناسب ومبدأ الاحتياط^(١) وأصدرت الجمعية العامة للأمم المتحدة قرارات عديدة بهذا الشأن منها قرارها الصادر في ٤ كانون الأول/ديسمبر ١٩٩٨ المرقم (٥٣/٧٠) وقرارها في ١ كانون الأول/ديسمبر في العام ١٩٩٩ الرقم (٥٤/٤٩) وقرارها الصادر في ٢٠ تشرين الثاني/نوفمبر ٢٠٠٠ المرقم (٥٥/٢٨) والقرار الصادر في ٢٩ تشرين الثاني/نوفمبر من العام ٢٠٠١ المرقم (٥٦/١٩) و القرار المرقم (٥٧/٥٣) الثاني من نوفمبر من العام ٢٠٠٢ والقرار (٥٨/٢٣) في ١٨ كانون الأول/ديسمبر من العام ٢٠٠٣ بخصوص التطورات في ميادين المعلومات والاتصالات في سياقات الأمن السيبراني. والقرارات

١ بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة، ٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال فيما يتعلق بنزع السلاح والأمن، الدورة ٦٦، اللجنة الأولى، البنود ٨٧ و ١٠٦ من جدول الأعمال، بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ تشرين الأول/أكتوبر ٢٠١١.

(٥٥/٦٣) ٤ كانون الأول/ ديسمبر من العام ٢٠٠٠ و القرار (٥٦/٢١) في ١٩ كانون الأول/ ديسمبر من العام ٢٠٠١ المعني بمكافحة الجريمة في اطار استخدام نظام المعلومات الادارية لتقنية المعلومات ودعا القرار أعضاء الأمم المتحدة لأن تضع تشريعات وطنية تكافح فيه اساءة استعمال تكنولوجيا المعلومات، ودعت الجمعية العامة في مختلف قراراتها الدول الأعضاء إلى ارساء ثقافة عالمية للأمن السيبرانية وحماية البنى التحتية للمعلومات وتشريع القوانين الوطنية لمكافحة اساء استخدام تكنولوجيا المعلومات، التي غالباً تكون قرارات الجمعية العامة للأمم المتحدة في الخصوص مماثلة لقرارات الاتحاد الدولي للاتصالات.^(١)

٢. قرارات المجلس الاقتصادي والاجتماعي لمواجهة الهجمات السبرانية

يتطلب التعاون الدولي جهوداً مشتركة لمكافحة الجريمة السيبرانية، وقد صدر عن المجلس الاقتصادي والاجتماعي قرارات عديدة داعية الدول للتعاون فيما بينها في مجال تبادل المعلومات السيبرانية وتقديم المساعدة الفنية والقانونية لمحاسبة المتورطين في الأنشطة السيبرانية غير القانونية، من هذه القرارات القرار (٢٠٠٦/٤٦) وقرار (٢٠٠٧/٨)، وقرار (٢٠٠٨/٣)، وكذلك قرار (٢٠٠٩/٧) والتي أحطت به علماً لجنة تسخير العلم والتكنولوجيا لأغراض التنمية بنتائج تنفيذ مؤتمر القمة العالمي لمجتمع المعلومات استناداً ما وصله من مساهمات قام بها كيانات الأمم المتحدة ذات الصلة بحسب اقتضاء الحاجة، زيادة على ذلك فإن المجلس الاقتصادي شرعت أقام دورته في العام ٢٠١٠ ضمن جلسة اعلامية خصه فيها التحديات التي تعنى بالأمن السيبراني فضلاً عن تهديدات، التي تصدر من خلال استخدام الانترنت الذي بات يتسع استخدامه^(٢).

وأكد المجلس مشدداً على أمور عديدة منها ضرورة اتخاذ مبادرات دولية تكفل وتسهل تبادل المعلومات والتدريب وأفضل الممارسات والبحث. قد أعلن المشاركون في الدورة يجب على الأمم المتحدة توحيد أدائها بخصوص هذا المسألة، ما يساهم بزيادة التعاون بين الدول والقطاعات الخاصة والبلدان فيما بينها لضمان الأمن السيبراني. ويدعو القرار إلى اتباع نهج قائم على ادراك المخاطر بحيث يعي جميع

١ بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة، مصدر سابق، البندان ٨٧ و ١٠٦.

٢ المجلس الاقتصادي والاجتماعي، الدورة الموضوعية ٢٠١٠، نيويورك، البند ١٣ (ب) من جدول الأعمال المؤقت والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي ومجتمع المعلومات على الصعيدين الإقليمي والدولي.

الأطراف هذه المخاطر ذات الصلة والتدابير الوقائية والردود على نحو مناسب^(١). وحذروا من نشوب حرب سيبرانية فعلية ذات عظمة ستحدث بشكل كبير ما لم يُتدارك الأمر، ولا بد أن تقابل هذه الدعوات باستجابة تنسيقية بين الدول، إذ لا تفي بالغرض الآن استراتيجيات اعتماد حلول على أساس مخصصة ومحددة تقوية الدفاع.

ثانياً: الاتحاد الدولي للاتصالات

لمعالجة مخاطر الأمن السيبراني المتنامية أنشأ الاتحاد الدولي فريقاً معنياً بالشبكات الذكية، لأجل توثيق وجمع المعلومات والمفاهيم، التي من الممكن ان تكون مفيدة لأجل اعداد توصيات تدعم الشبكات من منظور الاتصالات، و أن أحد الأدوار المهمة التي أنيط بها إلى الاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين والمفوضين لعام ٢٠٠٦ المتمثل ببناء الأمن والثقة باستخدام تكنولوجيا المعلومات والاتصالات. إذ قامت الدول بتكليف الاتحاد بأن يتخذ خطوات ملموسة واضحة لتقيص التهديدات والحد منها وانعدام الامن فيما يخص مجتمع المعلومات. أطلق الاتحاد في مايو ٢٠٠٧ برنامج عبر أمنيته خاص بالأمن السيبراني العالمي (g c o) لتوفير اطار يُمكن أصحاب المصلحة من تنسيق استجابة دولية للتحديات المتنامية التي يطرحها الأمن السيبراني. إذ يقوم البرنامج على التعاون الدولي الذي يهدف إلى مشاركة جمع المعنيين عبر جهود متضافرة بغية بناء الأمن والثقة ضمن مجتمع المعلومات. واقترح أمين الاتحاد مبادئ خمسة توجيهية غايتها حفظ السلام واحلاله دائماً، إذ إنه أدرك الخطر المتنامي للهجمات السيبرانية وأعدت لوائح تخص الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا، التي ترافق عالم الاتصالات الحديث، الذي تجسد في ثمانينيات القرن المنصرم^(٢). وأعدت اللوائح هذه بغية تعزيز الكفاءة والتنمية الدوليين، زيادة على أنها تظهر تركيز الاتحاد في حقه بحماية الاتصال، وفي الوقت ذاته يدري الضرر عن المستخدم، وقد تضمنت المبادئ الخمسة المقترحة من قبل الأمين فيما يتعلق بالأمن السيبراني مع تخصيص اجراءات والتزامات معينة أن تضمن السلام والاستقرار للفضاء السيبراني، ونصت هذه المبادئ على: ^(٣).

١ أميرة عبد العظيم محمد عبد الجواد، مصدر سابق، ص ٤٨٦ - ٤٨٧.

٢ لوائح الاتصالات الدولية: الوثائق الختامية للمؤتمر الإداري العالمي للبرق والهاتف، الاتحاد الدولي للاتصالات. الزيارة الساعة: ٥:٣٩. ٢٠٢٤/٥/٩ على الرابط <https://www.itu.int/osg/spu/intset/>

٣ قرارات المؤتمر العالمي لتنمية الاتصالات، ٢٠١٧ (17wtcd) مؤتمر المندوبين المفوضين (18-pp) دبي، الامارات، اكتوبر - نوفمبر، ٢٠١٨، الاتحاد الدولي للاتصالات.

- ١- على الحكومات أن تتيح نفاذ شعوبها إلى الاتصالات.
 - ٢- أن تلتزم الحكومات بتوفير الحماية في الفضاء السيبراني لشعوبها.
 - ٣- ينبغي على البلدان الالتزام بعدم ايواء الارهابيين/ المجرمين في أراضيهم.
 - ٤- على البلدان الالتزام بأن لا يكون الطرف البادئ بشن الهجوم السيبراني على غيره من الدول.
 - ٥- على الدول الالتزام بالتعاون مع غيره من الدول على ضمان الأمان في الفضاء السيبراني.
- وغاية البرنامج هذا تعزيز الثقة والأمن في مجتمع المعلومات، وقد جاء لتحقيق التعاون المشترك والكفاءة والتشجيع على التنسيق بين المعنيين. و أن هذا البرنامج هو الأول عالمياً بين أصحاب المصلحة، وأيضاً بين القطاع العام والقطاع الخاص لمكافحة التهديدات والمخاطر السيبرانية. وقع الاتحاد الدولي للاتصالات والشراسة الدولية المتعددة الأطراف مذكرة في العام ٢٠٠٨ لمكافحة التهديدات السيبرانية (إمباكت) (impact) وأصبح مقرها في شراسة (إمباكت في سايبير جايا بماليزيا)، الذي ضم أحدث ما توصلت إليه التكنولوجيا، المقر الفعلي للبرنامج^(١).

ثالثاً: اتفاقيات بودابست لمواجهة الجرائم السيبرانية والاتصالات لسنة ٢٠٠١.

إن اتفاقية مجلس أوروبا بخصوص الجرائم الإلكترونية، التي عرفت باسم اتفاقية بودابست، هي وثيقة دولية ملزمة تعمل كإطار عمل للتعاون الدولي بين الدول الأطراف في هذه المعاهدة. وعمل مجلس أوروبا على صياغة بروتوكول ملحق وإضافي ثاني للاتفاقية ليعالج تعزيز التعاون والكشف عن الأدلة الإلكترونية. ضمت أحدث نسخة لمسودة البروتوكول الإضافي الثاني أحكام تعلق ببيانات تسجيل اسم النطاق. ظهرت هذه النسخ لأول مرة في نسخة نوفمبر/ تشرين الثاني ٢٠٢٠ للبروتوكول، و أكدت في نسخة أبريل / نيسان ٢٠٢١، التي وافقت من خلالها اللجنة العامة لصياغة البروتوكول لمجلس أوروبا على استعمالها في المشاورات مع الهيئات ذات الصلة لمجلس أوروبا وأصحاب المصلحة^(٢).

منذ عام 1978 و ١٩٩٦ اتخذ المجلس الأوروبي الطابع الدولي للجرائم السيبرانية، وقد أنشأت اللجنة الأوروبية لمشاكلات الجرائم (cdpc) لجنة خبراء لتتعامل مع جرائم السيبرانية، فقد عملت اللجنة بين العاميين (١٩٩٧-٢٠٠٠) على ما اعتمده البرلمان الأوروبي من مشروع اتفاقية في الجزء الثاني في

١ أميرة عبد العظيم محمد عبد الجواد، مصدر سابق، ص ٤٩٢-٤٩٥.

٢ إيلينا بليكسيديا، التعليق على البروتوكول الإضافي الثاني لاتفاقية الجريمة الإلكترونية، ٢٣ أبريل، ٢٠٢١، مقال منشور

على الرابط [https://www.icann.org/ar/blogs/details/feedback-on-the-second-additional-](https://www.icann.org/ar/blogs/details/feedback-on-the-second-additional-protocol-to-the-convention-on-cybercrime-ends-early-may-23-4-2021-ar)

[protocol-to-the-convention-on-cybercrime-ends-early-may-23-4-2021-ar](https://www.icann.org/ar/blogs/details/feedback-on-the-second-additional-protocol-to-the-convention-on-cybercrime-ends-early-may-23-4-2021-ar)

جلسته العامة في نيسان ٢٠٠١ وصدقت الاتفاقية ٣٠ في العام ٢٠١٠. وتضمنت الاتفاقية العمل المشترك بين الدول الأعضاء، وأعضاء القطاعات وذوي المصلحة، لبناء ثقافة للأمن السيبرانية والمحافظة عليها، وإيجاد السبل لمكافحة الجريمة السيبرانية، وتقرر ما يأتي:

١- المواصلة في جعل أنشطة الأمن السيبراني في مقدمة أنشطة الاتحاد ذات الأولوية، والاستمرار في اطار مجالاته واختصاصاته الأساسية من خلال دراسة كيفية فرض الأمن وإيجاده وبناء الثقة في استعمالات الاتصال، عبر ترسيخ الوعي وتطوير مواد التدريب المناسبة لتعزيز ثقافة الأمن السيبراني.

٢- العمل على تعزيز العمل والتعاون وتبادل المعلومات مع كافة المنظمات الدولية والاقليمية فيما يخص المبادرات المتعلقة بالأمن السيبراني في سياق اختصاصاتها، مع أن تُرعى احتياجات البلدان النامية وما تحتاجه.

٣- تعين وتوفير أنظمة سريعة وفعال للتعاون الدولي، والمحافظة بشكل سريع ومتقدم على البيانات والمعلومات المحفوظة أو المخزنة على الحاسوب. ودخلت اتفاقية بودابست حيز التنفيذ في العام ٢٠٠٤، وتُعد خطوة سباقة ومهمة للتعاون على المستوى الدولي من أجل وضع اطار عالمي للتعاون الدولي لمواجهة ومكافحة الهجمات المتصلة بالفضاء السيبراني، وقد سمحت الاتفاقية للدول جميعها بالانضمام إليه ولم تقصر حق الانضمام على الدول الأوروبية (١).

نرى: إن تشكيل اتفاقية بودابست لمكافحة الجريمة السيبرانية، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة حتى اليوم، من حيث حجم الدول المنظمة اليها، وترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية، تلتزم الدول المنظمة بإدراجها في قوانينها الوطنية، مثل تلك الخاصة بجمع بيانات الاتصال وحفظها، بما يتيح تحديد مصدرها، وصلاحيات الجهات القضائية المعنية، والمساعدة المتبادلة وتسليم المجرمين.

يتضح مما تقدم: أن المجتمع الدولي بات يُدرك حجم التهديدات التي تفرضها الهجمات السيبرانية على الأمن والسلم الدوليين، وعلى سيادة الدول واستقرارها الداخلي. وقد تعددت الجهود الدولية لمواجهة هذه التحديات، سواء على صعيد الأمم المتحدة من خلال مجموعة الخبراء الحكوميين (GGE) ومجموعة العمل المفتوحة العضوية (OEWG)، أو عبر المبادرات الإقليمية والثنائية التي تهدف إلى وضع قواعد

١ أميرة عبد العظيم محمد عبد الجواد، مصدر سابق، ص ٤٩٦ - ٤٩٨.

سلوك طوعي، وتعزيز بناء القدرات، وتبادل المعلومات، وبناء الثقة بين الدول. وأدت منظمات دولية مثل الاتحاد الأوروبي، ومنظمة حلف الناتو، ومنظمة التعاون الاقتصادي والتنمية (OECD)، دوراً مهماً في صياغة سياسات واستراتيجيات دفاعية ضد الهجمات السيبرانية. وعلى الرغم من هذه الجهود، ما يزال هناك فراغ قانوني وتشريعي في مجال تنظيم الفضاء السيبراني على المستوى الدولي، لاسيما في ظل غياب اتفاقية شاملة وملزمة تنظم استخدام القوة السيبرانية، وتحدد مسؤوليات الدول والجهات الفاعلة من غير الدول

عليه يرى الباحث: أن الجهود الدولية الحالية في مواجهة الهجمات السيبرانية تمثل خطوات مهمة نحو بناء منظومة دولية مسؤولة في الفضاء السيبراني، إلا أن هذه الجهود ما تزال تعاني من التشتت وغياب التنسيق الشامل، فضلاً عن افتقارها إلى قوة الإلزام القانونية. وأن أغلب المبادرات القائمة، ومنها مبادرات الأمم المتحدة، تُعد توجيهية أو استشارية، ولا ترتقي إلى مستوى اتفاقيات دولية ملزمة، مما يحد من فاعليتها في الحد من تصاعد الهجمات السيبرانية، سواء تلك التي تنفذها دول أم جهات غير حكومية. وأن غياب التوافق الدولي حول تعريف الهجوم السيبراني، وحدود الاستخدام المشروع للقوة السيبرانية، وآليات المساءلة والعقاب، يمثل تحدياً رئيسياً أمام تحقيق نظام دولي عادل ومنظم في هذا المجال. ويخلص الباحث إلى أن التحديات السيبرانية تفرض ضرورة التحرك الجماعي العاجل نحو بناء منظومة قانونية دولية متكاملة، تستند إلى مبادئ القانون الدولي، وتراعي التوازن بين الأمن وحقوق الإنسان في العصر الرقمي.

وفي ختام الفصل يمكن القول: انه بازدياد تبادل المعلومات واعتمادنا المتزايد على التكنولوجيا الرقمية، و أصبحت الهجمات السيبرانية تمثل تهديداً متزايداً الخطورة على الصعيدين الفردي والمؤسساتي. تترأوح أهداف هذه الهجمات من سرقة البيانات الشخصية إلى التجسس الصناعي والتأثير على البنية التحتية الحيوية. يُظهر هذا التحدي المتزايد ضرورة تعزيز الوعي بالأمن السيبراني وتنفيذ استراتيجيات دفاعية فعالة. على الرغم من الجهود المبذولة لمكافحة الهجمات السيبرانية، فإن التحديات تبقى مستمرة وتطور بسرعة. لذا، يتعين علينا التفكير بشكل إبداعي واعتماد نهج شامل لحماية أنظمتنا وبنية تحتيتنا الرقمية. يجب أن تتضمن هذه الجهود التوعية المستمرة، والاستثمار في التكنولوجيا الحديثة، وتعزيز التعاون الدولي لمواجهة التهديدات السيبرانية المتزايدة. وكون الأمان السيبراني تحدياً عابراً للحدود، يجب أن نعمل معاً كمجتمع دولي لتعزيز الحماية السيبرانية وضمان استدامة وأمان البيئة الرقمية. إن التزامنا بتعزيز الأمن السيبراني لن يحمي فقط الأفراد والمؤسسات، بل سيعزز أيضاً التنمية الاقتصادية

والاجتماعية والثقافية في جميع أنحاء العالم. في النهاية، يتطلب التصدي للهجمات السيبرانية تضافر الجهود والتعاون الشامل بين الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية. إن الاستثمار في الأمن السيبراني يعد استثمارًا حيويًا للحفاظ على استقرار وأزدهاره في القرن الحادي والعشرين.

الفصل الثاني

حماية المناطق المحمية من الهجمات السيبرانية

شهد المجتمع الدولي خلال السنوات الماضية انتشاراً واسعاً لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية، التي أحدثت ثورة في حياتنا، مما سهل الوصول للبيانات وللمعلومات، واعتماد العديد من الخدمات والبنى التحتية الأساسية عليها، وبذلك شهد المجتمع الدولي تطوراً هائلاً في المعلومات، وتحكم مهم في الأشياء المادية مثل المحولات الكهربائية والقطارات والمستشفيات والرادارات والمعاملات التجارية وأسواق الأوراق المالية.

وعلى الرغم من التطور الهائل لثورة المعلومات، إلا أنها في ذات الوقت جعلت المجتمع الدولي يواجه مخاطر جديدة مرتبطة بهذا التطور، فقد برز الفضاء أو المجال السيبراني كمجال خامس للحرب، إلى جانب البر والبحر والجو، وأبرز ما يميز هذا المجال كوسيلة لاستخدام القوة أو انطلاق الهجمات منه هو أنه غير محسوس وغير حركي، إذ إن استخدام هذا المجال من أجل إحداث خلل سواء بشكله الوظيفي، التركيبي لا يتطلب نقلاً لقطع عسكرية من مكان إلى مكان آخر، فضلاً عن ذلك فإنه من غير الممكن التنبؤ بالموعد، التي سيستخدم فيها هذا المجال من أجل إحداث ذلك الخلل .

وظهرت الهجمات السيبرانية نتيجة ضعف في طبيعة شبكة المعلومات وقابليتها للاختراق بسبب الاعتماد المفرط على برامج الحماية المقدمة للجهاز، وعدم تغيير كلمات المرور، وتجاهل التحديثات والاتصالات العشوائية، فضلاً عن ذلك طمع الكثير من الدول الكبرى لاستخدام الهجمات السيبرانية إلى جانب الهجمات العسكرية الحركية لزيادة تداعيات العمليات العسكرية على الخصم، ليس هذا فقط بل يؤدي غموض تحديد هوية مرتكب الهجوم السيبراني إلى رغبة الدول في اعتماد الهجمات السيبرانية.

وظهرت نتيجة لذلك المخاوف الإنسانية بشكل واضح، فالهجمات لا تقتصر آثارها هذه على البيانات في أجهزة الكمبيوتر، أو أنظمة الكمبيوتر بل تهدف إلى خلق تأثير في العالم الحقيقي، ويكون المدنيين هم الضحايا الرئيسيين لمثل هذه الهجمات، وأبرز قانون دولي يسعى إلى حماية المدنيين من ويلات النزاعات المسلحة والهجمات العدائية على وجه الخصوص هو القانون الدولي الإنساني، مع الإقرار بخطورة هذه الهجمات واعتبار الفضاء السيبراني. وسنبحث هذا الموضوع عبر بحثين، نتناول في المبحث الأول: المبادئ الدولية المنظمة للمناطق المحمية في القانون الدولي الإنساني وفي المبحث الثاني: آثار الهجمات السيبرانية على المناطق المحمية

المبحث الأول

المبادئ الدولية المُنظمة للمناطق المحمية في القانون الدولي الإنساني

لا تقتصر الهجمات السيبرانية آثارها على البيانات في أجهزة الكمبيوتر أو أنظمتها، أنماً تتخطى ذلك لتقوم بالتأثير بشكل مباشر باختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية، وتعطيل عمل محطات الطاقة النووية والعديد من التأثيرات، التي قد تؤدي إلى وقوع حوادث كارثية.

وبخلاف الهجمات العسكرية التقليدية، التي تتم في الميدان المادي، تشن الهجمات السيبرانية في ميدان افتراضي على شبكة الإنترنت مع ما تتميز به من استخدام مزدوج عسكري ومدني، يكون المدنيين والأفراد هم المستهدفون الرئيسيون لهذه الهجمات، وبما أن القانون الدولي الإنساني يسعى لحماية المدنيين، فإنه يسعى لتوفير الحماية القانونية للمدنيين والأعيان المدنية من مختلف الانتهاكات والاعتداءات التي قد يتعرضون لها في النزاعات المسلحة، ومن أهم مبادئ إنشاء مناطق محمية في أثناء النزاعات المسلحة لا تمتد إليها العمليات العسكرية، وتكون بعيدة عنها، وتعد ضمان أساسي لحماية الأشخاص والأعيان المتواجدين داخلها من ضحايا الحروب والهجمات العسكرية، وضمن لعدم تعرضهم للقتل والاعتداء. وقد حرصت اتفاقيات القانون الدولي الإنساني، ولا سيما اتفاقيات جنيف الأربع لعام (١٩٤٩) والبروتوكولان الملحقان به لعام (١٩٧٧) لوضع مجموعة من المبادئ، التي تضمن احترام وتعزيز الحماية للأعيان والممتلكات ذات الطابع المدني في أثناء النزاع المسلح. سنبين في هذا المبحث المبادئ الدولية للمناطق المحمية في القانون الدولي الإنساني من خلال مطلبين إذ سنبحث في المطلب الأول: إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية، وفي المطلب الثاني: تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية.

المطلب الأول

تطبيق احكام القانون الدولي الإنساني على الهجمات السيبرانية

إن الاستخدام المتكرر للهجمات السيبرانية في سياق النزاعات المسلحة أو خارج سياقها، جعل القانون الدولي الإنساني أمام اختبار يدور حول مدى إمكانية تطبيق تلك القواعد الدولية عليها، لذلك سعى الخبراء القانونيين لبحث مدى إمكانية تطبيقه على الهجمات السيبرانية، وعند التعمق بقواعد القانون الدولي الإنساني نجد ويشكل واضح إلى أنه تم تبني التطورات الحديثة، التي قد تحدث في وسائل وأساليب القتال في المستقبل، وإن لأشكال الحديثة للهجمات السيبرانية، التي لم تُضمّن في

استخدامات الأسلحة التقليدية في الاتفاقيات الدولية، ترتبط بالقانون الدولي الإنساني وتخضع له كأى سلاح جديد عندما يُستخدم في أثناء النزاع المسلح.

انطلاقاً من هذا، تعد قواعد القانون الدولي الإنساني التي تطبق على الأهداف العسكرية المشروعة، أغلبها أصبحت قواعد عرفية ومعترف بها من قبل الدول. ومن ثم إمكانية تطبيقها على الهجمات السيبرانية. سنبحث هذا الموضوع عبر فرعين في الفرع الأول مبادئ القانون الدولي الإنساني وحظر الهجمات العشوائية، أما الفرع الثاني فسنحدث عن معايير تحديد الأهداف العسكرية المشروعة في أثناء الهجمات السيبرانية في القانون الدولي الإنساني.

الفرع الأول

حظر الهجمات السيبرانية ووقف احكام مبادئ القانون الدولي الانساني

ينطبق القانون الدولي الإنساني بمبادئه وقواعده بصفة عامة على أي نزاع مسلح بما فيها الهجمات السيبرانية، ويعد شرط (مارتينز) من المبادئ الراسخة في القانون الدولي الإنساني، الذي ينص صراحة على أنه "عند وجود حالة لا تغطيها اتفاقية دولية يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة، ومن مبادئ الإنسانية، وما يمليه الضمير العام"^(١). جاء في تقرير اللجنة الدولية للصليب الأحمر عام (٢٠١١) ينبغي أن يتوافق توظيف الهجمات السيبرانية في إطار النزاع المسلح مع جميع مبادئ القانون الدولي الإنساني وقواعده. وما يؤيد ذلك ما أشارت إليه محكمة العدل الدولية: إن مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تتكيف على جميع أنواع النزاعات وكذلك على كل الأسلحة ومن ضمنها الأسلحة المستقبلية. لذا فإن تطبيق مبادئ القانون الدولي الإنساني في الهجمات السيبرانية ممكناً على الرغم من أنها سلاح جديد^(٢).

١ مايكل ن، شميث، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص ٩٠.

٢ اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، ٢٠١١، ص ٥.

وبهدف معرفة أبعاد المسؤولية الدولية، التي تنشأ عن الهجمات السيبرانية سنقوم بالبحث في مفهوم المسؤولية الدولية في ظل السلوكيات الدولية الراهنة مثل قرارات المحاكم الدولية إلى جانب معتقدات وآراء كبار الفقهاء القانونيين المختصين بالقانون الدولي العام بخصوصها.^(١)

إن قضية المسؤولية الدولية قد تعرضت إلى العديد من المتغيرات بداية من الإدلاء بالنظريات التي لها علاقة بها والتي تتجسد بكل من نظريتي الخطأ والأخطار إلى جانب النظرية الموضوعية وتكون النهاية بالتنظيم الدولي الراهن والمتجسد بتدخل لجنة القانون الدولي بهدف إعداد مسودة بخصوص المسؤولية الدولية عن السلوكيات غير الشرعية، ولأن المهم هو إيضاح مفهوم المسؤولية الدولية في ظل الهجمات السيبرانية فسوف نقوم بالبحث في التعريف، الذي ورد في مشروع المسؤولية الدولية عن التصرفات والسلوكيات غير شرعية لسنة ٢٠٠١ والمادة (١) منه تحديداً، التي نصت على:

"كل عمل أو سلوك ليس مشروع من الناحية الدولية تقوم الدولة به يتبعه مسؤوليتها الدولية".

ومن الصحيح أن نقول إنه ليس من الممكن أن تقوم المسؤولية الدولية سوى في حال التأكد أن التصرف أو الفعل الذي تمت نسبته إلى دولة معينة كان يخالف أحكام القانون الدولي إما العرفية وأما التعاهدية ولكن هل هناك شرطاً وجود ضرر ناتج عن هذا الفعل وأو السلوك؟

إن العودة إلى أحكام المادة واحد من مشروع المسؤولية الدولية بخصوص الفعل غير المشروع لعام ٢٠٠١ يتبين أنها لم تشترط أن يحدث الضرر من أجل أن تتحرك المسؤولية الدولية.

إن المفهوم ذاته الذي أتت به المادة واحد التي ذكرنا سابقاً هو مفهوم مخالف لما تم الاستقرار عليه في الاجتهاد الدولي سواء من الناحية القضائية أم الفقهية، الذي اشترط وجود الضرر من أجل أن تقوم المسؤولية الدولية.

بينما على المستوى الفقهي فتعريف محمد حافظ غانم لها بأن المسؤولية الدولية تقع على عاتق كل من الدولة، وأي من أشخاص القانون الدولي إذا ما أتى ذلك الشخص أمراً يستلزم المؤاخذه، وذلك بحسب الأسس والمبادئ القانونية الشائعة في المجتمع الدولي^(٢).

أما فيما يتعلق بالقانون الدولي الإنساني، لأنه الأكثر قرباً إلى موضوع الدراسة سوف نتطرق إلى المسؤولية الدولية الناتجة عن الهجمات السيبرانية.

١ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، مكتبة زين الحقوقية، بيروت، لبنان، ٢٠١٨، ص ٦٦.

٢ المصدر نفسه، ص ٦٧.

من المعلوم أن أغلب أحكام الاتفاقيات والمعاهدات والمبادئ العرفية الدولية ذات العلاقة قد عملت على تحديد وبشكل واضح وجلي المسؤولية التي تلقى على عاتق الدولة سواء كان من ارتكب هذا السلوك أم الفعل من مؤسسات الدولة الرسمية أو شبه الرسمية بشرط ألا يكون لها المقدرة على السيطرة على أفعالها وضبطها وهو ما دلت عليه المادة (٣) من اتفاقية لاهاي بخصوص الحرب البرية لسنة ١٨٩٩ والتي عُدلت في سنة ١٩٠٧، التي كان نصها: يُلزم الطرف المتحارب الذي يخالف أحكام المادة المذكورة بدفع تعويض إذا استلزمت الحاجة وأنه يكون مسؤولاً عن كافة الأفعال، التي يقوم بها أفراد ينتسبون إلى قواته المسلحة^(١).

ولو أمعنا النظر تجاه المسؤولية الدولية، التي تنشأ عن الهجمات السيبرانية سنرى أنها تتباين من ظرف إلى ظرف آخر فلو كان الهجوم السيبراني ينصب على التسبب بعطل في وسائل الاتصال المدنية أو العسكرية خلال الاشتباك المسلح، فيكون الأمر خاضعاً إلى أحكام القانون الدولي الإنساني وبالتحديد الأحكام التي تسيطر على سلوكيات وأفعال المقاتلين وتضبطها وطرق العمليات العسكرية، التي تتأولنا قسماً منها فيما سبق من الدراسة.

وفي الخصوص ذاته فإن محمد حافظ غانم يضيف شرطاً آخر على ما ذكر سابقاً فيقول: ولما كان العرف الدولي قد ثبّت على أهمية الإعلان عن المعركة قبل أن تقع العمليات العدوانية فإن حدوث هذه العمليات من دون تصريح أو إعلان قد يسبب حروباً إذا ما كانت الظروف مواتية لذلك^(٢).

والسؤال الذي يطرح نفسه، هل الهجمات السيبرانية تنتهك مبادئ القانون الدولي الإنساني في حال استخدامها في أثناء النزاعات المسلحة الدولية وغير الدولية؟

إن الهجمات السيبرانية ينبغي أن تراعي عدد من المبادئ العامة التي ينص عليه القانون الدولي الإنساني، وذلك لتحقيق مشروعية الهجوم السيبراني، وسنوضح المبادئ المتمثلة بكل من مبدأ التمييز، ومبدأ الاحتياطات المستطاعة، ومبدأ التناسب، فيما يأتي:

أولاً مبدأ التمييز: يُعد مبدأ التمييز من أساسيات النزاعات المسلحة الحديثة، لأنه أساس المبادئ الرئيسة المتعلقة بمسألة الاستهداف القانوني، وقد تم النص عليه في البروتوكول الإضافي الأول لعام

١ احمد عبيس نعمة الفتلاوي، مصدر سابق، ص ٦٨.

٢ المصدر نفسه، ص ٦٩.

(١٩٧٧)^(١)، والقانون الدولي الإنساني العرفي^(٢)، ومن ثم ينطبق مبدأ التمييز في صياغته وتفسيره على نطاق واسع ولا يقتصر على أنواع معينة من الأسلحة أو وسائل الحرب، فهو قابل للتطبيق على الهجمات السيبرانية^(٣).

وجل أحكام هذا المبدأ تقوم على تقييد العمليات الحربية ووسائل وأساليب وأهداف القتال بما لا يلحق بالمدنيين معاناة وآلاماً لا ضرورة لها، وبما لا ينال بالضرر إلا بالأهداف العسكرية دون الأعيان المدنية، ويدخل في زمرة المدنيين ويأخذ حكمهم كل عسكري لم يعد قادراً على القتال كالمرضى والجرحى وأسرى الحرب، ويمتد هذا الحكم أيضاً إلى أفراد الخدمات الطبية والدينية، ولو كانوا من العسكريين^(٤).

ويُعد مبدأ التمييز من أهم المبادئ، التي جاء بها القانون الدولي الإنساني لضبط العمليات الحربية، ويتضمن هذا المبدأ تطبيقين أساسيين هما:

١- ضرورة التمييز بين المقاتلين السيبرانيين وغير المقاتلين السيبرانيين

يجب أن يتمتع المدنيون بالحصانة ضد الهجمات التي توجه إلى الأهداف العسكرية، إذ وردت الإشارة إلى مبدأ التمييز بين المقاتلين والمدنيين لأول مرة في متن إعلان سان بطرسبورغ لعام (١٨٦٨) عندما نص على أن: الهدف المشروع الوحيد الذي يتعين على الدول أن تسعى إلى تحقيقه أثناء الحرب هو إضعاف القوات العسكرية للعدو^(٥)، وقد جرى تقنين هذا المبدأ في البروتوكول الإضافي الأول المشار إليه في أعلاه، وأيضاً تطالب المادة (٥١) من البروتوكول الإضافي الأول بضمان الحماية العامة للمدنيين المهاجمين من الأخطار الناشئة عن العمليات العسكرية، أما بالنسبة للمدنيين الذين يشاركون بشكل مباشر في الأعمال العدائية كونهم يشاركون بأعمال قتالية مباشرة ومن

١ يُنظر: المادة (٤٨) البروتوكول الإضافي الأول لعام ١٩٧٧.

٢ جون ماري هكنرتس ودوزوالد-بك، لويز، مصدر سابق، ص ٣ - ٥.

3 Lulf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, Working Paper, Vol.3, No3, IFHV, Ruhr University Bochum, Germany, 2013, P7, Available at: <https://cutt.ly/sksxM79>

٤ أحمد لطفي السيد مرعي، نحو تفعيل الإنقاذ الجنائي الوطني لأحكام القانون الدولي الإنساني، ط١، دار الكتاب الجامعي للنشر والتوزيع، الرياض ٢٠١٦، ص ٤٩ - ٥٠.

٥ أحمد طوزان، قانون النزاعات المسلحة، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠، ص ٧٨.

ثم يعدون مقاتلين^(١)، وبصيغة صريحة أيضاً أكد النظام الأساسي للمحكمة الجنائية الدولية في المادة ٢/٨ (ب/١) على أنه يُعد من قبيل الانتهاكات الخطيرة للقوانين والأعراف السارية على النزاعات الدولية المسلحة، التي تدخل في معنى جرائم الحرب تعتمد توجيه هجمات ضد السكان المدنيين بصفة هذه أو ضد أفراد مدنيين لا يشاركون مباشرة في الأعمال الحربية يعد جريمة حرب.^(٢)

من خلال هذا المبدأ يجب على الطرفين في النزاعات المسلحة التفريق بين المقاتلين والمدنيين، إذ جاء في المادة (٤٨) من البروتوكول الإضافي الأول سنة ١٩٧٧ ما يأتي: في حالة النزاع المسلح يجب على الأطراف المتخاصمة التمييز بين سكان الدولة المدنيين والعسكريين والمسؤولين المدنيين والأهداف العسكرية، ويجب عليها مهاجمة الأهداف العسكرية فقط بقصد حماية السكان المدنيين والحفاظ على ممتلكاتهم^(٣).

وجاء في المادة (٥١) من البروتوكول الإضافي الأول ما يلي: "لا يمكن أن يكون السكان المدنيون أهدافاً لمواجهتها، ويجب منع استخدام القوة أو التهديد بها، التي تسبب الخوف والاضطراب عند السكان المدنيين".

ومن جهة القضاء الدولي يُعد الرأي الذي فرضته محكمة العدل الدولية بخصوص الإنذار باستخدام الأسلحة النووية سنة ١٩٩٦ هو أكثر المواقف تطبيقاً، إذ إنه: يسعى إلى حماية السكان المدنيين والتمييز بين المواطنين المسلحين وغير المسلحين، ويجب على الدول عدم اعتبار المدنيين أهدافاً لمهاجمتهم، وعدم استعمال الأسلحة، التي لا تميز بين السكان المدنيين والعسكريين^(٤).

وأكدت محكمة العدل الدولية على هذا المبدأ بوصفه أساساً ملزماً للأفراد بتنفيذه بقولها: المبادئ الأساسية في القانون الدولي الإنساني يجب على كل الدول الالتزام بتنفيذه إذا وقعت أو لم توقع على قرار الاتفاقيات، لأنها تمثل قرارات القانون الدولي الواجب الالتزام بها، ولا يجوز التعدي عليها.

١ يُنظر: المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧.

٢ يُنظر: نظام روما الأساسي للمحكمة الجنائية الدولية، المادة (٨)، الفقرة (٢)، ١٩٩٨، تاريخ الزيارة ٢٠٢٤/٦/١٢، الساعة ٥،٠٠، متاح على الرابط: <https://www.icrc.org/ar/doc/resources/doc/misc>

٣ أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص ٥٧.

٤ المصدر نفسه، ص ٥٨.

وأكدت المحكمة الدولية الخاصة في يوغوسلافيا سنة ١٩٩٣ على ذلك وأهمية تطبيقه في النزاعات المسلحة الدولية وغير الدولية بقولها: أن السكان المدنيين لا يجوز عدّهم أهدافاً عسكرية، وهذا مبدأ رئيسي في القانون الدولي، ويجب تطبيقه في حال قيام النزاعات المسلحة.

ولهذا يجب التمييز بين السكان المدنيين والعسكريين خلال الهجمات السيبرانية وهذا موضوع معقد وصعب بخلاف الهجمات العادية والتقليدية، بحيث تستخدم أسلحة للهجوم على أماكن محددة على بعد مسافات كبيرة، وهذا يجعل الأمر صعباً للتمييز بين السكان، لهذا قام المحامين الدوليين بالمطالبة بتنفيذ هذه القرارات في حال استخدام الطائرات بدون طيار في الهجوم^(١).

وقد دعا الفقيه (ماركو روسيني) في هذا الموضوع المحامين الدوليين للبحث والاستكشاف في قدرة التوافق التي تتميز به الهجمات الالكترونية على وفق قرارات القانون الدولي الإنساني، ولا سيّما بعد تعرض أغلب الدول إلى هجمات من مصادر مجهولة^(٢).

والغرض الأساسي من مبدأ التمييز هو لضمان استهداف أطراف النزاع للمقاتلين وليس المدنيين، وقد يكون من المستحيل عملياً التمييز بين المقاتل السيبراني أو فرد آخر مستهدف قانونياً لسببين رئيسيين هما:

أ- قد يكون من الصعب للغاية، إن لم يكن من المستحيل، تحديد ما إذا كان المدني على علم بأن جهاز شبكة الكمبيوتر الخاص به يشارك في هجوم سيبراني، وبذلك يصبح الأفراد الذين تسهم أجهزتهم الشبكية الحاسوبية في الهجمات السيبرانية دون علم مالكلهم، خاضعين للاستهداف القانوني^(٣)،

فالمهاجم السيبراني في هذه الحالة هو الذي يقوم بإجبار المدني على المشاركة في النزاع على سبيل المثال، عندما يخترق مهاجم سيبراني أجهزة كمبيوتر مدنية لدمجها في شبكة الروبوتات، ومن ثم يهاجم خصماً، وهناك نوعان من الانتهاكات المتضمنة:

١ أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص ٥٨.

٢ المصدر نفسه، ص ٥٩.

فالمهاجم السيبراني يهاجم بشكل غير قانوني أجهزة الكمبيوتر المدنية ببرامج ضارة تجبر الكمبيوتر على الاستجابة على أمر المهاجمين السيبرانيين، ويمكن أن ترد الدولة المستهدفة بهجوم مضاد متناسب يؤثر على أجهزة الكمبيوتر المخترقة، ويكون المهاجم السيبراني الأصلي مسؤولاً عن الضرر اللاحق للممتلكات المدنية بسبب الحالة المستهدفة.

والمهاجم السيبراني يجبر المدنيين بشكل غير قانوني على المشاركة المباشرة في الأعمال العدائية، وذلك من خلال صنع سلاح سيبراني يتكون من أجهزتهم الحاسوبية، هذا هو المهاجم السيبراني له الدرع البشري^(١)، ولا يمكن للدولة التي يُنفذ الهجوم عبر شبكاتها الحاسوبية المدنية، أن تخضع للمساءلة عن الهجمات ما لم يثبت أنه تم ذلك عن علم قادتها^(٢).

ب- لم يُعدّ المهندسين المدنيين ومصممي الأسلحة الآخرين أفراداً مستهدفين بشكل قانوني لأن دورهم كان ضئيلاً بالفعل مقارنة بالقادة العسكريين بما في ذلك المهندسين العسكريين والجنرالات، مع ذلك يُعد دور مهندسي البرمجيات المدنيين أكثر أهمية بشكل ملحوظ في سياق الحرب السيبرانية، لا سيما أنه بمجرد إطلاق هجوم سيبراني على شبكة الكمبيوتر، لم يعد هناك حاجة إلى مزيد من الإجراءات غالباً، نظراً لأن مساره وإجراءاته تمت برمجته تلقائياً فيمكن بسهولة إساءة استخدام ميزة الحرب السيبرانية هذه من قبل السلطات الرسمية للدولة، التي يمكن أن تنكر أي صلة بجماعة مدنية تدعي صراحة مسؤوليتها عن هجوم، لذلك، من الممكن أن تحتوي المعاهدة السيبرانية الجديدة على أحكام من شأنها أن تأخذ في الاعتبار مشاركة جميع المدنيين بنشاط، وعن علم في الهجمات السيبرانية بما في ذلك إعدادها وتنظيمها، كأفراد مستهدفين بشكل قانوني^(٣).

1 Gervais, Michael: Cyber Attacks and The Laws of War, Berkeley Journal of International Law, Volume 30, Issue 2, Article 6, 2012, PP 525-579, P567, Available at: <https://cutt.ly/mkp1eep>

2 Knopová, Eva: New IHL Framework for Cyber Warfare, op.cit, P56.

٣ أحمد طوزان، مصدر سابق، ص ٨٠.

٢. ضرورة التمييز بين الأعيان المدنية والأعيان العسكرية:

وأنه لا يجوز مهاجمة الأعيان المدنية بأي حال من الأحوال^(١). وتكمن صعوبة الهجمات السيبرانية في عدم وجود فاصل محدد وواضح بين الأعيان العسكرية والمدنية، ولتحديد ما إذا كانت الهجمات السيبرانية تفي بمتطلبات التمييز، يجب على المهاجم السيبراني أن يحدد:

أ- ما إذا كان الهجوم يميز بشكل كاف بين الأعيان المدنية والعسكرية، مع الأخذ في الحسبان الاستخدام المزدوج لمعظم البنية التحتية للإنترنت.

ب- ما إذا كانت الهجمات السيبرانية تتم بشكل عشوائي^(٢).

وقد تم الإشارة إلى الهجمات العشوائية المحظورة في المادة (٤٣،٥٠،٤٩) من دليل تالين، وتستند هاتان القاعدتان إلى المادة (٤/٥١) من البروتوكول الإضافي الأول، القاعدتين (١١،١٢) من القانون الدولي الإنساني العرفي.

ويُقيّم ما إذا كان الهجوم عشوائياً على أساس كل حالة على حدة، وتشمل العوامل التي يجب مراعاتها ما يأتي:

- طبيعة النظام الذي يتم إدخال البرامج الضارة فيه أو المعرضة للخطر.

- طبيعة أسلوب أو وسائل الحرب السيبرانية المستخدمة.

- مدى جودة التخطيط.

- أي دليل على اللامبالاة من جانب المشغل السيبراني في التخطيط للهجوم أو الموافقة عليه أو تنفيذه^(٣).

وقد تم التطرق إلى مبدأ التمييز بصورة واضحة في المادة (٤٨) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام (١٩٧٧) التي نصت على ما يأتي: "تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين

١ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلّي للعلوم القانونية السياسية، العدد ٤، العراق، ٢٠١٦، ص ٦٣٨.

2 Gervais, Michael: Cyber Attacks and The Laws of War, op.cit, p33.

3 Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (6) on Rule (49).

الأعيان المدنية والأعيان العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية^(١).

ويتبن دور منظمة الأمم المتحدة في التأكيد على مبدأ التمييز، وذلك من خلال العديد من القرارات الصادرة من مجلس الأمن، إذ أدان الهجمات ضد الأعيان المدنية في سياق نزاعات مسلحة، بما فيها النزاعات، التي جرت في البوسنة والهرسك، والسودان، ولبنان، والنزاع بشأن إيران والعراق، ومن القرارات الصادرة بهذا الشأن والمعلقة بحماية المدنيين في النزاعات المسلحة القرار ذي الرقم (١٢٦٥)، الذي تم اعتماده سنة (١٩٩٩)، وأن للقضاء الدولي دور ترسيخ مبدأ التمييز، ومنها الفتوى التي صدرت عن محكمة العدل الدولية حول مشروعية استعمال أو التهديد باستعمال الأسلحة النووية (١٩٩٦) إذ نصت على أنه ينبغي على "الدول ألا تجعل من المدنيين هدفاً للهجوم، ومن ثم يجب ألا تستعمل الأسلحة، التي لا تستطيع التمييز بين الأهداف العسكرية والمدنية"^(٢).

ومن الملاحظ ان مبدأ التمييز قد أسهم إلى حد كبير في حماية غير المقاتلين من الفئات، التي تتمتع بالحماية من: جرحى ومرضى، وأسرى حرب، ومدنيين، والقائمين بالخدمات الإنسانية، ومن ثم فقد كفل لهم حماية شرفهم وعقائدهم، وعاداتهم، ومعاملتهم بإنسانية ولا سيّما الحماية ضد أشكال العنف أو التهديد وغيرها، و ضمن مبدأ التمييز الحماية للأعيان غير العسكرية والمتمثلة في: الأعيان المدنية، والثقافية، والبيئية الطبيعية، والأشياء اللازمة لحماية السكان المدنيين^(٣).

ثانياً: مبدأ التناسب

يعني هذا المبدأ أن الميزة العسكرية التي تحصل عليها عملية معينة يجب أن تفوق الضرر الذي يلحق بالمدنيين والأعيان المدنية من جراء ذلك الإجراء، وقد تم التعبير عنه في متن المادة (٥٧) البند الثاني/الفقرة أ/ثالثاً، والبند الثالث، والمادة (٥٢) من البروتوكول الإضافي الأول لعام (١٩٧٧)، وإلى جانب الطابع التعاهدي البارز لهذا المبدأ يبرز طابعه العرفي الذي يؤكد وجوده كقاعدة أصلية من

١ يُنظر: المادة (٤٨) من لبروتوكول الإضافي الأول ١٩٧٧.

٢ إسراء صباح الياسري، التنظيم الدولي للمناطق المحمية-دراسة في ضوء القانون الدولي الإنساني، ط١، المركز العربي للنشر والتوزيع، مصر، ٢٠١٨، ص٥٧-٥٨.

٣ خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، اطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، الجزائر، ٢٠١٣، ص١٤٦.

قواعد القانون الدولي الإنساني العرفي، ومن ثم انطباقه على النزاعات المسلحة الدولية وغير ذات الطابع الدولي على حد سواء^(١).

ويعد مبدأ التناسب بحسب القانون الدولي الإنساني بأنه مقياس تحديد النسبة القانونية من وجهة نظر القانون الدولي بين التفوق العسكري الحاصل نتيجة استخدام الوسائل والأساليب العسكرية المختلفة وبين كمية سقوط الضحايا وسط السكان المدنيين نتيجة الهجوم على المنشآت العسكرية^(٢). ولذلك يسعى المبدأ إلى إقامة توازن بين مصلحتين متعارضتين، تتمثل الأولى بما تمليه الاعتبارات العسكرية الضرورية، بينما تتمثل الثانية فيما تمليه مقتضيات الإنسانية، حتى لا تكون هناك حقوق أو محظورات مطلقة^(٣).

ويُستخدم مبدأ التناسب في النزاعات المسلحة وذلك للحكم على أمرين هما: الأول: حق الحرب، وهو الحكم على شرعية الأهداف الاستراتيجية في استخدام القوة للدفاع عن النفس. الثاني: قانون الحرب، هو الحكم على شرعية أي نزاع مسلح يسبب خسائر مدنية، أي أن مبدأ التناسب تظهر قيمته كلما شن طرف هجوماً على هدف عسكري مخلفاً أضراراً مدنية أو أعيان غير عسكرية^(٤).

وبحسب المادة (٥/٥١) والمادة (٢/٧٥) من البروتوكول الإضافي الأول لعام (١٩٧٧) الملحق باتفاقيات جنيف لعام (١٩٤٩)، بأنه: "يحظر الهجوم الذي قد يتوقع منه أن يسبب خسائر في أرواح المدنيين أو إصابة بهم أو أضرار بالأعيان المدنية، أو أن يحدث خلطاً بين هذه الخسائر والأضرار بشكل يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة"^(٥).

وورد ذكر مبدأ التناسب في النظام الأساسي للمحكمة الجنائية في مادته (٢/٨) (ب/٤) عند تحديده الانتهاكات الخطيرة للقوانين والأعراف السارية على النزاعات المسلحة الدولية في النطاق الثابت للقانون الدولي، التي نصت على: "تعمد شن هجوم مع العلم بأن هذا الهجوم سيسفر عن خسائر تبعية في الأرواح أو عن إصابات بين المدنيين أو إلحاق أضرار مدنية أو إحداث ضرر واسع النطاق

١ جون ماري هنكرتس، ودزوالبك لويز، مصدر سابق، القاعدة (١٤) ص ٤١-٤٣.

٢ محمد فهادة شالدة، القانون الدولي الإنساني، منشأة المعارف، الإسكندرية، ٢٠٠٥، ص ٧٣.

٣ أحمد خضر شعبان، الحماية الدولية والشرعية لضحايا النزاعات المسلحة-دراسة مقارنة، ط ١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥، ص ١٩٨-١٩٩.

٤ أحمد لطفي السيد مرعي، مصدر سابق، ص ٤٨.

٥ جون ماري هنكرتس، المصدر السابق، ص ٣٥.

وطويل الأجل وشديد للبيئة الطبيعية يكون إفراطه واضحاً بالقياس إلى مجمل المكاسب العسكرية المتوقعة الملموسة والمباشرة^(١).

وبناءً على ما سبق، يتبين أن مبدأ التناسب يعد وسيلة للحد من الأضرار الناجمة عن العمليات العسكرية، وذلك للوصول إلى الغاية، وهي إرهاب الخصم باستعمال الأسلحة بالقدر الكافي، وتجنب إصابة المناطق المحمية قدر الإمكان. وبذلك يكون مضمونه هو التركيز على الآثار المتوقعة من الهجوم العسكري، وما ينتج عنه ومدى ملائمته لتحقيق الهدف العسكري المنشود، إلا أنه مهما يكن فإن مبدأ التناسب يضفي نوعاً من الحماية اللازمة للمناطق المحمية ضد أضرار النزاعات المسلحة، ومن ثم فإن أي عمل عسكري من شأنه أن يجعل تلك المناطق هدفاً للهجوم، فإنه يعد عملاً عسكرياً غير مشروع، ذلك لأن الأضرار بهذه المناطق والمواقع الذي ينجم عن استعمال بعض الوسائل القتالية تكون كفيفة بترك آثار وأضرار واضحة على الأشخاص والأعيان الموجودة داخل هذه المناطق^(٢).

ويرى الباحث: أن خصوصية الهجمات السيبرانية تفرض عدم وجود دولة بإمكانها فرض سيطرتها عليها، مما أدى إلى استخدامه بوضع يضر بالبشرية، ويمس بالأمن القومي للدولة، وأدت إل حدوث صراعات بين بعض الدول، مما دفع الجهود الدولية لوضع تنظيم قانوني لها، تتجسد بالقانون الدولي الإنساني، الذي يسعى إلى حماية المدنيين من ويلات النزاعات المسلحة والهجمات العدائية، باعتبار أن هدفه الرئيسي حماية الإنسانية، يصبح القانون الدولي الإنساني منطبقاً على الهجمات السيبرانية، وتندرج تلك الهجمات ضمن قواعده إذا كان هدف الهجمات هو تعريض الأشخاص المحميين وممتلكاتهم للخطر أو المخاطرة بحدوث ذلك، ولكن يبقى التحدي في مقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة.

ثالثاً. مبدأ الاحتياطات المستطاعة:

يستند مبدأ الاحتياطات المستطاعة في أساسه على القانون الدولي الإنساني، إذ تنص القاعدة العرفية (١٥) على: يتخذ كل طرف في النزاع جميع الاحتياطات الممكنة عند اختيار وسائل وأساليب الحرب لتجنب إيقاع خسائر أرواح المدنيين، أو إصابات بينهم، أو أضرار بالأعيان المدنية بصورة عارضة، وتقليلها على أي حال إلى الحد الأدنى. وورد هذا المبدأ في قاعدة عرفية أخرى تنص على: يتجنب كل

١ يُنظر: المادة (٨ / الفقرة ٢) نظام روما الأساسي للمحكمة الجنائية الدولية.

٢ إسراء صباح الياسري، مصدر سابق، ص ٧٢-٧٣.

طرف في النزاع، قدر المستطاع، وضع أهداف عسكرية داخل المناطق المكتظة بالسكان أو قريباً منها^(١).

وقد فرضت قابلية استخدام الفضاء السيبراني، لمثل تلك الأنشطة العدائية بعض التعقيدات بخصوص الإجراءات الاحتياطي الواجب اتخاذه قبل شن الهجمات السيبرانية والإجراء الاحتياطي الواجب اتخاذه لتلافي آثار هذه الهجمات^(٢).

وقد ورد مبدأ الاحتياطات المستطاعة في البروتوكول الإضافي الأول لعام (١٩٧٧) تحت عنوان التدابير الوقائية، التي ورد تفصيلها في نص المادتين (٥٧-٥٨)، وتنص على: تبذل رعاية متواصلة في إدارة العمليات العسكرية من أجل تفادي السكان المدنيين والأشخاص والأعيان المدنية، وتجنب إقامة أهداف عسكرية داخل المناطق المكتظة بالسكان أو بالقرب منها، واتخاذ الاحتياطات اللازمة لحماية ما تحت سيطرتها من سكان مدنيين وأعيان مدنية من الاخطار الناجمة عن العمليات العسكرية^(٣). وتتخذ الاحتياطات الآتية فيما يتعلق بشن الهجمات السيبرانية بما يأتي:

- أ. يجب على من يخطط لهجوم أو يتخذ قراراً بشأنه:
- أولاً: أن يبذل ما في طاقته عملياً للتحقق من أن الأهداف المقرر مهاجمتها ليست أشخاصاً مدنيين أو أعياناً مدنية وأنها غير مشمولة بحماية خاصة.
- ثانياً: أن يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم من أجل تجنب إحداث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم أو الإضرار بالأعيان المدنية.
- ثالثاً: أن يمتنع عن اتخاذ قرار بشن أي هجوم قد يتوقع منه بصفة عريضة أن يحدث خسائر في أرواح المدنيين أو إلحاق الأذى بهم، أو الإضرار بالأعيان المدنية، أو أن يحدث خطأً من هذه الخسائر والإضرار، مما يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة مباشرة.

١ جون ماري هنكرتس، دراسة حول القانون الدولي الإنساني العرفي-إسهام في فهم واحترام حكم القانون في النزاع المسلح، المجلة الدولية للصليب الأحمر، العدد ٨٥٧، ٢٠٠٥، ص ٣٣-٣٤.

٢ عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، ط٢، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩، ص ٢٨٣.

٣ يُنظر: المادة (٥٧-٥٨) من البروتوكول الإضافي الأول لعام ١٩٧٧.

ب. يلغى أو يعلق أي هجوم إذا تبين أن الهدف ليس هدفاً عسكرياً أو أنه مشمول بحماية خاصة أو أن الهجوم قد يتوقع منه أن يحدث خسائر في أرواح المدنيين أو الإضرار بالأعيان المدنية.

ج. يوجه إنذار مسبق وبوسائل مجدية في حالة الهجمات، التي تمس السكان المدنيين، مالم تحل الظروف دون ذلك^(١).

أما الاحتياطات الواجب اتخاذها لتلافي آثار الهجمات السيبرانية، فيعد الالتزام واجباً قانونياً أو طبيعة عرفية بالنسبة للنزاعات المسلحة الدولية وغير الطابع الدولي، وذلك بالاستناد إلى نص القاعدة (٢٢) من القانون الدولي الإنساني العرفي، وتمت الإشارة إليه في القاعدة (٥٩) من دليل تالين^(٢).

ومن الأمثلة على مبدأ الاحتياط، القيام بعزل البنى التحتية الإلكترونية العسكرية عن المدنية، وفصل الحاسوب، التي تعتمد عليها البنى التحتية الأساسية عن شبكة الانترنت، وعدم استخدام شبكة الاتصالات المدنية للأغراض العسكرية، ودعم البيانات المدنية الرقمية بنسخ احتياطية، واستخدام الإجراءات المضادة لفيروسات الحاسوب لحماية النظم المدنية، والقيام بتوزيع البرمجيات الواقية، ومراقبة النظم والشبكات الإلكترونية، وتطوير قدرات رد الفعل لمنع التسلل من قبل الخصم للنظم الإلكترونية المدنية^(٣).

زيادة على ذلك، إن طبيعة التقنية السيبرانية المختارة تحدد أيضاً ما إذا كان يمكن الوفاء بالالتزام، فمن الممكن تعطيل الهجمات إذا تم تصنيف الهدف بشكل خاطئ، فقط إذا كان المهاجم قادراً على التحكم في السلاح أو الوسيلة المنتشرة، إلا أنه وعلى سبيل المثال: إذا ما استخدم برنامج الدودة، التي تقوم بتكرار نفسها دون مزيد من التحكم في الشخص الذي أطلقها للاستهداف يكون من الصعب إيقافها بسبب الطبيعة التقنية لها، فلا يمكن الالتزام بالالتزام، مما يؤدي إلى انتهاك القانون الدول الإنساني، إلا أنه إذا تم تطويرها لتفوق كفاءة البشر، قد يكون لها القدرة على الامتثال لقواعد القانون الدولي الإنساني بشكل أفضل^(٤).

١ يُنظر: المادة (٥٧) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩.

٢ جون-ماري هنكرتس، ودزوالبك لويز، مصدر سابق، ص ٦١.

3 Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (1-9) on Rule (59).

٤ يحيى ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية، جامعة يحيى فارس، الجزائر، ٢٠١٨، ص ٩٩.

وبناءً على ذلك، فإن مبدأ اتخاذ الاحتياطات اللازمة من شأنه أن يوفر الحماية للمناطق المحمية، لكونه ألزم أطراف النزاع باتخاذ الاحتياطات المستطاعة في أثناء الهجوم، لتحقيق من أن الأهداف المقصودة هي أهداف عسكرية، ومن ثم يجوز مهاجمتها، أما إذا تبين العكس، أي: إن الأهداف المعنية ليست أهداف عسكرية أو أن الهجوم قد يتوقع منه أن يحدث خسائر وأضرار في هذه المناطق لما تحويه من أشخاص وأعيان محمية، ففي هذه الحالة يلغي أو يعلق الهجوم^(١).

نستخلص مما تقدم: من خلال استعراض القواعد الأساسية للقانون الدولي الإنساني، يتبين أن مبدأي التمييز والتناسب يشكلان العمود الفقري لحظر الهجمات العشوائية، ويؤسسان لقاعدة قانونية وأخلاقية تهدف إلى حماية السكان المدنيين والأعيان المدنية من ويلات النزاعات المسلحة. إن مبدأ التمييز يفرض على أطراف النزاع واجباً واضحاً في الفصل بين المقاتلين والمدنيين، وبين الأهداف العسكرية والممتلكات المدنية، بما يضمن توجيه الأعمال العدائية فقط نحو الأهداف المشروعة بموجب القانون الدولي. أما مبدأ التناسب، فيلزم أطراف النزاع بعدم تنفيذ هجمات قد تسبب خسائر في الأرواح أو أضراراً في الممتلكات المدنية تكون مفرطة بالمقارنة مع الميزة العسكرية المباشرة المتوقعة من الهجوم.

أما مبدأ الاحتياطات الممكنة، والذي ورد صراحة في المادة (٥٧) من البروتوكول الإضافي الأول لعام ١٩٧٧، فيلزم الأطراف باتخاذ كافة الاحتياطات المستطاعة في اختيار الوسائل والأساليب العسكرية، وفي تخطيط وتنفيذ الهجمات، من أجل تقليل الخسائر في أرواح المدنيين أو الأضرار، التي تلحق بالأعيان المدنية إلى الحد الأدنى الممكن. ويشمل ذلك التحقق من أن الأهداف المراد مهاجمتها هي أهداف عسكرية فعلاً، واختيار وسائل الهجوم التي تقلل من الأثر على المدنيين، وتأجيل أو إلغاء الهجمات إذا تبين أن أضرارها الجانبية ستكون غير متناسبة، وأن حظر الهجمات العشوائية ينطوي على حظر استخدام أسلحة أو وسائل قتال لا يمكن توجيهها بدقة إلى هدف عسكري محدد، أو تلك، التي لا يمكن حصر آثارها بما يسمح بالامتثال لمبادئ القانون الدولي الإنساني. وتشمل الهجمات العشوائية، على سبيل المثال، القصف المدفعي غير الدقيق على مناطق مأهولة، أو استخدام الأسلحة المتفجرة ذات الأثر الواسع في البيئات الحضرية، ما يؤدي إلى سقوط أعداد كبيرة من الضحايا المدنيين، دون وجود تبرير عسكري كافٍ. وعليه، فإن خرق هذه القواعد لا يمثل مجرد انتهاك قانوني

١ إسرائ صباح الياسري، مصدر سابق، ص ٦٩.

فحسب، بل يرتقي في حالات كثيرة إلى جرائم حرب تستوجب المساءلة الفردية، على وفق ما نصت عليه اتفاقيات جنيف لعام ١٩٤٩ وبروتوكولاتها الإضافيان لعامي ١٩٧٧ و ٢٠٠٥، فضلاً عن النظام الأساسي للمحكمة الجنائية الدولية لعام ١٩٩٨.

ويرى الباحث: أن تعزيز الالتزام بحظر الهجمات العشوائية يجب أن ينطلق من إدراك عميق لطبيعة النزاعات المسلحة المعاصرة، والتي غالباً ما تتسم بتداخل خطوط القتال ووقوعها في مناطق مكتظة بالسكان المدنيين، ما يزيد من احتمالية الإضرار بهم بشكل مباشر أو غير مباشر. ويرى الباحث أن تطور وسائل وأساليب القتال، بما في ذلك استخدام الطائرات بدون طيار، الأسلحة ذاتية التشغيل، والصواريخ بعيدة المدى، لا ينبغي أن يُستغل كذريعة لتجاوز القواعد الإنسانية، بل يجب أن يُواكب بتطوير الأطر القانونية والرقابية، التي تضمن احترام مبدأي: التمييز والتناسب.

الفرع الثاني

معايير تحديد الأهداف العسكرية المشروعة في أثناء الهجمات السيبرانية

شهدت نهايات القرن الثامن عشر وبدايات القرن التاسع عشر استقرار التفرقة بين المقاتلين وغير المقاتلين، وخير دليل على ذلك ما قاله المفكر الفرنسي الشهير جان جاك روسو في كتابه العقد الاجتماعي بالآتي: إن الحرب ليست علاقة بين إنسان وإنسان وإنما علاقة بين دولة ودولة، وليسوا أعداء إلا بصفة عرضية لا كأفراد أو مواطنين، ولكن كجنود وعداؤهم ليس على أساس أنهم ينتمون إلى الطرف المحارب بل كمدافعين عنه ^(١). وسوف نبين ذلك فيما يأتي:

أولاً: الأشخاص والأعيان المشروعة استهدافهم في أثناء الهجمات السيبرانية

تعد فئة المقاتلين هم أول فئة مشروعة تُستهدف في أثناء الهجمات السيبرانية، أما بالنسبة إلى الأعيان المباح استهدافها في أثناء الهجمات السيبرانية فهي التي تسهم مساهمة فعالة في العمل العسكري وينتج عنها ميزة عسكرية أكيدة، وسنتحدث بالتفصيل عن الأشخاص والأعيان المشروعة استهدافهم في أثناء الهجمات السيبرانية فيما يأتي:

١ جان جاك روسو، العقد الاجتماعي، مؤسسة هنداوي للتعليم والثقافة، القاهرة، ٢٠١٣ ص ٣٣، تاريخ الزيارة

٢٠٢٤/٦/١٥، الساعة ٣:٠٠، متاح على الرابط: <https://cutt.ly/WkpNp5Y>

١- الأشخاص والأعيان المشروع استهدافهم في أثناء الهجمات السيبرانية.

يوفر القانون الدولي الإنساني حماية خاصة لبنية تحتية معينة، مثل الخدمات الطبية والأعيان والتي لا استغناء عنها لبقاء المدنيين، بصرف النظر عن نوع العملية التي تلحق بها الضرر^(١). من وجهة نظر اللجنة الدولية، تعد العمليات السيبرانية التي تنفذ بواسطة الفيروسات والديدان الحاسوبية، التي تلحق ضرراً بأشخاص أو أضراراً مادية بممتلكات أخرى غير البرامج أو البيانات الحاسوبية التي تعرضت للهجوم نتيجة الآثار المباشرة أو غير المباشرة المتوقعة للهجوم بأنها أعمال عنف، أي: هجوم بالمعنى المنصوص عليه في القانون الدولي الإنساني^(٢).

ويدعى أحياناً بأن الهجمات السيبرانية لا تندرج في نطاق الهجوم ما دامت لا تتسبب في أضرار بدنية أو عندما يكون في الإمكان التخلص من الآثار الناجمة عنها، وإذا كان المراد بهذا الادعاء تسويق عدّ الهجوم على الممتلكات المدنية عملاً قانونية، فإن اللجنة الدولية تعدّه ادعاءً باطلاً، فلا يجوز بموجب القانون الدولي الإنساني توجيه الهجمات إلا إلى الأهداف العسكرية، ولا يجوز الهجوم على الأهداف المدنية^(٣).

يوضح دليل تالين أن الهجمات السيبرانية على الحواسيب وشبكات الحاسوب والبنية التحتية السيبرانية يجب أن تقتصر حصراً على الأهداف العسكرية، بينما لا يجوز أن تكون الأعيان المدنية هدفاً للهجوم السيبرانية، وبالنسبة للأعيان المزدوجة بين العين العسكرية والعين المدنية تصبح هدف عسكري طوال هذا الاستخدام، ويجب أن يستوفي الهدف العسكري شرطين لتصنيفه هدفاً عسكرياً أولاً: يجب أن يسهم الهدف مساهمة فعالة في العمل العسكري للطرف المعادي وثانياً: يجب أن يكون تدمير الهدف أو الاستيلاء عليه أو تعطيله يوفر للطرف المهاجم ميزة عسكرية أكيدة، ويقصد بمصطلح الميزة العسكرية استبعاد ميزة ليست عسكرية بطبيعتها، على وجه الخصوص، الميزة الاقتصادية أو السياسية أو النفسية. على سبيل المثال، إن الهجوم السيبراني على قطاع عمل مدني، ظناً من قبل المهاجم أنه سيضعف بشكل عام الدولة المعادية، لن يؤدي بالضرورة إلى ميزة عسكرية بالمعنى

١ يُنظر: المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧.

٢ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، ٢٠١٩، ص ٧.

٣ اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، ٢٠١١. الوثيقة IC٣١/١١/٥.١.٢، ص ٤٣-٤٢.

المطلوب، حتى أنه لا يعد هدف عسكري، لأنه لا يقدم مساهمة فعالة في العمل العسكري، فالتوصيف كهدف عسكري، يجب أن تكون الميزة العسكرية التي يحتمل أن تنتج واضحة^(١).
تتبنى مبادئ القانون الدولي الإنساني، وعلى رأسها مبدأ التمييز، إطاراً صارماً لتحديد الأهداف المشروعة في الهجمات السيبرانية أثناء النزاعات المسلحة. ويعد أي شخص أو مرفق يساهم فعلياً في القدرات القتالية للطرف المتحارب، من خلال خدمات لوجستية أو استخباراتية أو تقنية، هدفاً مشروعاً للهجوم.

ويشمل ذلك:

- القوات المسلحة النظامية،
 - المدنيين المشاركين مباشرة في الأعمال العدائية الرقمية (مثل مبرمجي البرمجيات الخبيثة)،
 - المرافق الرقمية المستخدمة لدعم العمليات العسكرية، مثل البنى التحتية الإلكترونية للقيادة والتحكم.
- لكن الأمر يختلف داخل المناطق المحمية كالمستشفيات ومحطات المياه ومراكز الإمداد الإنساني، إذ تُفرض شروط إضافية لضمان حماية هذه الأعيان، وهي:

١. عدم استخدام المنشأة لأغراض عسكرية؛
٢. الالتزام بمبدأ التناسب، بحيث لا يكون الضرر المدني الناجم عن الهجوم الرقمي أكبر من المكاسب العسكرية المتحققة؛

٣. تنفيذ إجراءات تقنية احترازية دقيقة تقلّل من الآثار الجانبية على المدنيين والبنى التحتية. وتؤكد اللجنة الدولية للصليب الأحمر أن استهداف مثل هذه الأعيان، عبر اختراق إلكتروني حين تكون محمية قانونياً، يعد انتهاكاً صارخاً لمبادئ التمييز والتناسب والاحتياط.

في سبتمبر ٢٠١٩، أكدت اللجنة الدولية للصليب الأحمر (ICRC) أن الهجمات السيبرانية استهدفت البنية التحتية المدنية - بما في ذلك المستشفيات وشبكات الماء والكهرباء - في بلدان نزاع في وسط وشرق أوروبا، مما أدى إلى تعطيل مؤقت لهذه الخدمات الحيوية، وذلك أثناء تصاعد التوترات العسكرية. وقد شكّل ذلك خطراً مباشراً على المدنيين المحميين وفقاً للقانون الدولي الإنساني داخل ما

^(١) ينظر: اللجنة الدولية للصليب الأحمر، متاح على الرابط: <https://www.icrc.org/en/document/action>

يُعد مناطق محمية طبيًا وإنسانيًا، إذ أن تعطل الكهرباء والماء عن المستشفيات يهدّد حياة المرضى ويقوض عمل فرق الطوارئ^(١).

٢- الأعيان ذات الاستخدام المزدوج.

نقصد بذلك الأعيان المدنية التي تستخدم لأغراض عسكرية في الوقت نفسه، نتيجة لذلك تصبح هدفاً عسكرياً طوال هذا الاستخدام^(٢)، وقد ذُكرت هذه القاعدة في إطار المادة (٢/٥٢) من البرتوكول الإضافي الأول، والقاعدة (٣٩) من دليل تالين، ولا بد من الإشارة إلى أن الهجوم على الأعيان ذات الاستخدام المزدوج تخضع لمبدأ التناسب، وشرط اتخاذ الاحتياجات في الهجوم^(٣).

ومن ثم تشكل الهجمات السيبرانية تحديات فريدة في هذا الصدد، فالشبكة الإلكترونية التي تستخدم للأغراض العسكرية والمدنية، قد يكون من المستحيل معرفة أي جزء من الشبكة سيمر عبر الإرسالات العسكرية، وأي منها في الأجزاء المدنية، ففي مثل هذه الحالات، الشبكة بأكملها أو جزء منها مؤهلة كهدف عسكري^(٤). ومن ثم تثير العواقب الإنسانية المترتبة على هذه الحالة قلقاً بالغاً على حماية السكان المدنيين، ففي عالم يعتمد فيه قطاع كبير من البنية الأساسية المدنية، والاتصالات المدنية، والشؤون المالية والاقتصاد والتجارة والصحة على البنية الأساسية الإلكترونية الدولية، يصبح من السهل للغاية أن تقوم الأطراف بتدمير هذه البنية الأساسية، ويسوّغ تعطيل الكابلات الرئيسية أو الشبكات وأجهزة التوجيه أو الأقمار الاصطناعية التي تعتمد عليها هذه النظم، دائماً بحقيقة أن هذه المسارات تستخدم لنقل معلومات عسكرية، وهي من ثم تُصنف كأهداف عسكرية^(٥).

١ موقع اللجنة الدولية للصليب الأحمر، متاح على الرابط: <https://www.icrc.org/en/document/cyber-attacks-are-known-threat-preventive-action>

٢ نيلس مليزر، مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٦، ص ٨٩.

3 Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (2) on Rule (39).

4 Ibid, comment (3) on Rule (39).

٥ دوريجي، كوردولا، لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والفانون الدولي الإنساني وحماية المدنيين، المجلة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦)، ص ٢٦٤٠١٢، تاريخ الزيارة ٢٠٢٤/٦/١٦، متاح على

الرابط: <https://cutt.ly/Okp7S5Z>

إن هناك بعض البيانات المدنية تتعلق بأعيان معينة تتمتع بحماية خاصة بموجب القانون الدولي للإنسان^(١)، وهي الأعيان والمواد، التي لا غنى عنها لبقاء السكان المدنيين، والأعيان الطبية، والأشغال الهندسية والمنشآت، التي تحوي على مواد وقوى وجاقات خطرة والبيئة الطبيعية، والأعيان الثقافية وأماكن العبادة^(٢)، فالالتزام وحماية هذه الأعيان الخاصة يفترض بأنه يشمل حماية البيانات الخاصة بهذه الأعيان أيضاً^(٣).

أما بالنسبة إلى البيانات المدنية الأساسية المتعلقة بالأعيان، التي لا تتمتع بالحماية الخاصة مثل بيانات الأمن الاجتماعي والضرائب السجلات والحسابات المصرفية فمن المحتمل أن تفلت من الامتداد التنظيمي لقانون الدولي الإنساني، ومن ثم تتعارض مع المبدأ أن السكان المدنيين يتمتعون بحماية عامة من آثار الأعمال العدائية^(٤). وبحسب رأي اللجنة الدولية للصليب الأحمر فإن استثناء البيانات المدنية الأساسية من الحماية التي يوفرها القانون الدولي الإنساني للأعيان المدنية من شأنه أن يؤدي إلى ثغرة كبيرة في هذه الحماية^(٥).

تعد الأعيان ذات الاستخدام المزدوج تلك التي تخدم أغراضاً مدنية وأهدافاً عسكرية في آن واحد، وقد نصّ عليها القانون الدولي الإنساني عبر اتفاقيات جنيف والبروتوكول الإضافي الأول. وتُعدها المادة ٢/٥٢ "أهدافاً عسكرية مشروعة" حين يُسهم استخدامها المدني بصفة مباشرة في القدرات الحربية للطرف المتحارب^(٦).

تشمل الأعيان الرقمية ذات الاستخدام المزدوج:

١ إيمان حمدان، التكنولوجيا الجديدة والقانون الدولي الإنساني - الحرب السيبرانية دراسات معمقة في القانون الدولي لإنساني-، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠، ص ٩.

٢ ياسر كلزي، النظرية العامة في القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠، ص ١٠٢.

٣ إيمان حمدان، مصدر سابق، ص ٩.

4 McCormack, Tim: International Humanitarian Law and The Targeting of Data, Volume 94, International Law studies, U.S. Naval War College, United States, 2018, PP223-240, P227, Available At: <https://cutt.ly/DksuNk5>

٥ إيمان حمدان، مصدر سابق، ص ٩.

٦ المادة ٥٢ (٢) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧.

الفصل الثاني: حماية المناطق المحمية من الهجمات السيبرانية:.....

- الكابلات البحرية لشبكات الإنترنت، التي تنقل - بجانب محتوى مدني - معلومات أو أوامر عسكرية حساسة^(١)
- أنظمة التحكم الصناعية (SCADA) في مرافق الطاقة والمياه، لاستخدامها في دعم العمليات العسكرية عند استهداف مواقع محمية^(٢)
- شبكات الاتصالات المشتركة بين القطاع المدني والعسكري، مما يجعلها عرضة لتصبح أهدافاً مشروعة حال استخدامها بنطاق عسكري^(٣)
- وإن كانت الأعيان ذات طبيعة مدنية، فإن استخدامها في أغراض عسكرية يجعلها هدفاً مشروعاً بشرط:

١. أن يساهم استخدام الأعيان فعلياً في القدرات القتالية.
 ٢. ألا يتجاوز استهدافها حد التناسب بين الفائدة العسكرية والأضرار المدنية المحتملة.
 ٣. أن تُتخذ احتياطات معقولة لخفض الأثر الجانبي على السكان المدنيين والبنى التحتية غير المعنية^(٤).
- ففي العام ٢٠١٠ أن فيروس Stuxnet دمر أجهزة الطرد المركزي في منشأة نانتز، وهو استهداف لمنشأة مدنية (نظام كهربائي صناعي) بهدف عسكري دقيق دون تعطيل الشبكة المدنية بالكامل .
- استهدف فيروس Stuxnet أنظمة التحكم الصناعي (SCADA) في منشأة تخصيب النووي في نطنز بإيران، ما أدى إلى تعطيل مئات أجهزة الطرد المركزي عن العمل لفترة محدودة عبر التحكم في سرعة دورانها—في خطوة موجهة بعناية لتقليل الأثر على باقي البنية التحتية المدنية”

١ Casebook ICRC، Iran, Victim of Cyber warfare (Tallinn Manual case study)؛ أن الكابلات البحرية تحمل الاتصالات العسكرية والمدنية. [turn0search0]

٢ Michael N. Schmitt (تحرير)، عشرة أعوام لدليل تالين ٢٠٠٠، كامبريدج ٢٠١٧، القاعدة ١٣١ (SCADA) كمرفق استخدام مزدوج).

٣ Digital safe havens: sheltering civilians... ICRC، يوليو ٢٠٢١ (أهمية فصل البنى التحتية المشتركة). [turn0search3]

٤ ICRC، “Cyber warfare: does international humanitarian law apply؟”، 25 فبراير ٢٠٢١ (التمييز والتناسب والاحتياط تنطبق على العمليات السيبرانية). [turn0search1]

ينظر: مقال منشور على الرابط <https://www.wired.com/2011/07/dhs-fears-stuxnet-attacks>

ثانياً: المدنيون الذين يشاركون مباشرة في الهجمات السيبرانية

يتأثر المدنيون بعواقب النزاعات المسلحة نتيجة الحروب والهجمات، وعلى الرغم أنهم يجب أن يبقوا خارج دائرة المعارك، فإن النزاعات المعاصرة كالهجمات السيبرانية تتجه إلى عكس ذلك^(١). فقد يشارك المدنيون مشاركة مباشرة في الهجمات السيبرانية، وعرفت المادة (١/٥٠) من البروتوكول الإضافي الأول المدنيون بأنهم الأشخاص الذين لا ينتمون إلى القوات المسلحة على المعنى المبين في الاتفاقية الثالثة، المادة ٤(أ) ١، ٢، ٣، ٦ والمادة (٤٣) من البروتوكول الأول^(٢).

ونصت الاتفاقية الرابعة على أنها "تحمي الأشخاص الذين يجدون أنفسهم ما وبأي شكل كان، في حالة قيام نزاع مسلح أو حالة احتلال، تحت سلطة طرف في النزاع ليسوا من رعاياه أو دولة احتلال ليسوا من رعاياها".

ولابد من الإشارة إلى القاعدة (٥) من "قواعد القانون الدولي الإنساني العرفي، والتي تطبق في النزاعات المسلحة الدولية وغير الدولية، إذ جاء فيها: المدنيون أشخاص لا ينتمون إلى القوات المسلحة. ويشمل مصطلح "السكان المدنيين" كل الأشخاص المدنيين"^(٣).

إذ يجب النظر إلى مفهوم المدنيين على أساس التأويل الواسع فقد خصص القانون الدولي الإنساني مزيداً من العناية لفئات محددة كالنساء والأطفال واللاجئين وعديمي الجنسية والصحافيين، وليس ذلك بسبب انتفاء صفتهم المدنية، وإنما تحسباً لما ينالهم من أعمال وتجاوزات في أثناء النزاعات المسلحة^(٤).

أما مفهوم المشاركة المباشرة في العمليات العدائية يشير إلى: أعمال محددة يقوم بها الأفراد كجزء من سير العمليات العدائية بين الأطراف في نزاع مسلح^(٥). وقد استخدم مفهوم المشاركة المباشرة في

١ شهاب مفيد، دراسات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر بعثة القاهرة، دار المستقبل العربي، لبنان، ٢٠٠٠، ص ١٢١.

٢ يُنظر: المادة (١/٥٠) البروتوكول الإضافي الأول لعام ١٩٧٧.

٣ يُنظر: اتفاقية جنيف الرابعة، المادة (٤)، فقرة (١).

٤ شهاب مفيد، مصدر سابق، ص ١٢٢-١٣٢.

٥ أحمد طوزان، مصدر سابق، ص ٧٨.

العمليات العدائية من الجملة المستخدمة في المادة الثالثة المشتركة من اتفاقيات جنيف الأربع، بعبارة الذين لا يشتركون مباشرة في الأعمال العدائية^(١).

ويتطلب القانون الدولي الإنساني لإضفاء وصف المشاركة المباشرة على شخص من المدنيين، توافر ثلاثة شروط للوصول إلى حد حصول الضرر والارتباط بالعمل الحربي والعلاقة السببية بينهما. وفي إطار الأعمال التحضيرية للهجمات السيبرانية، غالباً ما تُصمم وتُبرمج الأسلحة السيبرانية بصورة خاصة لتنفيذها على أهداف معينة ومحددة مسبقاً، مما يجعل من جميع هذه الأفعال بصورة واضحة، مشاركة مباشرة في الهجمات السيبرانية التي يترتب عليها فقدان الحماية من الهجمات المباشرة وآثار القتال، فضلاً عن العقاب، الذي يمكن أن يتعرض له المدني المشارك مشاركة مباشرة في الأعمال العدائية السيبرانية عن طريق تصميم وبرمجة الفيروسات والأسلحة السيبرانية على وفق القانون الوطني^(٢).

ولا بد من الإشارة إلى أنه تحت توجيهات حديثة من اللجنة الدولية للصليب الأحمر، يمكن استهداف المدنيين الذين يتبنون مهمة قتالية مستمرة، فالمبرمج، الذي يعمل مع المخابرات العسكرية بتعديل الكود لتنفيذ مقاصد الهجوم، حتى لحظة الهجوم. يمكن تصور أفعال مثل هذا المدني وظيفة مستمرة تتضمن التحضير أو التنفيذ أو القيادة لأعمال أو عمليات ترقى إلى المشاركة المباشرة في الأعمال العدائية. نتيجة لذلك، قد يُنظر إلى المدنيين المتورطين في الهجمات السيبرانية على أنهم يؤدون مهام قد تغير وضعهم بموجب قانون الدولي الإنساني، مما يجعلهم أهدافاً مشروعة^(٣). ولقد أُنقِ غالبية الخبراء الدوليين في دليل تالين على غرار قواعد القانون الدولي الإنساني أن المدنيين يحتفظون بوضع المدنيين حتى لو شاركوا بشكل مباشر في الأعمال العدائية السيبرانية، ولكنهم يصبحون معرضين للاستهداف^(٤).

١ نيلس ميلزر، دليل التفسير لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٠، ص ٤١-٤٣.

٢ علي محمد كاظم، المشاركة المباشرة للهبة الحماية في الهجمات السيبرانية، مجلة كلية الحقوق، جامعة النهرين، بغداد، العراق، ٢٠١٩، ص ٢٥ - ٥٨.

3 Hathaway, Oona A. & Others: The Law of Cyber-Attack, Op.cit, P40.

4 Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, Comment (3) On Rule (29).

في ظل تعاظم دور الفضاء السيبراني في النزاعات المسلحة، أضحت من غير الممكن إغفال التحديات القانونية التي تفرزها مشاركة المدنيين، سواء من حيث تنفيذ الهجمات السيبرانية أو دعمها، وبالأخص عندما تُوجّه هذه الهجمات نحو المناطق المحمية بموجب القانون الدولي الإنساني، مثل المستشفيات، ملاجئ المدنيين، ومحطات المياه والكهرباء ذات الطابع الإنساني الصرف. وتثير هذه الظاهرة المعاصرة جملة من التساؤلات القانونية العميقة، تتصل بفقدان الحماية القانونية التي يتمتع بها المدني في النزاعات المسلحة، وانطباق المسؤولية الجنائية الفردية عليه، فضلاً عن صعوبة التمييز بين المقاتلين وغير المقاتلين في السياق السيبراني.

وفي أول توثيق رسمي لهذه الظاهرة، أصدرت اللجنة الدولية للصليب الأحمر في الرابع من أكتوبر عام ٢٠٢٣ وثيقة بعنوان "قواعد مشاركة المدنيين في النزاعات السيبرانية"، تضمنت مبدأً صريحاً يحظر استهداف المرافق الطبية والإنسانية عبر الوسائل السيبرانية، مؤكدة أن أي هجوم يستهدف تعطيل هذه المنشآت يُعد انتهاكاً للقانون الدولي الإنساني، ولو جاء من طرف مدني لا ينتمي إلى القوات المسلحة لأي طرف في النزاع^(١). وقد مثّلت الحرب الجارية في أوكرانيا مثالاً تطبيقياً صارخاً على هذه الإشكالية، حين تم تنفيذ سلسلة من الهجمات السيبرانية ضد الشبكات الإلكترونية للمستشفيات، من قبل مجموعات مدنية من القراصنة (هاكرز)، بدعوى أن هذه المنشآت تُستخدم بشكل غير مباشر لخدمة أغراض دفاعية أو لإسناد العمليات المعلوماتية في النزاع^(٢).

ويبرز التكييف القانوني لهذه الأفعال من خلال ثلاثة أبعاد أساسية؛ أولها ما يتعلق بفقدان الحماية القانونية للمدنيين، بموجب المادة (٣/٥١) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧، والتي تنص على أن "المدنيين يتمتعون بالحماية من الهجوم ما داموا لا يشاركون مباشرة في الأعمال العدائية". فإذا ثبتت هذه المشاركة، سواء عبر الهجوم السيبراني أو عبر دعم لوجستي أو تقني، فإن الحماية تسقط عن الفاعل، ويُعامل قانوناً كطرف في النزاع المسلح. وقد فسّرت اللجنة

١ مقال متاح على الرابط <https://blogs.icrc.org/law-and-policy/wp>

٢ تقرير "مستشفيات حرب أوكرانيا السيبرانية: القراصنة المدنيون والمواقع المحمية"، الصادر عن Cyber Peace Institute عام ٢٠٢٣، يتناول أثر العمليات السيبرانية على البنى التحتية الصحية في أوكرانيا متاح على الرابط

<https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian>

الدولية للصليب الأحمر المشاركة المباشرة بأنها تشمل الأفعال التي تؤثر تأثيراً مباشراً في العمليات العسكرية، سواء من حيث توقيت الفعل، أو وظيفته، أو أثره العملياتي^(١).

أما البعد الثاني فيتصل بالطبيعة القانونية للمستشفيات والمنشآت الطبية، إذ تُعد من المناطق المحمية بموجب القانون الدولي الإنساني، ويُحظر استهدافها بأي شكل، سواء بالوسائل التقليدية أو الإلكترونية. وتؤكد لوائح اللجنة الدولية للصليب الأحمر أن أي هجوم سيبراني يُفضي إلى تعطيل الخدمات الطبية، يُعد جريمة بموجب القانون الدولي، سواء كان مرتكب الجريمة فرداً أم دولة^(٢).

أما البعد الثالث فهو المسؤولية الجنائية الفردية، التي يُمكن أن تنشأ بموجب نظام روما الأساسي للمحكمة الجنائية الدولية، إذا ما ثبت أن الفعل السيبراني تسبب في نتائج خطيرة بحق المدنيين أو البنى التحتية ذات الطابع الإنساني. ويُلاحظ أن النظام لا يُميز بين المدني والعسكري في هذا السياق، بل يركز على توافر أركان الجريمة من حيث القصد الجنائي، والعلاقة السببية، ونتيجة الفعل^(٣).

وتتخذ المشاركة المدنية في الحرب السيبرانية أشكالاً متعددة، منها تنفيذ هجمات برمجية ضد أنظمة التحكم في المستشفيات أو شبكات الكهرباء المغذية لها، أو نشر برمجيات خبيثة (Malware) تستهدف شل أنظمة الدعم الإنساني، أو تقديم خدمات تقنية أو لوجستية لمصلحة طرف مسلح، أو حتى الانخراط في هجمات حجب الخدمة (DDoS) على مواقع إلكترونية مدنية. وفي ضوء تفسير اللجنة الدولية للصليب الأحمر، فإن هذه الأفعال تدرج تحت مفهوم "المشاركة المباشرة في الأعمال العدائية"، مما يفقد المدني بموجبها حمايته القانونية.

وإذا كانت الهجمات تستهدف مناطق تحظى بوضع قانوني خاص، كالمستشفيات أو مناطق الإيواء، فإن مشاركة المدنيين في هذه الأفعال تُثير نتائج قانونية خطيرة؛ إذ قد تُفقد هذه المواقع صفتها المحمية إذا تم استخدامها لأغراض عسكرية سيبرانية. كما يُصبح المدني عرضة للهجوم المشروع، وقد تُقام عليه دعوى جنائية دولية إذا توافرت أركان الجريمة، الأمر الذي يفتح الباب أمام توسع خطير

١ ينظر: المادة (٣/٥١) من البروتوكول الإضافي لاتفاقيات جنيف الصادر في ١٢ أغسطس ١٩٤٩

٢ اللجنة الدولية للصليب الأحمر، دليل تفسير مفهوم المشاركة المباشرة في الأعمال العدائية بموجب القانون الإنساني الدولي، جنيف، مايو.

٣ ينظر: المادة (٨) من نظام روما الأساسي للمحكمة الجنائية .

في نطاق الأعمال العدائية، لا سيما حين تُستخدم مشاركة بعض المدنيين كذريعة من قبل أطراف النزاع لشن هجمات مضادة على مناطق مدنية واسعة النطاق.

وتُعد هذه المعضلات القانونية انعكاساً لصعوبات واقعية حقيقية، على رأسها غياب القدرة على التمييز الدقيق بين المقاتل والمدني في الفضاء السيبراني، خاصة مع تنامي ظاهرة الجماعات اللامركزية من قراصنة الإنترنت الذين يعملون بدوافع قومية أو شخصية. ويُضاف إلى ذلك الضعف الكبير في وسائل الإثبات والإسناد التقني التي يمكن من خلالها تحديد الجهة المنفذة للهجوم، لا سيما مع استخدام أدوات إخفاء الهوية^(١).

وما تزال القواعد العرفية الدولية المتعلقة بمسؤولية الأفراد المدنيين عن الأفعال السيبرانية في النزاعات المسلحة في طور التبلور، ما يفرض تحدياً كبيراً على الممارسة الدولية من حيث تطوير سوابق قانونية، وتحديد المسؤوليات، وإرساء معايير موضوعية للتقييم.

وفي المحصلة، فإن الانخراط المدني في الهجمات السيبرانية يُعد من أبرز مظاهر تعقيد النزاعات المسلحة المعاصرة، ويستدعي تطويراً عاجلاً في أدوات التكيف القانوني والردع والمساءلة، بما يتوافق مع الطبيعة اللامادية واللامركزية لهذا النوع من الحروب، مع الحفاظ على المبادئ الأساسية للقانون الدولي الإنساني، وفي مقدمتها مبدأ التمييز، ومبدأ التناسب، ومبدأ الضرورة العسكرية^(٢).

يتضح مما تقدم: من خلال استعراض الأدبيات القانونية والممارسات الدولية، يتبين أن الهجمات السيبرانية أصبحت تُشكل أحد أبرز ملامح النزاعات المسلحة المعاصرة، مما يستدعي إخضاعها لأحكام القانون الدولي الإنساني، ولا سيما لمعيار التمييز في تحديد الأهداف العسكرية المشروعة. وقد أكدت العديد من الوثائق التفسيرية، مثل دليل تالين الصادر عن مجموعة خبراء القانون الدولي بشأن الفضاء السيبراني، أن الهجمات السيبرانية، التي ترتقي إلى حد النزاع المسلح تُخضع أطراف النزاع لواجبات قانونية من أبرزها عدم استهداف المدنيين أو الأعيان المدنية.

^١ مصطفى السيد عبد السلام أبو النور وآخرون، "مواجهة الحرب السيبرانية أثناء النزاعات المسلحة في ضوء القانون الدولي الإنساني"، مجلة كلية الشريعة والقانون بنقهننا الأشراف، المجلد ٢٩، عدد ٣، ٢٠٢٤.

^٢ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، متاح على

ويُستخلص كذلك أن تحديد الهدف العسكري المشروع في الفضاء السيبراني يتطلب تقييم طبيعة الوظيفة أو التأثير الذي يحدثه الكيان المستهدف، وليس فقط طبيعته المادية أو شكله القانوني. فمثلاً، قد يكون خادم إلكتروني تابع لوزارة مدنية هدفاً عسكرياً إذا ثبت استخدامه بشكل مباشر لدعم العمليات العسكرية، كأن يكون جزءاً من شبكة القيادة والسيطرة أو يُستخدم في توجيه الأسلحة. وأن الأهداف المدنية التي تسهم في المجهود الحربي بطريقة فعالة وتُتيح ميزة عسكرية واضحة تصبح، بموجب القانون الدولي، أهدافاً مشروعة يمكن استهدافها، شريطة أن تراعى مبادئ التناسب والاحتياطات الممكنة. وعليه، فإن المعايير المعتمدة في تحديد الأهداف العسكرية المشروعة في الهجمات السيبرانية تتمثل في: الطبيعة (كون الهدف منشأة أو نظاماً عسكرياً بحثاً)، الموقع (مثل مركز عمليات عسكرية أو بنية تحتية حيوية تستخدم في العمليات)، الغرض (إذا كان يخدم أهدافاً عسكرية مباشرة)، والاستخدام الفعّال (أي تسخير الأنظمة المعلوماتية أو الرقمية بشكل يُسهم فعلياً في العمليات الحربية).

المطلب الثاني

تحديد انطباق القانون الدولي الإنساني على الهجمات السيبرانية

يواجه انطباق القانون الدولي الإنساني على الهجمات السيبرانية تحديات عدة، والتساؤل المهم الذي يطرح نفسه هو مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية؟ خصوصاً والقانون الدولي الإنساني لا يتضمن أية قواعد صريحة بشأن الهجمات السيبرانية في الفضاء السيبراني، والسبب في ذلك هو أنها لا تكون هذه الهجمات حركية، أي ليست هجمات مسلحة بالمعنى التقليدي، إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل بحماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقاً، وتندرج تلك الهجمات ضمن قواعده إذا كان هدف الهجمات السيبرانية هو تعريض الأشخاص المحميين وممتلكاتهم للخطر أو المخاطرة بحدوث ذلك، ولكن يبقى التحدي في مقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة.

والتساؤل هنا بالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل بحماية المدنيين من ويلات الحروب هل يصبح القانون الدولي منطبقاً على الهجمات السيبرانية إذا تمكنت الهجمة من تحقيق أهدافها وغاياتها إن كانت مدنية أم عسكرية؟ وهذا يحيلنا إلى سؤال آخر، ما هو موقف اتفاقيات جنيف الأربع من الهجمات السيبرانية، وكيف عالجت حماية المعنيين بالحماية في أثناء النزاعات المسلحة؟

ركزت اتفاقيات جنيف الأربع لعام ١٩٤٩ على حماية الأشخاص في حالة النزاعات المسلحة دون الإشارة إلى الهجمات السيبرانية، ودون الإشارة إلى استخدام أسلحة معينة. إلا أنه تعد البروتوكولات

الإضافية أكثر ملاءمة لتقديم موقفها من استخدام الهجمات السيبرانية، و أشرنا سابقاً المادة (٣٦) و (٣٥) الفقرة (١) من البروتوكول الإضافي الأول لعام ١٩٧٧ فضلاً عن شرع مارتينز والرأي الاستشاري لمحكمة العدل الدولية بشأن شرعية التهديدات بالأسلحة النووية أو استخدام هذه الأسلحة، فكلها تدل على أن القانون الدولي الإنساني قابل للانطباق على الهجمات السيبرانية، التي تحدث في سياق النزاع المسلح، إلا إن الهجوم السيبراني إذا لم يحدث في سياق نزاع مسلح ولكن آثاره وتداعيات هذا النزاع المسلح فيمكن انطباق القانون الدولي الإنساني عليه، ولكن بالمقابل إذا ما كانت آثاره لا تصل إلى تأثير الهجوم العسكري الفعلي نفسه، لا يمكن انطباق القانون الدولي الإنساني عليه، بل يخضع للقانون الدولي لحقوق الإنسان وللقوانين الجنائية الوطنية. سنبحث هذا المطلب عبر فرعين، في الفرع الأول الهجمات السيبرانية في سياق النزاع المسلح، وفي الفرع الثاني سنبحث الهجمات السيبرانية خارج سياق النزاع المسلح.

الفرع الأول

انطباق القانون الدولي الإنساني على الهجمات السيبرانية في سياق النزاع المسلح

ويعد القانون الدولي الإنساني الحد الأساس، الذي يضع قيوداً على اللجوء إلى الهجمات السيبرانية في أثناء النزاع المسلح، ويحمي السكان المدنيين من الأضرار المحتملة. وعرفت "اللجنة الدولية للصليب الأحمر" الهجمات السيبرانية في أثناء النزاع المسلح: "إنها عمليات تستهدف أنظمة إلكترونية أو شبكات الحاسوب أو أي جهاز آخر متصلًا، عبر تدفق البيانات، حين استخدامها وسيلةً أو أسلوباً للحرب في سياق نزاع مسلح^(١)."

نرى أن "اللجنة الدولية للصليب الأحمر" منذ البداية كان لها الموقف الإيجابي والواضح، وترى "اللجنة الدولية للصليب الأحمر" أنه لا شك أن "القانون الدولي الإنساني" ينظم الهجمات السيبرانية في أثناء النزاعات المسلحة أو الحرب السيبرانية- شأنه شأن أي سلاح أو أسلوب ووسيلة قتال يلجأ إليها

١ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف مقدمة 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، ٢٠١٩، تاريخ الزيارة ٢٠٢٤/٦/١٦، الساعة ١٢:٠٠، متاح على الرابط: [www.icrc.org/ara/document/international-humanitarian-law-and-cyber-operations-during-](http://www.icrc.org/ara/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts)

أي طرف من الأطراف المتحاربة في النزاع، أكانت قديمة أم حديثة. وأن اعتماد الهجمات السيبرانية على تقنية جديدة ومتطورة باستمرار لا يمنع هذا تطبيق "القانون الدولي الإنساني" على استخدام هذه التقنيات بوصفها من وسائل أو أساليب القتال. ويصح ذلك سواء أكان الفضاء السيبراني يُعد ساحة جديدة للقتال على غرار الجو والأرض والبحر والفضاء الخارجي أم نوعاً جديداً من الميادين، لأنه من صنيعة الإنسان، بينما الأول طبيعي، أو لا يُعد ميداناً على هذا النحو^(١).

ويرى الباحث: إن تأييداً واضحاً قوياً لهذا الرأي في اتفاقيات "القانون الدولي الإنساني"، وفي الاجتهادات القضائية لمحكمة العدل الدولية، وفي الآراء التي أبدتها كثير من الدول والمنظمات الدولية. وتعد الهجمات السيبرانية جزء مهم من النزاع المسلح سواء أكان النزاع المسلح دولياً أم أنه نزاع مسلح غير دولي، لأن "القانون الدولي الإنساني"، هو مجموعة القواعد، التي تهدف إلى الحد من آثار النزاعات المسلحة وتقليصها لدواعٍ إنسانية، ومن ثم فإن ميدان "القانون الدولي الإنساني" النزاع المسلح، وعليه ينبغي أن يُرسمَ خط واضح يميز بين الحالات التي تُعدّ نزاعاً مسلحاً والحالات، التي لا تُعدّ نزاعاً مسلحاً، لكنها مهمة ليست يسيرة، ولا سيما أن الهجمات امتازت في أنها يمكن أن تُرتكب في ظروف غير منتظمة بصورة أساسية^(٢).

وأن غاية "القانون الدولي الإنساني" هو تنظيم النزاعات المستقبلية، أي التي تقع بعد أن اعتُمدت معاهدة من معاهدات القانون الدولي الإنساني. وأدرجت الدول، عند اعتمادها "معاهدات القانون الدولي الإنساني"، القواعد، التي تستشرف تطوير واختراع وسائل وأساليب حديثة للنزاعات، وقد افترضت أن "القانون الدولي الإنساني" سينطبق عليها. ففي عام (١٨٦٨)، كان إعلان سان بطرسبورغ يسعى إلى الحفاظ على مبادئ قد وضعها بشأن التحسينات المستقبلية، التي قد يسخرها العلم إلى تسليح الجيوش ويدخلها عليها^(٣). لذلك يجب أن تمتثل وسائل وأساليب الحرب القائمة على التكنولوجيا

١ القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، ٢٠١١ (تقرير التحديات لعام ٢٠١١ الصادر عن اللجنة الدولية)، الصفحات ٣٦-٣٩، تاريخ الزيارة ١٦/٦/٢٠١٢ الساعة ٤:٠٠، متاح على الرابط: التالي:

<https://www.icrc.org/ar/document/international-armed-conflicts>

٢ عمر مكي، القانون الدولي الإنساني في النزاعات المسلحة المعاصرة، اللجنة الدولية للصليب الأحمر، سويسرا، ٢٠١٧، ص ٩٣.

٣ يُنظر: إعلان سان بطرسبورغ بغية حظر استعمال قذائف معينة في زمن الحرب، سان بطرسبورغ، ٢٩ تشرين الثاني/نوفمبر - 11 كانون الأول/ديسمبر ١٨٦٨.

السيبرانية، عند استخدامها في نزاع مسلح من قبل أو لصالح أو نيابة عن أحد أطراف النزاع القائم لقواعد ومبادئ القانون الدولي الإنساني، و هو الحال مع أي سلاح جديد أو أسلوب جديد لتنفيذ العمليات. و أوضحت ذلك المادة (٣٦) من البروتوكول الإضافي الأول لعام (١٩٧٧)، والتي تنص على ما يأتي: يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد^(١)، وبالمثل تنص المادة (٤٩) منه على أن قواعد هذا البروتوكول تنطبق على الحروب البرية، وعلى جميع أنواع الحروب الأخرى التي قد تضر المدنيين على البر، وهذا ينطبق على الحرب السيبرانية، التي تخاض ولو جزئياً من بنية تحتية أساسية موجودة على البر وتوجه ضد أهداف على البر، وتتطوي على مخاطر تؤدي إلى إلحاق الأذى بالمدنيين على البر^(٢).

ومن ثم، ليس ثمة شك في أن هذا الالتزام استند إلى افتراض، جوهره أن "القانون الدولي الإنساني" ينطبق على الأسلحة والوسائل والأساليب الجديدة، وإلا لا ضرورة من استعراض مشروعيتها على وفق أحكام القانون الحالية، وهذا يشمل على الأسلحة ووسائل وأساليب القتال، التي اعتمادها الأكبر على التكنولوجيا السيبرانية.

ويلقى "القانون الدولي الإنساني"، الذي يتكيف على العمليات السيبرانية في أثناء النزاع المسلح مزيداً من التأييد في الآراء، التي صدرت عن محكمة العدل الدولية، إذ إنها ذكرت، بفتوة لها بشأن شرعية التهديدات بالأسلحة النووية أو استخدامها، أن القانون الدولي الإنساني تنطبق قواعده المستقرة، المنطبقة في أثناء النزاع المسلح على جميع أشكال النزاعات، وكل أنواع الأسلحة، ومن ضمنها "ما سيكون في المستقبل"^(٣).

بالمقابل التأكيد على أن "القانون الدولي الإنساني" ينطبق على العمليات السيبرانية في أثناء النزاع المسلح لا يشجع على عسكرة الفضاء السيبراني، ولا يجب -مهما كان الأمر- أن يفهم على أنه يضيف الشرعية على الهجمات السيبرانية، وأن أي لجوء من الدول إلى القوة، أكان اللجوء ذا طابع سيبراني

١ يُنظر: المادة (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧.

٢ يُنظر: المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧.

٣ محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى، ٨ تموز/يوليو ١٩٩٦، الفقرة ٨٦.

أو حركي، فهو يبقى-أبدًا- خاضعًا إلى "ميثاق الأمم المتحدة، والقانون الدولي العرفي"، ولا سيّما الحظر المفروض على استخدام القوة^(١).

ويفرض "القانون الدولي الإنساني" القيود على سير الأعمال العدائية متى قررت الدول أو الأطراف من غير الدول اللجوء إلى العمليات السيبرانية في أثناء النزاع المسلح. وعلى وجه التحديد، أن القانون الدولي الإنساني يحمي المدنيين والأعيان المدنية من آثار الأعمال العدائية من خلال تحجيم وتقليص خيارات المتنازعين إلى وسائل وأساليب القتال، بصرف النظر عن شرعية أو عدم شرعية استخدام القوة. وهذا يعني أن "القانون الدولي الإنساني" عوضاً عن إضفاء الشرعية على العمليات السيبرانية أو على كل العمليات العسكرية الأخرى في أثناء النزاع المسلح، فإنه يضع قيوداً فضلاً عن القيود الواردة في ميثاق الأمم المتحدة و "القانون الدولي العرفي" - قانون مسوغات الحرب. زيادةً على ذلك، يضع القانون الدولي الإنساني واقعاً بعض القيود على عسكرة الفضاء السيبراني، فهو يحظر -مثلاً- تطوير القدرات السيبرانية، التي يمكن عدّها أسلحة، وتكون عشوائية على وفق طبيعتها أو من شأنها تحقق إصابات غير مسوّغة أو معاناة غير لازمة أو ضرورية^(٢).

ويمكن أن ينقسم نطاق تطبيق قواعد القانون الدولي الإنساني، التي تنظم وسائل وأساليب النزاع على: قواعد تنطبق على كافة الأسلحة ووسائل وأساليب النزاع، أينما لزم استخدامها "مثل مبادئ التمييز والتناسب والاحتياط"، و قواعد مختصة بأسلحة محددة "مثل معاهدات الأسلحة" أو مجالات أخرى معينة "مثل القواعد التي تنظم الحرب البحرية تحديداً". وتعود كافة المبادئ والقواعد العرفية الرئيسة المنظمة لسير الأعمال العدائية إلى الفئة الأولى وتطبق -فعلاً- على العمليات السيبرانية في أثناء النزاع المسلح، ومن ناحية أخرى، يلزم إجراء تحليل أكثر تفصيلاً بشأن انطباق قواعد القانون الدولي الإنساني المتعلقة -على وجه الخصوص- بأسلحة معينة أو مجالات معينة.

من المتفق عليه أن القانون الدولي الإنساني ينطبق على الهجمات السيبرانية، التي تحدث في سياق نزاع مسلح قائم بالفعل، فينبغي على الدول أن تحترم قواعد القانون الدولي الإنساني عندما تشن هجمات سيبرانية في إطار النزاع المسلح، بغض النظر عما إذا كان الفضاء السيبراني معترفاً به

١ يُنظر: ميثاق الأمم المتحدة، المادة (٤/٢).

٢ جون-ماري هنكرتس ولويس دوزوالد-بك، القانون الدولي الإنساني العرفي، المجلد الأول: القواعد، القاهرة، ٢٠٠٧، (دراسة اللجنة الدولية للقانون العرفي)، القاعدتان ٧٠ و٧١.

كميدان قتال اصطناعي جديد، يضاف إلى الميادين الطبيعية للحرب المتمثلة بالبر والجو والبحر والفضاء الخارجي، ويرتب بجميع هذه الميادين الطبيعية، أم لم يُعد ميدانياً للحرب في حد ذاته^(١).

وهناك حالات حصل فيها هجمات سيبرانية في سياق نزاع مسلح قائم بالفعل، فضلاً عن ذلك يحقق تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في مصلحة جميع الدول، إذ إنه يخدمها في أن يضمن توافق سلوك قواتها المسلحة مع المبادئ والاتفاقيات الدولية.

وقد تحدثت الهجمات السيبرانية في ساحة موازية لحرب تقليدية أو نزاع مسلح دائر على الأرض، ويكون ذلك تعبيراً عن حدة النزاع القائم بين لأطراف، وقد يمهّد لعمل عسكري، وهنا تدور الحروب السيبرانية عن طريق اختراق المواقع الإلكترونية، وتدميرها، وشن حرب معلوماتية وتجسسية ضد الخصوم. ويستمد هذا النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، ولا سيما في ظل بعض التقديرات التي تشير إلى أن نفقات هذه الحروب أقل من نفقات نظيراتها من الحروب التقليدية، ويمكن تمويل حرب متكاملة وتحقيق أهدافها عبر الانترنت بتكلفة دبابية^(٢).

و نجد حالات تطبيقية لهذه الهجمات السيبرانية في حرب كوسوفو عام (١٩٩٩)، إذ استهدفت الهجمات السيبرانية تعطيل شبكة الاتصالات للخصوم، وأيضاً برزت خلال الحراب بين الجمهورية العربية السورية والكيان الصهيوني عام (٢٠٠٧)، وكذلك بين روسيا وجورجيا في عام (٢٠٠٨)^(٣). ونرى، على الرغم من تحقق أسباب قانونية دامغة وتزايد التأييد الدولي للاستنتاج، الذي توصل إلى أن "القانون الدولي الإنساني" ينطبق على الهجمات السيبرانية في أثناء النزاع المسلح، فإن المسألة لا حظ لها من اتفاق عالمي حتى الآن. ومن ناحية أخرى، فإن التمهّص الدقيق في الحجج المختلفة، التي أثيرتها المناقشات العديدة التي حصلت بين الأطراف يبين أن تأكيد انطباق "القانون الدولي الإنساني" لا يضيف الشرعية لأن يُعسكر الفضاء السيبراني أو اللجوء إلى الهجمات السيبرانية المضرة، وزيادةً

١ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، تشرين الثاني ٢٠١٩، ص ٢٣.

٢ عادل عبد الصادق، مصدر سابق، ص ٢٨٦.

٣ موسى بن تغري، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، المجلد ١٢، العدد ٢٢، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠، ص ٢٠٥.

على ذلك، هذا لا يمنع أن تُضع قواعد جديدة مستقبلية محتملة، أنما يوفر الإطار القانوني الرئيس، يُمكن القواعد الجديدة المحتملة من أن تستند إليه.

يتضح مما سبق: أن الهجمات السيبرانية، حينما تُنفذ في سياق نزاع مسلح دولي أو غير دولي، قد ترقى إلى مستوى الأعمال العدائية التي تُخضع أطراف النزاع للقيود التي يفرضها القانون الدولي الإنساني. فالهجوم السيبراني، وإن كان لا يحدث دماراً مادياً ظاهراً دائماً، إلا أن أثره على الأهداف العسكرية أو المدنية قد يكون بالغاً، ولا سيما إذا استهدف بنى تحتية حيوية كشبكات الكهرباء، وأنظمة الاتصالات، والمنشآت الصحية، أو تسبب في شلل مؤسسات الدولة. ومن ثم، فإن هذه الهجمات تخضع للضوابط القانونية ذاتها التي تنطبق على الوسائل والأساليب التقليدية في القتال، وعلى رأسها مبادئ التمييز والتناسب والاحتياطات الممكنة. وأن بعض الهجمات السيبرانية، التي تُحدث آثاراً مدمرة وتستهدف السكان المدنيين أو تعطل الخدمات الأساسية، قد تُشكل جرائم حرب تستوجب المساءلة الدولية. وقد أظهرت ممارسات الدول ومواقف المنظمات الدولية وجود ميل متزايد نحو عدّ الهجمات السيبرانية، التي تبلغ حد الهجوم بموجب المادة (٤٩) من البروتوكول الإضافي الأول، خاضعة لأحكام القانون الدولي الإنساني.

ويرى الباحث: أن الاعتراف بالهجمات السيبرانية كوسائل قتال في أثناء النزاعات المسلحة يفرض تحديات قانونية وعملية كبيرة على القانون الدولي الإنساني، ويستدعي تحديثاً للمفاهيم التقليدية التي لم تكن مصممة إلى تعامل مع الفضاء الرقمي. ويرى الباحث أن الطبيعة غير المادية لهذه الهجمات، والقدرة على إخفاء مصدرها، وصعوبة التحقق من آثارها المباشرة أو غير المباشرة، تجعل من الضروري اعتماد منهج جديد في تفسير وتطبيق قواعد القانون الإنساني.

الفرع الثاني

انطباق القانون الدولي الإنساني على الهجمات السيبرانية خارج سياق النزاع المسلح

لا تُشن الهجمات السيبرانية بالضرورة في أثناء نزاع مسلح قائم بالفعل، بل نتيجة التطور التكنولوجي والاعتماد الشامل على أجهزة الحاسوب وشبكات الاتصالات، يمكن أن نجد لها مجال تطبيق واسع في كل الأوقات، فقد تستخدم هذه الهجمات في أوقات السلم، كاستخدامها نتيجة توتر سياسي أو اقتصادي بين بلدين أو لاتباع سياسة معينة غير محبذة من قبل دولة أخرى أو لأسباب كثيرة أخرى، وقد تستهدف الهجمات السيبرانية البنى التحتية للمعلومات والانترنت أو توجه ضد البنى التحتية الحرجة المعتمدة على شبكات الحاسوب والانترنت في تشغيلها وعملها، وقد تستهدف القطاع

الخاص من شركات ومصارف، وهناك إجماع بين المختصين في القانون الدولي الإنساني بأن الهجمات السيبرانية، التي تقع خارج نزاع مسلح حركي قائم ليس من الشرط أن ينظمها القانون الدولي الإنساني، ويذهب إلى ذلك لوران جيزيل المستشار القانوني للجنة الدولية للصليب الأحمر بقوله: يعني ذلك إن القانون الدولي الإنساني ينطبق على جميع العمليات الإلكترونية، أو كل ما يطلق عليه الهجمات السيبرانية في اللغة الشائعة، فالقانون الدولي الإنساني لا ينظم العمليات الإلكترونية، التي تقع خارج سياق النزاع المسلح^(١).

وعلى الرغم من ذلك تجدر الإشارة إلى أن اتفاقيات جنيف لعام (١٩٤٩) استبدلت مصطلح الحرب المستخدم في اتفاقيات لاهاي بمصطلح النزاع المسلح من أجل توسيع النطاق المادي لتطبيق الاتفاقيات، وجعل القانون الدولي الإنساني قابلاً للتطبيق بناءً على تقييم واقعي لكل حالة. ووفقاً لدائرة الاستئناف التابعة للمحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية تاديتش، لكي نكون أمام نزاع مسلح دولي يجب توافر عنصرين: أولهما نزاع بين دولتين على الأقل، وثانيهما لجؤهما إلى القوة المسلحة ضد بعضهما بعض، ولا يقصد باللجوء إلى القوة المسلحة أن تقوم الدولة باستخدام قواتها المسلحة، إنما اللجوء إلى الأعمال العدائية الحربية ضد دولة أخرى، وهذا ما تبناه دليل تالين، إذ نص على أنه يوجد نزاع مسلح دولي عندما تكون هناك أعمال عدائية، التي قد تشمل أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر، إذ يقصد بالأعمال العدائية التطبيق الجماعي لوسائل وأساليب الحرب. ويعتمد تطبيق القانون الدولي الإنساني على الحالة الواقعية وليس على إدراك حالة النزاع المسلح من جانب الأطراف فيه^(٢). فإذا نفذ عملاء المخابرات المدنية بعمليات سيبرانية تصل إلى حد القوة المسلحة، وتسبب أو من المحتمل أن تتسبب في أضرار مادية للممتلكات أو فقدان الأرواح أو إصابة الأشخاص فقد يكون هناك نزاع مسلح، وإذا أمكن إثبات نسب الهجمات السيبرانية إلى دولة معينة لكان من الممكن انطباق القانون الدولي الإنساني مثلما لو تم تنفيذ الهجوم بوسائل حركية من ناحية أخرى، أما إذا كانت القوات المسلحة تشارك فقط في أنشطة تجسس أو أعمال شغب وتخريب دون التسبب بضرر مادي حقيقي، فلا يمكن القول إنها ترقى إلى نزاع مسلح في غياب الأعمال العدائية المتزامنة، بالمقابل لو أن مثل هذا الهجوم السيبرانية استهدف مثلاً شبكة الكهرباء

١ زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، جامعة الكوفة، كلية القانون، النجف الاشرف، العراق، ٢٠١٦، ص ٤٢-٤٤.

٢ كودولار دوريحي، مصدر سابق، ص ٥٤٣.

الوطنية واستمر لمدة طويلة، مع تداعيات سلبية شديدة على توفير الخدمات الطبية والنقل والأسواق المالية، والأمن فيمكن عدّ مثل هذه الهجمات أعمالاً عدائية، ترقى إلى استعمال القوة المسلحة، وإذا أمكن نسبة هذه الهجمات السيبرانية لدولة معينة أو مجموعة مسلحة، لكان ممكناً انطباق القانون الدولي الإنساني عليها^(١).

وقد تحدثت الهجمات السيبرانية في ساحة منفردة وغير متوازية مع الأعمال العسكرية التقليدية، أي تحدثت في حالة لا يكون فيها حرب تقليدية أو أي نزاع مسلح، ولكن هذه الهجمات السيبرانية إذا كانت ترقى إلى مستوى نزاع مسلح، وتسببت في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة الأشخاص وكان في الإمكان إثبات نسبة الهجمات إلى دولة معينة فعندئذ نطبق القانون الدولي الإنساني، أما إذا كان من الصعب إثبات نسبة الهجوم السيبرانية إلى دولة معينة لا يمكن تطبيق القانون الدولي الإنساني عليها وعوضاً عن ذلك يمكن تطبيق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة المعنية وتاريخياً نجد حالات تطبيقية لهجمات السيبرانية تحدث خارج سياق نزاع مسلح مثل الهجمات السيبرانية بين الصين والولايات المتحدة الأمريكية، وأيضاً ترزت خلال الهجوم السيبراني على استونيا عام (٢٠٠٧) ، وكذلك الهجوم السيبرانية على المنشآت النووية الإيرانية من نهاية عام (٢٠٠٩) إلى منتصف عام (٢٠١٠)^(٢) في عام ٢٠١٣، تعرّض نظام التحكم الخاص بـ سد (Bowman Avenue) الواقع في مدينة (ري Rye)، في ولاية نيويورك، إلى هجوم سيبراني نفذته مجموعة مرتبطة بالحكومة الإيرانية. إذ تمكن المهاجمون من الدخول إلى نظام التحكم الخاص بالسد عبر الإنترنت، وكان بإمكانهم نظرياً فتح البوابة المائية، ما قد يؤدي إلى تدفق غير مسيطر عليه للمياه. لم يحدث ضرر فعلي لأن بوابة السد كانت غير فعالة وقتها بسبب الصيانة^(٣).

١ إيمان حمدان، مصدر سابق، ص ٦.

٢ زهراء عماد محمد كلنتر، مصدر سابق، ص ٤٥.

٣ ينظر: البيان الصادر عن وزارة العدل الأمريكية ، متاح على الرابط

<https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>

تاريخ الزيارة ٢٠٢٥/٢/٢٢

وفي العام ٢٠٢٢، أجهضت إيران محاولة تخريبية منسوبة إلى الكيان الصهيوني، كان الهدف منها (موقع فوردو) لتخصيب اليورانيوم، عبر تجنيد عاملين داخل المنشأة ومحاولة زرع أجهزة تخريبية أو برامج خبيثة^(١).

. تبين لنا: من خلال استعراض الإطار القانوني الدولي أن الهجمات السيبرانية التي تقع خارج سياق النزاع المسلح لا تخضع مباشرةً لأحكام القانون الدولي الإنساني، بوصفه قانوناً يُطبق حصرياً في حالات النزاع المسلح الدولي أو غير الدولي. ومع ذلك، فإن هذه الهجمات قد تثير إشكاليات قانونية متعددة تتعلق بانتهاك سيادة الدول، أو تدخل غير مشروع في الشؤون الداخلية، أو حتى تهديد السلم والأمن الدوليين، بحسب طبيعتها وأثرها ودرجة الضرر الذي تحدثه. وقد أوضحت العديد من الوثائق الدولية، مثل دليل تالين ٢.٠، أن بعض الهجمات السيبرانية التي لا ترقى إلى مستوى الهجوم المسلح قد تخضع لأحكام القانون الدولي العام، ولا سيما مبدأ عدم التدخل، ومبدأ السيادة، وعدم استخدام القوة أو التهديد بها و ورد في ميثاق الأمم المتحدة. ويُستخلص كذلك أن غياب الضرر المادي لا يعني بالضرورة انتفاء الأثر القانوني للهجوم، إذ إن تعطيل أنظمة صحية، أو نشر برامج خبيثة تؤدي إلى توقف خدمات عامة أساسية، أو التأثير في نظم الانتخابات، قد يُعد من أشكال التدخل غير المشروع ويستلزم استجابة قانونية مناسبة.

ونرى: إن القانون الدولي الإنساني لا ينطبق خارج سياق النزاع المسلح، ولكن إذا حدث هجوم سيبراني سبب أو من المحتمل أن يسبب في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص يمكن أن ترقى هذه الهجمات السيبرانية إلى وصف نزاع مسلح، قياساً على الهجمات العدائية الحركية، التي ترقى إلى نزاع مسلح، ويطبق عليها القانون الدولي الإنساني.

المبحث الثاني

آثار الهجمات السيبرانية على المناطق المحمية

ينجم عن النزاعات المسلحة التي تمر على مختلف العصور مآسي وأهوال، وترتكب بحق الإنسان جرائم مختلفة، وتعد انتهاك لحقوقه، وعلى الرغم من فرض عقوبات، وتحريم استعمال القوة والعنف أو التهديد بها من قبل عصبة الأمم ومن ثم الأمم المتحدة، وفرض عقوبات من قبل المحاكم الشرعية

١ ينظر: مقال متاح على الرابط <https://farsnews.ir/showcase> تاريخ الزيارة ٢٠٢٥/١/٢

الدولية إلا أن الحرب ما تزال حل تلجأ إليه الدول لحل نزاعاتها وفرض سيطرتها على الدول الأخرى.

لذلك لجأ المجتمع الدولي لوضع مجموعة من القواعد القانونية تعمل على ضبط الحروب والنزاعات المسلحة وآثارها، وتأمين الحماية الكافية للأفراد كافة، ويطلق عليها قواعد القانون الدولي الإنساني التي تقوم بحماية حقوق الإنسان في النزاعات المسلحة الدولية أو غير دولية، لحماية الأفراد المدنيين والأعيان المتضررين من النزاع المسلح.

وتعد من أولى أهداف القانون الدولي الإنساني توفير الحماية اللازمة للأفراد والأعيان المدنية وذلك من خلال إنشاء مناطق محمية بموجب قواعده، وفرض على أطراف النزاع المسلح عدم التعرض لها باعتبارها ليست من الأهداف العسكرية، وأنشأت خصيصاً لإيواء الأشخاص المتضررين من العمليات العسكرية، ومن اللازم تطبيق قواعد القانون الإنساني الخاص بحماية المناطق المحمية، والآليات التي وضعها القضاء الدولي الجنائي، التي تعمل على تحريم ومنع الاعتداءات، التي قد تتعرض لها المناطق المحمية من قبل أطراف النزاع المسلح في أنظمتها الأساسية، ومحاكمة كل من يقوم بانتهاك تلك القواعد وفرض عقوبات بحقهم. وسنبحث هذا الموضوع عبر مطلبين، نناقش في المطلب الأول مخاطر الهجمات السيبرانية، وفي المطلب الثاني دور القانون الدولي الإنساني في مواجهة آثار الهجمات السيبرانية.

المطلب الأول

مخاطر الهجمات السيبرانية على المناطق المحمية

لا تتغير المخاطر في حد ذاتها، ولكن سماتها هي التي تتغير مع تطور الأدوار والوسائل المستخدمة، فقد أصبحت الدول تهتم بتكنولوجيا المعلومات ودورها في الصراعات والحروب المستقبلية استعداداً لمواجهة ما ينشأ عنها من مخاطر، التي يتوقع الكثير حدوثها في الهجمات السيبرانية، ولذا نجد أن هناك عديد من المحاولات التي أُجريت تدريباً على هذا النوع الجديد من الصراع، وكيف يمكن مواجهته والاستعداد له، وبات من الصعب تخيل صراع عسكري اليوم دون أن يكون لهذا الصراع أبعاد سيبرانية، وأصبحت في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل، وحدث بين روسيا وإستونيا عام ٢٠٠٧، مما دفع العديد من الدول مثل الولايات المتحدة الأمريكية والصين على الرغم من التقدم التكنولوجي لها ببناء وحدات إلكترونية على شبكات الإنترنت للحماية من مئات وآلاف القرصنة المحترفين.

وأصبحت الهجمات السيبرانية بديلاً لتلك الحروب التقليدية، التي كانت تعتمد على جيوش عسكرية وأسلحة قتالية، فالهجمات السيبرانية على الرغم من أنها بدون نار أو قصف ولكن لها جانباً عنيفاً من

حيث السيبرانية على الرغم من أن الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وعلى الرغم من فداحة الخسائر، فإن الأسلحة بسيطة فهي عبارة فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وتتميز هذه الحروب بالسرعة والدقة في تنفيذ العمليات العسكرية وتعد من أدوات الحرب الشاملة. ولتسليط الضوء أكثر على هذا الموضوع سنقسم هذا المطلب على فرعين سنتناول في الفرع الأول مخاطر الهجمات السيبرانية على المناطق المحمية والأفراد، وفي الفرع الثاني الآثار الايجابية والسلبية على المناطق المحمية والأفراد.

الفرع الأول

مخاطر الهجمات السيبرانية على المناطق المحمية والأفراد

يضمن القانون الدولي الإنساني توفير الحماية اللازمة للمدنيين والأعيان المدنية، ومن أهم آلياتها إنشاء المناطق المحمية، التي عملت قواعده على حمايتها، إلا أنه قد تتعرض هذه المناطق للاعتداءات من قبل طرفي النزاع المسلح، لذلك كان من اللازم ضمان توفير حماية أكثر من خلال محاكمة مرتكبي هذه الاعتداءات ومعاقبتهم، نظراً للمخاطر، التي قد تؤدي إليها الهجمات السيبرانية. وتتماشى فكرة إنشاء وتحديد مناطق محمية تماشياً مع متطلبات القانون الدولي الإنساني، الذي يقوم على مجموعة من القواعد القانونية سواء أكانت الاتفاقية أم العرفية، التي تهدف أساساً إلى توفير الحماية لفئات معينة من الأفراد والممتلكات والأعيان ذات الطابع المدني، وتحريم تعرضهم لأيّة هجمات في أثناء النزاعات المسلحة الدولية وغير الدولية.

أولاً. المناطق المحمية:

للدواعي الإنسانية، التي تعد غاية القانون الدولي الإنساني، يستلزم إنشاء مناطق يمكن وصفها بالمحمية، وذلك باتفاق بين أطراف النزاع أو من دون موافقة بعض أو كل الأطراف، والتي قد تشترك في توفير الحماية والمساعدة للفئات المتضررة من المدنيين وكذلك الجرحى والمرضى من المقاتلين، فضلاً عن حماية الأعيان ذات الطابع المدني^(١).

١ اللجنة الدولية للصليب الأحمر، البروتوكولين الإضافيين لاتفاقيات جنيف لعام ١٩٤٩ (Protocol II و Protocol I)،

متاح على الرابط: [https://shop.icrc.org/the-protocols-additional-to-the-geneva-conventions-](https://shop.icrc.org/the-protocols-additional-to-the-geneva-conventions-of-12-august-1949-pdf-ar.html?utm_source=chatgpt.com)

[of-12-august-1949-pdf-ar.html?utm_source=chatgpt.com](https://shop.icrc.org/the-protocols-additional-to-the-geneva-conventions-of-12-august-1949-pdf-ar.html?utm_source=chatgpt.com)

وأيضاً: <https://www.icrc.org/en/article/protocols-i-ii-geneva-conventions>

على أن هذه المناطق قد تتميز فيما بينها على وفق القواعد القانونية لتي تحكمها. لذلك حرصت اتفاقيات القانون الدولي، ولا سيما اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولات الإضافيين بها لعام ١٩٧٧ على بيان التنظيم القانوني، لهذه المناطق، نظراً لما لها من أهمية خاصة في توفير الملاذ الآمن للمتواجدين فيها، فضلاً عن احترام وتعزيز الحماية للأعيان والممتلكات ذات الطابع المدني.

في خريف عام ٢٠٢٠، وبينما كانت الولايات المتحدة تواجه ذروة تفشي جائحة كوفيد-١٩، وقع حدث سيبراني خطير سلّط الضوء على هشاشة البنية التحتية الصحية، ليس فقط أمام الأمراض، بل أمام الهجمات الرقمية المنظمة.

ففي الأسبوع الأخير من شهر أكتوبر، تعرّضت عدة منشآت طبية أمريكية، من بينها مستشفيات في ولايات نيويورك، كاليفورنيا، رود آيلاند، وأوريغون، لهجوم رقمي واسع النطاق نفذته مجموعة قرصنة يُعتقد أنها تستخدم برمجية الفدية المعروفة باسم Ryuk.

هاجم المهاجمون الأنظمة الرقمية للمستشفيات، وقاموا بتشفير سجلات المرضى والبيانات الطبية الحيوية، وطالبوا بفدية مقابل فك التشفير. ونتيجة لذلك، تعطلت خدمات الطوارئ في عدد من المستشفيات، وتم تأجيل عمليات جراحية، وأرغم الطاقم الطبي على العودة لاستخدام الملفات الورقية في ظل ضغط استثنائي تفرضه الجائحة.

على رغم من أن الهجوم لم يُستخدم فيه سلاح مادي، إلا أن أثره كان مماثلاً لهجوم فعلي على مرفق إنساني محمي. لم تميز البرمجية الخبيثة بين هدف عسكري وآخر مدني، ولم يُظهر منفذوها أي اعتبار لسلامة المرضى أو خصوصية البيانات الصحية أو الحق في العلاج، بل أطلقوا الهجوم بطريقة عشوائية أربكت النظام الصحي في لحظة حرجية^(١).

من منظور القانون الدولي الإنساني، يُعد هذا الهجوم خرقاً واضحاً لمبدأ التمييز، حيث استهدفت المنشآت الصحية المدنية دون وجود ضرورة عسكرية مبررة، كما خرق مبدأ التناسب لأن الأذى الذي لحق بالمدنيين - بما في ذلك الخطر المباشر على حياتهم - كان مفرطاً وغير متناسب مع أية فائدة محتملة من الهجوم (كالحصول على فدية).

1 Department of Homeland Security, AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector, October 2020, <https://www.cisa.gov> تاريخ الزيارة:

والأهم من ذلك أن الهجوم لم يتضمن أي احتياطات مستطاعة لتفادي الإضرار بالمؤسسات المحمية أو تقليل الخسائر، مما يشكل انتهاكاً للمادة ٥٧ من البروتوكول الإضافي الأول لعام ١٩٧٧. لقد أظهر هذا الهجوم كيف يمكن للأدوات الرقمية أن تُستخدم بشكل فعال لتقويض الوظائف الإنسانية المحمية بموجب القانون الدولي، وهو ما يُوجب توسيع نطاق المساءلة ليشمل الهجمات السيبرانية غير التمييزية، خصوصاً تلك التي تستهدف المنشآت الصحية أثناء الأزمات^(١).

ثانياً. المناطق غير المحمية:

وهي مكانات أو مواقع مأهولة قريبة من ميدان النزاع أو في أنها مناطق تكون فيها القوات المسلحة على تماس بعضها مع بعض، التي تكون تحت سيطرة لاحتلال، لأجل تجنبها النزاع والتدمير. ويؤكد "القانون الإنساني" أنه من الممكن تعريف مناطق محددة على أنها غير محمية بغية تجنب أن يحدث قتال هناك، والقصد هو حفظ السكان المدنيين والممتلكات المدنية الموجودة فيها وحمايتهم، وعليه يحظر على أطراف النزاع مهاجمة مثل هذه المواقع بأي وسيلة كانت^(٢).

ويخضع تعيين موقع منطقة غير محمية والعلامة المميزة لها إلى أنظمة مفصلة، وينبغي على أطراف النزاع الاتفاق على علامات لتمييزها، عند إنشائها^(٣). ينبغي الوفاء بشروط معينة لضمان تعيين موقع ما على أنه غير خاضع للحماية، نذكرها فيما يأتي:

- ينبغي إجلاء كل المقاتلين فضلاً عن الأسلحة المتنقلة والمعدات العسكرية المتنقلة.
- يحظر استغلال المنشآت والمؤسسات العسكرية الثابتة لأغراض عدائية.
- يمنع ارتكاب أي عمل عدائي من قبل السلطات أو السكان.
- يحظر القيام بنشاطات تناصر العمليات العسكرية^(٤).

ثالثاً. مناطق ومواقع المستشفيات:

وهي المناطق والمواقع التي تقام على أراضي طرف من أطراف النزاع أو على أرض محتلة بهدف حماية الجرحى والمرضى من أفراد القوات المسلحة، فضلاً عن أفراد الخدمات الطبية المعيّنين

١ وزارة الأمن الداخلي الأمريكية، وكالة الأمن السيبراني وحماية البنية التحتية، تحذير: أنشطة برمجيات الفدية التي تستهدف قطاع الصحة العامة والرعاية الصحية، تشرين الأول/أكتوبر ٢٠٢٠. متاح على: <https://www.cisa.gov>

٢ يُنظر: المادة (١/٥٩) البروتوكول الإضافي الأول لعام ١٩٧٧.

٣ يُنظر: المادة (٧/٥٩، ٩/٥٩) البروتوكول الإضافي الأول لعام ١٩٧٧.

٤ يُنظر: المادة (٢/٩٥) البروتوكول الإضافي الأول لعام ١٩٧٧.

في كل منطقة، من آثار الحرب. وترى اتفاقية جنيف الأولى قيام الدول بإنشاء مثل هذه المواقع حتى في أوقات السلم وتوقيع اتفاقيات خاصة مع الطرف الخصم في أوقات النزاع، وبهذا الصدد، توفر المعاهدة مشروع اتفاق بشأن مناطق ومواقع الاستشفاء^(١).

ويجب على الأطراف المعنية توقيع اتفاقيات بشأن التمييز المشترك لمناطق ومواقع المستشفيات التي أقاموها، والتي يجب تمييزها بشعار مناسب وواضح، ويتكون هذا الشعار من صليب أحمر أو هلال أحمر أو الأسد أو الشمس الأحمرين على خلفية بيضاء يوضع على الفناء الخارجي وعلى المباني. وينبغي على الأطراف المعنية توقيع اتفاقيات بشأن التمييز المشترك لمناطق ومواقع المستشفيات التي أقاموها، التي يجب تمييزها بشعار مناسب وواضح، ويتكون هذا الشعار من صليب أحمر أو هلال أحمر أو الأسد أو الشمس الأحمرين على خلفية بيضاء يوضع على الفناء الخارجي وعلى المباني^(٢).

وتؤكد هذه المعاهدة كذلك على أن الدول الحامية المعنية بتوفير الحماية واللجنة الدولية للصليب الأحمر مدعوة إلى تقديم مساعيها الحميدة لتسهيل إنشاء مناطق ومواقع الاستشفاء والأمان.

رابعاً. المناطق المحايدة:

يمكن إقامة مناطق محايدة في مناطق يقع فيها قتال، وتهدف مثل هذه المناطق إلى حماية الأشخاص المحددين فيما يلي دون تمييز من آثار الحرب، وهم: الجرحى والمرضى من المقاتلين وغير المقاتلين، والمدنيين الذين لا يشاركون في أعمال عدائية ولا يؤدون عملاً ذا طبيعة عسكرية أثناء إقامتهم في هذه المناطق. ويمكن لأطراف النزاع، والدول المحايدة أو المنظمات الإنسانية أن تبادر إلى إقامة منطقة محايدة، ويجب على أطراف النزاع عقد وتوقيع اتفاق كتابي، يحدّد بداية ومدة تحديد المنطقة، فضلاً عن تفاصيل موقعها الجغرافي، والإدارة، والمواد الغذائية، والإشراف^(٣).

في خضم النزاعات المسلحة المعاصرة، التي تتداخل فيها أشكال العنف المادي مع المعاناة الإنسانية اليومية، لا تزال المبادئ الراسخة في القانون الدولي الإنساني تسعى إلى تثبيت حد أدنى من الحماية للفئات غير المشاركة في القتال. ومن أبرز الوسائل التي صاغها هذا القانون نجد ما يُعرف بـ “المنطقة المحايدة”، وهي مساحة جغرافية محددة يتم استئناؤها مؤقتاً من الأعمال العدائية باتفاق

١ يُنظر: اتفاقية جنيف الأولى عام ١٩٤٩ المادة (١٤).

٢ يُنظر: اتفاقية جنيف الأولى عام ١٩٤٩ المادة (٢٣).

٣ يُنظر: المادة (١٥) اتفاقية جنيف الرابعة ١٩٤٩.

صريح أو ضمني بين أطراف النزاع، بغرض تأمين الحماية للجرحى والمرضى والمدنيين العاجزين عن الدفاع عن أنفسهم. وقد كرّست المادة (١٥) من اتفاقية جنيف الأولى لعام ١٩٤٩ هذا المفهوم، حيث أجازت صراحةً إنشاء مثل هذه المناطق، شريطة موافقة أطراف النزاع المعنية، وألزمت الجميع باحترامها وعدم استغلالها عسكرياً^(١).

وتتجلى الأهمية العملية لهذا المفهوم في مثال ميداني واضح خلال النزاع الليبي في عام ٢٠١١، حيث تم إعلان منطقة إنسانية محايدة مؤقتة في مدينة نالوت غربي ليبيا، بالقرب من الحدود التونسية، خلال تصاعد الاشتباكات بين قوات حكومة القذافي وقوات المعارضة. وقد دعت منظمات دولية، بما في ذلك اللجنة الدولية للصليب الأحمر، إلى ضرورة إنشاء منطقة آمنة لضمان الإجلاء الطبي ونقل المساعدات الإنسانية، خصوصاً مع تدفق أعداد متزايدة من الجرحى إلى مشفى المدينة، الذي كان مهدداً بالقصف^(٢). وبالرغم من غياب أي اتفاق مكتوب أعلن بين الأطراف المتحاربة، فقد تم التوصل ميدانياً إلى تفاهات ضمنية - بوساطة من الهلال الأحمر الليبي ومنظمات دولية - لتجميد القتال مؤقتاً في محيط المشفى والطريق المؤدي إلى المعبر الحدودي مع تونس، من أجل تسهيل عمليات الإغاثة والإخلاء الطبي. وقد تم احترام هذه الترتيبات خلال فترة زمنية محددة، إذ امتنعت الأطراف المتصارعة عن تنفيذ أي أعمال عسكرية في المنطقة المعلنة، وجرى نقل الجرحى إلى تونس، وإدخال مساعدات طبية بإشراف من منظمات دولية. وكان ذلك التجسيد الواقعي للمنطقة المحايدة مثالاً على تفعيل المادة (١٥) في نزاع غير دولي، دون الحاجة إلى إجراءات رسمية معقدة أو موافقات دولية، بل بمجرد توافق ميداني إنساني^(٣).

ويبين هذا المثال أن المنطقة المحايدة لا تشترط وجود نزاع دولي بين دولتين كي تُفعّل، بل يمكن إنشاؤها داخل نزاع داخلي تتواجه فيه حكومة مركزية وقوى معارضة مسلحة، متى ما توفرت الإرادة الإنسانية لدى الأطراف. كما يُظهر أن القانون الدولي الإنساني يملك من المرونة ما يسمح بتطبيقه في الميدان حتى عندما تتعذر الآليات الدبلوماسية التقليدية. ومن هنا، فإن المنطقة المحايدة تُمثل أداة

١ ينظر: المادة (١٥) من اتفاقية جنيف الأولى لعام ١٩٤٩

٢ اللجنة الدولية للصليب الأحمر، "ليبيا: تزايد الحاجات الطبية مع تصاعد النزاع"، بيان صحفي، متاح على الرابط:

[-https://www.icrc.org/en/doc/resources/documents/news](https://www.icrc.org/en/doc/resources/documents/news)

٣ ماركو ساسولي، القانون الدولي الإنساني: القواعد، الإشكاليات، والحلول العملية للنزاعات المسلحة، دار إدوارد إغرا للنشر، ٢٠١٩، ص. ٢٢٦.

قانونية بالغة الأهمية تتيح حماية مستهدفة وعاجلة للفئات الضعيفة، حتى في البيئات التي يغيب فيها الاستقرار أو تخضع فيها مناطق معينة لحصار أو اشتباكات متقطعة. ومن الزاوية الفقهية، يُعد هذا النموذج الليبي تجسيداً ميدانياً لما يُعرف بـ “الحماية الموضعية” التي لا ترتبط بوقف شامل للقتال، بل تُنجز بوسائل مؤقتة وواقعية تُراعي الضرورات الإنسانية العاجلة. وهي صيغة تُستمد من جوهر القانون الإنساني الذي يُعطي الأولوية لحماية الكرامة الإنسانية في لحظة الحرب، على حساب الحسابات العسكرية البحتة.

في السياق المعاصر، ومع تصاعد التهديدات غير التقليدية التي باتت تفرضها الحرب السيبرانية، لم تعد الحاجة إلى حماية المناطق المحايدة مقتصرة على الوسائل المادية للهجوم، بل أصبحت الأنظمة الرقمية في المنشآت الطبية والإنسانية معرضة للخطر بذات القدر. فخلال خريف عام ٢٠٢٠، وفي ذروة تفشي جائحة كوفيد-١٩، تعرّضت عدة مستشفيات في الولايات المتحدة لهجوم سيبراني واسع النطاق، نفذته جماعة قرصنة يُعتقد أنها استخدمت برمجية الفدية المعروفة باسم Ryuk. وقد استهدف الهجوم البنية التحتية الرقمية للقطاع الصحي، حيث جرى تشفير قواعد بيانات المرضى وتعطيل أنظمة الطوارئ والرعاية، ما أدى إلى تأجيل العمليات الطبية، وتوقف بعض خدمات الإنعاش، واضطر الطاقم الطبي للعودة إلى السجلات الورقية^(١). وعلى الرغم من أن الهجوم لم يُستخدم فيه أي سلاح تقليدي، إلا أن أثره كان بمثابة ضربة مباشرة لمرفق إنساني محمي، سواء من حيث خطره الفعلي على حياة المرضى أو من حيث انتهاكه لمبدأ التمييز.

وبحسب قواعد القانون الدولي الإنساني، ولا سيما المادتين (٤٨) و(٥١) من البروتوكول الإضافي الأول، فإن على أطراف النزاع التمييز في جميع الأوقات بين الأعيان المدنية والأهداف العسكرية، وألا توجه الهجمات إلا نحو أهداف عسكرية مشروعة. كما تنص المادة (٥٧) على ضرورة اتخاذ جميع الاحتياطات الممكنة لتجنب إلحاق الضرر بالمدنيين والبنى المحمية، وهو ما لم يحصل في هذا الهجوم الرقمي، حيث تم إطلاق البرمجية الخبيثة بشكل عشوائي، دون تقدير أو تمييز^(٢).

وتُثير مثل هذه الأفعال أسئلة قانونية جوهرية حول مدى كفاية المفاهيم التقليدية لحماية المناطق المحايدة في العصر الرقمي، وحول الحاجة إلى تطوير قواعد خاصة تحظر الهجمات السيبرانية ضد

١ انظر: “مقال متاح على الرابط: <https://www.healthcareitnews.com/news/us-hospitals-targeted>

-targeted

٢ ينظر: المواد (٤٨، ٥١، و ٥٠) من البروتوكول الإضافي لاتفاقيات جنيف الأربع.

المنشآت الإنسانية، حتى إن لم تكن هذه المنشآت ضمن ساحة القتال الفعلي. كما أن من يقف وراء هذه الهجمات، سواء كانوا أفرادًا أو جهات مدعومة من دول، قد يُسألون جنائيًا إذا ثبت أن الهجوم أدى إلى ضرر جسيم، أو عرض حياة المدنيين للخطر، وفقًا لنظام روما الأساسي للمحكمة الجنائية الدولية، ولا سيما المادة (٨) المتعلقة بالهجمات ضد الأعيان المحمية^(١).

إن استمرار الصمت القانوني الدولي تجاه هذا النوع من الهجمات السيبرانية غير التمييزية يُهدد بتحديد الحماية التي تضمنها اتفاقيات جنيف والبروتوكولات الإضافية، ويستدعي تحركًا تشريعيًا دوليًا يُعيد الاعتبار إلى مبدأ الحصانة الإنسانية للمرافق المدنية حتى في الفضاء الرقمي. فالمنطقة المحايدة، سواء كانت على الأرض أو على الشبكات، يجب أن تبقى خارج دائرة الاستهداف، وأن يتم توسيع حمايتها لتشمل الأنظمة التقنية التي تعتمد عليها لاستمرار خدماتها. وفي ظل تزايد تعقيد بيئة النزاع، فإن الجمع بين المعايير التقليدية وأدوات الحماية الرقمية أصبح ضرورة فقهية وعملية لا يمكن تجاهلها.

خامساً المناطق المنزوعة السلاح:

وهي المناطق التي يحظر فيها على أطراف النزاع القيام بعمليات عسكرية، أو استعمال هذه المناطق لأي هدف يرتبط بسير العمليات العسكرية، ويجب أن تحدّد هذه المناطق في اتفاقية صريحة، تبرم إما في وقت سلام أو بعد اندلاع العمليات العدائية. ويمكن أن تكون اتفاقية شفوية أو مكتوبة وتبرمها أطراف النزاع مباشرة أو من خلال وساطة دولة حامية أو منظمة إنسانية محايدة. ويجب وضع علامة واضحة على منطقة منزوعة السلاح إلى الحدّ الممكن بعلامات يجري الاتفاق عليها مع الطرف الآخر.

ولكي تكون منطقة ما منزوعة السلاح، يجب أن تفي بالشروط الآتية:

- أن تُجلى كل القوات المقاتلة، وكذلك الأسلحة المتحركة والمعدات العسكرية المتحركة عنها.
- ألا تستخدم المنشآت والمؤسسات العسكرية الثابتة استخدامًا عدائيًا.
- ألا ترتكب أية أعمال عدائية من قبل السلطات أو السكان.

١ ينظر: المادة (٨) من النظام الأساسي للمحكمة الجنائية الدولية، وينظر أيضًا: ويليام أ. شاباس، مقدمة إلى المحكمة الجنائية الدولية، منشورات جامعة كامبريدج، ٢٠٢٠.

■ أن يتوقف أي نشاط يتواصل ويتعلق بالمجهود الحربي^(١).

ولا يجوز لأي طرف من أطراف النزاع أن يلغي من طرف واحد وضع منطقة منزوعة السلاح، ما لم يفشل أحد أطراف النزاع في احترام هذه الشروط أو يستخدم المنطقة لأغراض ترتبط بإدارة العمليات العسكرية. وفي مثل هذه الحالات، يُعفى الطرف الآخر من التزاماته بموجب اتفاقية أولية، وفي مثل هذه الحالة، تفقد المنطقة وضعها، ولكنها تظل متمتعة بالحماية، التي توفرها قواعد القانون الإنساني^(٢).

وقد أضاف مجلس الأمن التابع للأمم المتحدة مفاهيم جديدة للمناطق المحمية، التي تستخدم لتوفير الحماية للمدنيين، وتعرف باسم المناطق الآمنة أو المناطق الإنسانية الآمنة على سبيل المثال، ولم تتوافق المناطق الآمنة التي أقامتها الأمم المتحدة في يوغسلافيا السابقة في ١٩٩٣ والمناطق الإنسانية الآمنة في رواندا في ١٩٩٤ بمعايير القانون الإنساني الخاصة بالمناطق الآمنة. وقد فوّض الفرنسيون والسنغاليون والموريتانيون، الذين شاركوا في هذه العملية باستعمال القوة لحماية هذه المنطقة، وعندما انسحب الجيش الفرنسي وحلّت محله قوات حفظ السلام التابعة للأمم المتحدة بموجب تفويض مختلف، تعرّض السكان الذين ما زالوا موجودين في هذه المنطقة إلى هجمات وعمليات قتل من جانب الجيش الرواندي. وأصبح ما بين ستة آلاف وثمانية آلاف شخص في عداد المفقودين. ومرة أخرى، لم تكن مسؤوليات قوات الأمم المتحدة محدّدة بما فيه الكفاية فيما يتعلّق بحماية السكان، ولمنع هذه المذابح الجماعية^(٣).

وتستند هذه المناطق على مفهوم اتفاقية جنيف للمناطق الآمنة، إلّا أنه لا يفي بالمعايير التي يحدّدها القانون الإنساني. وفي الحقيقة تحظى هذه المناطق بالحماية بوجود جنود الأمم المتحدة الذين تكون قدراتهم ومسؤولياتهم العسكرية الخاصة بحماية السكان المدنيين رمزية أكثر من أنها حقيقية بصورة عامة، وبقيت مسألة من هو المسؤول عن حماية السكان المدنيين مسألة غير واضحة، وكانت وسائل فرض مثل هذه الحماية غير مناسبة، وتظهر القصة المأساوية للأفراد الذين يُجمعون في هذه المناطق ضرورة الدراسة الدقيقة لمفهوم مثل المناطق المحمية.

١ يُنظر: المادة (٦٠) البروتوكول الإضافي الأول عام ١٩٧٧.

٢ يُنظر: المادة (٦٠/٦ و ٧/٦٠) من البروتوكول الإضافي الأول عام ١٩٧٧.

٣ يُنظر: القاموس العملي للقانون الإنساني، تاريخ الزيارة ٢٠/٦/٢٠٢٤، الساعة ٦:٠٠، متاح على الرابط :

<https://ar.guide-humanitarian-law.org/>

ونرى، يمنح كل مبدأ من مبادئ القانون الإنساني حقوقاً والتزامات تفصيلية، ويشمل هذا التوزيع الدقيق للمسؤوليات الخاصة بحماية الأفراد المتجمعين في المناطق المخصصة لضمان سلامتهم، وفي كل حالة، يجب على منظمات الإنسانية في هذه المناطق المحمية مراقبة ضمانات الحماية، التي تقدم للسكان المدنيين فضلاً عن تقديم المساعدات وتوفير المسؤولية وسلسلة من الموارد المختلفة المتوفرة في مثل هذه العمليات.

ويعنى القانون الدولي الإنساني بحماية الأشخاص المتضررين من النزاعات المسلحة. وهكذا، يتعين على الدول، بمجرد اللجوء إلى القوة المسلحة، أن توجه هجماتها نحو الأهداف العسكرية وليس إلى المدنيين أو الأعيان المدنية، ويجب أن تتوخى الحذر باستمرار لتجنب إصابة الفئة الأخيرة. ولا يهم ما إذا كان هناك مدني واحد أو أكثر يحتاجون إلى الحماية من الهجوم^(١)، وينطبق القانون الدولي الإنساني على الأقل في الحالات، التي يؤدي فيها استخدام العمليات السيبرانية بين الدول إلى تأثيرات مشابهة للتأثيرات، التي تخلفها وسائل وأساليب الحرب التقليدية.

ومن أجل الحماية من عواقب الهجمات السيبرانية يجب حماية مجموع سكان البلدان المشتركة في النزاع، دون أي تمييز محجف يرجع بشكل خاص إلى العنصر، أو الجنسية أو الدين، أو الآراء السياسية، والمقصود بها تخفيف المعاناة الناجمة عن الحرب^(٢).

ويجوز للأطراف السامية المتعاقدة في وقت السلم، ولأطراف النزاع بعد نشوب الأعمال العدائية أن تنشئ في أراضيها، أو في الأراضي المحتلة إذا دعت الحاجة، مناطق ومواقع استشفاء وأمان منظمة بكيفية تسمح بحماية الجرحى والمرضى والعجزة والمسنين والأطفال دون الخامسة عشر من العمر، والحوامل وأمهات الأطفال دون السابعة^(٣).

ويجوز للأطراف المعنية أن تعقد عند نشوب نزاع وخلال اتفاقات فيما بينها للاعتراف المتبادل بالمناطق والمواقع، التي تكون قد أنشأتها، ولها أن تطبق لهذا الغرض مشروع الاتفاق الملحق بهذه الاتفاقية مع إدخال التعديلات التي قد تراها ضرورية عليه.

١ يُنظر: التعليق على اتفاقية جنيف الأولى: الاتفاقية الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان، ط٢، جنيف، سويسرا، ٢٠١٦، الفقرات ٢٣٦-٢٤٤.

٢ يُنظر: اتفاقية جنيف بشأن حماية الأفراد من الحرب عام ١٩٤٩ المادة (١٣).

٣ اتفاقية جنيف بشأن حماية الأشخاص المدنيين في وقت الحرب، المادة (١٤).

والدول الحامية واللجنة الدولية للصليب الأحمر مدعوة إلى تقديم مساعيها الحميدة لتسهيل إنشاء مناطق ومواقع الاستشفاء والأمان والاعتراف بها.

وتنص المادة (١٥) "يجوز لأي طرف في النزاع، أن يقترح على الطرف المعادي، إما مباشرة وأما عن طريق دول محايدة أو هيئة إنسانية، إنشاء مناطق محايدة في الأقاليم، التي يجري فيها القتال بقصد حماية الأشخاص المذكورين في أدناه من أخطار القتال دون أي تمييز:

أ - الجرحى والمرضى من المقاتلين وغير المقاتلين،

ب- الأشخاص المدنيين الذين لا يشتركون في الأعمال العدائية ولا يقومون بأي عمل له طابع عسكري في أثناء إقامتهم في هذه المناطق" (١).

وعليه بمجرد اتفاق أطراف النزاع على الموقع الجغرافي للمنطقة المحايدة المقترحة وإدارتها وتمويلها ومراقبتها، يعقد اتفاق كتابي ويوقعه ممثلو أطراف النزاع. ويحدد الاتفاق بدء تحديد المنطقة ومدته.

نستخلص مما تقدم: إن حماية الأفراد والمناطق المحمية - مثل المدنيين، والكوادر الطبية، والبعثات الإنسانية، والمنشآت الصحية، والمدارس، والمواقع الدينية والثقافية - تُعد من المبادئ الجوهرية، التي لا يجوز انتهاكها في أثناء النزاعات المسلحة. ومع تطور طبيعة الحروب وظهور الهجمات السيبرانية كأداة من أدوات النزاع المسلح، باتت هذه الهجمات تُشكل تهديدًا حقيقيًا وخفيًا للمناطق المحمية والأشخاص المحميين، ليس من خلال التدمير المادي فقط، وإنما من خلال تعطيل الخدمات، أو التلاعب بالمعلومات، أو التسبب في أضرار نفسية أو إنسانية جسيمة.

فالهجمات السيبرانية، التي تستهدف المستشفيات أو أنظمة الإمداد بالمياه أو شبكات الكهرباء الخاصة بالمناطق المدنية قد تؤدي إلى آثار إنسانية كارثية، حتى دون استخدام الأسلحة التقليدية. وأن استهداف قواعد بيانات إنسانية أو أنظمة تعقب اللاجئين والمفقودين، يمكن أن يُعرض الأفراد المحميين إلى مخاطر الاعتقال أو الإخفاء أو الاستهداف، ومن ثم، فإن هذا النوع من الهجمات، وإن لم يحدث ضررًا ماديًا، إلا أنه يُعد انتهاكًا جسيمًا للضمانات القانونية التي كفلها القانون الدولي الإنساني.

١ الأمم المتحدة لحقوق الإنسان، اتفاقية جنيف بشأن حماية الأشخاص المدنيين في وقت الحرب ١٩٤٩، تاريخ الزيارة ٢٣/٦/٢٠٢٤، الساعة ٧:٠٠، متاح على الرابط: <https://www.ohchr.org/>

ويرى الباحث: إن الهجمات السيبرانية تُعد من أكثر التحديات المستحدثة، التي تُقوّض الحماية القانونية للأفراد والمناطق المحمية في النزاعات المسلحة، نظراً لطبيعتها غير المرئية، وصعوبة إسنادها، واتساع آثارها، واحتمالية استخدامها من جهات فاعلة من غير الدول. ويرى الباحث أن الإخفاق في تكيف القانون الدولي الإنساني ليتماشى مع تطورات الحرب السيبرانية قد يؤدي إلى فراغ قانوني يُستغل للمساس بالفئات المحمية دون ردع أو محاسبة. وأن الضرر الناتج عن الهجمات السيبرانية على المناطق المحمية قد يكون مساوياً - أو أشد - من الهجمات التقليدية، ولا سيما إذا أدى إلى حرمان السكان من الرعاية الصحية، أو تعطيل الإمدادات الإنسانية، أو التسبب في حالة من الهلع الجماعي عبر أنظمة الإعلام أو الاتصالات. لذا يرى الباحث أن هناك حاجة ماسة لتوسيع تفسير مفهوم الهجوم في القانون الدولي الإنساني، ليشمل الأفعال السيبرانية، التي تؤدي إلى تعطيل أو تقييد الوصول إلى الخدمات الأساسية، أو تهدد حياة الأشخاص المحميين.

الفرع الثاني

الآثار الإيجابية والسلبية للهجمات السيبرانية

يمنح التطور التكنولوجي المعلومات والاتصالات، بما في ذلك الاتصال عبر شبكات الكمبيوتر (الفضاء السيبراني)، فوائد وفرصاً كبيرة إلى والمجتمعات والأفراد في المجالات الاجتماعية والاقتصادية والتنموية والمعلوماتية ومجالات الاتصال، فضلاً عن مجالات أخرى. ويعتمد المجتمع الدولي والمجتمعات، وكل فرد منا بشكل متزايد على الأدوات الرقمية، يزيد من اعتمادنا على استمرار تشغيل هذه التقنيات، ومن ثم يزيد من تعرضنا للعمليات السيبرانية. ولذلك، فإن الطبيعة السريعة التطور، التي يتسم بها الفضاء السيبراني والتكنولوجيا السيبرانية، والتكلفة البشرية المحتملة للعمليات السيبرانية، تتطلبان رصدًا وتقييمًا مستمرين^(١).

أولاً: الآثار الإيجابية

إن استخدام الأدوات السيبرانية باعتبارها من وسائل أو أساليب القتال يتيح للجيش إمكانية تحقيق أهدافها دون التسبب بالضرورة في إلحاق ضرر مباشر بالمدنيين أو إلحاق أضرار مادية بالبنية التحتية المدنية. وبحسب الظروف، قد تتيح الهجمات السيبرانية استهداف هدف عسكري مع تقليل

١ المجلة الدولية للصليب الأحمر، التقنيات الإلكترونية والحرب، بعد عشرين عاماً القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، ٢٠٢٠، ص ٢٩٣.

الأضرار العرضية المتوقع أن تلحق بالأعيان المدنية مقارنة باستخدام وسائل الحرب الأخرى. وفي المناقشات الحكومية الدولية الأخيرة، شددت بعض الدول على أن تكنولوجيا المعلومات والاتصالات إذا وُظفت بطريقة مسؤولة وعلى وفق القانون الدولي، فإن استخدامها في السياقات العسكرية قد تكون له الأفضلية عن استخدام الأسلحة الحركية ويمكن أن يؤدي إلى التهدة^(١). في المقابل، حذرت الدول الأعضاء في منظمة شنغهاي للتعاون من تطوير واستخدام أسلحة المعلومات و التحضير لحرب المعلومات وشنها^(٢).

وإن تطبيق قواعد القانون الدولي الإنساني في أثناء النزاعات المسلحة، ومن وجهة نظر عملية، في جوهرها، الدعوة التي تقوم على احترام أسس موضوعية شرعتها قواعد القانون، فلا يُسمح لجندي -مثلاً، قتل مدنياً وإن توفرت لديه أسباب وجيهة لكرهه، في حين يسمح له قتل المقاتل، ولو كان المقاتل سمحاً لطيفاً، وعليه، فإن التكنولوجيا إذا استُخدمت في بيئة عملية سليمة ربما، أن الالتزام بقواعد القانون الدولي الإنساني يكون أكثر، لهذا نرى عدداً كبيراً من المقاتلين في ساحات المعارك أو في بيئة عدائية في أثناء مشاعر الكره أو الخوف أو الجوع أو التعب أو غريزة البقاء على قيد الحياة قد تجعلهم يُقدمون على ارتكاب أعمالاً وحشية، في حين يكون من الممكن تجنبها بالاستخدام الامثل للتكنولوجيا المتطورة و هذا في إطار الهجمات السيبرانية^(٣).

ومن جانب آخر، أن استخدام الهجوم السيبراني في أثناء النزاعات المسلحة قد يجعل من النزاعات أكثر إيذاءً من النزاعات التقليدية، وأن الحروب يجب أن تكون عقلانية ومقبولة بشكل أكبر، فإن النظر إلى هذه القضية من جوانب أخرى قد تتضمن مسألة إيجابية، تتعلق بحسب وجهة نظر بعضهم بأن الحرب إذا ما كانت أكثر إيذاءً وترويعاً فستعمل على منع الدول، والبشر من اللجوء إليها^(٤).

1 ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts, forthcoming.

٢ المجلة الدولية للصليب الأحمر، بعد عشرين عاماً: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، تاريخ الزيارة ٢٠٢٤/٦/٢١، الساعة ٢:٠٠، متاح على الرابط:

<https://international-review.icrc.org>

3 Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal, P 232.

٤ يحيى ياسين سعود، مصدر سابق، ص ٩٨.

ومن جهة أخرى، إن استخدام التقنية المتطورة الحديثة، من بينها الهجمات السيبرانية في أثناء النزاعات المسلحة قد تقلص بشكل كبير من إمكانية استخدامها من قبل البشر بشأن الاحتيايل على القواعد القانونية أو اتخاذ أي قرار من وجهة نظر نفعية صرفة، على الرغم ما تنثيره هذه الهجمات و في بعض الأسلحة الأخرى في أثناء النزاعات المسلحة من جدال في العلاقة حول انطباق "قواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، فأن الهجوم على هدف ما في إطار القانون الدولي الإنساني من مواقع تبعد عن مناطق أو ميادين النزاع الحقيقي يثير مسألة السيادة لأي من القانونيين يمثل هذه الظروف (١).

وبناءً على تقدم، فإن استخدام التقنية المتطورة الحديثة، ومنها الهجمات السيبرانية في ضوء النزاع المسلح، ينبغي ألا تُقيم بإزاء فكرة مثالية افتراضية، أما ينبغي أن تقارن بالبشر في خلال الظروف والالتباسات المحيطة في أثناء النزاع المسلح، وحيثما نظرنا إلى القواعد الحالية للقانون، والتي جزء كبير منها يقع على مبدأ التدابير الاحتياطية المستطاعة، فهذه الاحتياطات، التي من الممكن أن تكون متاحة في الاستخدامات التقنية الحديثة (٢)، ولاسيما إذا ما طُورت لتتفوق على كفاءة البشر في الامتثال لقواعد القانون الدولي الإنساني عبر وسائل تكنولوجية تقنية بحيث تجدها لها القدرة على أخذ المعلومات، التي تنص على ضرورة وقف الهجوم، إذا ما وجد أن ما تشكله الهجمات انتهاكاً لقواعد ذلك القانون، وهي بهذا قد تتميز حتى على بعض الأسلحة التقليدية، ومنها -مثلاً- عدم قدرة إلغاء أو تأجيل هجوم شُنّ بواسطة المدفعية أو القذائف بعد إطلاقها، أي في اللحظات الأخير (٣).

وخلاصة القول: إن وفرة هذه التقنيات ووجودها وقدرتها العسكرية ينبغي ألا تُفسر -دائماً- أن ضرورة عسكرية قائمة لاستخدامها في حال كان استخدامها يحدث ضرراً للأفراد والأعيان المدنية وأضراراً مادية وخسائر فادحة لكل أطراف النزاع المسلح.

١ القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، اللجنة الدولية للصليب الأحمر، تاريخ الزيارة ٢٠٢٤/٦/٢١، الساعة ٩:٠٠، متاح على الرابط: www.icrc.org

٢ نوال أحمد بسبح، القانون الدولي الإنساني وحماية المدنيين والأعيان المدنية في زمن النزاعات المسلحة، ط١، منشورات الحلبي الحقوقية، ٢٠١٠، ص ٨٧.

٣ المصدر نفسه، ص ٩٨.

ثانياً: الآثار السلبية

ليس لآثار الهجمات السيبرانية حدود، فبإمكانها التسبب بانفجارات في مخازن الوقود والمحطات النووية، وكافة المراكز الحيوية أو تعطيل وسائل النقل براً وبحراً وجواً أو تغيير مسار الرحلات، إضافة لتعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها، وكذلك تعطيل أنظمة التحكم والتشويش على الصواريخ والطائرات وتغيير مسارها أو تعطيل أنظمة الدفاع أو حواسيب أمن المعلومات وتصل قدراتها لتعطيل أجهزة الاتصالات بكل أنواعها، ناهيك عن اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات^(١). وسنوضح أهم الآثار السلبية الناشئة عن الهجمات السيبرانية في عدة مجالات فيما يأتي:

١- الآثار السلبية للهجمات السيبرانية على المناطق المحمية في المجال العسكري:

لقد أدت التكنولوجيا دوراً مهماً في المجال العسكري، إذ تعتمد عليها معظم الأنظمة العسكرية اليوم، وتتمثل الميزة النسبية للتكنولوجيا في قدرتها على ري الوحدات العسكرية معاً، لتسمح بتبادل المعلومات وتدفقها بسهولة، والسرعة في إعطاء الأوامر العسكرية، والقدرة على تدمير الأهداف عن بعد. وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة السيبرانية المستخدمة آمنة تدرجاً كافية، فقد تؤدي الهجمات السيبرانية ضد الشبكات الخاصة بالمؤسسات الأمنية والعسكرية إلى السيطرة عليها، مما يؤدي إلى وقوع ضحايا في صفوف المقاتلين والمدنيين، وتهديد السلم والأمن الدوليين، ومن ثم فإن الهجمات السيبرانية على المجال العسكري لها النتائج الناجمة نفسه عن الاستخدام المادي للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدولة، ووقوع وفيات بين العسكريين والمدنيين^(٢).

ففي عام ٢٠٠٧، تعرضت وزارة الدفاع الإستونية لهجوم سيبراني واسع النطاق استهدف شبكاتها العسكرية والبنى التحتية الحيوية، في أعقاب خلاف سياسي مع روسيا. أدت الهجمات إلى تعطيل نظم الاتصالات العسكرية، وشلت لفترة قصيرة قدرات الرد الإلكتروني، ما كشف عن هشاشة البنية

١ غيث علاو، الهجمات السيبرانية أكبر من حرب نووية بوسائل إلكترونية، موقع متخصص في الشؤون الإيرانية،

تاريخ الزيارة ٢٠٢٤/٦/٢١، الساعة ٩:٠٠، متاح على الرابط: <https://jadehiran.com/archives/16835>

٢ إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، موقع المستقبل للأبحاث والدراسات المتقدمة، تاريخ الزيارة ٢٠٢٤/٦/٢١، الساعة ١٠:٠٠، متاح على الرابط:

<https://cutt.ly/rkpu3>

الدفاعية الإلكترونية للبلاد، ودفع حلف الناتو إلى إعادة تقييم استراتيجيته للأمن السيبراني وإنشاء مركز الدفاع السيبراني التابع له في العاصمة الإستونية تالين^(١)

٢- الآثار السلبية عن الهجمات السيبرانية على المناطق المحمية في المجال الاقتصادي:

أصبحت صناعة تكنولوجيا المعلومات والاتصالات مورداً اقتصادياً مهماً لكثير من الدول، إذ أسهمت ثورة تكنولوجيا المعلومات والاتصالات في جعل أصحاب القرار يتخذون قرارات استثمارية رشيدة، ومن ثم أسهمت في زيادة معدلات التنمية الاقتصادية، ومن الأمثلة على استخدام التكنولوجيا في المجال الاقتصادي ما يأتي: إعلانات المنتجات الجديدة، والأخبار الصحفية عنها، ومعلومات ترويجية حول مبيعات محددة وخاصة، وعرض دراسات السوق، وأبحاث العملاء، وجمع المعلومات الخاصة بخدمة العملاء، والتسويق الإلكتروني. فأى هجوم سيبراني على هذا المجال سوف يؤثر ويخلف العديد من الآثار السلبية، وسيكون المدنيون عاطلين عن العمل وغير محميين، وستتعطل العمليات من منطقة إلى أخرى مسببة تدهوراً اقتصادياً على مستوى الدولة، ومثال على ذلك الاحتيال في تحويل الأموال بالوسائل السيبرانية، وسرقة الأرصدة وتحويلها إلى أنشطة إجرامية^(٢).

وقد حدث في عام ٢٠١٧، تعرضت شركة Maersk، وهي واحدة من أكبر شركات الشحن والنقل البحري في العالم، لهجوم سيبراني من خلال فيروس NotPetya. تسبب الهجوم في تعطيل أنظمتها الرقمية العالمية بالكامل، بما في ذلك أنظمة الحجز ومتابعة الحاويات، مما أدى إلى توقف عمليات الشحن في موانئ عديدة حول العالم. تكبدت الشركة خسائر مباشرة تُقدَّر بحوالي ٣٠٠ مليون دولار أمريكي، بالإضافة إلى اضطرابات في سلاسل التوريد العالمية^(٣)

٣- الآثار السلبية عن الهجمات السيبرانية على المناطق المحمية في المجال الصحي.

أصبح استخدام أجهزة وبرامج الكمبيوتر في الوقت الحالي دوراً مهماً في تحسين جودة وكفاءة الرعاية الصحية وتقليل تكلفتها، ومن أهم ما تم تطويره فكرة السجلات الطبية الإلكترونية التي تشمل

1 Tikk, Eneken; Kaska, Kadri; Vihul, Liis. Cyber Attacks Against Georgia: Legal Lessons Identified. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2008 . متاح على

<https://ccdcoe.org/> 2025/2/5 الرابط:

٢ عبد الرحمن العتيبي، دور الامن السيبراني في تعزيز الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، الرياض، السعودية، ٢٠١٧، ص ٦٢.

3 Maersk Group, "Maersk: Cyber Attack Cost up to \$300 Million," in Annual Report 2017, A.P. Møller - Mærsk A/S, 2018 : <https://www.maersk.com> (2025/1/7).

المعلومات الخاصة بالمريض والتاريخ الطبي والعلاجات السابقة، والأدوية المستخدمة سابقاً، وحالات الحساسية، والأعراض، ونتائج الأمراض المختلفة والاختبارات التشخيصية، وكذلك مواعيد زيارة الأجباء أو المستشفيات والعلاجات، التي تلقاها المريض، وصور الأشعة التشخيصية والموافقات القانونية، ولقد أثرت التكنولوجيا الجديدة بشكل كبير على المجال الصحي، فظهر مفهوم الطب عن بعد الذي يهدف بشكل أساسي إلى تقديم الخدمات الطبية وخفض التكاليف بشكل أساسي في الدول الفقيرة أو المناطق الريفية بما يتماشى مع تلك المقدمة في المدن الكبرى والعواصم، وتقليل نفقات انتقال المريض والتواصل بين المريض والطبيب وتقديم التشخيص ومتابعة حالة المريض إلكترونياً^(١).

ويعد الهجوم السيبراني على هذه السجلات الطبية بمثابة خرق خطير للأمن السيبراني للرعاية الصحية، ومن ثم إحداث اضطراب كبير في المجال الصحي للدولة^(٢).

وقد أدى أحد أكبر الهجمات السيبرانية في القطاع الصحي إلى شلل كامل في الأنظمة الطبية في المملكة المتحدة، حينما ضرب هجوم "WannaCry" الخبيث في مايو/أيار ٢٠١٧ نظام هيئة الخدمات الصحية الوطنية (NHS)، ما تسبب في تعطيل أكثر من ٨٠ مستشفى وعيادة، وتأجيل آلاف العمليات الجراحية، وتعطيل الوصول إلى الملفات الطبية للمرضى، مما عرض حياتهم للخطر بشكل مباشر^(٣).

وفي ضوء الأهمية الخاصة لقطاع الرعاية الصحية في تخفيف المعاناة في جميع الأوقات، ولا سيما في أثناء النزاعات المسلحة والأزمات الصحية، دعت اللجنة الدولية جميع الدول إلى احترام الخدمات الطبية والمرافق الطبية وحمايتها من الهجمات السيبرانية من أي نوع، سواء في وقت السلم أم في وقت النزاع، وإعادة تأكيد القواعد الدولية، التي تحظر هذه الأعمال وإعادة الالتزام بها، وبينما تجسد هذه الدعوة الالتزامات القائمة بموجب أحكام القانون الدولي الإنساني المنطبقة على العمليات السيبرانية في أثناء النزاع المسلح^(٤).

١ سليمان ملكية، فطيمة عبد العزيز، الطب عن بعد: إبداع في الخدمات الطبية، المؤتمر الدولي حول الإبداع والتغيير التنظيمي في المنظمات الحديثة: دراسة وتحليل تجارب طبية ودولية، جامعة سعد دحلب البليدة، كلية العلوم الاقتصادية، الجزائر، ٢٠١١، ص ٦٢.

٢ عبد الرحمن العتيبي، مصدر سابق، ص ٦٤.

3 National Audit Office, "Investigation: WannaCry cyber attack and the NHS," UK Government, October 2018. Available at: <https://www.nao.org.uk>
<https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs>
 (2025/1/5)

٤ سليمان ملكية، فطيمة عبد العزيز، المصدر السابق، ص ٧.

٤- الآثار السلبية للهجمات السيبرانية على المناطق المحمية في البنية التحتية:

قد تتسبب العمليات السيبرانية التي تستهدف البنية التحتية المدنية الحيوية، مثل الكهرباء والمياه والصرف الصحي، في إحداث أضرار جسيمة بالبشر، وغالباً ما تُشغل هذه البنية التحتية عن طريق نظم التحكم الصناعية. ويحتاج الهجوم السيبراني، الذي يستهدف نظام التحكم الصناعي قدرًا معينًا من الخبرة والتطور، وفي كثير من الأحيان برامج ضارة مخصصة. ولأن كانت الهجمات التي تستهدف نظم التحكم الصناعية أقل تواترًا في حدوثها مقارنة بسائر أنواع العمليات السيبرانية، تشير التقارير إلى أن وتيرتها آخذة في الزيادة، وقد تطورت خطورة التهديد بسرعة أكبر مما كان متوقعًا قبل بضع سنوات فقط، وأشار متخصصون في الأمن السيبراني إلى أنه لما كان من المحتمل أن تؤدي الهجمات السيبرانية المادية إلى إحداث تأثير حركي وإصابات، فمن المُح والمهم بالنسبة للأوساط الدولية للمتخصصين في أمن تكنولوجيا المعلومات والحكومات والخبراء القانونيين المتخصصين في مجال العمل الإنساني التحاور بشأن كيفية تنظيم تنفيذ الهجمات السيبرانية المادية^(١).

قد ينطوي تنفيذ عمليات سيبرانية شديدة التمييز تتوافق مع القانون الدولي الإنساني وتتفادي إصابة السكان المدنيين على تحديات تقنية. والترابط الذي يميز الفضاء السيبراني يعني أن أي شيء له واجهة بنية تتصل بالإنترنت يمكن أن يتأثر بالعمليات السيبرانية، التي تُنفذ في أي مكان في العالم. وقد يخلف الهجوم السيبراني، الذي يستهدف نظامًا معينًا تداعيات على نظم أخرى مختلفة، بغض النظر عن مكان وجود تلك النظم. وثمة خطر حقيقي من أن تؤدي الأدوات السيبرانية - سواء عمدًا أو خطأ - إلى آثار واسعة النطاق ومتنوعة على البنية التحتية المدنية الحيوية. وترابط الفضاء السيبراني يعني أيضًا أن جميع الدول ينبغي أن تهتم بالرقابة الفعالة عليه: الهجمات التي تُشن ضد دولة واحدة يمكن أن تؤثر على العديد من الدول الأخرى - بغض النظر عن مكان وجودها وعن مشاركتها في النزاع^(٢). وأظهرت العمليات السيبرانية، التي نفذت على مدى السنوات الأخيرة - أساسًا

١ المجلة الدولية للصليب الأحمر، بعد عشرين عامًا: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، تاريخ الزيارة ٢١/٦/٢٠٢٤، الساعة ٨:٠٠، متاح على الرابط:

<https://international-review.icrc.org>

٢ اتفاقية التعاون في مجال ضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون، يكاترينبورغ، ١٦ حزيران/يونيو ٢٠٠٩ (اتفاقية منظمة شنغهاي للتعاون)، ترجمة غير رسمية في وزارة الدفاع في الاتحاد الروسي.

خارج نطاق النزاعات المسلحة - أن البرامج الضارة سرعان ما تنتشر في جميع أنحاء العالم، وتؤثر على البنية التحتية المدنية وتوفير الخدمات الأساسية، نتيجة لذلك، يحذر المعلقون من أن الهجمات الإلكترونية الصناعية تمثل أزمة إنسانية في طور التكوين^(١).

في فبراير ٢٠٢١، تعرّضت منشأة لمعالجة المياه في مدينة أولدسمار بولاية فلوريدا الأمريكية لهجوم سيبراني خطير، حيث نجح أحد القراصنة في التسلل إلى نظام التحكم الصناعي (SCADA) وزاد عن بُعد نسبة مادة هيدروكسيد الصوديوم (الصودا الكاوية) في المياه المعالجة إلى مستويات خطيرة. وقد كاد هذا الهجوم، لولا اكتشافه في الوقت المناسب، أن يتسبب في كارثة صحية تهدد آلاف المدنيين. تعتبر محطات المياه من المناطق المحمية بموجب القانون الدولي الإنساني، كونها من البنى التحتية الحيوية اللازمة لبقاء السكان المدنيين على قيد الحياة، مما يبرز الأثر الخطير للهجمات السيبرانية على المرافق المدنية المحمية^(٢).

وبموجب المادة ٥٦ من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧، تُصنّف السدود من بين "المنشآت التي تحتوي على قوى خطيرة" وتُمنح حماية خاصة، لا سيما في حال وقوع نزاع مسلح. ويمثل الهجوم السيبراني، حتى خارج النزاع التقليدي، تهديدًا مباشرًا لهذه الحماية ونسعين بالمثال الذي أشرنا إليه سابقاً حول الاعتداء على السدود كما حدث في عام ٢٠١٣، تعرض سد بومان (Bowman Dam) في ولاية نيويورك لهجوم سيبراني منسوب إلى قراصنة مدعومين من الحرس الثوري الإيراني. اخترق المهاجمون أنظمة التحكم الصناعي بالسد، وهو ما كان يمكن أن يؤدي، في ظروف تشغيلية عادية، إلى فتح بوابات السد أو التلاعب بمستوى المياه، مما يهدد بإغراق مناطق سكنية مجاورة وتعريض أرواح المدنيين للخطر^(٣).

نستنتج: إن آثار الهجمات السيبرانية على كل من المجالات العسكرية والاقتصادية والصحية والبنية التحتية، خطيرة جداً، وقد تؤدي إلى كوارث كبيرة ولا سيما إذا كانت نتائجها مماثلة للاستخدام المادي

١ المجلة الدولية للصليب الأحمر، بعد عشرين عاماً: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، تاريخ الزيارة ٢٠٢٤/٦/٢١، الساعة ٨:٠٠، متاح على الرابط:

<https://international-review.icrc.org>

2Federal Bureau of Investigation (FBI). Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility, U.S. Department of Homeland Security – CISA, February 2021. Available at: <https://www.cisa.gov> (2025/1/10)

٣ ينظر: البيان الصادر عن وزارة الدفاع الأمريكية - https://time.com/4270728/iran-cyber-attack-dam-fbi/?utm_source=chatgpt.com (٢٠٢٤/١٢/٢٥)

للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدول، ووقوع وفيات بين العسكريين والمدنيين، وإحداث اضطراب كبير في المجال الصحي والأذى والدمار للنظام البيئي، لذا نؤكد مرة أخرى على ضرورة الحد من استخدام الهجمات السيبرانية.

المطلب الثاني

دور القانون الدولي الإنساني في مواجهة آثار الهجمات السيبرانية

على الرغم من تزايد الهجمات السيبرانية والخطورة الناشئة عنها، إلا أن المجتمع الدولي يفتقر إلى إطار قانوني دولي شامل ينظمها، ومع ذلك فهو أمر لا يعني صحة القول بعدم وجود جهود دولية لتنظيم الهجمات السيبرانية بشكل مطلق، إذا هناك جهود تقدم بعض السبل، التي يمكن توظيفها للسيطرة على هذا التهديد المتنامي، وأبرز هذه الجهود كانت من قبل القانون الدولي الإنساني المعني بحماية المدنيين من الهجمات السيبرانية، وسنبحث في هذا المطلب عبر فرعين، في الفرع الأول التطبيقات العملية لمواجهة الآثار السلبية، وفي الفرع الثاني التعاون الدول للحد من آثار الهجمات السيبرانية على المناطق المحمية.

الفرع الأول

الجهود الدولية والوطنية لمواجهة الهجمات السيبرانية

ظهرت الهجمات السيبرانية مؤخراً كسلاح آخر غير التقليدي مسخر بأيدي الجيوش والأفراد، يقوم باختراق ومهاجمة الأجهزة الالكترونية بغية سرقة المعلومات أو تحطيمها أو محو معلومات وإضافة معلومات غير صحيحة ليُضرب المستخدم الرئيس فقد تخلف هذه الهجمات السيبرانية أضراراً كبيرة حتى على مستوى البنى التحتية لذا كان من الضروري مواجهة أخطارها وآثارها على المستويين الوطني والدولي، وقد لجأ العالم إلى درء هذه المخاطر ومواجهة آثارها عبر وسائل عديدة بينها التطبيقات العملية لمواجهة هذه الآثار:

أولاً: الجهود العملية الوطنية من أجل مواجهة الآثار السلبية للهجمات السيبرانية

١- بناء الجيوش السيبرانية.

كان للتطور السريع للتكنولوجيا، ولا سيما الحرب السيبرانية تحدياً لمفاهيم الأمن القومي، إذ صارت مسألة الدفاع عن البنية القومية للمعلومات ذات أهمية الكبرى، وعليه سعت غالبية الدول إلى تأسيس جيوش سيبرانية ورصدت ميزانيات كبيرة لتطويرها في مجال الهجوم والدفاع والحماية.

وبحسب الوكالة الروسية للاستشارات الأمنية (زيكوريون) فإن الولايات المتحدة تتفق أكثر على أمن الفضاء السيبراني أكثر من أي بلد آخر، فوزارة الدفاع لديها ميزانية سنوية تبلغ ٧ مليارات دولار للأمن السيبراني، وعدد الموظفين القراصنة يبلغ أكثر من ٩٠٠٠ موظف، وتتفق كل من الصين والمملكة المتحدة سنوياً ١.٥ مليار دولار و ٤٥٠ مليون دولار، على التوالي، في حين خصصت كوريا الشمالية نحو ٢٠% من الميزانية العسكرية للأمن السيبراني، ويحتل الجيش السيبراني الروسي المرتبة الخامسة في العالم، إذ تظهر التقارير أن قوات الأمن السيبراني الروسية وصلت إلى ١٠٠٠ موظف، وتتفق وزارة الدفاع الروسية حوالي ٣٠٠ مليون دولار سنوياً على مثل هذه الأنشطة^(١).

٢- تشكيل هيئات وطنية للأمن السيبراني:

بما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري، سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبراني، تكون مهمتها إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها. وكذلك وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه. ومن مهامها أيضاً وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، وأطر الاستجابة للحوادث والاختراقات، ومن مسؤوليتها أيضاً تحديد السياسات والمعايير الوطنية للتشفير، ورفع مستوى الوعي بالأمن السيبراني.

ويحدد الاتحاد الدولي للاتصالات ITU خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي كالتالي: معايير تشريعية، تقنية، تنظيمية، بناء القدرات ومعياري التعاون^(٢).

٣- التشريعات الوطنية للأمن السيبراني

وضعت العديد من دول العالم قوانين لمواجهة التهديدات السيبرانية، بعد أن ظهر جلياً مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها، وأجمع أغلب هذه القوانين أن هذه التهديدات ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام التقنية، وخصص جزء كبير من هذه القوانين عقوبات رادعة. هذا فضلاً عن أن معظم الدول الأوروبية والآسيوية، والعربية، وغيرها من دول العالم التي أضافت إلى قانونها الجزائري ملحقاً خاصاً لمكافحة الجريمة السيبرانية مثل الجزائر وهناك ثلاث دول عربية فقط وضعت قوانين مستقلة لمكافحة الجرائم والهجمات السيبرانية، هي

١ سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٨، ص ١٥.

٢ المصدر نفسه، ص ٥٢.

السعودية وعمان والإمارات العربية المتحدة، هذه الأخيرة، التي تُعد رائدة في المنطقة العربية في إصدار تشريعات الأمن السيبراني، إذ صدر قانون مكافحة الهجمات السيبرانية عام ٢٠١٢، ثم تم تعديله في ٢٠١٦، وقد دعم بمجموعة من السياسات التنظيمية والمعايير التقنية، لتمكين مستخدمي الفضاء السيبراني ومقدمي الخدمات من الحصول على الظروف الأمنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلاً عن حماية المستخدمين^(١).

ثانياً: الجهود العملية الدولية من أجل مواجهة الآثار السلبية للهجمات السيبرانية

١- الحد من سباق التسلح السيبراني

يؤدي التسليح أهمية استراتيجية في توازن القوى على المستوى العالمي، في ظل بيئة يسودها الشك وعدم اليقين وقابلية تدمير المصالح الاستراتيجية بسرعة الضوء، وهو ما يحمل خطورة عسكرية الفضاء السيبراني، وبتبني عدد الدول استراتيجية الحرب السيبرانية كحرب للمستقبل، واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة، لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، كانت بداية ظهوره يُعد المختصون هذه الأسلحة السيبرانية بدائية (في الصراع الروسي-الاستوني، والروسي-الجورجي، والتطور البارز مع فيروس ستاكسنت الموجه ضد البرنامج النووي الإيراني)، الذي يتهم بتطويره كل من الكيان الصهيوني والولايات المتحدة^(٢). واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع والردع أم الهجوم، فضلاً عن الحماية بنيته القومية للمعلومات، وذلك من خلال السعي إلى امتلاك التكنولوجيا وأنظمة الحماية، والعمل على تحقيق التفوق التقني. وعليه، فإن المشكلة في سباق التسلح السيبراني تكمن في تحديد ماهية تلك الأسلحة، ومن ثم لا يصبح لدى المجتمع الدولي القدرة على التدخل لاحتواء التقدم في مجال تلك الأسلحة.

إذ قاومت الولايات المتحدة ما اعتبرته محاولة للحد من القدرات الأمريكية، وما تزال تُعد هذه المعاهدة عامة مضللة لا يمكن التحقق منها، وعوضاً عن ذلك اتفقت الولايات المتحدة وروسيا و١٣

١ حسن بن أحمد الشهري، الإرهاب الإلكتروني - حرب الشبكات، المجلة العربية الدولية للمعلوماتية، (المجلد ٤، العدد ٨) المملكة العربية السعودية، ٢٠١٥، ص ١٩.

٢ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد ٣٢، مكتبة الإسكندرية، ٢٠١٦، ص ٤٦، تاريخ الزيارة ٢٠١٤/٦/١٦، الساعة ٤:٠٠، متاح على الرابط:

دولة أخرى على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين، التي اجتمعت لأول مرة في العام ٢٠٠٤، وقد أسفرت تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول ٢٠١٥ أصدرت تقارير أقرتها مجموعة العشرين، يقضي بوضع معايير مقترحة لبناء الثقة. وعلى الرغم من صعوبة عملية الرقابة والتفتيش على الأسلحة السيبرانية، فإن السعي نحو الحد من انتشار هذه الأسلحة، يتطلب وجود إطار دولي تشارك فيه العديد من الدول والجماعات عبر العالم، إلى جانب وجود الإطار القانوني الدولي، الذي يحدد الالتزامات والواجبات لجميع الفاعلين. إن أي اتفاق من شأنه تنظيم الاستخدام العسكري للفضاء السيبراني، يجب أن يعمل على منع نشر الأسلحة السيبرانية في وقت السلم، والسماح بالجهود الجماعية للدول أو المنظمات لتجنب التأثير على الاستخدام المدني للفضاء السيبراني^(١).

٢- دليل تالين

نظراً لصعوبة الحد من سباق التسلح السيبراني من جهة، وقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية من جهة أخرى، تم إبرام صك قانوني عام ٢٠١٣ يدعى دليل تالين (Tallinn manual)، الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي (NATO)، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل، الذي شنته روسيا ضد إستونيا عام ٢٠٠٧، ويحتوي دليل تالين على ٥٩ قاعدة، وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين والبنية التحتية الضرورية لحياتهم، وهذا نتيجة وجود فضاء سيبراني واحد تتقاسمه القوات المسلحة والجيش السيبرانية مع باقي المستخدمين المدنيين^(٢).

ويجيب دليل تالين على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، كمفهوم النزاع المسلح في إطار الحرب السيبرانية، وكذا مفهوم الجيوش السيبرانية وكيفية إدارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفة المقاتل السيبراني فضلاً عن إمكانية مراعاة القانون الدولي الإنساني المعروفة كمبدأ

١ سليم دحماني، مصدر سابق، ص ٥٥ - ٥٦.

٢ سعيد درويش، ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر (١)، العدد ٢٩، الجزء الثاني، ٢٠١٨، ص ١١٩، تاريخ الزيارة ٢٢/٦/٢٠٢٤، متاح على الرابط: <https://cutt.ly/2kpMul>

التمييز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالتائرات العسكرية بدون طيار.

ويقصر دليل تالين الهجوم السيبراني على أنه عملية إلكترونية سواء هجومية أم دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها، لكن لم يتفق الخبراء حول الضرر، فهو يتوقف على كل بلد أن يقرر حجم الضرر الكافي لتسويغ خوض الحرب، وهذا ما يعرف بنظرية الجوء إلى الحرب، بحيث يشترط أن تكون مسوغة وعادلة، لكي يمكن إضفاء صفة المشروعية عليها^(١).

الفرع الثاني

الجهود الإقليمية والدولية لتعزيز الامن السيبراني للمناطق المحمية

بعد التطور التكنولوجي المتسارع واتكاء الدول بشكل كبير على بنية تحتية حديثة فقد صار الامن السيبراني واحد من الركائز المهمة على الصعيد القومي والاقتصادي والاجتماعي. وبعد إن ازدادت مخاطر التهديدات السيبرانية دعت الحاجة الماسة إلى تعزيز التعاون على المستويين الإقليمي والدولي لدرء هذه التحديات فعلى المستوى الإقليمي: أن عديداً من المنظمات والتجمعات بذلت جهوداً كبيرة لوضع الأطر التنظيمية والتشريعية، التي تعزز القدرات الدفاعية في الفضاء السيبراني، مثل الاتحاد الأوروبي ورابطة دول جنوب شرق آسيا (ASEAN) والاتحاد الأفريقي. أما على الصعيد الدولي: فإن الأمم المتحدة ومنظمات أخرى مثل الاتحاد الدولي للاتصالات (ITU) عملت على استحداث استراتيجيات شاملة لتعزيز الأمن السيبراني عبر إبرام الاتفاقيات وإنشاء المعايير الدولية وتسهيل تبادل المعلومات بين الدول.

أولاً: الجهود الإقليمية لتعزيز الامن السيبراني للمناطق المحمية:

تتسجم الاتفاقيات الإقليمية مع متطلبات مواكبة سرعة تطور التهديدات السيبرانية، ويسجل في هذا المجال، عدد من المبادرات نذكر منها:

في عام (٢٠٠٢) وضعت مجموعة بلدان قانوناً نموذجياً لمكافحة الهجمات والجريمة السيبرانية، فضلاً عن قانون الإثبات الرقمي.

١ سعيد درويش، مصدر سابق، ص ١٢١.

في عام (٢٠٠٩) بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إقرار توصية لمكافحة الهجمات والجريمة السيبرانية، تشكل الإطار القانوني لعمل الدول الأعضاء.

جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام (٢٠١١)، لتعزيز التعاون بين الدول العربية لمكافحة الهجمات والجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

وتُعد اتفاقية بودابست (٢٠٠١) الاتفاقية الأوروبية لمكافحة الهجمات السيبرانية خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها، دخلت حيز التنفيذ عام ٢٠٠٤، وتُعد أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، وقد شددت على ضرورة تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول^(١).

ثانياً : الجهود الدولية لتعزيز الامن السيبراني للمناطق المحمية:

- أما على المستوى الدولي، فقد أدت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلامة في الفضاء السيبراني، وتوعية الوعي العالمي بالأمن السيبراني دوراً في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية، ومن أهم القرارات الصادرة عن الهيئة^(٢):
١. قرار صادر عام ١٩٩٠ حول قانون جرائم المعلوماتية^(٣).
 ٢. قرار صادر عام ١٩٩١، حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات.
 ٣. تم إنشاء مجموعة الخبراء الحكومية GGE، بدأت عملها في ٢٠٠٤، لمناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والإجراءات الممكنة لوضع الأسس الدولية، التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية.
 ٤. صدر قرار خاص في عام ٢٠٠٣ حول الأمن السيبراني، ركز على القدرة على مكافحة الجريمة السيبرانية.

١ منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، لبنان، ٢٠١٧، ص ١٠٣ - ١٠٤.

٢ حمزة بن فهم السلمي، الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي، مجلة الجامعة العراقية، العدد (٥٩) الجزء (١)، بغداد، العراق، ٢٠٢٣، ص ٥٨٩.

٣ قرار هافانا ١٩٩٠ المنبثق عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا في ٢٧ آب/ أغسطس - ٧ أيلول/ سبتمبر ١٩٩٠، جاء مقتنا للجرائم المعلوماتية.

٥. صدر قرار حول الأمن السيبراني في عام ٢٠١٠، وملحق حول ضرورة أن تلجأ الدول، لمعرفة مدى تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية.

٦. قرار بودابست عام ٢٠٠٠ لمكافحة الجريمة المعلوماتية، تتعلق هذه الاتفاقية بمعالجة كل ما يخص الجرائم المعلوماتية ضمن الإطار الأوروبي، وتلخصت أهدافها بالسعي نحو توحيد التدابير التشريعية للوقاية، من هذه الجرائم بين الدول^(١).

و قد ذلت جهود عدة، من قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات لإقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام السلمي للمجال السيبراني. وإن عقد اتفاقيات دولية لها أطراف عديدة من شأنها تنظيم هجمات السيبرانية وسيتعرض لصعوبات من قبل الدول العظمى وبالأخص الصين وروسيا الاتحادية والولايات المتحدة الأمريكية و هو حال أغلب المواضيع الدولية التي لها علاقة بالأمن والسلم الدوليين، والتي كانت تعاني لفترات طويلة من التعطيل ومن أهم العقبات التي تواجه عقد اتفاقية دولية معينة هو تقييد الحظر أو حظر استعمال طرائق أو الوسائل الإلكترونية من أجل تنفيذ الهجمات.

إن إجراءات بناء الثقة بين الدول وبالأخص تدابير الشفافية تمثل نقطة الارتكاز لأي اتفاقية تعنى بتقييد أو حظر استعمال أي طريقة قتالية أو سلاح ولا بد في هذا الشأن أن نقوم بتحديد معنى الشفافية وهو مصطلح اتبعته معظم اتفاقيات الحد من السلاح أو نزعه والمقصود به تلك التدابير التي يتوجب على الدول الأطراف أن يتبعوها في أية اتفاقية من أجل نزع السلاح والدول الأطراف تكشف عن خلاله عن معلومات دقيقة تخص برامج السلاح المعني بالتقييد أو الحظر مثل معلومات عن بدايات برنامجها التسليحي. ولا سيما في حقل الحد من الأسلحة أو نزعها وذلك من أجل امتثال أحسن لأحكام هذه الاتفاقيات^(٢). شكلت الأمم المتحدة العديد من اللجان لتقصي الحقائق كان الهدف منها تقسيم معايير الامتثال للدول، وقد حققت الأمم المتحدة (١٦) مبدأ من أجل تعزيز الامتثال.

إن الاهتمام المتزايد لمعالجة الهجمات السيبرانية من خلال أطر قانونية مشتركة، جعل أغلب المنظمات الدولية تسعى إلى وضع تنظيم قانوني للحد من آثار الهجمات السيبرانية، وسنبين أبرز هذه الجهود فيما يأتي:

١ اتفاقية بودابست الصادرة عن المجلس الأوروبي في ٢٣ تشرين الثاني/ نوفمبر ٢٠٠١ لمكافحة الجرائم المعلوماتية.

٢ احمد عبيس نعمة الفتلاوي، مصدر سابق، ص ١٠٠.

أولاً: جهود الأمم المتحدة في الحد من الهجمات السيبرانية على المناطق المحمية : لقد سعت الأمم المتحدة إلى تأمين سلامة استخدام التكنولوجيا، والشبكات المعلوماتية بشكل عام، وشارك كل من الجمعية العامة ومجلس الأمن ومكتب مكافحة الإرهاب التابع للأمم المتحدة في كثي رمن المفاوضات بغية الوصول إلى توافق في الآراء لغرض وضع معايير توفر الحماية لشبكات الانترنت.^(١) وهناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الهجمات السيبرانية نوضح منها:

١. قرارات الجمعية العامة للأمم المتحدة:

تعد الجمعية العامة الجهاز الوحيد من أجهزة الأمم المتحدة الذي تشترك في عضويته جميع الدول الأعضاء المنظمة، وقد أصدرت الجمعية بعض القرارات بهدف الحد من آثار الهجمات السيبرانية على المناطق المحمية، وذلك تدعيماً للالتزام بمبادئ القانون الدولي الإنساني، لأنها تعمل على احترام حقوق الإنسان، ولا سيما في النزاعات المسلحة، والتي يقع ضمنها حماية المناطق المحمية التي تشكل أحد أوجه الحماية، ومن تلك القرارات العامة رقم (٢٤٤٤) الصادر لعام ١٩٦٨ بشأن احترام حقوق الإنسان في النزاعات المسلحة، الذي جاء فيه: إذ تقر بضرورة تطبيق المبادئ الإنسانية الأساسية في جميع النزاعات المسلحة، تؤكد الجمعية العامة على المبادئ الآتية من أجل الامتثال لها من قبل جميع الدول.

إن حق أطراف النزاع في اعتماد وسائل إصابة الخصم ليس حقاً غير محدود.

يحظر شن هجمات ضد المناطق الإنسانية الآمنة وضد السكان المدنيين بصفتهم هذه.

يحظر التمييز في كل الأوقات بين المشاركين بالأعمال العسكرية وأفراد السكان المدنيين من أجل تجنب هؤلاء الأفراد قدر المستطاع^(٢).

وإن الحقوق الإنسانية الأساسية المقبولة في القانون الدولي وفي الاتفاقيات الدولية، يستمر انطباقها كلياً في حالات النزاع المسلح. ويجب التمييز في كل الأوقات في أثناء سير العمليات العسكرية المشاركين فعلياً في الأعمال العسكرية والسكان المدنيين. إذ ينبغي ألا يكون السكان المدنيون بصفتهم

١ لبكي، جورج: المعاهدات الدولية للانترنت: حقائق وتحديات، مجلة الدفاع الوطني، بيروت، العدد ٨٣، كانون الثاني، ٢٠١٣، تاريخ الزيارة ٢٢/٦/٢٠٢٤، الساعة ٧:٠٠، متاح على الرابط: <https://cutt.ly/nh5Hell>

٢ ماركو ساسولي وآخرون، كيف يوفر القانون الحماية في الحرب. مختارات من القضايا الخاصة بممارسات معاصرة في القانون الدولي الإنساني، ط١، ICRC، المركز الإقليمي للأعلام، القاهرة، ٢٠١١، ص ٣٣٤.

هدفاً للعمليات العسكرية. وكذلك يجب ألا تكون المناطق والمدن المجردة من وسائل الدفاع والمناطق والمواقع المنزوعة السلاح هدفاً للعمليات العسكرية. وإلا تكون الأماكن أو المناطق المخصصة فقط لحماية المدنيين كمناطق الاستشفاء والأمان والمناطق المحايدة هدفاً للعمليات العسكرية. وأيضاً ألا يكون السكان المدنيون أو الأفراد المدنيون هدفاً للاقتصاص أو النقل القسري أو غير ذلك من الاعتداء على سلامتهم. وتقديم الإغاثة الدولية للمدنيين أمر متفق مع ميثاق الأمم المتحدة والإعلان العالمي لحقوق الإنسان وغيرها من الاتفاقيات الدولية^(١).

ومن أهم القرارات التي أصدرتها الجمعية العامة للأمم المتحدة للحد من الهجمات السيبرانية :

١. القرار (٥٥/٦٣) والقرار (٥٦/١٢١) الذين يصفان الإطار القانوني^(٢)، فضلاً عن ذلك القرار

(٥٧/٢٣٩) الذي يهدف إلى انشاء ثقافة أمنية عالمية للفضاء الحاسوبي^(٣).

٢. القرار (٥٨/١٩٩) المتعلق بإرساء ثقافة عالمية للأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات^(٤).

٣. القرار ٧٣/١٨٧ المتعلق بمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الجرمية^(٥).

٤. القرار ١٧٣/٧٤ المتعلق ب تعزيز المساعدة التقنية وبناء القدرات للتدابير الوطنية والتعاونات الدولية في مجال مكافحة الجريمة السيبرانية، بما يسمح تبادل المعلومات^(٦)

وتسعى الأمم المتحدة إلى أن تقوم بدور ريادي، فقد أعريت الدول الأعضاء للأمم المتحدة، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب في القرار ٢٨٤ / ٧٢ الصادر عن

١ القرار رقم (٢٦٧٥) الصادر عن الجمعية العامة للأمم المتحدة بتاريخ ١٩٧٠.

2 GA. Res. 55/63, 121/56 UN. Doc. No, A/RES/55/63 (Jan, 22, 2001), Available at:

<https://undocs.org/ar/A/RES/55/63> / <https://undocs.org/ar/A/RES/56/121>

3 GA. Res. 57/239, UN. Doc. No, A/RES/57/239 (Jan, 31, 2003), Available at:

<https://undocs.org/ar/A/RES/57/239>

4 GA. Res. 58/199, UN. Doc. No, A/RES/58/199 (Jan, 30, 2004), Available at:

<https://undocs.org/ar/A/RES/58/199>

5 GA. Res. 73/187, UN. Doc. No, A/RES/73/187 (Jan, 14, 2019), Available at:

<https://undocs.org/ar/A/RES/73/187>

6 GA. Res. 74/173, UN. Doc. No, A/RES/74/173 (Jan, 7, 2020), Available at:

<https://undocs.org/ar/A/RES/74/173>

الجمعية العامة، عن قلقها بإزاء استخدام الإرهابيين تكنولوجيا المعلومات والاتصالات، ولا سيما شبكة الإنترنت وغيرها من الوسائل لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها^(١).

نستنتج: إن الجمعية العامة للأمم المتحدة في كافة قراراتها، التي أصدرتها تدعو إلى إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات، ووضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في الحسبان عواقب الهجوم السيبراني، وبذلك يتضح أن للجمعية العامة للأمم المتحدة دوراً إيجابياً للحد من آثار الهجمات السيبرانية وتوفير الحماية للمناطق المحمية في أثناء النزاعات المسلحة.

٢. قرارات مجلس الأمن

أصدر مجلس الأمن العديد من القرارات الخاصة بالحد من الهجمات الإرهابية والسيبرانية ومن بين هذه القرارات:

أ- القرار ٢٣٤١ (٢٠١٧) الذي يهيب فيه الدول الأعضاء إلى إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين: العام والخاص، بحسب الاقتضاء، لتبادل المعلومات والخبرات من أجل من الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ، وأيضاً يسلم بأن جهود الحماية تتوزع على مسارات متعددة منها أمن الفضاء السيبراني^(٢).

ب- القرار (٢٣٧٠) عام ٢٠١٧، الذي يحث فيه الدول الأعضاء على العمل بصورة تعاونية لمن الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيا المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي^(٣).

1 GA. Res. 72/284, UN. Doc. No, A/RES/72/284 (July, 2, 2018), Available at:

<https://undocs.org/ar/A/RES/72/284>

2 SC. Res. 2341, UN. Doc. No, S/RES/2341(2017) (February, 13, 2017), Available at:[https://undocs.org/ar/S/RES/2341\(2017\)](https://undocs.org/ar/S/RES/2341(2017))

3 SC. Res. 2370, UN. Doc. No, S/RES/2370(2017) (August, 2, 2017), Available at:

<https://digitallibrary.un.org/record/1298189?ln=ar>

٣. مكتب مكافحة الإرهاب:

لقد اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات في مجال التكنولوجيا الجديدة منها برنامج أمن الفضاء الإلكتروني، الذي يهدف إلى:

١- تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على من إساءة استعمال الإرهابيين والمتطرفين العنيفين التطورات التكنولوجية، والتصدي لخطر الهجمات السيبرانية، التي تشنها الجهات الفاعلة الإرهابية على البنى التحتية الحيوية.

٢- تطوير استخدام وسائل التواصل الاجتماعي لمكافحة الإرهاب والتطرف العنيف على الإنترنت، في ظل احترام حقوق الإنسان.

٣- تخفيف آثار الهجمات السيبرانية واستعادة وإصلاح النظم المستهدفة، في حال حدوث تلك الهجمات^(١).

ثانياً: جهود حلف شمال الأطلسي (الناتو) في الحد من الهجمات السيبراني للمناطق المحمية.

أدت تداعيات الهجمات السيبرانية، التي استهدفت البنية التحتية الرقمية لإستونيا عام ٢٠٠٧، أيضاً الهجمات السيب ارنية ضد جورجيا خلال نزاعها المسلح مع روسيا عام ٢٠٠٨، إلى سعي حلف شمال الأطلسي للتصدي للهجمات السيبرانية، فقد عمد إلى إنشاء مركز الدفاع الإلكتروني التعاوني للتميز، وفي المدة ما بين عامي ٢٠٠٩ و ٢٠١٢، ويطلب من مركز الدفاع الإلكتروني التعاوني للتميز، قامت مجموعة من الخبراء والباحثين القانونيين تقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية^(٢)، وتُوجت هذه الجهود بنشر دليل يعرف باسم دليل تالين، وهو وثيقة قانونية غير ملزمة، تنظم قواعد الاشتباك عبر الانترنت. ويقر الدليل بأن الهجمات السيبرانية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف، ولاسيما الآثار المدمرة لتلك الهجمات، وعلى الرغم من عدم إلزامية

١ اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، ٢٠١٩.
٢ بهاء عدنان السعيرى، عماد عيد خضير، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٧٢، العدد ٤، بابل، العراق، ٢٠١٩، ص ٤٨٣.

الدليل، فإنه وثيقة أخلاقية للدول الأعضاء في الحلف على الأقل، وينظم استخدامهم للهجمات السيبرانية خلال مدة النزاع المسلح^(١).

ويوضح دليل تالين، القوانين الدولية التي يمكن تطبيقها على الحرب السيبرانية وهو يشتمل على كل من مبدأ حق اللجوء إلى الحرب أي القواعد الدولية، التي تحكم وتنظم استخدام القوة من قبل الدول، ومبدأ سلوكيات الحرب أو قانون النزاعات المسلحة أو القانون الدولي الإنساني، أي: القواعد التي تنظم سلوك الأطراف المتنازعة في أثناء النزاع. و إن دليل تالين لا يركز إلا على الهجمات السيبرانية في مواجهة هجمات سيبرانية أخرى، على سبيل المثال ينظم الهجوم السيبراني الذي يستهدف أنظمة القيادة أو السيطرة التابعة للعدو، ولا يشمل الغارة الجوية ضد مركز السيطرة السيبراني، ويعالج هذا الدليل كلا من النزاعات المسلحة الدولية وغير الدولية، ويجمع الفقهاء في ضوء دليل تالين، بأن النزاع المسلح الدولي يحصل متى ما قامت دولة ذات سيطرة كاملة على مجموعة من الأفراد بتوجيه تلك المجموعة لتنفيذ هجمات سيبرانية ضد دولة أخرى. أما إذا كانت لا تملك إلا سيطرة فعالة على تلك المجموعة فعندئذ تلك الهجمات لا تبلغ مستوى النزاع المسلح الدولي .
(٢)

ثالثاً: جهود مجلس أوروبا في الحد من الهجمات السيبراني للمناطق المحمية.

يعد مجلس أوروبا^(٣)، أول من اتخذ خطوات جدية ومباشرة لتنظيم جزء من الأمن السيبرانية لأي منظمة دولية أو إقليمية أخرى، فقد قام بإنشاء اتفاقية بودابست المتعلقة بالجريمة السيبرانية وتعد هذه الاتفاقية أولى المعاهدات الدولية، التي سعت إلى معالجة الهجمات السيبرانية من خلال تنسيق القوانين الوطنية، وزيادة التعاون بين الدول في محاربة الهجمات السيبرانية، وتمت في العاصمة المجرية بودابست في ٢٣ / ١١ / ٢٠٠١ ، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال

١ إيهاب خليفة، القوة الإلكترونية كيف يمكن أن تدير الدول شئونها في عصر الانترنت، الولايات المتحدة، ط١، العربي للنشر والتوزيع، القاهرة، مصر، ٢٠١٧، ص ١٦٦.

٢ زهراء عماد محمد كلنتر، مصدر سابق، ص ٢٠.

٣ مجلس أوروبا هو منظمة دولية معنية بالدفاع عن حقوق الإنسان في القارة الأوروبية، موقعه الرسمي:

<https://www.coe.int/en/web/portal/home>

تكوين التضامن الدولي ضد تلك الجرائم والهجمات التي تتم عبر شبكة الانترنت والاستخدام السيء لها^(١).

إن الاتفاقية قد وضعت الإطار القانوني الدولي الأكثر تطوراً، الذي ينظم الهجمات السيبرانية إلا أنها لا تأخذ سوى جزء من التحدي العام، مع ذلك، فإنها توفر نقطة انطلاق لتصميم إطار دولي شامل لتنظيم الهجمات السيبرانية غير القانونية^(٢).

ويمكن القول: إن الهجمات السيبرانية تتضمن الجرائم الواردة في اتفاقية بودابست، التي تتعلق وتمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر لاسيما تلك المتعلقة بالنفاد غير المشروع الكامل أو الجزئي إلى نظام كمبيوتر والتدخل في البيانات (وذلك عن طريق إتلافها، حذفها، إفسادها، تعديلها أو تدميرها)، والتدخل في النظام عن طريق الإعاقة الخطيرة لاشتغال نظام الكمبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها^(٣)، ومثلاً، تتطلب المادة (٢) من الاتفاقية أن تتبنى الدول تدابير تشريعية وغيرها من التدابير لتجريم الأفعال الجنائية بموجب قانونهم المحلي، عند ارتكابها عمداً، وبغير حق النفاذ الكامل أو الجزئي إلى نظام كمبيوتر.

رابعاً: جهود منظمة شنغهاي للتعاون (SCO) في الحد من الهجمات السيبراني للمناطق المحمية.

اتخذت منظمة شنغهاي خطوات أولية مهمة بقصد التعاون في مجالات الأمن السيبراني ففي العام ٢٠٠٦ وقع رؤساء الدول الأعضاء إعلاناً حول أمن المعلومات الدولية. وفي عام ٢٠٠٩ قد صدر "إعلان يكاترينبورغ" وذلك في قمة منظمة شنغهاي للتعاون، التي عقدت في يكاترينبورغ، في روسيا الاتحادية، وقد أبدت المنظمة من خلاله استعدادها للتعاون والالتزام^(٤)، والحاجة الملحة للرد على التهديدات السيبرانية، وعُدَّ أمن المعلومات على أهمية السيادة الوطنية نفسها، والأمن الوطني، والاستقرار الاجتماعي والاقتصادي إذ جاء في الفقرة السابعة: "تؤكد الدول الأعضاء في منظمة

١ حسين شيخة الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية،

المجلد ١٧، العدد ١، جامعة الشارقة، الإمارات العربية المتحدة، ٢٠٢٠، ص ص ٧٤٠-٧٢٢، ص ٧٥٣-٧٥٤.

2 Hathaway Oona A. & Others: The Law of Cyber-Attack, op.cit, P864-863.

٣ مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست)، مجموعة المعاهدات الأوروبية رقم ١٨٥، ٢٠٠١، المواد (٥،٤،٢)، تاريخ الزيارة ٢٢/٦/٢٠٢٤، الساعة ٩:٠٠، متاح على الرابط: <https://cutt.ly/YkpJX>

4 Maonga, Sharon Kerubo: A Case of Incapacity: The Interrogation of International Humanitarian Law as A Satisfactory Regulator of Cyber Warfare, Strathmore University, Strathmore Law School ,2017, P 40, Available at: <https://cutt.ly/QjqA9H>

شنغهاي للتعاون على أهمية ضمان أمن المعلومات الدولي كأحد العناصر الرئيسية للنظام العام للأمن الدولي" (١).

أما في عام ٢٠١١ فقد تقدمت دول منظمة شنغهاي للتعاون بمشروع قرار للجمعية العامة للأمم المتحدة بشأن أمن المعلومات (٢).

خلاصة القول: إن ما قُدم من جهود دولية ولو لم يرقَ إلى مستوى تنظيمي دولي شامل، إلا أنها تظهر مدى الاهتمام الدولي المتزايد لوضع أطر تنظيمية للتصدي للهجمات السيبرانية، وفضلاً عن ذلك تعد الخطوة الأولى نحو اتفاقية متعددة الأطراف تنظم استخدام هذه الهجمات وتقلل من آثارها الجسيمة على البشر. إن هذه الجهود والمقررات والتوصيات على الرغم من قيمتها على المستوى الدولي، غير كافية ولا فاعلة، نظراً لعدم إلزاميتها القانونية، ولعدم إتاحتها إمكانية العقاب، هذا عدا عن الهوة الرقمية بين الدول، التي تزرع الشك بدل الثقة، ولا سيما مع سيطرة الولايات المتحدة الأمريكية على الانترنت.

1 Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009), Available at: <http://eng.sectsco.org/load/198293>

2 Kutnayeve, Nuria: Cybersecurity in Central Asia, Unipath-Magazine, United States Central Command (CENTCOM), August 20 ,2015, Available At: <https://cutt.ly/ijquJ7A>

الفصل الثالث

المسؤولية الدولية الناشئة عن الهجمات السيبرانية على المناطق المحمية وفق القانون

الدولي الإنساني

تطورت منظومة القانون الدولي المعنية بتنظيم الحروب قانونياً بالتزامن مع تطور الحروب وأدوات وأساليب القتال والسلاح المستخدم فيها، هذا التطور يفترض أن يكون مستمراً باستمرار تطور أساليب القتال وأدواته. ومع تزايد الاعتماد على الشبكات وتكنولوجيا المعلومات في النواحي العسكرية وفي إدارة مختلف مناحي وشؤون الحياة، بدأ نوع جديد من المواجهات بالظهور، يتخذ من الفضاء الإلكتروني ميداناً له عُرفت بالهجمات السيبرانية، ما فرض تحدياً جديداً في ميدان القانون الدولي حول التنظيم والتأطير القانوني لهذه الهجمات، وذلك من حيث إدارة الأطراف الضالعة بها، وما يترتب عليها من مسؤولية دولية جراء ذلك.

ومع تزايد الهجمات السيبرانية وبروزها في العقد الأول من الألفية الثالثة، بدأت بالتزامن مع ذلك معضلة المسؤولية الدولية لهذه الهجمات، وبرز وبالتحديد التساؤل حول المسؤولية الدولية الناشئة عن الهجمات السيبرانية على وفق القانون الدولي، إذ تعد المسؤولية أساس في الوجود القانوني، وتتوقف فاعلية قواعده على مدى نضوج قواعد المسؤولية فيه، فالمسؤولية هي أداة تطور للقانون، فهي قادرة على تحويل القانون من مجرد قواعد نظرية إلى التزامات قانونية.

زيادةً على ذلك، تعد المسؤولية الدولية من واحدة من أهم الموضوعات القانونية الدولية في وقتنا الحاضر، فحين النظر إلى التطورات العلمية الحديثة التي أثرت تأثيراً كبيراً على العلاقات الدولية نجد مشكلات جديدة قد ظهرت لم يعرفها القانون الدولي أو ينظمها، مما استدعى ضرورة معالجتها بطرائق جديدة تتوافق و طبيعتها، فضلاً عن ذلك فإن قواعد المسؤولية الدولية يشوبها الغموض وعدم الوضوح بشكل عام، وبشكل خاص فيما يتعلق بالهجمات السيبرانية، وما ينتج عنها من أضرار، ومدى خضوعها لقواعد القانون الدولي.

وبذلك سيُسلط الضوء على إمكانية انطباق المسؤولية الدولية عن الأضرار، التي يخلفها الهجوم السيبراني في القانون الدولي، ومدى تطبيق قواعد المسؤولية الدولية التقليدية عليها، في ظل الانتشار الهائل لهذه الهجمات في الوقت الراهن، نتيجة تزايد ارتباط العالم بالفضاء الإلكتروني، التي تعرض الدول لمخاطر كبيرة، نتيجة لما تتعرض له من هجوم يمس سيادة الدولة ويهدد استقرارها ويعرض مصالحها للخطر في شتى المجالات، ومن هذا المنطلق سنبحث في المسؤولية الدولية مفهومها،

أركانها، والتكيف القانوني للهجمات السيبرانية عبر مبحثين نناقش في المبحث الأول المسؤولية الدولية عن اضرار الهجمات السيبرانية تجاه المناطق المحمية، ونناقش في المبحث الثاني المناطق المحمية بموجب القانون الدولي الإنساني وآليات محاكمة منتهكيها أمام القضاء الدولي الجنائي.

المبحث الأول

المسؤولية الدولية عن أضرار الهجمات السيبرانية تجاه المناطق المحمية

تعد المسؤولية الدولية من المواضيع المهمة، التي هي ضمانة لكفالة تطبيق القانون الدولي، وذلك بسبب غياب سلطة عليا مستقلة عن الدول، تمتلك الشرعية لتحديد نظام المسؤولية، وفرض احترامها و في القانون الدولي.

وتقوم المسؤولية الدولية عن الأضرار، ومنها الأضرار بالمناطق المحمية على وفق المفهوم التقليدي على الأساس الإخلال بالتزام تفرضه قواعد القانون الدولي، على أن يقتصر هذا الإخلال بالضرر الذي يترتب الحق في المطالبة بإصلاحه بعد إثبات واقعة الإخلال وإسنادها إلى الشخص محل المسؤولية، أو تأسيس المسؤولية على العمل الدولي غير المشروع من دون اشتراط حصول الضرر، بل يكفي إثبات الانتهاك للقواعد المنظمة لتلك المناطق، إذ يعد مجرد حدوث الانتهاك لها كافياً لقيام المسؤولية.

بينما تقوم المسؤولية الدولية عن الأضرار، ومنها الأضرار بالمناطق المحمية على وفق المفهوم الحديث لها على أساس النتائج الضارة عن النشاط الدولي، حتى وإن كان هذا النشاط ليس محظوراً بموجب قواعد القانون الدولي طالما اتسم بطبيعته الخطيرة، على أنه على وفق الفقه الدولي لابد من توافر شروط معينة لتحقيق تطبيق المسؤولية الدولية عن الأضرار بتلك المناطق.

لذلك فإن المسؤولية الدولية تنشأ عند قيامها بعمل مخالف للالتزامات الدولية المتعلقة بالمناطق المحمية، أو قيامها بممارسة نشاط غير مشروع ذي صفة خطرة، وما يترتب بتلك المناطق والمستهدفين بالحماية من إنشائها فتصبح الدولة ملزمة بإصلاح الأضرار الناجمة عن هذه التصرفات. واستناداً لما سبق، سنقسم هذا المبحث على مطلبين، سأتناول في الأول مفهوم المسؤولية وأركان أو عناصر المسؤولية الدولية، والمطلب الثاني سنتطرق للتكيف القانوني للهجمات السيبرانية في ضوء المسؤولية الدولية.

المطلب الأول

مفهوم المسؤولية وأركان أو عناصر المسؤولية الدولية

تعد المسؤولية محور أي نظام قانوني، فهي جزء منه، ولما كانت العلاقات بين الدول قد شهدت تطوراً كبيراً منذ نشأتها، وأصبحت العلاقات الدولية أكثر تعقيداً وتداخلاً في المعاملات والعلاقات فكان لابد من وجود نظام قانوني يحكم تلك المعاملات والعلاقات، ويضمن التزام كل دولة تجاه باقي الدول في المجتمع دول ويضمن تحمل كل دولة نتيجة تلك الالتزامات أو الإخلال بها، وقد جاء ذلك في صورة قواعد المسؤولية الدولية، التي تُعد ركيزة أساسية لقواعد القانون الدولي، فهي تضمن التزام الدول بتحملها نتيجة التزاماتها.

لذا تعد المسؤولية الدولية الحارس الذي يسعى إلى ضمان احترام القانون، فقواعد المسؤولية بصفة عامة هي حجر الأساس في كل نظام قانوني.

وتتميز المسؤولية الدولية في القانون الدولي المعاصر في قواعدها وشروطها انطباقها من مجال إلى آخر، إذ إن الفقه الدولي لم يستقر حتى الآن على تعريف محدد لها، ويرجع ذلك إلى التطور الذي لحق بفكرتها وبالأساس القانوني، الذي تستند إليه، فضلاً عن الاختلاف في ماهية الأشخاص القانونيين مناط المسؤولية دولياً، سنتناول هذا الموضوع عبر فرعين نناقش في الفرع الأول تعريف المسؤولية الدولية وفي الفرع الثاني أركان أو عناصر المسؤولية.

الفرع الأول

تعريف المسؤولية الدولية

إن موضوع المسؤولية الدولية قد تعرض إلى العديد من المتغيرات بداية من طرح النظريات التي لها علاقة بالموضوع والتي تتمثل بنظريات الخطأ والمخاطر والنظرية الموضوعية، حتى الوصول إلى التنظيم الدولي المعاصر، والذي يتمثل بتدخل لجنة القانون الدولي من أجل اعداد مسودة فيما يتعلق بالمسؤولية الدولية عن الأفعال والأعمال، التي ليست مشروعة.^(١)

١ أحمد عبيس الفتلاوي، مصدر سابق، ص ٦٦.

تنوعت التعريفات المتعلقة بالمسؤولية الدولية، إلا أنه يجمع بينها أمر مشترك واحد هو أنها عبارة عن خرق لالتزام دولي من قبل دولة أخرى، الأمر الذي يستوجب مساءلتها من الناحية القانونية تجاه الدولة التي تم الاعتداء عليها، أو التي تضررت بسبب العدوان.^(١)

وردت تعريفات عديدة للمسؤولية الدولية تضمنتها كتابات المختصين في القانون الدولي، فالفقيه (هانس كلسن) عرفها بأنها: " المبدأ الذي ينشئ التزاماً بإصلاح أي انتهاك للقانون الدولي، ارتكبه دولة مسؤولة ويرتب ضرراً " ^(٢)، في حين عرفها الفقيه (دي فيشر) بأنها: " فكرة واقعية تقوم على التزام الدولة بإصلاح النتائج المرتبة على عمل غير مشروع منسوب إليها " ^(٣).

وعرفها الدكتور عصام العطية بأنها: " عبارة عن نظام قانوني تلتزم بمقتضاه الدولة التي تأتي عملاً غير مشروع طبقاً للقانون الدولي العام بتعويض الدولة، التي لحقها ضرر من جراء هذا العمل " ^(٤).

بينما يرى الدكتور (طلعت الغنيمي) أن المسؤولية الدولية: الالتزام الذي يفرضه القانون الدولي على الشخص بإصلاح الضرر لصالح من كان ضحية سواء كان تصرف أم امتناع وتحمل العقاب جزاء هذه المخالفة. ^(٥) وعرفت المسؤولية الدولية في مشروع المسؤولية الدولية عام ٢٠٠١: نصت المادة (١) منه "كل فعل غير مشروع دولياً تقوم به الدولة يستتبع مسؤولياتها الدولية".

وعرفت لجنة القانون الدولي المسؤولية في مشروعها بخصوص المسؤولية الدولية لعام ١٩٥٧ بأنها: إسناد فعل غير مشروع دولياً لأحد أشخاص القانون الدولي العام، مما يترتب التزامه بدفع التعويض أو جبر الضرر الذي حدث نتيجة هذا الفعل غير المشروع دولياً. ^(٦)

١ أحمد سيف الدين، المسؤولية الدولية: ماهيتها وآثارها وأحكامها، مجلة الجيش اللبناني، العدد ٣١٨، لبنان ٢٠١١، ص ٥٠ - ٥٤.

2 Kelsen, State Responsibility and the Abnormally Dangerous Activity, Columbig jolumbig journal of international Law, vol (2), 1972, P. 198.

٣ عماد خليل إبراهيم، مسؤولية المنظمات الدولية عن أعمالها غير المشروعة. ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص ١٤٣.

٤ عصام العطية، القانون الدولي العام. ط١، المكتبة القانونية، بغداد، ٢٠١٠، ص ٥١٧.

٥ محمد طلعت الغنيمي، الوسيط في القانون السلام. منشأة المعارف، الإسكندرية، ١٩٨٢، ص ٤٣٩.

٦ أحمد أبو الوفاء، شروط المسؤولية الدولية. مجلة الدبلوماسية، معهد الدراسات الدبلوماسية، العدد (١٣)، المملكة العربية السعودية، ١٩٩٠، ص ٤٥-٤٧.

وقد عرفها بعضهم بأنها ارتكاب شخص من أشخاص القانون الدولي عملاً غير المشروع طبقاً لأحكام القانون الدولي ينجم عنه ضرر بأفراد أو أموال شخص من أشخاص القانون الدولي، مما يوجب أداء التعويض للمضرور.^(١)

وتُعرف المسؤولية الدولية بأنه كل عمل يصدر عن الدولة يخرق التزاماً دولياً لها كان قد فرض عليها بموجب قواعد القانون الدولي العام، ومن ثم يترتب على هذا الخرق مساءلتها قانوناً، وعلى هذا الأساس يحق لكل دولة لحقها ضرر ما مساءلتها والمطالبة بالتعويضات.^(٢)

ويعد تعريف الدكتور (السيد أبو عطية) الملم لكل هذه العناصر إذ عرفها بأنها: " عملية إسناد إلى أحد أشخاص القانون الدولي، سواء أكان هذه الفعل يحظره القانون الدولي أم لا يحظره، ما دام قد ترتب عليه ضرر لأحد أشخاص القانون الدولي، مما يقضي توقيع جزاء دولي معين، سواء أكان هذا الجزاء ذا طبيعة عقابية أم كان ذا طبيعة غير عقابية " ^(٣).

ومن ثم فإن مفهوم المسؤولية الدولية يرمي إلى تحقيق هدفين، هما منع وتقليل الخسارة أو الضرر الناجم عن مزوالة أنشطة لا يحرمها القانون الدولي، والهدف الثاني يتعلق بإلزام أشخاص القانون الدولي بإصلاح ما يترتب عليه من أضرار ^(٤).

وقد عرفت اتفاقية لاهاي المسؤولية الدولية بأن أي دولة في حال إخلالها بأحكام اتفاقية لاهاي تكون ملتزمة بالتعويض إن كان ذلك ممكناً، و تكون الدولة أيضاً مسؤولة عن جميع الأفعال التي الواقعة من قبل أي شخص من أشخاص قواتها المسلحة ^(٥).

وعرفها معهد القانون الدولي: بأن الدولة تسال عن كل امتناع أو فعل متنافي مع التزاماتها الدولية مهما كانت سلطة الدولة التي أتمته تنفيذية أو قضائية أو تأسيسية كانت. و عرفت لجنة التحكيم في قضية نيرة (بين الولايات المتحدة والمكسيك) المسؤولية الدولية:

أ) الدولة تتحمل المسؤولية الدولية في حال فشل أحد الأعضاء من هيئاتها في أن ينفذ الالتزامات الدولية التي تلقى على عاتق الدولة وتسبب في أضرار لانتزال الأجانب أو لأشخاص في أراضيها.

١ عصام جميل العسلي، دراسات دولية. اتحاد كتاب العرب، سوريا، ١٩٩٨، ص ٥٤.

٢ محمد حافظ غانم، المسؤولية الدولية. ط١، معهد الدراسات العربية، مصر، ١٩٦٢، ص ١٤.

٣ السيد أبو عطية، الجزاءات الدولية بين النظرية والتطبيق. مؤسسة القافة الجامعية، مصر، دون سنة نشر، ص ٢٤٩.

٤ رشاد محمد جواد الليثي، حظر وتقييد استخدام الأسلحة في القانون الدولي العام، مصر، ٢٠١٠، ص ١٠٠-١٠١.

٥ اتفاقية لاهاي ١٩٠٧، المادة (٣).

ب) المسؤولية الدولية معناها أنه من الواجب إعطاء التعويض الناتج عن الفشل في الإذعان للالتزامات الدولية.

ج) تُسأل الدولة حين يقع على عاتقها واجب في التعويض لصالح دولة ثانية عن أضرار أصابت الدولة الأخيرة نتيجة لأضرار أصابت أحد رعاياها.^(١)

بينما عرفت الجمعية اليابانية للقانون الدولي: إن الدولة تسأل عن الأضرار، التي يتحملها الأجانب في ممتلكاتهم وأشخاصهم بسبب أفعال عمدية أو امتناعها عن قيامها بأفعال من الواجب عليها أن تقوم بها، من قبل موظفي سلطاتها عندما يقومون بتأدية واجباتهم الوظيفية في حال كانت الأفعال، أو الامتناع عنها تنتج عن انتهاكها لواجب دولي واقع على عاتق الدولة التي تتبعها السلطات المذكورة^(٢).

وإن المسؤولية الدولية للهجمات السيبرانية على المناطق المحمية هي التزام قانوني ينشأ في مواجهة الدولة أو الكيان الذي يرتكب، أو يشارك، أو يسهل تنفيذ هجوم سيبراني يستهدف منشآت أو مناطق محمية بموجب القانون الدولي، خصوصاً تلك الضرورية لبقاء السكان المدنيين، مثل المستشفيات، السدود، محطات المياه، أو المناطق المنزوعة السلاح.

تتحقق هذه المسؤولية متى ما توافرت شروط:

١. الركن المادي (العمل غير المشروع بموجب القانون الدولي)، و
٢. إسناد الفعل إلى الدولة (سواء من خلال الأجهزة الرسمية أو الفاعلين من غير الدول بتوجيه أو دعم مباشر).

وتترتب عليها التزامات قانونية، منها التعويض، وضمان عدم التكرار، وتحمل التبعات الدولية تستند المسؤولية هنا إلى مبدأ الحماية الخاصة المنصوص عليه في اتفاقيات جنيف (وخاصة المادة ٥٦ من البروتوكول الإضافي الأول لعام ١٩٧٧).

وإن الهجمات السيبرانية التي تؤدي إلى أذى واسع النطاق في المناطق المحمية قد تُشكل خرقاً للمبادئ الأساسية للقانون الدولي الإنساني، حتى في غياب نزاع مسلح تقليدي^(٣)

ونرى: إن مفهوم المسؤولية الدولية قد تطور تطوراً كبيراً، فلم يعد قاصراً على الآثار القانونية التي يربتها القانون الدولي مخافة أحكامه، بل إن مفهوم المسؤولية الدولية قد اتسع ليشمل وظيفة وقائية

١ خالد طعمة صعفك الشمري، القانون الجنائي الدولي، ط٢، الكويت، ٢٠٠٥، ص ٣٢-٣٨.

2 International. Law association, report 34 conference. 1926 p 382.

3 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, 2001, Articles 1-2, 4-8.

بجانب وظيفته العلاجية التقليدية، وهو مفهوم يسعى إلى منع وقوع الضرر بشكل عام، ومنها الأضرار بالمناطق المحمية بشكل خاص أو الحد منه إلى أكبر قدر ممكن، وذلك بوضع نظام قانوني اتفاقي لمواجهة أي ضرر بتلك المناطق.

ومن كل ما تقدم يمكن أن نعرف المسؤولية الدولية بأنها الالتزام الذي يفرضه القانون الدولي على الطرف الذي ينتهك القواعد المنظمة لحظر استخدام الأسلحة أو تقييده، بإصلاح الضرر الناشئ عن هذا الانتهاك، ويجب أن يكون التعريف ألي مصطلح قانوني جامع مانع، جامع لكل العناصر التي تدخل في نطاقه، ومانع من دخول أي مصطلح يشته به، أو يدخل عليه ما ليس منه؛ وعليه ينبغي أن يكون التعريف للمسؤولية الدولية جامع لنوعي المسؤولية المدنية والجنائية، سواء كانت هذه المسؤولية ناتجة عن فعل مشروع يحظره القانون الدولي لكن يترتب عليه ضرر لأحد الأشخاص الدولية أو التابعين لها، أو نتيجة فعل يعد انتهاكا لاحد الالتزامات الدولية، والنتيجة المترتبة على توافر هذه المسؤولية ودور المجتمع في توقيع العقاب المناسب.

وللمسؤولية الدولية العديد من المعطيات، التي تتمثل ب:

١. المسؤولية الدولية تقع على عاتق دولة، والدولة لوحدها هي المسؤولة وصاحبة الالتزام بإصلاح الأضرار، التي سببها تصرفاتها غير مشروعة، وليس هناك مانع من أن تترتب المسؤولية على منظمة دولية.

٢. تتقرر المسؤولية الدولية بسبب مصلحة دولة بالاستناد إلى مبدأ مراقبتها لحسن تطبيق القانون الدولي ومواجهة أي تقصير قد يوقعه تطبيق القانون نحوها.

٣. إن الدولة هي التي تضررت من أفعال مخالفة للقانون بأعمال قواعد المسؤولية الدولية.^(١)

أنواع المسؤولية الدولية:

يوجد نوعان للمسؤولية الدولية: تقصيرية وتعاقدية.

١. المسؤولية التعاقدية تنشأ عندما تخل الدولة بالتزاماتها التعاقدية مع البلدان الأخرى، على سبيل المثال اخلالها بالاتفاقات التجارية أو المالية، وحين يحصل إخلال، يجب أن تُلزم الدولة، التي أخلت بأن تعوض عن الأضرار الناتجة، ولو لم يُنص صراحة على ذلك في الالتزام الذي تم الاخلال به من قبلها.

١ أحمد سيف الدين، مصدر سابق، ٢٠١١، ص ١٠٨.

وفيما يخص إخلال بلد بتعهد تجاه رعايا بلد أجنبي، يميز الفقه بين حالتين: الحالة الأولى هي حالة الدولة كشخص عادي معنوي، والحالة الثانية هي حالة الدولة بوصفها سلطة عامة. إذ إنه في أول حالة لا تتحمل الدولة المسؤولية بشكل مباشر، وأي شخص من الرعايا الأجانب يصاب بأضرار معينة، فيجب عليه مراجعة القضاء ذي الاختصاص المناسب.

وأما في ثاني حالة فإن الأمور تبدو أكثر تعقيداً لأن التزامات الدولة متعلقة بحق السيادة، وهو من الحقوق، التي لا تقبل تدخل القضاء ومراجعته فيها. ويكون الحل عند ذلك هو لجوء الأجنبي، الذي أصابه الضرر إلى حكومة بلاده من أجل أن تسعى من خلال أساليبها الخاصة لكي تحصل حقوقه. وأيضاً هناك تحمل للدولة لمسؤولياتها الدولية عندما تنضم إلى معاهدة تقوم بتحريم الحرب، وبعد ذلك تخرج على قواعد الحرب أو تقوم بحرب عدوانية، إذ يمكن اعتبار تلك الأعمال إخلال من قبل الدولة بالتزام تعاقدى الأمر الذي يستوجب المسؤولية الدولية.

٢. المسؤولية التقصيرية هي النوع الثاني من المسؤولية الدولية وهي المسؤولية الناشئة عن تصرفات أو أفعال تصدر عن إحدى سلطات الدولة أو الهيئات العامة فيها، وتشكل إخلال بقواعد القانون الدولي، حتى ولو كانت تلك الأفعال غير متعارضة مع أحكام القانون المدني.^(١)

ومن الأمثلة على ذلك مسؤولية الكيان الصهيوني عن أضرار حروبها على لبنان: وفي عرف القانون الدولي المسؤولية تعني أن تقوم دولة بعمل غير مشروع أو تمتع عن عمل ينتج عنه الأضرار بالآخرين، فيجب على الذي يقوم بارتكابه أن يصلح كل ما يترتب عليه نتيجة الأضرار التي الحقها من خلال أحد وسائل الإصلاح.

إذ ينطبق ما سبق ذكره على الكيان الصهيوني وما قامت باقترافه بحق لبنان وفلسطين من مجازر ودمار وحروب منذ عام ١٩٤٨، و ما تزال تهدد بالمزيد منه حتى الآن، الأمر الذي يقوم بتحميلها المسؤولية الدولية الكاملة.

بإمكاننا أن نقول بشكل مختصر ان جرائم الكيان الصهيوني بحق لبنان وفلسطين ليس بالإمكان أن تُرتكب جرائم أشنع منها بحق شعب ووطن وبحق الإنسانية فيما تُرتكب من إجرام دولي. فضلاً عن ذلك لا يوجد وثيقة أو عرف أو أي قانون دولي أو أي ميثاق دولي لم تقم الكيان الصهيوني بخرقه، الأمر الذي يحتم أن تقوم مسؤولية دولية بحق الكيان الصهيوني.^(٢) مما تقدم نستخلص بأنه،

١ أحمد سيف الدين، مصدر سابق، ص ١٠٩.

٢ المصدر نفسه، ص ١٠٨.

يمكن إذا قدم أحد أشخاص القانون الدولي على استهداف المناطق المحمية في أثناء النزاعات المسلحة، فإنه يكون قد أخل بالتزاماته الدولية، وأضرّ بهذا المناطق، ما يستوجب قيام مسؤوليته الدولية ومعاقبته على ما ارتكبه من أضرار بها.

في عام ٢٠٢١، تعرضت عدة مستشفيات فرنسية لهجمات سيبرانية عبر برامج فدية (Ransomware)، أدت إلى شلل في أنظمة الرعاية الصحية، تأجيل عمليات جراحية حرجية، وتعطيل السجلات الطبية. أبرز هذه الحالات كانت في مستشفى فيليرانش-سور-ساون (Villefranche-sur-Saône) ^(١).

ويعلق الباحث على هذه الحادثة : تُعد المستشفيات من المناطق المحمية وفق المادة (١٨) من اتفاقية جنيف الرابعة، والمادة (١٢) من البروتوكول الإضافي الأول، التي تنصّ على أن "الوحدات الطبية يجب ألا تكون هدفاً للهجوم" فإذا ثبت أن الهجوم تم برعاية أو دعم أو تساهل من دولة معينة، فإن تلك الدولة: تكون مسؤولة عن فشلها في احترام أو ضمان احترام الحماية للمرافق الطبية، وتحمل مسؤولية خرق التزاماتها بموجب اتفاقيات جنيف. وحتى في حال عدم وجود نزاع مسلح، يمكن مساءلة الدولة بموجب قواعد مسؤولية الدولة عن الأفعال غير المشروعة دولياً، إذا أدى الهجوم إلى تهديد مباشر لحقوق الإنسان الأساسية، كحق الحياة والصحة.

فإن الهجمات السيبرانية التي تستهدف منشآت طبية محمية، سواء خلال نزاع مسلح أو في زمن السلم، قد تؤسس لمسؤولية دولية مباشرة للدولة إذا كان لها دور مباشر أو غير مباشر في التنفيذ أو الإهمال في منع الهجوم، خصوصاً عندما يكون الأثر مهدداً لحياة المدنيين ويخرق الحماية الخاصة للمرافق الإنسانية .

الفرع الثاني

أركان المسؤولية الدولية عن الهجمات السيبرانية على المناطق المحمية .

هناك تشابه واضح بين الأنظمة القانونية الداخلية والنظام القانوني الدولي، فإذا عُد شخص النظام القانوني الداخلي الفرد، فإن النظام القانوني الدولي يكون أشخاصه خاصون ومن بينهم الدول، إذ إنه النظام القانوني الدولي التزامات على أشخاصه، ويرتب الحقوق لهم، فالدولة التي تقوم فعل يُحدث ضرراً في دولة أخرى أو دول، فتتحمل الدولة، التي أوقعت الضرر، أو تسببت فيه، تبعات المسؤولية

1 French Ministry for Solidarity and Health, Cyberattacks Against French Hospitals: Impact and Response, Government Press Release, March 2021. Available at: <https://solidarites-sante.gouv.fr> (<https://solidarites-sante.gouv.fr/>) (Accessed: 19 July 2025)

الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، و تؤدي إلى أضرار، وبذلك تكون تلك الهجمات السيبرانية مستوفية شروط قيام المسؤولية الدولية لكن لنقص القواعد القانونية، وصعوبة إثبات مصدر تلك الجهات فإنه يتعذر ذلك.^(١) سنتطرق لأركان المسؤولية الدولية للهجمات السيبرانية، التي تتمثل على النحو الآتي:

أولاً: نسبة الفعل إلى الدولة:

لا يفي القول بوجود المسؤولية أن يكون الفعل ضاراً، أي: إن الفعل غير مشروع، إنما ينبغي أن يُسند الفعل غير المشروع إلى الدولة، إذ إن في القوانين الوطنية يشترط القانون أن يُسند الفعل إلى فاعل ما. أي: إلى شخص ما، لقيام المسؤولية في مواجهته، أي: ليس كافياً نسبة العمل إلى دولة ما، إنما ينبغي أن تكون الدولة -صاحبة الفعل- تامة وكاملة السيادة، بمعنى: إنها دولة مستقلة تامة الأهلية أو السيادة، حتى تُسأل عن أفعال التي تصدر عن سلطاتها الثالث: (التشريعية والتنفيذية والقضائية)، وتُسأل أحياناً عن الأعمال التي تصدر عن الأفراد العاديين، أو الموظفين الرسميين، وبهذا فإن الدولة المنضمة إلى دولة اتحادية لا تُسأل عن أعمالها؛ لأنها لم تعد من أشخاص القانون الدولي العام، وأن الدولة غير تامة السيادة أو الأهلية لا تُسأل عما تمارسه من أعمال، لأنها لا تمارس حقوق الدولة التامة الأهلية.^(٢)

وفي حالة الهجمات السيبرانية، فإن الضرر يعدّ متحققاً بمجرد إطلاق تلك الهجمات، ولا سيما أن الهجمات تستهدف وتُقصد بنى تحتية عائدة إلى إحدى الدول، ما قد ينجم عنها أضراراً كبيرة، وأن من يوجه هذه الهجمات هي الدول المتقدمة الحائزة على القوة الإلكترونية بشكل كبير، وقد توجه الهجمات أطراف كثيرة، لا سيما في أثناء الانتشار الإلكتروني يُسر الوصول إليه، وكثرة اعتماد الدول على الفضاء السيبراني، فقد توجه الدول القومية هذه الهجمات، أو المنظمات الحكومية سواء أكانت عالمية أم إقليمية، أو بعض الأفراد ممن تمكنوا دون سواهم من التحرك على قاعدة واسعة نوعاً ما من الاتصالات الدولية، أو إرهابيون -جماعات- والمتمردون، وحركات التحرر الوطني، وعامة، أن هؤلاء من -الفاعلين السيبرانيين- ينطبق عليهم الركن الأول، وهو أن يُنسب الفعل إلى دولة ما، إذ إن

١ نيا ببدانية، الأمن وحرب المعلومات. دار الشروق للنشر والتوزيع، الأردن، ٢٠٠٣، ص ٢٣.

٢ طلال ياسين العيسى، وعدي محمد عئاب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. مجلة الزرقاء والدراسات الإنسانية، المجلد (١٩)، العدد (١) جامعة عجلون الوطنية، الأردن، ٢٠١٩، ص

الدول هي من تساءل عن أفعال رعاياها في حالة التقصير^(١). من الثابت قانوناً وفقها أن المسؤولية الدولية لا تقوم من دون عمل غير مشروع يمثل إخلالاً بالتزام دولي مفروض على الدولة، وثابت ونافذ في حقها، وذلك سواء كان مصدره قاعدة عرفية أم اتفاقية أم قاعدة تمثل مبدأً من المبادئ العامة للقانون الدولي العام، التي أقرتها الأمم المتحدة في ميثاقها، أو كان التزاماً نص عليه قرار من القرارات، التي تشكل قواعد عامة صادرة عن المنظمات الدولية وأهمها على الإطلاق قرارات مجلس الأمن والجمعية العامة للأمم المتحدة، ويستوي أن يكون الإخلال بالالتزام عملاً غير مشروع، أي: إخلالاً إيجابياً أو مباشراً بالالتزام الدولي المفروض على الدولة (الخطأ) أم سلبياً كالامتناع عن القيام بعمل يترتب عليه تطبيق التزام دول، لكن هذه النقطة بالتحديد أثارت خلافاً فقهيّاً في تحديد المسؤولية الدولية عن الأضرار بشكل عام، ومنها الأضرار بالمناطق المحمية بشكل خاص، وظهرت بشأنها ثلاث نظريات، وهي: نظرية الخطأ والنظرية الموضوعية ونظرية المخاطر^(٢)، وسنتحدث عنها بالتفصيل فيما يأتي:

١. نظرية الخطأ

ذهب بعض الفقهاء منهم (جورسيون) إلى أنه ينبغي تأسيس المسؤولية الدولية على أساس نظرية الخطأ، ومفاد هذه النظرية عدم إمكانية مساءلة الشخص القانوني الدولي عن الأضرار، ومنها الإضرار بالمناطق المحمية في في أثناء النزاعات المسلحة، إلا إذا ارتكب فعل خطأ نتيجة عمد أو إهمال، وبناء على ذلك ليس بمقدوره الطرف المتضرر تحريك دعوى المسؤولية إن لم يستطيع إثبات الخطأ في جانب الطرف الآخر مرتكب الفعل غير المشروع، وعلى أساس ذلك فإن تطبيق هذه النظرية في مجال المسؤولية الدولية عن الأضرار بتلك المناطق في في أثناء النزاعات المسلحة يستلزم من الطرف المدعي إثبات الخطأ في جاني الطرف الآخر المتسبب في إحداث تلك الأضرار، فإذا أخفق في إثباته أنتفى أساس المسؤولية الدولية، ويستند هذا الرأي إلى الشخص القانوني الدولي لم يتخذ التدابير اللازمة لمنع هذه الأعمال، أو أنه لم يعاقب مرتكبيها لتحمل المسؤولية الناتجة عن خطأه، ويعزز هذا الرأي الفقيه (أوبنهايم)، الذي يرى بأنه لا وجود للمسؤولية الدولية من دون وجود خطأ.

١ ذياب البدانية، مصدر سابق، ص ٢٤.

٢ إسراء صباح الياسري، التنظيم الدولي للمناطق المحمية-دراسة في ضوء القانون الدولي الإنساني ط١، المركز العربي للنشر والتوزيع، مصر، ٢٠١٨، ص ٢٤١.

٢. النظرية الموضوعية (العمل غير المشروع)

وقد نادى بعض الفقهاء بالاستناد إلى النظرية الموضوعية، التي تجنبت عناء البحث عن أساس الخطأ الذي أخذت به النظرية السابقة في وضع أساس المسؤولية الدولية. ويرى بعض الفقهاء ومنهم (أنزلوتي) أن أساس المسؤولية الدولية، هو العمل غير المشروع، الذي يعني مخالفة للالتزام قانوني دولي، ومن ثم فإن المسؤولية الدولية تترتب بصورة كاملة بما فيها تعويض المتضرر، إذا كان هناك إخلال واضح بالقواعد القانونية الدولية، والتي تقع من ضمنها الاحتلال بالقواعد المنظمة للمناطق المحمية استناداً إلى فكرة العمل غير المشروع^(١). من دون ذلك يتعدى الأمر إلى البحث عن الدوافع والأسباب وما إذا كان الفعل قد اقتترف عمداً أو إهمالاً أو تقصيراً^(٢).

ويتضح: أن أي طرف من أطراف النزاع ينتهك التزاماته الدولية، ولا سيما تلك المناطق المحمية في أثناء النزاعات المسلحة عند عمله غير مشروع، وشكل أساساً قانونياً لقيام المسؤولية الدولية عن الأضرار بتلك المناطق، ومع ذلك فإن التقدم العلمي في جميع شؤون الحياة، وما نتج عنه من استعمال الطاقة الذرية وإطلاق الصواريخ في الفضاء الخارجي والتلوث البحري إلى غير ذلك من الوسائل العلمية المتقدمة التي تسبب مخاطر وأضرار استثنائي في نطاق العلاقات الدولية^(٣). أدى إلى البحث عن أساس آخر للمسؤولية الدولية فجاءت نظرية المخاطر.

٣. نظرية المخاطر

نادى بعض الفقهاء بالاستناد إلى نظرية المخاطر، التي تركز هذه النظرية على أساس الضرر، أي في حالة ممارسة أحد أشخاص القانون الدولي لنشاط ذي طبيعة خطيرة غير مألوفة، ففي هذه الحالة يتحمل المسؤولية عن الأضرار، ومما الأضرار بالمناطق المحمية، التي تتجم عن ممارسة هذه الأنشطة، وفي هذه الحالة يعفى الطرف المتضرر من إثبات الخطأ واللاشريعة، وتتاح له فرصة الحصول على تعويض عن الأضرار، التي تصب هذه المناطق جراء هذه الأنشطة الخطيرة^(٤).

١ رشيد مجيد الربيعي، مبدأ حسن النية في تنفيذ الالتزامات الدولية. رسالة ماجستير، كلية القانون والسياسة، جامعة بغداد، ١٩٨٣، ص ٦٥.

٢ جعفر عبد السلام، مبادئ القانون الدولي. ط ٢، دار النهضة العربية، مصر، ١٩٨٦، ص ٢٣٧.

٣ محمد عبد العزيز أبو سخيلة، مصدر سابق، ص ٢١٨.

٤ محمد سعادي، المسؤولية الدولية للدولة في ضوء تشريع والقضاء الدوليين. دار الجامعة الجديدة، الإسكندرية، ٢٠١٣، ص ٦١-٣٢.

ومن ثم لو تعرضت منطقة محمية تابعة لأحد أطراف النزاع للمخاطر والاضرار من قبل أحد أشخاص القانون الدولي، نتيجة قيامه بإجراء تجارب نووية على إقليمه، أو القيام بأعمال في مجال استكشاف الفضاء كإطلاق الصواريخ والأقمار الصناعية وسفن الفضاء، ففي هذه الحالة يحق للطرف المتضرر، طلب وقف هذه الاعمال الضارة إذا كانت هذه الاعمال مشروعة على أساس الأضرار التي تعرضت لها.

في فبراير ٢٠٢١، تعرضت محطة لمعالجة المياه في مدينة أولدسمار بولاية فلوريدا الأمريكية لهجوم سيبراني، حيث تمكن المهاجم من زيادة تركيز مادة هيدروكسيد الصوديوم (الصودا الكاوية) في المياه إلى مستوى خطر يهدد حياة المدنيين.

رغم أن التدخل البشري أوقف الكارثة قبل وقوعها، إلا أن هذا الهجوم أبرز أن البنى التحتية المدنية - كمحطات المياه - عرضة لخطر دائم بسبب الطبيعة المتصلة والرقمية لهذه الأنظمة، ما يُبرر تحليل الهجوم ضمن نظرية المخاطر^(١)

ويعلق الباحث المادة (٥٦) من البروتوكول الإضافي الأول (١٩٧٧) تنص على حماية المنشآت التي تحتوي على "قوى خطرة"، مثل السدود أو محطات المياه، حتى لو لم تكن هدفاً عسكرياً. إذا لم تتخذ الدولة خطوات لمنع الهجمات أو تأمين تلك المنشآت، فقد تُحمّل المسؤولية حتى من دون وقوع ضرر مباشر، بسبب إنشاء بيئة محفوفة بالمخاطر تهدد السكان المدنيين.

فإن نظرية المخاطر تُعد أداة قانونية مناسبة لتحليل مسؤولية الدولة أو الفاعل السيبراني عند تعريض المناطق المحمية للخطر عبر الإهمال أو ضعف الحماية، حتى لو لم يقع ضرر مادي فعلي. وتُستخدم هذه النظرية لتأكيد أن المسؤولية الدولية قد تنشأ من التهديد ذاته، لا من النتيجة فقط

ونرى: إن النظريات التي تحدد أساس المسؤولية الدولية عن الأضرار، و لاسيما متعلقة بالمناطق المحمية، أن العمل غير مشروع دولياً، كقاعدة عامة هو أساس المسؤولية الدولية عن الأضرار بتلك المناطق، مع إمكانية الأخذ بنظرية الخطأ في بعض الحالات، ويأخذ بنظرية المخاطر في حالة حدوث ضرر بتلك المناطق ناتج عن أفعال مشروعة، وإن هذه النظريات كلها صارت أو ضمنّت بنصوص قانونية .

1 Federal Bureau of Investigation (FBI), Cyber Intrusion Targeting U.S. Water Treatment Facility, Joint Advisory with CISA, February 2021. Available at: <https://www.cisa.gov>

ثانياً: أن يكون الفعل غير مشروع دولياً

وقد أجمع الفقه الدولي بأنه ذلك الفعل الذي يعد انتهاك الفعل غير المشروع، لأحكام القانون الدولي إذ هو الفعل الذي يكتنف مخالفة لقواعد القانون الدولي، أو لمبادئ القانون العامة، فالفعل الذي يعد فلاً غير مشروع دولياً هو السلوك الذي يُنسب إلى إحدى الدول على وفق القانون، الذي يتمثل في القيام بفعل، أو امتناع عن القيام بفعل، يعد مخالفة لالتزامها الدولي، فمقياس عدم المشروعية أو معيارها هو المعيار أو المقياس الدولي الموضوعي، لا عبرة فيه لقيام الالتزام، لأن مخالفة التزاماً دولياً ما، مهما كان منبعه، يُنشأ المسؤولية الدولية دون أن يُنظر إلى وصف الفعل في القانون الوطني، ولا يعتد بالوسيلة، التي يتحقق من خلالها الانتهاك الدولي، أو انتهاك القانون الدولي، سواء أكان الانتهاك بفعل أم كان الانتهاك بامتناع عن فعل، أم إهمال.^(١)

وفي التطبيق على الهجمات السيبرانية، نرى أنها الهجمات السيبرانية تُخالف قواعد القانون الدولي لأنها تخلف الأضرار المادية والبشرية الكبيرة، وهذا ما يخالف مقاصد الأمم المتحدة، والقانون الدولي الإنساني وسواها.

ثالثاً: الضرر

يقصد بالضرر كشرط من شروط المسؤولية الدولية، كل ضرر يلحق مصلحة أو حق مشروع لأحد أشخاص القانون الدولي العام. وهذا الضرر قد يكون مادياً أو معنوياً.^(٢)

ويعد الضرر واحداً من أهم عناصر المسؤولية؛ إذ إن في انعدامه تنعدم المسؤولية، وأن الضرر على أنواع، تقسم تبعاً لصالح المعتدى عليه، أو من لحقه الضرر: (ضرر مباشر وضرر غير مباشر)، فمن حيث مصلحة من اعتدى عليه فإن الضرر نوعان، الأول: ضرر مادي، وهو أي مساس يصيب حقاً من من حقوق أشخاص القانون الدولي المادية، أو يصيب حقوق رعاياه، ما يشكل عليه أثراً ملموساً واضحاً وظاهر للعيان، ويكون ضرراً مباشراً، أن الضرر الثاني، هو الضرر المعنوي: وهو أي مساس بشرف أو اعتبار أشخاص القانون الدولي، أو بأحد رعاياه، أي: إن الضرر المعنوي هو أي اعتداء يصيب حقاً من حقوق الأشخاص الدوليين أو رعاياهم، يخلف أثراً غير ملموساً.

١ صلاح الطائي، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديث، القاهرة، مصر، ٢٠٠٩، ص ٨٩.

٢ سالم عبد الخالق، المسؤولية والعقاب على جرائم الحرب مع دراسة تطبيقه على جرائم الحرب في البوسنة والهرسك. دار الجامعة الجديدة للنشر، مصر، ٢٠٠٤ ص ٢٨، ٢٩.

وعند التطبيق على الهجمات السيبرانية، فإن الضرر نراه يتحقق من تلك الهجمات، بجميع أشكاله، سواء أكان الفاعل دولة قومية، و حدث في الهجوم الفيروسي على البرنامج النووي الإيراني أم ما تقوم به منظمات إجرامية تلحق الضرر الفادحة بالآخرين، لا سيما في الهجمات، التي تسعى لقرصنة المعلومات أو تهدف لاختراق الحسابات المصرفية، وأو تهدف إلى سرقة أرقام بطاقات الائتمان، إذ تكلف سرقة أرقام بطاقات الائتمان تريليون دولار سنوياً.

و في عام ٢٠٠٧ قامت الكيان الصهيوني بهجوم ضد سوريا أدى إلى توقف منظومات الاتصال في المطارات المدنية و العسكرية و توقفت أجهزة الرادار عن العمل، خلال هجوم قام به سلاح الجو الكيان الصهيوني على مواقع سورية، و هنا يُعد الهجوم هجوم سيبرانياً و يُعد طريقة من طرق القتال يدخل ضمن الخطط العسكرية أدى إلى إلحاق أضرار بدولة معينة، و من الممكن أن تكون الهجمات السيبرانية تسبب أذى و ضرراً لدولة محددة أيضاً و حدث في إيران، الأمر الذي يجعل الهجوم دولياً من دولة إلى دولة إذ من الممكن أن يعطى الهجوم نظام التحكم و الحماية بعمليات دقيقة في محطة نووية معينة وتسخيرها لخدمة الدولة المهاجمة، فضلاً عن إدخال بيانات مغلوطة عن العمل في المحطة مثل رفع درجة الحرارة في أجهزة الكرد المركزية وهو أمر يمكن أن يؤدي إلى أن تنفجر المحطة أو تتعطل جزئياً أو كلياً أو تتأخر المهام المطلوبة. وفي هجوم الولايات المتحدة الأمريكية على محطة (نطانز) الإيرانية عام ٢٠١١، إذ استخدمت أمريكا برنامج قام بتعطيل بعض العمليات الحساسة الأمر الذي الحق ضرر بتخصيب اليورانيوم. وهنا نلاحظ حجم الضرر الكبير الذي الحقته دولة بدولة أخرى. من خلال الهجمات السيبرانية.^(١)

لكن على الرغم من توافر أركان المسؤولية الدولية في الهجمات السيبرانية، إلا أن الكشف عن هوية الفاعلين ومراقبتهم وتتبعهم؛ من أجل تقديمهم للمحاكمة، تكون مصحوبة بالصعوبة البالغة؛ لما يتمتع به الفضاء السيبراني من قابلية التخفي.^(٢)

ففي مايو ٢٠١٧، ضرب هجوم سيبراني عالمي ببرمجية فدية تُدعى WannaCry مئات الأنظمة حول العالم، وكان من أبرز المتأثرين خدمة الصحة الوطنية البريطانية (NHS). توقفت خدمات عدد

١ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية، مصدر سابق ص ٢١-٢٢.

٢ إسراء صباح الياسري، مصدر سابق، ص ٢٥١.

كبير من المستشفيات، وألغى أكثر من ١٩ ألف موعد طبي، وتعرض المرضى للخطر نتيجة تعطل أجهزة التشخيص والرعاية^(١)

ويعلق الباحث: إن الهجوم تسبب فعلياً في تعطيل رعاية صحية حيوية لآلاف المدنيين. فقد وقع الضرر على منشآت محمية بموجب المادة (١٨) من اتفاقية جنيف الرابعة، والمادة (١٢) من البروتوكول الإضافي الأول (١٩٧٧). وإن الضرر لم يكن محتملاً فقط، بل واقعياً وواضحاً: تأخير العمليات، تعريض حياة المرضى للخطر، إلغاء مواعيد العلاج الطارئة.

ومن ثم: تُطبق نظرية الضرر هنا لأنها تعتمد على النتيجة المؤكدة (الضرر الطبي المباشر) وليس فقط على الخطر أو الاحتمال. إذ تفترض هذه النظرية أن المسؤولية تنشأ حين يؤدي فعل غير مشروع أو إهمال إلى إحداث ضرر فعلي وقابل للقياس (مادي، أو جسدي، أو معنوي)، ويُعد هذا الفعل أساساً لطلب التعويض أو المساءلة

ونرى: أن القواعد القانونية المنظمة للمسؤولية الدولية، أصلها قواعد عرفية متعارف عليها ضمن المجتمع الدولي، وكانت أول محاولة لتقنينها خلال مؤتمر لاهاي، الذي جرى عقده عام ١٩٣٠م، ولكن المجتمع الدولي حينها لم يتفق على صيغة عامة لهذه المسؤولية، من ثم تولت لجنة القانون الدولي التابعة للجمعية العامة للأمم المتحدة عام ١٩٦٣ إلى أن تم الاتفاق على أركان المسؤولية الدولية من قبل المجتمع الدولي للآن.

المطلب الثاني

التكييف القانوني للهجمات السيبرانية والتعويض عنها

يعدّ ظهور شبكة الإنترنت وتوسعها على الصعيد العالمي سبباً في حدوث أقوى ثورة تكنولوجية وأسرعها في التاريخ البشري، إذ إنه في غضون العقدين الماضيين، ارتفع عدد الأفراد الذي يستخدمون الإنترنت من (١٦) مليون شخص في عام (١٩٩٥)، إلى أكثر من (١.٨) مليار في أواخر عام (٢٠١٦)، وبفعل تلك الثورة أصبحت الدول والمجتمعات غير الحكومية، والأعمال التجارية، والأوساط الأكاديمية، والأفراد، مترابطة إلى حد لا يمكن تخيله من قبل، وفي الوقت نفسه ازداد الاعتماد العسكري على أنظمة الحواسيب وشبكاتها زيادة هائلة: مما فتح المجال الخامس من القتال الحربي إلى جانب المجالات المعترف بها تقليدياً: الأرض، والبحر، والجو، والفضاء الخارجي.

هذا التطور الكبير وبشكل خاص في مجال تكنولوجيا المعلومات والاتصالات، أدى إلى حدوث العديد من التغيرات في جميع نواحي الحياة، وبشكل خاص في المجالات الأمنية والعسكرية، إذ أصبح هناك أبعاد جديدة في أسلوب بناء قدرات القوات المسلحة وفي طريقة القتال، ويرجع ذلك نوعاً ما إلى المستجدات، التي حصلت على طريقة وأشكال التفكير الاستراتيجي، إذ تبلورت عقائد قتالية جديدة تتناسب مع الواقع الذي يتغير باستمرار. سنبحث هذا المطلب عبر فرعين، نناقش في الفرع الأول التكيف القانوني للهجمات السيبرانية، أما الفرع الثاني فنناقش فيه التعويض عن الهجمات السيبرانية.

الفرع الأول

التكيف القانوني للهجمات السيبرانية

إن الأبحاث والدراسات القانونية، التي ظهرت في هذا المجال فيُعد (ديفيد رونفليد وجون اركويلا) من الأوائل الذين بحثوا في أمور الهجمات السيبرانية عام ١٩٧٧ في الكتاب الذي سموه: الحرب السيبرانية قادمة، إذ تمت الإشارة في الكتاب إلى أنظمة الاتصال الإلكترونية والدور الفعال لها في المستقبل فيما يتعلق بالنزاعات المسلحة. وفيما يتعلق بالدول، التي كانت تطور برامج لقدراتها السيبرانية فقد تكتمت على الموضوع أول الأمر وعدّته عنصراً مهماً من عناصر أمنها القومي.^(١) رأى بعض الفقهاء من الباحثين أن قواعد القانون الدولي الإنساني لا تكفي في تنظيم أو تكيف الهجمات السيبرانية ويجب إعادة النظر فيها، إذ أشاروا إلى المدة التي تم فيها إبرام الاتفاقيات، مثل اتفاقيات لاهاي ١٨٩٩-١٩٠٧، واتفاقيات جنيف الأربعة ١٩٤٩، البروتوكولين الإضافيين الملحقين بها لعام ١٩٧٧، إذ لم تكن الهجمات السيبرانية في ذلك الوقت لها تأثير كبير، ويرجع السبب في التأخر في الوصول إلى اتفاقيات دولية محددة، ومعينة ولا سيما بالهجمات السيبرانية إلى تكتم الدول وانفرادها بهذا الاستخدام، فلا ترغب في طرح هذا الموضوع في المحافل الدولية، فهو قطاع حيوي بالنسبة للدول التي تستخدمه، ومن أهم أسباب أمنها القومي^(٢).

وهذا الاتجاه من التطورات، التي أحدثتها الفضاء السيبراني على الساحة الدولية، يثير التساؤل إلى أي مدى أن يكون القانون الدولي قائماً، ويمكن نقله إلى المجال السيبراني؟ من حيث المبدأ، إذ إن القانون الدولي القائم يحكم أنشطة الدولة أينما كانت بما في ذلك الفضاء السيبراني، ومع ذلك، فإن تطبيق القواعد القانونية الموجودة مسبقاً، والمفاهيم والمصطلحات إلى تكنولوجيا جديدة قد تنطوي على

١ أحمد عبيس الفتلاوي، الهجمات السريانية دراسة قانوني. تحليلية، مصدر سابق، ص ٢٤.

٢ ، المصدر نفسه، ص ٤٠.

بعض الصعوبات، في ضوء خصائص المتميزة للفضاء السيبراني، لذلك سنوضح التكيف القانوني للهجمات السيبرانية.

ويعد تكيف الهجمات السيبرانية على وفق المبادئ الرئيسية في القانون الدولي، التي نص عليها ميثاق الأمم المتحدة منها مبدأ السيادة للدول، ومبدأ حظر استخدام القوة أو التهديد باستخدامها، وبما أن التطور الحاصل أظهر مجالات جديدة كالسيادة السيبرانية، وما يهدد تلك السيادة من هجمات، لذلك هل تعد الهجمات الإلكترونية استخدام للقوة ضد سيادة الدولة؟، وما مدى انطباق هذه المبادئ على الهجمات الإلكترونية؟ وعليه سنتناول هذين المبدأين على وفق الآتي:

أولاً: مبدأ السيادة:

يرجع مفهوم السيادة بشكل عام إلى معاهدة وستفاليا لعام (١٩٤٨)، التي كانت أول من أرسى هذا المبدأ، وُقصد به) أن تقوم الدولة بأدراة شؤونها دون تدخل من أي دولة أو دول أخرى^(١). هذا وتعد فكرة السيادة والاعتراف بها من المبادئ، التي يُتفق عليها ميثاق الأمم المتحدة، إذ جاء فيه بأن "تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها"^(٢).

وطراً على المفهوم التقليدي للسيادة تغييرات بسبب التطور التكنولوجي وظهور الفضاء الافتراضي، فبرز ما يسمى السيادة السيبرانية^(٣)، ما دفع دول العالم لفرض الرقابة الأمنية عليها، فهي مفهوم جديد مشتق من مصطلح الأمن السيبراني، الذي يتعلق بحماية البنى التحتية الرقمية والتقنيات والمحتويات الرقمية والاتصالات، وكل ما يمكن أن يرتبط بالفضاء السيبراني^(٤). هذا وواجهت السيادة تحدي جديد، وهو الهجمات الإلكترونية فأن من يقوم بهذه الهجمات عبر شبكات الانترنت في الفضاء الخامس ينتهك في سبيل ذلك السيادة الوطنية لدولة ما عندما يكون مصدر الهجوم قد وقع ضمن سيادة دولة أخرى، وعلى هذا فأن مفهوم السيادة التقليدي بدء يتقلص بسبب وسائل الاتصال الإلكترونية، التي

1 Marie Baezner, Patrice Robin, Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), 2018, p7.

٢ يُنظر المادة: (٢) الفقرة (١) من ميثاق الأمم المتحدة. السيادة السيبرانية (هي بسط الدولة سيطرتها وولايتها الفضائية على الفضاء الرقمي المتمثل بشبكة الانترنت).

٣ حسام جاسم، محمد أحمد الدليمي، التطور التكنولوجي وأثره في سيادة الدول. رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الأنبار، العراق، ٢٠١٨، ص ١١٤.

٤ فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمية: الصين نموذجاً، المجلة الجزائرية للأمن الإنساني. المجلد (٥)، العدد (١)، محور الأمن الإنساني، جامعة باتنة، الجزائر، ٢٠٢٠، ص ٧٩٨.

جعلت الحدود الإقليمية تتضاءل شيئاً فشيئاً، والاضمحلال تلك الحدود في الفضاء الافتراضي، وما ينتج عنها من مخاطر، فقد قامت الدول بتطور تشريعاتها الوطنية لاستيعاب الجرائم التي تحدث في ذلك الفضاء.^(١)

هذا و ينطبق مبدأ السيادة الإقليمية على الفضاء السيبراني، ويشمل البنية التحتية الإلكترونية كشبكات الاتصال، وتنظيم الحواسيب وقطاعات الطاقة والنقل... الخ، إذ يكون للدولة حق في أن تمارس الرقابة على أنشطة تلك البنية التحتية، ولها حق سيادي عليها وممارسة تلك السيادة مقيدة بالمبادئ العرفية أو المقننة في القانون الدولي^(٢)، وذهب خبراء حلف الناتو برأي لهم إلى أبعد من ذلك فأكدوا أن على الدول واجب منع استخدام البنى التحتية السيبرانية، التي تقع على إقليمها وتخضع لسيطرتها في نشاطات تمس الحقوق السيادية لدول أخرى، وأن سيادة الدولة تكون ليست على البنى المشيدة في أراضيها فقط، إنما حتى على البنى التحتية التي تحت سيطرتها، وأن كانت على إقليم دولة أخرى.^(٣)

ويمكن القول: إن الهجمات السيبرانية، التي تقوم بها دولة ضد دولة أخرى تكون خرقاً لسيادة تلك الدولة، ومن ثم نطبق مبدأ السيادة في الفضاء السيبراني، ليس بالشكل الذي ينطبق فيه بالعالم الواقعي، لأن الفضاء الافتراضي لا يعرف الحدود، وعلى الرغم من ذلك أقرت السيادة للدولة في هذا الفضاء، لأن آثار الهجمات السيبرانية (الإلكترونية) قد تكون خطيرة.

ثانياً: مبدأ حظر استخدام القوة والتهديد باستخدامها:

ورد هذا المبدأ في ميثاق الأمم المتحدة الذي نص على أن (بمتنع أعضاء الهيئة علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي دولة لأي دولة).^(٤) وعند التدقيق في هذه المدة نلاحظ أنها تحظر أن تتدخل دولة في الشؤون الداخلية لأي دولة أخرى من الدول الأعضاء في الأمم المتحدة. ولكن ما علاقة هذا النص بالهجمات السيبرانية؟ لقد كان هناك

١ أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونية والسياسية، المجلد (٤٤)، العدد (١)، كلية القانون والعلوم السياسية، جامعة الكوفة، النجف الاشرف، العراق، ٢٠٢٠، ص ٥٧.

2 Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies, U. S. Naval war college, Vol 89,2013, p128.

٣ علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية. المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص ٢.

٤ ينظر: المادة (٢) الفقرة (٤) من ميثاق الأمم المتحدة.

إشارة من قبل عدد من الباحثين عند دراستهم لموضوع الهجمات السيبرانية الجدلية إلى تكيف تلك الهجمات في حال وقوعها إذ يُعد خرقاً صريحاً لحكم الفقرة (٤) من المادة (٢)، ومن بينهم ماركو روسيني و شين، و أشار الفقهاء عند تفسير الفقرة (٤) من المادة (٢) إلى رأيين: الأول: أشار إلى أن نص الفقرة منطلق علل الاستخدام الفعلي للقوة المسلحة، أو التهديد فقط، وهذا الاتجاه تتبناه الدول التي تدعم المجموعات المسلحة، أو ما يعرف بالتدخل لأجل المسؤولية أو التدخل الإنساني، والاتجاه الثاني تؤيده دول العالم الثالث، الذي يشير إلى مفهوم أوسع نطاق، فاستخدام القوة أو التهديد لا يغني أنه الوسيلة الوحيدة من أجل التدخل في الشؤون الاقتصادية أو السياسية، و يُعد كتدخل في استقرار الدول و سيادتها^(١).

ويستكمل الحظر المنصوص في الميثاق بقاعدة أخرى في القانون الدولي العرفي، وهي قاعدة عدم التدخل في الشؤون الداخلية للدول، وهذا ما قرره محكمة العدل الدولية في أن هذه القاعدة متوافقة مع ما جاء في الميثاق^(٢)، على الرغم من أهمية هذا المبدأ في حفظ السلم والأمن الدوليين، إلا أنه يرد عليه استثنائين:

الأول: هو ما ورد في المادة (٣٩) من الميثاق، التي نصت على أن "مجلس الأمن أن يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان"، وقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام الماديتين (٤١-٤٢) لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

الثاني: ما ورد في المادة (٥١) منه التي تتعلق بحق الدفاع الشرعي للدولة في حال تعرضت لأي اعتداء، التي نصت على أنه "ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير، التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فوراً، ولا تؤثر تلك التدابير بأي حال في فيما

١ احمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية، مصدر سابق، ص ٤٦.

2 Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School, United States of America, Vol. 100:817, 2012, p842

للمجلس بمقتضى سلطته ومسؤولياته أنه المستمرة من أحكام هذا الميثاق الحق في يتخذ أي وقت ما يرى ضرورة لاتخاذ من الأعمال لحفظ السلم والأمن الدول أو إعادته إلى نصابه" (١).

و كان هناك سوابق قضائية في محكمة العدل الدولية ذهبت إلى أن نطاق الهجوم المكاني، وآثاره هما المعنيان في تحديد ما هي ردة فعل الدولة، التي تم الاعتداء عليها(٢).

ومن خلال قراءة نصوص المادتين يثار التساؤل إذا كان نص هاتين المادتين يطبق على الهجمات التقليدية واستخدام القوة في المجال الواقعي، هل يمكن أن تطبق ذاتها على الهجمات الإلكترونية في الفضاء الافتراضي؟، وهل يكون للدولة، التي تتعرض للهجوم السيبراني حق الدفاع عن نفسها؟، ولغرض الإجابة على هذين السؤالين نستعرض أهم النظريات، التي عالجت الهجمات الإلكترونية السيبرانية وهي:

١. نظرية النهج القائم على الوسيلة:

تستند هذه النظرية إلى الوسيلة التي تستخدم في الهجوم، إذ تؤكد على أن الهجوم السيبراني وحده لا يكون هجوم مسلح، ومن ثم لا يكون للدولة حق في الدفاع عن نفسها على وفق المادة (٥١) من ميثاق الأمم المتحدة سالف الذكر، لأن هذا الهجوم ليس فيه الخصائص الفيزيائية، التي ترتبط بالإكراه العسكري، وتعتبر آخر فهو لا يحتوي على الطاقة الحركية،(٣) وفي الأسلحة التقليدية، فليس بالإمكان بحسب رأي بعض الفقهاء أن يُحس بالهجوم بشكل مادي أو على نحو مادي ، فضلاً عن أن وسيلة الهجمات السيبرانية ليست محتوية على مواد ذات انفجار شديد، وبذلك يقومون باستبعادها بسبب طبيعتها من مجموعة الأسلحة وطائفتها، و يستبعدنها أيضاً من تنظيمها دولياً. وفي هذا الموضوع كان هناك رأي مخالف لهذا الرأي من قبل بعض الفقهاء؛ إذ إن أبعاد الهجمات السيبرانية بهذه الطريقة من فئة الأسلحة هو رأي غير حكيم وغير صائب، إذ إنه من غير الضروري أن يشترط في الأسلحة بشكل عام أن تحتوي على طاقة حركية، أو تحتوي على مواد ذات انفجار شديد، وأيضاً لا يشترط وسيلة

١ ينظر: المادة (٥١) من ميثاق الأمم المتحدة، ويُنظر: أيضاً احمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية، المصدر السابق، ص ٤٩.

٢ المصدر نفسه، ص ٥٠.

٣ أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، ص ٥٩.

حركية عند استخدامها، وبمعنى آخر ممكن أن تستخدم من غير أن يكون هناك حاجة إلى القذائف أو الصواريخ.^(١)

وما يزيد هذه النظرية هو ما ورد في القرار الصادر عن الجمعية العامة للأمم المتحدة، والذي جاء في أن العدوان "هو قيام القوات المسلحة لدولة ما بمهاجمة القوات البرية والبحرية والجوية أو الاسطولين البحري والجوي لدولة ما" مثلاً ورد في المادة الثالثة منه أعمال العدوان، التي جاءت على سبيل المثال لا الحصر،^(٢) وعلى الرغم من سهولة تطبيق هذه النظرية إلا أنها لا تؤخذ بالحسبان الهجمات الإلكترونية، التي قد تسبب أضراراً بالغة.

٢. نظرية النهج القائم على الأهداف:

تؤكد هذه النظرية أن استهداف الهجوم السيبراني نظاماً مهماً للدولة يمكن عدّه هجوماً مسلحاً يبيح للدولة حق الدفاع عن النفس، ومثال على ذلك استهداف البنى التحتية للدولة معينة، فيكون الهجوم السيبراني على تلك البنى التحتية المهمة للدولة هجوماً مسلحاً على وفق هذه النظرية، لكن هذه النظرية أنقذت، لأنها تجاهلت مفهوم البنى التحتية الحرجة وجسامة الهجوم السيبراني وآثاره^(٣).

٣. نظرية النهج القائم على الآثار:

تعد هذه النظرية بين النظريتين السابقتين، فهي تقوم على خطورة آثار الهجوم، فعلى وفقها يعد الهجوم الإلكتروني مسلحاً إذا كانت آثاره خطيرة، مثال ذلك الهجوم ضد نظام مراقبة الملاحة الجوية والتسبب بحوادث للطائرات، فيعد هذا الهجوم هجوماً مسلحاً، لأنه من المتوقع أن يسبب خسائر في الأموال والأرواح، ومن ناحية أخرى فالهجوم الإلكتروني على شبكة الويب أو مجرد اختراق لنظام الكمبيوتر بشكل عام فهذا لا يعد بمثابة هجوم مسلح مالم ينتج عنه أضراراً مالية وجسدية، ومن ثم يمكن القول أن هذا الاتجاه هو الأكثر قبولاً من الاتجاهات، التي ذكرناها، وعلى الرغم من ذلك فأن

١ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة تحليلية، مصدر سابق، ص ٢٢.

2 United Nations Audiovisual Library of International Law, General Resolution 3314, Defining aggression, p5.

٣ أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مصدر سابق، ص ٦٠.

هذه النظرية لا تنطبق إلا على مجموعة صغيرة من الهجمات الإلكترونية الضارة، التي يكون لها آثاراً تشبه آثار الأسلحة التقليدية، من ناحية الأضرار^(١).

مما تقدم يمكننا القول: إن الهجوم السيبراني متى ما كانت آثاره ضارة يكون بمثابة هجوم مسلح واستخدام للقوة ضد دولة ما، وبذلك يكون للأخيرة حق الدفاع عن نفسها، فطبق الاستثناء الوارد في الوثائق، وهو حق الدفاع الشرع التي نصت عليه المادة (٥١)، وهذا بدلالة القاعدة (١٣) من دليل تالين بقولها "يجوز للدولة التي تكون هدفاً للعمل السيبراني التي تصل لمستوى الهجوم المسلح أن تمارس حقها الطبيعي في الدفاع عن النفس"^(٢). أما بخصوص المادة (٢) الفقرة (٤) من الميثاق المذكور سلفاً، التي حظرت استخدام القوة أو التهديد باستخدامها، فإن الهجمات الإلكترونية إذا لم تصل إلى حد النزاع المسلح، ولم تكن آثارها ضارة هنا لا يمكن أن تعد استخدامها للقوة على وفق مفهوم هذه الفقرة، إنما يمكن أن تعد شكلاً آخر يشبه أعمال الضغط السياسي والاقتصادي، ومن ثم فإن الخرق في هذه الحالة يكون لقاعدة (عدم التدخل) الواردة في القانون العرفي^(٣). وهذا يعني أن ميثاق الأمم المتحدة بشكل عام والمبدأين المذكورين ينطبقان على الهجمات الإلكترونية، وأن الأخيرة تشكل تهديداً لهذه المبادئ الرئيسية في القانون الدولي، وهذا الرأي بدلالة ما جاء بتقرير فريق الخبراء الحكوميين بقولهم: إن ميثاق الأمم المتحدة قابل للتطبيق وضروري للحفاظ على سلم واستقرار بيئة تكنولوجيا المعلومات والاتصالات، وأن مبدأ السيادة ينطبق على تصرفات الدول في المجال السيبراني^(٤)، أما من ناحية تطبيقها على تلك الهجمات واقعياً فمن وجهة نظرنا، يكون بشكل يختلف عن تلك المطبقة على الهجمات التقليدية.

ونرى: بأن الهجمات السيبرانية تعد إحدى الوسائل الحديثة والأكثر استخداماً لحسم الصراعات بين الدول، لسرعتها وسهولة استعمالها وقلة تكلفتها، إذ يمكن، لأي دولة أن تعطل المنشآت والبنى التحتية

1 Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School, United States of America, Vol. 100:817, 2012, p848.

٢ علي محمد كاظم الموسوي، مصدر سابق، ص ٤.

٣ أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مصدر سابق، ص ٦١.

4 Report of the Group of Governmental Experts on Developments in (the Field of Information and Telecommunications in the Context of International Security, Sixty-eighth session, document (A/68/98), 2013, p8.

العسكرية أو المدنية، لدولة أخرى بالضغط على بعض الأزرار، ومن ثم إخضاعها دون استخدام الوسائل التقليدية للحرب.

الفرع الثاني

التعويض عن ضرر الهجمات السيبرانية على المناطق المحمية

قد يكون وقف العمل أو تقديم ضمانات بعدم تكراره الهجمات السيبرانية لا يكفي لتحقيق العدالة، ولاسيما إذا نتج عن العمل الموجه أضراراً تستلزم إصلاحه، وهنا لابد من إلزام الشخص محل المسؤولية بإزالة ما ظهر من آثار نتيجة ذلك، ويكون ذلك عن طريق تعويض وإصلاح الضرر الناشئ عن ذلك التدمير. غير أن تحليل موضوع تعويض الضرر يستنتج بالضرورة شرح أساس التعويض في القانون الدولي، ومن ثم التمييز بين أشكال هذا التعويض، وذلك بالمفهوم الواسع له، فهناك من ناحية إعادة الحال إلى ما كان عليه إذا كان ذلك ممكناً، ومن ناحية أخرى التعويض المتمثل بدفع مبلغ من المال، وكذلك الترضية، التي تتجه نحو تعويض الضرر المعنوي. على أن أشكال التعويض يستلزم بالضرورة معرفة تقديم التعويض، وهم الأشخاص الذين تضرروا من جراء العمل الضار بالمناطق المحمية.

أولاً: أساس التعويض عن ضرر الهجمات السيبرانية على المناطق المحمية في القانون الدولي الانساني

اهتم القانون الدولي بالتعويض على غرار القانون الوطني، وهذا في العديد من القضايا الدولية التي رفعت نتيجة إقامة المسؤولية الدولية على الشخص الدولي المتسبب في الضرر، وكان التعويض هو الحل الأنسب فيه حين يستحيل إصلاح الضرر للشخص الدولي عن طريق الترضية. فالتعويض في القانون الدولي العام غايته إزالة كافة الآثار المترتبة على وقوع الفعل غير المشروع، سواء ما لحق المضرور من خسارة أم ما فاتته من سبب، ولهذا وجب أن يكون مسأولاً لحجم الضرر وقيمة خسائره الحاضرة المستقبلية ولا سيما ما فات المضرور من كسب وما لحقه من خسارة.^(١)

و يُعد التعويض في القانون الدولي العام أنه التأثير الأساسي للفعل غير مشروع دولياً وهو من القواعد العامة التي تم التسليم بها ضمن مبادئ المسؤولية الدولية المقننة على وفق المشروع النهائي الذي صدر عن لجنة القانون الدولي لعام ٢٠٠١ إلى جانب أن التعويض في القانون الدولي يجسد النتيجة

١ زازة الخضر، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام. دار الهدى، الجزائر، ٢٠١١، ص٥٢٣-٥٢٤.

القانونية للمسؤولية الدولية حين يتسبب شخص دولي بإلحاق الضرر بشخص دولي ثاني، وهذا ما أكد عليه كل من القانون الدولي والقضاء الدولي في كثير من القضايا الدولية والاتفاقيات، ومن ضمنها على سبيل المثال:

١. إعلان الأمم المتحدة الذي يتعلق بمبادئ العدل الأساسية المرتبطة بضحايا الإجرام والتعسف في استخدام السلطة والذي ورد فيه: إجبار من يرتكب الأعمال الإجرامية على تعويض الضرر، الذي لحق بالضحايا أو أسرهم أو الأفراد الموجودين تحت رعايتهم بشرط أن يضم هذا التعويض إعادة الممتلكات وجبراً للأضرار أو الخسائر التي أصابت الضحايا إلى جانب التعويض عن الأموال، التي قاموا بصرفها بسبب اتهامهم، وأيضاً تقديم الخدمات وإعادة الحقوق.

واجب الدولة على كفالة جبر أو تعويض نقدي للضحايا كلما كان من الصعوبة تحصيل تعويض شامل من قبل من قام بارتكاب الجريمة أو من جهة ثانية.^(١)

٢. مشروع المسؤولية الدولية التي قامت بإعداده جامعة هارفرد عام ١٩٦١، الذي ورد فيه: تُسأل الدولة عن العمل أو عدم القيام بالعمل المنسوب إليها، الذي يلحق الضرر بالأجانب وتتكفل بإصلاح الضرر الذي لحق بالأجنبي بشكل مباشر أو من يحل محله أو الدولة التي تطالب به^(٢) قرار محكمة العدل الدولية في قضية (شورزو)، الذي جاء فيه الآتي:

من قواعد القانون الدولي وأيضاً من القواعد العامة للقانون أن انتهاك أي التزام ينتج عنه التزام بتعويض الضرر وأن الالتزام بتعويض الضرر هو المكمل الأساسي لعدم تطبيق الاتفاقية. و لو لم يرد في الاتفاقية على ذلك وأيضاً هو النتيجة الحتمية، لأي انتهاك بأي من التعهدات الموجودة بين الدول وبين بعضها بعض^(٣).

٣. اجتهاد المحكمة الأمريكية لحقوق الإنسان والذي صدر بتاريخ ١٩٨٨/٧/٢٩ في لاسكيس رودريغيز ضد دولة الهندوراس، الذي جاء فيه: من واجبات الدولة فيما يتعلق بمنع حدوث

١ باية فتحية، التعويض في القانون الدولي العام، مجلة القانون والتنمية المحلية، محور القانون والتنمية المحلية، ادرار-الجزائر المجلد (١) العدد (٢)، الجزائر، ٢٠١٩، ص ٢.

٢ جمال عبد الفتاح عثمان، المسؤولية الدولية عن عمليات البث المباشر العابر للحدود في ضوء أحكام القانون الدولي، دار الكتاب القانوني، مصر، ٢٠٠٩، ص ٣١٥.

٣ المصدر نفسه، ص ٣٠٩.

الاختراق متعلق بواجبها في إصلاح الوضع وتعويض الأضرار وتغطية الخسائر بشكل ملائم، الذي يُعد من قواعد القانون الدولي^(١).

لدرجة أن الفقه الدولي في هذا الخصوص يوشك على الإجماع أن اعتبار التعويض هو الشكل المألوف لجبر الضرر الناتج عن الفعل الدولي غير مشروع، وفي هذا الصدد يقول الفقيه (لوتر باخت) النتيجة القانونية الأساسية للمسؤولية الدولية، هي التعويض المادي والمعنوي عن الضرر الناجم^(٢). أما الفقيه (أوبنهايم) فيقول إن التأثيرات الرئيسية للخطأ الدولي فهي التعويض عن الأضرار المادية والمعنوية^(٣).

إن التعويض في القانون الدولي العام عن الفعل غير مشروع يُعد نظرية قائمة بحد ذاته لها قواعدها وضوابطها وكان تاريخ ظهور هذه النظرية مرتبطاً بالمعارك والحروب والصراعات المسلحة وبالمسائل التي تخترق فيها حقوق الإنسان، وقد يكون من ضمن الأمثلة التقليدية، التي تم العمل فيها بالتعويض المالي في المعارك أو النزاعات نذكر: الحرب التي قامت بين نابليون ودول الحلفاء والتي انتهت عام ١٨١٥ والحرب الأمريكية، التي نشبت بين القوات في الجنوب وبين القوات في الشمال والتي تدعى بقضية الألباما لعام ١٨٧٢ فقد قام التحكيم الدولي بفرض مبلغ مالي على بريطانيا بمثابة تعويض عن اختراقها لمبادئ الحياد وتدخلها في أطراف الصراع^(٤).

وأيضاً الحرب بين كل من الكيان الصهيوني وفلسطين بسبب إشادة جدار الأرض الفلسطينية المحتلة، فقد أقرت محكمة العدل الدولية عند النظر في اختراقات القانون الدولي الإنساني لهذه الحرب في ٢٠٢٤/٧/٩ عن تعهد الكيان الصهيوني بتقديم تعويض لكافة الأشخاص الذين لحق بهم الضرر.

ولقد أهتم القانون الدولي العام بالتعويض كأثر جوهري للمسؤولية الدولية فمثلاً قد أخذت به لجنة القانون الدولي في المادة (٣٦) من مشروعها النهائي، الذي نصت فيه على ما يلي: على الدولة المسؤولة عن العمل غير مشروع دولياً التزاماً بالتعويض عن الضرر الناتج عن هذا الفعل في حال عد

١ باية فتحية، التعويض في القانون الدولي العام ، المصدر السابق ، ص ٣.

٢ غسان الجندي، المسؤولية الدولية مطبعة التوفيق ماني الطبعة التوفيق، الأردن، ١٩٩٠، ص ٦٣.

٣ جمال عبد الفتاح عثمان، مصدر سابق، ص ٣١١.

٤ باية فتحية، المصدر السابق، ص ٤.

إصلاح هذا الضرر بالرد، يشمل التعويض أي ضرر يكون قابلاً للتقييم من الناحية المالية بما في ذلك ما فات من الكسب بقدر ما يكون هذا الكسب مؤكداً.^(١)

و أخذ مجلس الأمن بالتعويض في العديد من قراراته ومنها على سبيل المثال القرار رقم (٣٨٧) لعام (١٩٧٦)، الذي فرض على جنوب إفريقيا بعد اعتدائها على أنغولا بالتعويض الكامل عن الأضرار، التي لحقت بها وطالبها بإعادة كل المعدات التي صادرتها القوات البريتوريا.^(٢) ويقصد بالتعويض إلزام يُلقى على عاتق دولة ما في أعقاب حرب بتقديم تعويضات كافية عن الأضرار التي أصابت دولة أخرى أو رعاياها بسبب الحرب.

وألزمت المبادئ العامة للاتفاقيات لاهاي الأربعة لعام (١٩٠٧) احترام قوانين وأعراف الحرب البرية، وأوجبت على المحارب الذي يخل بأحكامها دفع تعويض إذا اقتضت الحاجة، ويكون مسؤولاً عن جميع الأعمال التي يرتكبها أشخاص ينتمون إلى قواته المسلحة وأشارت فتوى محكمة العدل الدولية الانتهاكات القانون الإنساني وحقوق الإنسان في الأراضي الفلسطينية المحتلة عن إلزام إلكيان الصهيوني بتقديم تعويضات لجميع الأشخاص الطبيعية الأفراد والمعنوية جراء ما لحق بهم من أضرار، وذلك بالنظر إلى أن تشييد الجدار والنظام المرتبط به، قد ترتب عليه الاستيلاء على المنازل ومشاريع تجارية، وأراضي زراعية وتدميرها، وألزمت المحكمة إلكيان الصهيوني بجبر الضرر، الذي لحق بجميع الأشخاص الطبيعيين والاعتباريين المعنيين.

إن أغلب القواعد العرفية واحكام الاتفاقيات الدولية ذات الصلة قامت وبشكل واضح بتحديد المسؤولية، التي تقع على الدولة على حد سواء إن تم ارتكاب التصرف من قبل مؤسسات الدولة شبه الرسمية أو الرسمية بشرط أن يكون لها القدرة على أن تضبط تصرفاتها، وفي حال الهجمات السيبرانية إذا كانت الهجمات منصبة على تعطيل وسائل الاتصال المدنية أو العسكرية خلال النزاع المسلح فيخضع الأمر عندئذ إلى أحكام القانون الدولي الإنساني، وبشكل خاص الأحكام، التي تضبط طرائق العمليات العسكرية وتصرفات المقاتلين.^(٣)

١ لجنة القانون الدولي، الدورة الثالثة والخمسين حول المسؤولية الدولية ٢٠٠١، تاريخ الزيارة ١٢/٨/٢٠٢٤، الساعة

١٧:٠٥ متاح على الرابط: <https://legal.un.org/ilc/sessions/53/>

٢ غسان الجندي، المسؤولية الدولية. ط١، مطبعة التوفيق، الاردن، ١٩٩٠، ص٦٣.

٣ احمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص

تعد فكرة تعويض ضحايا انتهاكات القانون الدولي الإنساني وانتهاكات حقوق الإنسان من الأفكار الحديثة بشكل نسبي في القانون الدولي، ويُعد التعويض جزءاً من حق الوصول إلى طرق الإنصاف القضائي الذي تم الاعتراف به من القانون الدولي لضحايا الانتهاكات الخطيرة لحقوق الإنسان والقانون الإنساني الدولي. وبشكل قانوني، فإن ذلك الحق في الوصول إلى طرق التعويض والإنصاف القضائي يركز بشكل أساسي على التشريعات الوطنية. إلا أنه يوجد القليل من الهيئات الدولية القضائية بإمكانها كذلك إصدار قرارات بخصوص تعويض الضحايا الأشخاص. وحق تعويض الضحايا مختلف عن نظام المسؤولية الدولية بين البلدان، الذي يقوم بإجبارها على أن تدفع التعويضات عن الأضرار التي تلحق ببلد آخر نتيجة انتهاك التزاماتها الدولية. ومحكمة العدل الدولية هي من تنظر في المسائل المختصة بتسوية أمور التعويضات والمسؤولية بين البلدان. وبإمكان الدول كذلك تطبيق آليات للتعويض عندما يكون الأمر متعلق بالمسؤولية عن الأضرار، التي لحقت بأشخاص أجانب أو هيئات، وذلك يحصل بشكل كبير في العمليات العسكرية الدولية، والقرارات تتخذ في الغالب على أساس التسويات الودية التي تباشرها القوات المسلحة.^(١)

ركزت الجهود القانونية والتعاقدية في السنوات الأخيرة على تحديد آليات تعويض فعالة للمتضررين من الهجمات السيبرانية التي تستهدف مناطق محمية، ويُعزى ذلك إلى امتزاج الطابع المدني والبشري لهذه المنشآت مع طبيعة الاعتداء السيبراني الذي قد يُعد جريمة دولية أو مدنية في آنٍ واحد.

في القطاع التأميني، برزت قضية شركة Merck إثر هجوم NotPetya عام ٢٠١٧، وهي البرمجية التي استُخدمت ضد البنية الأوكرانية ولكنها انتشرت عالمياً مسببة أضرار تُقدَّر بمليارات الدولارات. حاولت Merck تحصيل تعويض من شركات التأمين، ولكنها وُجِّهت باستثناءات "العمل العدائي"^(٢). في مايو ٢٠٢٣، قضت محكمة نيو جيرسي بأن الحكم بأن NotPetya "عمل عدائي" هو

١ صندوق الأمم المتحدة الطوعي للأشكال المعاصرة للتعذيب/ صندوق الأمم المتحدة الطوعي لضحايا التعذيب، مكتب مفوضية الأمم المتحدة لحقوق الإنسان، <https://ar.guide-humanitarian-law.org/content/article/5/jbr-ldrr-t-wyd/>، تاريخ الزيارة ١١/٨/٢٠٢٤ الساعة ١١:٣٧.

2 Article, Reliance on war exclusion clause after cyberattack fails; insurers must pay out over a billion dollars in damages, Stibbe, 26 May 2023, <https://www.stibbe.com/publications-and-insights/reliance-on-war-exclusion-clause-after-cyberattack-fails-insurers-must>

تفسير غير مبرر لأحكام السياسة التأمينية، وصدرت تسوية تلزم شركات التأمين بتحمل الخسارة^(١). ويُعد هذا حكمًا فعليًا ومعتبرًا في مجال تعويض الأضرار من هجمات رقمية مرتبطة بالبنية التحتية. أما في المجال الصحي، فقد شمل الهجوم الطائفي على المركز الطبي بجامعة فيرمونت عام ٢٠٢٠، إذ اختراق برمجي أدى إلى إغلاق خدمات حرجية في مستشفى كان يعد منطقة محمية قانونيًا بسبب كونه منشأة طبية. رفعت الإدارة الحكومية دعوى أمام القضاء الفيدرالي الأميركي، واقتُلِفَ فعلته بالمخالفة لشروط مكافحة التواطؤ وغسيل الأموال، ما أدى إلى إقرار تعويض يُقدَّر بما بين ٣٠ و ٥٠ مليون دولار^(٢).

ebenfalls تعرضت شبكة الصحة الوطنية في المملكة المتحدة NHS لهجوم برمجي من نوع WannaCry عام ٢٠١٧، مما عرقل آلاف العمليات السريرية وكبد الخزنة العامة خسائر تُقدَّر بنحو ٩٢ مليون جنيه^(٣). وقد استخدم التأمين الحكومي آليات التعويض الداخلي لتغطية نفقات التعافي، رغم الشكوك حول الاستعداد والتأمين المناسب.

في حوادث إضافية، استهدفت كل من الهيئة الصحية الأيرلندية (HSE) عام ٢٠٢١، ومجلس خدمات الصحة في نيوزيلندا (Waikato DHB) بنفس السنة، ما أدى إلى انقطاع مئات المرافق وخسائر مالية تجاوزت ٥٠ مليون يورو متعلقة بتعويض المرضى عن تأجيل العلاج وتأثيرات نفسية^(٤). كما وقَّعت Lehigh Valley Health Network تسوية مدنية بمبلغ ٦٥ مليون دولار لتغطية الأضرار التي لحقت بأكثر من ١٣٠ ألف مريض^(٥).

1 Alysia Horn, "Merck Settles \$700M Insurer Battle Over NotPetya," Lawfare, Jan. 2024, مقال تاريخ الزيارة ٢٠٢٥/٦/٦ <https://www.lawfaremedia.org/article/building-a-cyber-insurance-backstop-is-harder-than-it-sounds> متاح على الرابط

2 AP News, "Ukrainian man pleads guilty in cyberattack that temporarily disrupted major Vermont hospital," Feb. 2024, مقال متاح على الرابط

<https://www.apnews.com/article/6ce4feb4c9af0799ab751bfcee73c744> تاريخ الزيارة ٢٠٢٥/٦/٦

3 Wikipedia, "WannaCry ransomware attack," last updated July 2025, مقال متاح على الرابط https://en.wikipedia.org/wiki/WannaCry_ransomware_attack تاريخ الزيارة ٢٠٢٥/٦/٦

4 Wikipedia, "Health Service Executive ransomware attack," May 2023, مقال متاح على الرابط https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack تاريخ الزيارة

٢٠٢٥/٦/٦

5 SecurityWeek, "Healthcare Provider to Pay \$65M Settlement Following Ransomware Attack," 11 Sep 2024, مقال متاح على الرابط <https://www.securityweek.com/pennsylvania-healthcare-provider-to-pay-65m-settlement-following-ransomware-attack> تاريخ الزيارة

٢٠٢٥/٦/٦

يتضح لنا: إن التعويض عن هجمات سيبرانية على مناطق محمية يُطبَّق عبر ثلاثة مسارات متداخلة: التعويض التأميني (مثل Merck) مع تجاوز استثناءات "العمل العدائي". و التحقيقات والشكاوى الجنائية/المدنية على أساس تأثر وظائف محمية (كالضرر النفسي أو فقدان الرعاية الصحية). التسويات الجماعية التي تغطي الضرر المادي والنفسي لآلاف المتضررين (Lehigh Valley, HSE).

وقد أنشأ صندوق الضحايا، الذي ورد ذكره سابقاً في المادة (٧٩-١) من نظام روما الأساسي، بشكل رسمي في أيلول ٢٠٠٢ من خلال القرار رقم (٦) من جمعية الدول الأطراف. وهذا القرار يحدد قواعد وشروط التعويض عن الضرر الذي يلحق بالضحايا وعائلاتهم، وليس التعويضات المباشرة من جانب الأشخاص.^(١)

وهناك مجلس إدارة يقوم بإدارة هذا الصندوق يتألف من خمسة أعضاء يُنتخبون من قبل جمعية الدول الأطراف لمدة ثلاثة أعوام وبالإمكان أن يعاد انتخابهم لمرة وحيدة. ويُمول هذا الصندوق من الغرامات والممتلكات المصادرة من قبل المتهمين بالاستناد إلى قرار المحكمة الجنائية الدولية والمساهمات الطوعية للمنظمات الدولية والأفراد أو الحكومات وصناديق أخرى تم تخصيصها من قبل الجمعية العامة للدول الأطراف.

ونص التنظيم (٥١) لصندوق الضحايا على أنه بإمكان الصندوق تنفيذ مشروعات، وأنشطة يكون الهدف منها الدعم المادي أو إعادة التأهيل النفسي، أو غير ذلك من الأنشطة بعد أن يبلغ نيته إلى المحكمة.^(٢)

ويجب على أي نشاط أو مشروع يقوم الصندوق بإدارته لا يبت بشكل مسبق في أمر ما ستقوم المحكمة بالبت فيه، ولا يخالف افتراض براءة المتهم، ولا يتحامل على محاكمة محايدة وعادلة.^(٣)

١ ينظر: المادة (٧٩-١) النظام الأساسي للمحكمة الجنائية الدولية.

٢ صندوق الأمم المتحدة الطوعي للأشكال المعاصرة للتعذيب/ صندوق الأمم المتحدة الطوعي لضحايا التعذيب ، مكتب مفوضية الأمم المتحدة لحقوق الإنسان ، <https://www.unhcr.org/refugees/article/content/org.law-humanitarian-guide.ar://https-jbr/5/> ، تاريخ الزيارة ٢٠٢٤/٨/١١ الساعة ١٨ : ١٢ ، ويُنظر أيضاً : المادة (٧٥-١) النظام الأساسي للمحكمة الجنائية الدولية.

٣ صندوق الأمم المتحدة الطوعي للأشكال المعاصرة للتعذيب/ صندوق الأمم المتحدة الطوعي لضحايا التعذيب ، مكتب مفوضية الأمم المتحدة لحقوق الإنسان ، <https://www.unhcr.org/refugees/article/content/org.law-humanitarian-guide.ar://https-jbr/5/> ، تاريخ الزيارة ٢٠٢٤/٨/١١ الساعة ٤٢ : ١٢

ولمعرفة الأساس الدولي في التعويض، سنبحث المبادئ الدولية لجبر الضرر (التعويض) والتعويض من جانب المحاكم الإقليمية لحقوق الإنسان، وكما يأتي:

١. المبادئ الدولية لجبر الضرر

في عام ٢٠٠٥، اعتمدت المبادئ والتوجيهات الأساسية من قبل لجنة الأمم المتحدة لحقوق الإنسان، فيما يخص الحق في الجبر والانتصاف لضحايا الانتهاكات الجسيمة للقانون الدولي لحقوق الإنسان، فضلاً عن الانتهاكات الخطيرة للقانون الإنساني الدولي، واعتمدتها الجمعية العامة للأمم المتحدة عام ٢٠٠٦، إذ شددت المبادئ وأكدت على البلدان، لتعزيز سبل الانتصاف، التي تناسب ضحايا الانتهاكات^(١). إن مبادئ الأمم المتحدة تؤكد أنه من الضروري تضمين القوانين الوطنية العديد من الاحكام العقابية عن انتهاكات القانون الدولي الإنساني وقانون حقوق الإنسان وإمكانية أن يصل الضحايا إلى المعلومات، فضلاً عن حماية الضحايا من الأفعال ذات الطبيعة الانتقامية، وتلك المبادئ تؤكد على أنه بحسب القانون الدولي والقوانين المحلية، ومن خلال مراعاة الظروف الفردية، من الواجب حصول الضحايا و الذين تعرضوا لانتهاكات كبيرة وجسيمة للقانون الدولي الإنساني ولحقوق الإنسان وللقانون الدولي، بحسب ما يقتضي الأمر وبطريقة مناسبة لحجم الانتهاك والظروف المرافقة لكل حالة، على تعويضات فعالة وكاملة وفعالة، وذلك بحسب المادة (١٨). وبالإمكان أن يكون التعويض أو جبر الضرر بالعديد من الأشكال: التسوية المالية، رد الحقوق، إعادة تأهيل، تعويض، فضلاً عن ضمانات عدم التكرار المبادئ (١٩-٢٣). ويجب أن يعيد رد الحقوق، عندما يكون ذلك بالإمكان، الضحايا الذين تعرضوا للانتهاكات والضرر إلى وضعهم الأصلي قبل أن تقع الانتهاكات الكبيرة للقانون الدولي الإنساني والانتهاكات الكبيرة للقانون الدولي لحقوق الإنسان. وأنه بالإمكان أن يشتمل رد الحقوق على استعادة الحرية، والتمتع بحقوق الإنسان والهوية والمواطنة وحياة الأسرة وان يرجع الإنسان إلى موطنه أو المكان، الذي كان يقيم فيه، واسترجاع الممتلكات والعودة إلى الوظيفة.

وفي ضوء الممارسة العملية والصكوك الدولية، بالإمكان التأكيد أن مبادئ تعويض ضحايا انتهاكات حقوق الإنسان والقانون الدولي الإنساني ما تزال ترتبط بمسؤولية الدولة، وهذا أيضاً يستتبع التزام الدولة بالتعويض المالي أو جبر الضرر إلى دولة الأخرى في حال كان هناك سلوك دولي غير مشروع تجاهها. والقانون الدولي يعترف بتلك المبادئ إلا أنه لا يقوم بإنشاء أي حق فردي من أجل

١ الأمم المتحدة. المبادئ والمبادئ التوجيهية الأساسية بشأن الحق في علاج وتعويض ضحايا انتهاكات حقوق الإنسان والقانون الإنساني الدولي. الوثيقة E / CN.4 / RES / ٢٠٠٥ / ٣٥، ٢٠ أبريل ٢٠٠٥.

التعويض. وبإمكان المحاكم المحلية فقط أن تنفذ هذا الإجراء من أجل منح تعويضات لها علاقة وصلة مباشرة بسلطاتها الوطنية. ومن الأمثلة على ذلك الحكم الذي قامت بإصداره محكمة العدل الدولية سنة ٢٠١٢ بخصوص ما يتعلق بالنزاع بين إيطاليا وألمانيا عن تعويض المانيا لضحايا النازية. إذ إن المحكمة أكدت أنها لن تقوم بإصدار حكم عن تواجد حقوق فردية في التعويض بالقانون الدولي، وهو قابل للإنفاذ بشكل مباشر ويُمنح إلى ضحايا انتهاكات القانون الدولي الإنساني^(١).

٢. التعويض من جانب المحاكم الإقليمية لحقوق الإنسان

أما على المستوى الإقليمي، فاتفاقيات حقوق الإنسان نصت بطريقة واضحة وصريحة على مبدأ الحق في التعويض للضحايا، ولاسيما ما يرتبط بالتزام البلدان والحكومات بضمان الحق في الحصول على سبل الانتصاف الفعال لضحايا انتهاكات حقوق الإنسان. وبإمكان محاكم حقوق الإنسان الأفريقية والأمريكية والأوروبية أن تقوم بإجبار الحكومات على أن تعوض ضحايا انتهاكات حقوق الإنسان. وعلى وفق المادة (٣-٢) من البروتوكول التكميلي ٢٠٠٥ لمحكمة العدل بالمجموعة الاقتصادية لدول غرب أفريقيا والمادة (١٣) من الاتفاقية الأوروبية لحقوق الإنسان والضمانات الرئيسية، والمادتان (٢٨-ز) و(٤٥) من بروتوكول ٢٠٠٨ المعني بالنظام الأساسي للمحكمة الأفريقية للعدالة وحقوق الإنسان، المادتان (٢٥) و(٦٣) من اتفاقية الدول الأمريكية لحقوق الإنسان والضمانات الأساسية^(٢). و (أنه من الواجب على الدولة أن تقدم تعويض مالي عن الأضرار التي قامت بالتسبب فيها للضحايا. والأحكام الصادرة عن تلك المحاكم تلتزم بها الدول)^(٣).

ثانياً: أشكال التعويض عن المسؤولية الدولية عن الهجمات السيبرانية على المناطق المحمية

تترتب على المسؤولية الدولية عدة آثار قانونية يأتي في مقدمتها التزام الدولة المسؤولة بجبر الضرر الذي نشأ عن التصرف غير المشروع، وأكد هذا المبدأ القضاء الدولي في العديد من أحكامه،

١ منظمة أطباء بلا حدود، القاموس العلمي للقانون الإنساني، تاريخ الزيارة ١٣/١١/٢٠٢٤، الساعة ١٥:١٦. على الرابط:

<https://ar.guide-humanitarian-law.org/content/article/5/jbr-ldrr-t-wyd/>

٢ ندوة عن الضحايا في القانون الجنائي الدولي. مجلة العدالة الجنائية الدولية ٨، لا. ١ (٢٠١٠): ٧٥-١٧٩

٣ <https://ar.guide-humanitarian-law.org/content/article/5/jbr-ldrr-t-wyd/> تاريخ الزيارة

١٠/١١/٢٠٢٤ الساعة ٠٩:١٠.

ويتخذ التعويض عدة أشكال، فينقسم من حيث المصلحة المعتدي عليها على ضرر مادي وضرر معنوي، فالأول هو كل مساس بحق من حقوق الشخص القانوني الدولي المادية أو بحقوق رعاياه، فيرتب ضرر مادي ملموس وظاهر للعيان، ومنها الأضرار بالمناطق المحمية أو الحاق أضرار بسفارة، أو قتل رعايا الدولة، أو إحداث إصابات جسيمة، في حين أن الضرر المعنوي هو مساس باعتبار أو شرف الشخص القانوني الدولي، أو بأحد رعاياه، فتكون الآثار مؤلمة وغير ملموسة، كإهانة علم دولة، أو بث الذعر في أوساط المدنيين أو التهديد أو الإعلان باستهداف المناطق المحمية^(١).

وسنحاول أن نستعرض أهم أشكال التعويض الناتج عن الضرر المعنوي والضرر المادي وطرق تقدير التعويض فيما يلي:

أولاً: التعويض العيني

يقصد به إعادة الشيء إلى أصله أو إعادة الأوضاع إلى ما كانت عليه قبل حدوث الضرر الذي ترتب عليه المسؤولية الدولية^(٢). يعد التعويض العيني الصورة الأصلية في التعويض الدولي بحيث يمكن اللجوء التعويض النقدي إلا إذا استحال الأمر، والغاية من هذا إزالة الضرر الذي رتبة الفعل غير المشروع وإرضاء الدولة التي أصابها الضرر^(٣). ولهذا عرف بعض الفقهاء التعويض العيني بأنه: إرجاع الحالة إلى ما كانت عليه قبل ارتكاب الفعل غير المشروع وذلك عند الإمكان^(٤).

ويولجئ إلى هذه الوسيلة بعد وقف العمل الضار وتقديم ضمانات كافية على عدم تكراره أن كان مستمراً، إذ إن ها التصرف يتفق ومنطق الأشياء، و أنه يؤدي إلى إعادة الأمور إلى نصابها، وذلك بإعادة الحقوق إلى أصحابها، كذلك يؤدي إلى إعادة التوازن، الذي أخل به العمل الضار^(٥).

ولكي يكون إعادة الحال إلى ما كان عليه ممكناً (جبر الضرر) لابد من توافر الشروط الآتية:

أ- أن لا يكون الرد العيني مستحيلاً من الناحية المادية.

ب- أن لا يؤدي القيام به إلى الإخلال بقاعدة أمرة من قواعد القانون الدولي.

١ مريم ناصري، فعالية العقاب على الانتهاكات الجسيمة لقواعد القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الحاج الخضر، الجزائر، ٢٠٠٩، ص ٧٧.

٢ جمال عبد الفتاح عثمان، مصدر سابق، ص ٢٦.

٣ المصدر نفسه، ص ٣١٤.

٤ عمير نعيمة، النظرية العامة لمسؤولية الدولة الدولية. محاضرات حقوق، كلية الحقوق، جامعة الجزائر، ٢٠١١، ص ٨٧.

٥ هديل صالح الجنابي، مسؤولية المنظمة الدولية. ط ١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٢، ص ٢٣٨-٢٣٩.

ج - أن لا يعرض الاستقلال السياسي أو الاستقرار الاقتصادي للدولة الملزمة بالرد العيني إلى التهديد الخطير

ومن دون أن تتعرض الدولة المضرومة لأخطاء مماثلة إن لم تحصل على الرد العيني.^(١) وإعادة الحال إلى ما كانت عليه فيما يخص الأضرار بالمناطق المحمية لا ينصرف إلى إنهاء الأضرار بهذه المناطق فحسب، بل يتعين على الذي قام بالأضرار أن يعيد تلك المناطق إلى حالتها الطبيعية، كأن يسمح بإعادة الممتلكات بعد أن قام بسرقتها، أن يقوم بإعادة ترميم هذه المناطق التي تضررت من جراء القصف العشوائي أو المعتمد. لذا يعد الرد العيني أفضل صور التعويض قبولاً طالما كان ممكناً، إذ إنه يزيل أثر السلوك أو العمل الضار بالمناطق المحمية

وقد طبق القضاء الدولي التعويض العيني كأثر مترتب على قيام المسؤولية الدولية عن الأضرار بالمناطق المحمية في مناسبات عدة، يمكن أن نذكر منها حكم محكمة العدل الدولية في قضية المعبد تايلاند وكمبوديا عام ١٩٥٢، إذ أقرت المحكمة على تايلند ليس بوقف احتلال المعبد وسحب العناصر المسلحة من محيطه، وإنما أيضاً رد جميع المقتنيات التاريخية والفنية التي سرقت من المعبد خلال مدة احتلال القوات التايلندية له منذ عام ١٩٥٤^(٢). ولقد أخذت العديد من المعاهدات الدولية بمبدأ التعويض العيني ومنها معاهدة فرساي لعام (١٩١٩)، التي أعطت لفرنسا حق استغلال مناجم الفحم في إقليم المنار لمدة (١٥) عاماً تعويضاً عن مناجم فحمها التي دمرت خلال الحرب العالمية الأولى^(٣). وأيضاً المادة (٣٥) من تقنين المسؤولية الدولية من خلال مشروع لجنة القانون الدولي التابعة للأمم المتحدة حول المسؤولية الدولية نصت على ما يأتي: على الدولة المسؤولة عن فعل غير مشروع دولياً التزم بالرد، أي: إعادة إلى ما كان إليه سبل ارتكاب الفعل غير المشروع دولياً، بشرط أن يكون هذا الرد وبقدر ما يكون: غير مستحيل مادياً، وغير مستتبّع لعبء يتناسب إطلاقاً مع المنفعة المتأتية من الرد بعد من التعويض.^(٤)

١ عادل أحمد الطائي، المسؤولية الدولية عن الأفعال المحظورة دولياً. مجلة بيت الحكمة، العدد (٣)، العراق، ٢٠٠٠، ص ٣٢.

٢ محمد صنيّتان الزعبي، المسؤولية الدولية عن الأضرار التي تسببها النفايات النووية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٠، ص ٨٩.

٣ غسان الجندي، مصدر سابق، ص ٦٣.

٤ لجنة القانون الدولي، الدورة الثالثة والخمسين حول المسؤولية الدولية ٢٠٠١، تاريخ الزيارة ١٢/٨/٢٠٢٤،

الساعة ١٧:٠٥ متاح على الرابط: <https://legal.un.org/ilc/sessions/53/>

ومن نص المادة في أعلاه يلاحظ أن التعويض العيني يجب أن يكون السبيل الرئيسي في تحقيق الإصلاح من طرف الشخص الدولي المتسبب في الضرر للغير، وفي حالة الاستحالة يمكن اللجوء إلى التعويض النقدي.

وفي هذا الصدد يضرب الفقه الدولي أمثلة عديدة بقضايا دولية طبق فيها التعويض العيني ومنها قرار محكمة العدل الدولية الذي جاء فيه: إن إعادة الحال إلى ما كانت عليه الصورة الأساسية لإصلاح الضرر، وإنما التعويض النقدي يحل محلها إذا لم تكن الإعادة العينية ممكنة.

ومنها قرار محكمة العدل الدولية في قضية مصنع (شروزو) ١٩٢٧ الذي أكد على أن المبدأ الأساسي، الذي يستخلص من العمل ولاسيما في قضايا التحكيم أن التعويض يجب أن يزيل بقدر الإمكان نتائج العمل المرتكب، من ذلك يتضح تفضيل العمل الدولي للرد العيني بوصفه الأكثر ولاً وتحقيقاً للاستقرار والعدالة.^(١)

ثانياً: التعويض المادي عن اضرار الهجمات السيبرانية على المناطق المحمية إعادة الحال إلى ما كانت عليه قد تكون مادية كإرجاع الضرائب التي تكون قد حصلت بغير وجه وكذلك الاجلاء من الإقليم، الذي احتل بطريقة غير مشروعة وتسليمه إلى الدولة صاحبة الحق في السيادة عليه وإعادة الدولة المسؤولة أموال الأجانب وممتلكاتهم، التي استولت عليها أو صادرتها بوجه غير مشروع والإفراج عن الأجانب الذين قبضت عليهم بغير حق، أما الإعادة القانونية فتتمثل في إلغاء الأحكام والقرارات، التي أصدرتها الدولة المسؤولة مخالفة بذلك قواعد القانون الدولي أو إعلانها إلغاء نص في اتفاقية يتعارض تنفيذه مع معاهدة دولية أبرمتها مع الدولة المدعية.^(٢)

وفي هذا الصدد يقول بعض الفقهاء: إن التعويض العيني يعد الإصلاح الأمثل في نظر القانون والقضاء الدوليين وذلك في حدود إمكانيات المادية وبشرط أن لا يؤدي إلى أضرار بالدولة المسؤولة وإلحاقها بأعباء تفوق الأضرار الحاصلة، مما يجعل من التعويض العيني ليس قاعدة الأساسية في المسؤولية الدولية من أجل إصلاح ما حصل، ولكنها تصبح قاعدة جزيئة تفوق أو تتجاوز طبيعتها الإصلاحية أو التعويضية، و أن التعويض المادي تحديداً فيعرف: بأنه التعويض، الذي يكون في شكل مباشر بإصلاح الضرر الناتج عن الفعل غير المشروع، وذلك عن طريق تقديم المقابل عن الخسائر، التي لحقت بالدولة المضرورة.

١ محمد صنيثان الزعبي، مصدر سابق، ص ٨٥.

٢ جمال عبد الفتاح عثمان، مصدر سابق، ص ٣١٧.

ويعد التعويض النقدي من أسهل الطرق لإصلاح الضرر في مجال المسؤولية الدولية ويقصد به دفع مبلغ من المال يتناسب مع ما لحق المضرور من خسارة، وما يكون قد فاتته من كسب^(١). ومن ثم يقصد بالتعويض النقدي دفع مبلغ من المال من قبل الشخص محل المسؤولية إلى الطرف الآخر المتضرر، لإصلاح الضرر، ويعد التعويض المالي من أكثر أشكال التعويض شيوعاً في دعاوى المسؤولية عموماً، وغالباً ما يتم اللجوء إلى هذه الصورة لمعالجة آثار المسؤولية الدولية، إذا لم يصلح الرد العيني للضرر تماماً، وبالقدر اللازم، كل ذلك لإعادة التوازن بين حقوق والتزامات كل من أطراف دعوى المسؤولية.^(٢)

والجدير بالذكر بأن التعويض النقدي في حالة المناطق المحمية، لأنها تتسجم كثيراً مع طبيعة تلك المناطق والهدف من إنشائها، ذلك إنها أنشأت لإسباغ الحماية لأشخاص بحاجة إلى حماية خاصة وكذلك أعيان على قدر من الأهمية يستلزم المحافظة عليها، وليس التعويض المالي عنها.

وبشأن تقدير التعويض فإنه يتم بشكل رضائي بين الشخص المتضرر وبين مسبب الضرر، إذ يعد التعويض الرضائي أنسب الأشكال لتقديره، ففي قضية التعويضات، التي سببتها الكونترا في نيكاراغوا، وجدت محكمة العدل الدولية عبر قرارها الصادر عام ١٩٨٦،^(٣) أن الولايات المتحدة الأمريكية قد أخلت ببعض التزاماتها بموجب القانون الدولي العرفي، ومنها الاستعمال غير المشروع للقوة، فطلبت نيكاراغوا من المحكمة أن تقضي لها بالتعويض، فردت المحكمة بأن عليها الامتناع عن أي عمل غير ضروري من شأنه أن يضع العراقيل أمام تسوية النزاع تفاوضياً، إذا أن للمحكمة أن تحدد شكل ومقدار التعويض في حالة فشل الأطراف في الاتفاق على ذلك، ولذلك فإن المحكمة ترجئ النظر في اتخاذ هذا الإجراء اللاحق.^(٤)

غير أنه لا يمكن الحديث عن التعويض النقدي إذا كان تقييم الضرر بالمال ممكناً، وفي غير ذلك من الحالات، فإن المبلغ المدفوع يكون له صفة الترضية.^(٥)

١ مصطفى سيد عبد الرحمن، القانون الدولي العام. دار النهضة العربية، مصر، ٢٠٠٣، ص ٥١١.

٢ عادل أحمد الطائي، مصدر سابق، ص ٣٣.

٣ أرشيف محكمة العدل الدولية، ملخص قضية نيكاراغوا ضد الولايات المتحدة الأمريكية، تاريخ الزيارة ٢٠٢٤/٨/١٢، متاح على الرابط: <https://www.icj-cij.org/case/70>

٤ علي زعلان نعمة وآخرون، القانون الدولي الإنساني. مكتبة السيسبان، العراق، ٢٠١٥، ص ٣٢٥.

٥ جمال عبد الفتاح عثمان، مصدر سابق، ص ٣٢٢.

وتجدر الإشارة في هذا الصدد إلى أن التعويض النقدي غايته تعويض المضرور عن جميع نتائج الفعل غير المشروع بما في ذلك ما لحق من خسارة، وما فاتته من كسب متوقع ومصاريف، و أنها تُعد الصورة الوحيدة لتعويض الأضرار المعنوية، التي تصيب رعايا الدولة المدعية، أما التعويض العيني فغايته إعادة الحال إلى ما كان عليه سابق قبل وقوع الضرر. ^(١)

وخلاصة القول، قد يتم التعويض مالياً عن الضرر الناتج عن الفعل غير المشروع، وأشارت إلى التعويض المالي محكمة التحكيم الدائمة بأنه: ليس بين مختلف مسؤوليات الدول فروق أساسية، ويمكن تسويتها جميعاً بدفع مبلغ من المال، وقد يُتفق على التعويض نتيجة لمفاوضات تتم بين الأطراف المعنية ويعقبها اتفاق على مقدار ونوع التعويض.

ثالثاً: التعويض المعنوي عن اضرار الهجمات السيبرانية على المناطق المحمية :

يتم اللجوء إلى التعويض المعنوي عندما يكون الضرر غير قابل للتقويم بالنقود أي الأضرار المعنوية أو الأدبية، والتي أكثر وقعاً من الأضرار المادية بالنسبة للدول. ^(٢)

لذا يمكن التعبير عنه: إنه وسيلة إنصاف بموجبها يُصالح الضرر، الذي يصيب الشخص القانوني الدولي بحقوقه غير المالية، وتعد هذه الصورة من صور إصلاح الضرر الأنسب للتعويض عن الأضرار المعنوية، التي تصيب الدولة أو أية شخصية دولية بسمعتها أو بكرامتها أو بشرفها، لما تتضمنه من تناسب بين نوع وحجم الضرر وبين نوع وكيفية التعويض عنه، ويمكن أن يكون ذلك بوسائل مختلفة كالاعتذار، الذي تقدمه الدولة المسؤولة بالطرق الدبلوماسية، أو معاقبتها جنائياً أو تأديبياً للأفراد المسؤولين عن الانتهاكات، ولاسيما تلك الموجهة إلى المناطق المحمية، أو إقرارها بعدم مشروعية سلوكها تجاه الدولة المتضررة، وإذا كان لا جلود ما يمنع من مقابلة الضرر المعنوي بتعويض مادي فإن إصلاح الأضرار المعنوية بتعويضات مالية مناسبة يخرج هذا التعويض عن طبيعته المعنوية (الترضية)، إذ نكون أمام تعويض مادي عن ضرر معنوي، ولكن قد يكون التعويض المادي رمزياً عندما لا يتناسب مع حجم الضرر الحاصل، إذ يعد التعويض في هذه الحالة من قبيل

١ سمير محمد فاضل، المسؤولية الدولية عن الأضرار الناتجة عن استخدام الطاقة النووية وقت السلم، عالم الكتب، القاهرة، بدون سنة نشر، ص ١١٤.

٢ صوفيا شراد، تطبيق قواعد المسؤولية الدولية في أحكام المحكمة الدولية لقانون البحار-دراسة تطبيقية لمبدأ التعويض عن الضرر. أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خضير، الجزائر، ٢٠١٣، ص ٥٦.

التعويض الرمزي عن الضرر المادي يحمل معه أيضاً معنى التنازل عن الحق في المطالبة بالتعويض.^(١)

ومن أمثلة هذا النوع من التعويض ما أعلنته محكمة العدل الدولية: إدانة فرنسا وتقرير مسؤوليتها ونشر هذه الإدانة علناً أمام الرأي العام يشكل ترضية مناسبة عن الأضرار القانونية والمعنوية، التي أصابت نيوزيلندا.^(٢)

وعليه فالترضية عن الاعتداء على المناطق المحمية بأنواعها المختلفة قد تتخذ شكل الاعتراف بعدم مشروعية الاعتداء أو الهجوم على هذه المناطق، ومن ثم ملاحقة الجناة المتسببين في هذا الاعتداء ومعاقبتهم.

وبناءً عليه نستنتج، إن التعويض يأخذ أشكال مختلفة بحسب نوع الضرر فقد يكون تعويض عيني بإعادة الحقوق لأصحابها، وقد يكون تعويض مادي على شكل تعويضات مادية، وقد يكون تعويض معنوي كأن تصدر الدولة اعتذاراً وأسفاً على ما يصدر من أخطاء صادرة عن جنودها أو موظفيها في أثناء قيامهم بواجبهم الرسمي، وعادة يتم ذلك بالطرق الدبلوماسية رابعاً: طرق تقدير التعويض:

تختلف طرق تقدير التعويض بحسب نوعه و هو موضح في الآتي:

١- تقدير التعويض العيني: لتقدير التعويض العيني في القانون الدولي العام وجب التمييز بين التعويض العيني في التصرفات العادية، وفي التصرفات القانونية، ففي الأولى يمكن تقدير التعويض المادي الذي يؤدي إلى إعادة الشيء إلى حالته مثل إعادة الأموال أو الأملاك المصادرة، أم في الحالة الثانية فهو خاص بتعويض الدولة عن انتهاكها لالتزاماتها القانونية كإصدار قانون أو حكم أو إلغاء عقد أو معاهدة إذ لا يمكن إلزام الدولة على إعادة الحال إلى ما كان عليه أو إلغاء التصرف نهائياً، ولكن يظهر التعويض العيني في هذه الحالة من خلال قيام الدولة بتصرفات من عدم التطبيق أو المساس بالدولة الضحية كرد الشيء إلى وضعه السابق أو إعادة الشيء إلى أصله أو وضعه الطبيعي.^(٣)

٢- تقدير التعويض المالي: الذي يتم من خلال إيجاد حسابات تقريبية ومتماثلة مع حالات مشابهة تشمل كافة الآثار المباشرة للفعل الدولي غير المشروع وحتى الآثار غير المباشرة إذا كانت

١ عادل أحمد الطائي، مصدر سابق، ص ٣٥.

٢ علي إبراهيم، الحقوق والواجبات الدولية في عالم متغير. دار النهضة العربية، القاهرة، ١٩٩٧، ص ٦٦٢.

٣ عمير نعيمة، النظرية العامة لمسؤولية الدولة الدولية، ص ٨٨.

امتداداً لهذا الفعل، وتقويم المبلغ يجب أن يتم على وفق قواعد القانون الدولي، التي تحكم العلاقة بين الدولتين المتنازعتين وليس على وفق قواعد القانون الوطني، وأيضاً يتّحسب قيمة التعويض في تاريخ استحقاقه ودفعه، وليس في تاريخ وقوع الفعل بما يناسب القيم المالية الحالية، وتطور المشروع وارتفاع الأسعار.^(١)

نموذج عن تطبيقات التعويض في القانون والقضاء الدوليين:

لا تتضح أهمية دراسة التعويض في القانون الدولي العام سوى إذا كانت مقترنة بنماذج عملية تبين المجالات، التي يتم فيها تطبيق التعويض في المسائل الدولية، وتدل الكتابات في القانون الدولي العام إلى وجود العديد من الأمثلة على جبر الضرر، والتعويض قام القانون الدولي والقضاء الدولي بتقديمها. التعويض عن انتهاكات حقوق الإنسان:

بسبب إرادة المجتمع الدولي للتقليل من التأثيرات السلبية للاعتداءات على حقوق الإنسان، فإن المواثيق الدولية، التي صدرت عن أجهزة الأمم المتحدة قد نصت على لزوم منح تعويض للمجني عليهم ولأفراد عائلاتهم بشكل كافٍ، وفي هذا السياق فإن لجنة حقوق الإنسان التابعة للأمم المتحدة أصدرت القرار المرقم (١٩٩٨/٤٣)، الذي أكد على الحق في الاسترجاع والتعويض وإعادة الاعتبار لضحايا الاختراقات الجسيمة للحريات الأساسية ولحقوق الإنسان.^(٢)

وكذلك فإن النظام الأساسي للمحكمة الجنائية في مادته (٥٧) قد نص بأنه يحق للمحكمة أن تقوم بتحديد التعويض اللازم دفعه من قبل الجاني إلى الضحايا أو من يرثهم، وأن هذا التعويض لا يسبب ضرراً لحقوق الجاني، أو من يرثه بحسب القانون الداخلي أو الدولي.^(٣)

وورد في المادة (٨٥) من نفس النظام بأنه يتحدد الحق في التعويض لمن ألقي القبض عليه، وقد أكدت المادة (٦/١٤) من العهد الدولي للحقوق السياسية والمدنية لعام ١٩٦٦ أنه في حال أدين شخص بأحد الجرائم الجنائية واتضح بعد ذلك أنه كان بسبب خطأ قضائي، فيحق لهذا الشخص أن يحصل على تعويض على وفق القانون.^(٤)

١ زازة الخضر، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام، ص ٥٢٧.

٢ نجاة احمد أحمد إبراهيم، مصدر سابق، ص ٣٠٥.

٣ نجاة احمد أحمد إبراهيم، مصدر سابق، ص ٣٠٧.

٤ المادة ٦/١٤ من العهد الدولي للحقوق السياسية والمدنية لعام ١٩٦٦.

ومن الملاحظ القضاء الدولي قد أدلى بحكمه في كثير من قضايا انتهاك حقوق الإنسان بمنح تعويض للضحايا ومثال على ذلك ما جرى في إقليم الكونغو الديمقراطية من انتهاك لحقوق الإنسان وقد تم إحالة هذه القضية إلى المحكمة الجنائية الدولية في ابريل ٢٠٠٤ ان المدعي العام للمحكمة الجنائية الدولية قد تحصل على العديد من الأدلة، التي تؤيد سقوط آلاف القتلى في الكونغو منذ ٢٠٠٢ إلى جانب كثير من الجرائم، التي تدخل في إطار تخصص المحكمة، وقام المدعي العام بمباشرة تحقيقه في الجرائم، التي ارتكبت في إقليم جمهورية الكونغو الديمقراطية عام ٢٠٠٤، وقامت الدائرة التمهيدية باتخاذ قرار بإيقاف رئيس الكونغو (توماس لوبانغا ديبلو) بتهمة اقتراف جرائم حرب والقيام بالتجنيد الاجباري لأطفال تقل أعمارهم عن خمسة عشر عاماً في أعمال عدوانية^(١).

ونتيجة المتابعة القضائية الدولية فإن المحكمة الجنائية الدولية قد أصدرت حكماً على رئيس الكونغو الديمقراطية توماس لوبانغا بمنح تعويضات وقدرها عشرة ملايين دولار للأطفال الذين جندهم بشكل إجباري في جرائم الحرب^(٢).

وفي ذات السياق أصدرت محكمة العدل الدولية عام ٢٠٠٥ ، حكمها في القضية المرتبطة بالنشاطات المسلحة في أراضي الكونغو، التي قامت بها أوغندا، بأن ألزمت المحكمة أوغندا بتقديم التعويض عن كافة الأضرار التي أصابت الكونغو^(٣).

ونرى: بعد دراسة بعض المشاكل القانونية الناتجة عن مسألة التعويض في القانون الدولي العام من الممكن تأكيد أن التعويض هو النتيجة القانونية، التي تترتب على إثارة المسؤولية الدولية في حق الشخص الدولي مهما كان مبدأ هذه المسؤولية وقد يكون (جبر الضرر) في القانون الدولي إما عينياً وهو الأساس إذ يجري إعادة الوضع إلى ما كان عليه قبل حدوث الفعل غير مشروع ومن الممكن أن يكون مالياً يتم فيه مراعاة حسابات تقريبية تضم جميع التأثيرات المباشرة وغير مباشرة للفعل الدولي غير مشروع وليس من الممكن اتباع هذه الطريقة قبل الحصول على التعويض العيني، وكذلك ليس من الممكن اللجوء إلى التعويض المالي سوى حين يكون من الممكن تقدير الضرر بالمال، وهو الشكل الوحيد الذي يمكن عن طريقه تعويض الأضرار المعنوية التي تلحق برعايا الدولة المدعية وهدفه ليس

١ هشام محمد فريجة، القضاء الدولي الجنائي وحقوق الإنسان، دار الخلدونية، الجزائر، ٢٠١٢، ص ٢٧٦ و ٢٧٨.

٢ بآية فتيحة، مصدر سابق، ص ١١.

٣ موجز الأحكام والفتاوى الصادرة عن محكمة العدل الدولية ٢٠٠٧ - ٢٠٠٣، منشورات الأمم المتحدة، ٢٠٠٨، ص ١٥١ و ١٥٣.

إعادة الوضع إلى ما كان عليه، ومن الممكن تقدير التعويض العيني في التصرف العادي عن طريق إعادة الوضع إلى ما كان عليه بينما في التصرف القانوني، فيكون عن طريق إلغاء اتفاقية أو القرار أو العقد أو الحكم ويُقدر التعويض المالي عن طريق إيجاد حسابات تقريبية ومماثلة تضمن جبر الأضرار، ويُعوض بمبلغ من المال بحسب قواعد القانون الدولي العام. أما فيما يخص الضرر المعنوي ففي العادة فهو يلحق بالأشخاص مثلما يلحق بالدولة في سيادتها ويُقدر بشكل نقدي. وقد عُميت نظرية التعويض الدولي حالياً لكافة مجالات التعامل الدولي بعد أن كانت في بداية ظهورها تقتصر على انتهاك حقوق الإنسان وانتهاك القانون الدولي الإنساني^(١).

المبحث الثاني

الوسائل الدولية لتعزيز الحماية للمناطق المحمية في الهجمات السيبرانية

لقد فرضت الجرائم الدولية وانتهاكات حقوق الإنسان المرتكبة في أثناء النزاعات المسلحة الدولية منها أو غير دولية، على المجتمع إقرار العديد من القواعد القانونية من أجل توفير لحماية اللازمة لضحايا هذه النزاعات، وهي القواعد الخاصة بالقانون الدولي الإنساني الذي يهدف إلى حماية المتضررين من العمليات العدائية من مدنيين وأعيان مدنية، وحتى يستطيع القانون الدولي الإنساني تحقيق ذلك فقد عمل على إنشاء المناطق المحمية، وإقرارها في اتفاقيات جنيف الأربع عام ١٩٤٩، والبروتوكولين الإضافيين عام ١٩٧٧، وتوفير الحماية لها من خلال إلزام أطراف النزاع المسلح بعدم التعرض والاعتداء عليها وتطبيق مبادئ القانون الدولي الإنساني عليها. وحتى تكون حماية القانون الدولي الإنساني للمناطق المحمية ذات فاعلية كان لابد من ضمان محاكمة كل من ينتهك هذه المناطق، ويعتدي عليها، وتوقيع الجزاء عليه وتحمله المسؤولية الدولية الجنائية، وهذا ما تضمنه القضاء الدولي الجنائي.

ومن أجل توفير الحماية للمناطق المحمية من الهجمات السيبرانية بموجب القانون الدولي الإنساني، وإلزام أطراف النزاعات بعدم التعرض لها بوصفها ليست من الأهداف العسكرية، كان لابد من إيجاد آليات تضمن تطبيق قواعد القانون الدولي الإنساني الخاصة بحماية المناطق المحمية من الهجمات السيبرانية، وهي آليات أوجدتها الاتفاقيات الدولية والقضاء الدولي الجنائي المتمثلة في المحاكم الدولية التي عملت أولاً على تجريم الاعتداءات، التي قد تتعرض لها المناطق المحمية من

١ هشام محمد فريجة، مصدر سابق، ص ١٤.

أطراف النزاع المسلح في أنظمتها الأساسية، وضمان محاكمتها لمنتهم في القواعد المتعلقة بحماية هذه المناطق ومعاقبتهم، وسوف نناقش هذا الموضوع عبر مطلبين، نناقش في المطلب الأول دور الاتفاقيات الدولية في تعزيز الحماية للمناطق المحمية، وسنبحث في المطلب الثاني دور القضاء الجنائي الدولي في تعزيز الحماية للمناطق المحمية.

المطلب الأول

دور الاتفاقيات الدولية في تعزيز الحماية للمناطق المحمية في الهجمات السيبرانية

إن الهدف من وراء إقرار قواعد القانون الدولي الإنساني كان توفير الحماية القانونية إلى المدنيين والاعيان المدنية وغيرها من أي انتهاك وهجوم قد يواجهونه أو يتعرضون له جراء النزاعات المسلحة، لذا يمكن أن تُعدّ أهم اليات توفير الحماية انشاء المناطق المحمية التي يمنع القانون الدولي الإنساني استهدافها اثناء العمليات العسكرية، تتضمن هذه العمليات هجمات عسكرية وحتى مدنية مختلفة برزت في الأونة الأخيرة. وبما أن الهدف من اي قانون هو تحقيق مصالح معينة من خلال تنظيمها والتعرض لها بحسب منهج منطقي يقوم بحماية المصالح التي استهدفها التشريع والقانون العام الدولي يسعى إلى نفس الهدف وهو أن ينظم العلاقة بين أفراد القانون الدولي العام على الرغم من عدم وجود سلطة تشريعية عالمية مثلما هو حال التشريعات الداخلية للدول.^(١)

وتأتي اتفاقيات جنيف وبروتوكولاتها الإضافية في صلب القانون الدولي الإنساني، الذي ينظم السلوك في أثناء النزاعات المسلحة، ويسعى إلى الحد من تأثيراتها، وتوفر الاتفاقيات الحماية للأشخاص الذين لا يشاركون في الأعمال العدائية "المدنيون وعمال الصحة وعمال الإغاثة"، والذين توقفوا عن المشاركة في الأعمال العدائية "الجرحي، والمرضى، وجنود السفن الغارقة، وأسرى الحرب".

وتدعو الاتفاقيات وبروتوكولاتها إلى الإجراءات، التي يتعين اتخاذها منعاً لحدوث كافة الانتهاكات أو وضع حد لها، وتشمل قواعد صارمة للتصدي لما يُعرف بـ الانتهاكات الخطيرة، إذ يتعين البحث عن الأشخاص المسؤولين عن الانتهاكات الخطيرة، وتقديمهم إلى العدالة، أو تسليمهم، بغض النظر عن جنسيتهم، سنبحث هذا المطلب عبر فرعين، الفرع الأول اتفاقيات جنيف الأربعة لعام ١٩٤٩، والفرع الثاني البروتوكولين الإضافيين لعام ١٩٧٧.

١ محمد طي، شرعية التصدي لقرارات مجلس الأمن الدولي: حق الدول وولاية القضاء، المركز الاستشاري للدراسات والتوثيق، بيروت، ٢٠١٣، ص ٥١-٥٢.

الفرع الأول

دور اتفاقيات جنيف الأربع لعام ١٩٤٩ في تعزيز الحماية للمناطق المحمية

عند الناس إلى ممارسة القسوة والعنف بهدف إيجاد حلول الخلافات والنزاعات، وأكدت الثقافات المعاصرة أنه يجب وضع حدود لمحاولات العنف لمنع تطورها وحدوث الحروب والتصرفات الوحشية مثل: وضع قواعد لحماية، الذين لم يشاركوا في الحروب والجرحى والمرضى، وهذه القواعد نص عليها القانون الدولي الإنساني.

وأن اتفاقية جنيف بشأن حماية الأشخاص المدنيين في وقت الحرب، التي أُرخت في ١٢ آب ١٩٤٩ واعتمدت وعُرضت للتصديق والتوقيع والانضمام من قبل المؤتمر الدبلوماسي لوضع اتفاقيات دولية لحماية ضحايا الحروب، الذي انعقد في جنيف خلال مدة زمنية امتدت من ٢١ نيسان/أبريل إلى ١٢ آب/أغسطس ١٩٤٩ ومن تاريخ بدء النفاذ: ٢١ تشرين الأول/أكتوبر ١٩٥٠ على وفق أحكام المادة (٥٣) الفقرة (١) منها.

إن اتفاقيات جنيف الأربع عام ١٩٤٩، تؤكد على وجوب حماية الجرحى والمرضى من القوات المسلحة البرية، ومن تعرض للغرق من القوات المسلحة البحرية، وأسرى الحروب، والناس المدنيين الذين يكونون تحت حكم أجنبي بطريقة قسرية.^(١) إذ إنها تتعلق بحماية الأشخاص المدنيين، وقت الحرب وتعدّ تقدماً ملحوظاً للقانون الدولي الإنساني، وهو الأمر الذي لم تعالجه اتفاقية منفردة، إذ إنصب الاهتمام في التشريع السابق على حماية المقاتلين وحدهم، على أنّ المدنيين خارج الأعمال العدائية^(٢). وإن هذه الاتفاقية تداولت حماية المدنيين في قت قيام النزاعات المسلحة، وهي أول اتفاقية من نوعها إذ كانت لائحة لاهاي لعام ١٩٠٧ أخذت جوانب محدودة من العلاقة بين المحتل وسكان الأراضي المحتلة إلا أنّ اتفاقية جنيف الرابع كانت أول نص شامل أخذت موضوع حماية المدنيين وأن الاتفاقيات الأربع -جنيف لعام ١٩٤٩- هي اتفاقيات دولية تضم عدد من القواعد التي غايتها التقليل من استخدام العنف والوحشية في الحروب وتحجيمه، إذ تمنح الناس الحماية، من الذين لا يشاركون في القتال في أثناء الحروب مثل المدنيين والممرضين وعمال الإغاثة، والذين لم يكونوا

١ جامعة مينيسوتا، مكتبة حقوق الإنسان على الرابط التالي <http://hrlibrary.umn.edu/arab/b093.html>

تاريخ الزيارة ٢٠٢٤/١١/٩ الساعة ٢٠:٥٨.

٢ فاضل عبد الزهرة الغراوي، المهجرون والقانون الدولي الإنساني، ط١، مطبعة الحلبي الحقوقية، بيروت ٢٠١١، ص ٢٤.

قادرين على القتال مثل المقاتلين الجرحى والمرضى وأسرى الحرب والغارقين في البحار وكذلك عدم المساس بالمناطق المحمية على وفق هذه الاتفاقيات^(١). إن فحوى اتفاقيات جنيف الأربع يصب في عمق القانون الدولي الإنساني، إذ هو أحد فروع القانون الدولي الذي ينسق النزاعات المسلحة والتقليل من آثاره، و أنها توفر الحماية للأشخاص غير المشاركين في الأعمال الحربية مثل المدنيين العزل والعاملين في مجال الصحة وعمال الإغاثة، والعاجزين عن القيام بالحروب مثل الجرحى والمرضى والغارقين في البحار وأسرى الحروب، وكذلك ممن شملتهم الاتفاقيات عبر وجودهم في المناطق المحايدة أو المناطق منزوعة السلاح أو المناطق المحمية بموجب القانون الدولي الإنساني، وأن اتفاقيات جنيف تدعو إلى ابداء الآراء والقرارات اللازمة لمنع كافة الاعتداءات أو التقليل منها. وقد حثت على اتباع أنظمة وطرق وقواعد قاسية وقوية ضد كل يرتكب المخالفات الجسيمة إذ تدعو هذه الاتفاقيات إلى ملاحقتهم ومحاكمتهم وتسليمهم للقضاء الدولي مهما كانت جنسياتهم.^(٢)

وتنقسم اتفاقيات جنيف الأربع المكونة للقانون الدولي الإنساني على:

أولاً: اتفاقية جنيف الأولى: تُعد اتفاقية جنيف الأولى لعام ١٩٤٩ الأساس القانوني الأول في منظومة القانون الدولي الإنساني لحماية الجرحى والمرضى والمنشآت الطبية أثناء النزاعات المسلحة، وقد أُرست قواعد واضحة تحظر أي اعتداء أو تعطيل للأعمال الإنسانية الطبية. وعلى الرغم من أن هذه الاتفاقية صيغت في زمن لم تُعرف فيه بعد التهديدات المرتبطة بالفضاء السيبراني، فإن المبادئ التي تتضمنها، ولا سيما تلك المتعلقة بالحماية الوظيفية للمرافق الصحية، تسمح بتكييف أحكامها لتشمل الأفعال العدائية ذات الطابع الرقمي، ما دامت تُلحق ضرراً فعلياً بمنشآت طبية محمية بموجب الاتفاقية.

تنص المادة ١٩ من الاتفاقية على أن الوحدات الطبية، سواء كانت ثابتة أم متحركة، يجب أن تُحترم وتُحمى في جميع الأحوال، ولا يجوز مهاجمتها إلا إذا استُخدمت لأغراض تُضر بالعدو^(٣). هذا النص يمنح حماية قانونية مطلقة للمستشفيات والمنشآت الطبية من أي هجوم، ما لم تتحول إلى أهداف عسكرية. وتُعزز المادة ٢٤ هذه الحماية من خلال تحصين العاملين في المجال الطبي من أي اعتداء

١ اللجنة الدولية للصليب الأحمر تاريخ الزيارة ٢٠٢٤/١١/١١ الساعة

١٠:٢٧ <https://www.icrc.org/ar/publication/0173-geneva-conventions-august-12-1949>

٢ اللجنة الدولية للصليب الأحمر ١٢-١٩٤٩ تاريخ الزيارة ٢٠٢٤/١١/١٠ الساعة ٠٨:٠٧

<https://www.icrc.org/publication/0173-geneva-conventions-august-12-1949>

٣ ينظر: المادة (١٩) من اتفاقية جنيف الأولى لعام ١٩٤٩.

أو تدخل يعيق أداءهم الإنساني. كما تلزم المادة ٣٥ أطراف النزاع بضمان وصول المساعدات الطبية دون عوائق. ومع تطور البنية التقنية للمؤسسات الصحية، والتي باتت تعتمد بشكل كبير على شبكات الاتصال وأنظمة السجلات الرقمية وأجهزة العناية المركزة المتصلة بالإنترنت، فإن القراءة الوظيفية لهذه النصوص توجب اعتبار الهجمات السيبرانية التي تستهدف تلك البنى بمثابة خرق للاتفاقية.

وبالاستناد إلى المادة ٣١ من اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩، التي تقر التفسير الغائي القائم على "النية والغرض"، يُمكن القول إن اتفاقية جنيف الأولى يجب أن تُفسر تفسيراً تطورياً، يُراعي طبيعة التهديدات الحديثة^(١). وبالتالي، فإن أي هجوم رقمي يؤدي إلى تعطيل منشأة طبية أو تقويض قدرتها على تقديم الخدمة، يدخل في حكم الهجوم غير المشروع. وتكمن خطورة هذه الأفعال في استخدامها المتممّ ضمن نزاع مسلح كوسيلة لإضعاف الخصم أو لإجبار السكان المدنيين على الانصياع عبر حرمانهم من العلاج أو المساعدة الطبية.

ويُجسد ذلك الهجوم السيبراني ببرمجية **Ryuk**، الذي استهدف قطاع الرعاية الصحية في الولايات المتحدة الأمريكية في أكتوبر ٢٠٢٠، حيث استهدفت مجموعة من القراصنة ما لا يقل عن ٤٠٠ منشأة طبية بأنظمة فدية إلكترونية، ما أدى إلى توقف عمل غرف الطوارئ، وتأجيل العمليات الجراحية، بل ووُثقت حالات وفاة نتيجة تعطيل الأنظمة الطبية الحيوية. وقد أصدرت وكالة الأمن السيبراني وأمن البنية التحتية (**CISA**) الأمريكية تحذيراً رسمياً، صنفت فيه هذا الهجوم على أنه تهديد مباشر لأرواح المدنيين، مشددة على مخاطره على الأمن الصحي القومي^(٢). وعلى الرغم من أن هذا الهجوم لم يقع في سياق نزاع مسلح، إلا أنه يُشكّل مثالاً واضحاً على الأثر الإنساني المماثل الذي يمكن أن تُخلّفه الهجمات السيبرانية، ما يفتح الباب لتطبيق قواعد القانون الدولي الإنساني حال وقوع مثل هذه الأفعال في إطار نزاع مسلح، كما حدث لاحقاً في أوكرانيا، حيث سُجّلت هجمات سيبرانية على منشآت طبية أثناء النزاع^(٣).

بناءً عليه، فإن أي هجوم إلكتروني على منشآت طبية أو أنظمتها التشغيلية أثناء النزاعات المسلحة يُعد انتهاكاً صريحاً لأحكام اتفاقية جنيف الأولى، سواء بالنظر إلى مبدأ التمييز أو من زاوية الحماية

١ ينظر: المادة (٣١) من اتفاقية فيينا لقانون المعاهدات، ١٩٦٩.

٢ وزارة الأمن الداخلي الأمريكية، متاح على: <https://www.cisa.gov>

٣ معهد السلام السيبراني، "مستشفيات الحرب السيبرانية في أوكرانيا: ناشطون مدنيون ومواقع محمية"، ٢٠٢٣ متاح

على الرابط: <https://cyberconflicts.cyberpeaceinstitute.org/>

الخاصة التي تتمتع بها تلك المنشآت. كما أن هذا النوع من الأفعال، إذا أثبت ارتكابه عمداً، قد يندرج ضمن الجرائم الدولية بموجب نظام روما الأساسي للمحكمة الجنائية الدولية، لا سيما إذا ترتب عليه ضرر جسيم أو وفاة مدنيين^(١)

ثانياً: اتفاقية جنيف الثانية: تشكل اتفاقية جنيف الثانية لعام ١٩٤٩ إحدى الركائز الأساسية للقانون الدولي الإنساني، حيث تُعنى بحماية الجرحى والمرضى وأفراد الطواقم الطبية في النزاعات المسلحة البحرية، إلى جانب السفن الطبية والمستشفيات العائمة ووسائل الإغاثة المرتبطة بها. وعلى الرغم من أن الاتفاقية وُضعت في سياق تقليدي يركز على الأعمال العدائية المادية، إلا أن مبادئها الموضوعية تبقى ذات صلة مباشرة بالتحديات الحديثة، لاسيما الهجمات السيبرانية التي باتت تُستخدم بشكل متزايد في النزاعات المسلحة.

إن المفهوم القانوني للحماية المقررة بموجب اتفاقية جنيف الثانية لا يقتصر على الحماية من التدمير المادي المباشر، بل يمتد ليشمل كل فعل من شأنه تعطيل الوظيفة الإنسانية التي تؤديها المنشآت البحرية الطبية أو إعاقاتها. فالمادة (٢٢) من الاتفاقية تنص صراحةً على ضرورة احترام السفن الطبية وحمايتها في جميع الأوقات، مما يعني أن أي عمل عدائي يؤدي إلى شل حركتها، سواءً عبر قصف مادي أو عن طريق اختراق نظمها الإلكترونية وإحداث خلل في بنيتها الرقمية، يشكل انتهاكاً لصريح الأحكام^(٢). كما أن المادة (٣٤) تؤكد على حماية أفراد الطواقم الطبية البحرية، وتسمح بتفسيرها لتشمل الهجمات السيبرانية التي تستهدف نظم الاتصالات والبرمجيات التي يعتمد عليها هؤلاء الأفراد في أداء مهامهم الإنسانية.

وبالاستناد إلى التفسير الديناميكي لأحكام القانون الدولي، وخصوصاً ما تقرره المادة (٣١) من اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩، ينبغي قراءة أحكام اتفاقية جنيف الثانية بما يتوافق مع

١ ينظر المادة: (٢/٨/ب/٢-٤) من نظام روما الأساسي للمحكمة الجنائية الدولية، وينظر أيضاً: ويليام أ. شاباس،

مقدمة إلى المحكمة الجنائية الدولية، مطبعة جامعة كامبريدج، ٢٠٢٠.

٢ ينظر: المواد (٢٢، و ٣٤) من اتفاقية جنيف الثانية ١٩٤٩. وينص التفسير الخاص بالمادة (٢٢) على أن الحماية تشمل حالة عدم تحميل السفينة مرضى، وتظل محمية في جميع الظروف، ما لم تُستخدم في أعمال عدائية، وهذا يشير إلى شمول هذه الحماية لأية أدوات قد تُشغل وظائفها الإنسانية بما في ذلك الهجمات السيبرانية.

التطورات التكنولوجية والمخاطر السيبرانية^(١). وعليه، فإن الهجوم السيبراني الذي يعطل منظومات القيادة الرقمية لسفينة طبية أو يعوق الاتصال بين طاقمها والقيادة العليا، أو يمنع تشغيل أجهزة الرصد الحيوي، يُعدّ هجوماً عدائياً محظوراً، لأنه يؤدي إلى تعطيل تقديم الرعاية الطبية، وبالتالي يرقى إلى مستوى الاعتداء غير المشروع

ثالثاً: اتفاقية جنيف الثالثة: تشكل اتفاقية جنيف الثالثة لعام ١٩٤٩ الإطار القانوني الأساس لتنظيم معاملة أسرى الحرب، وتكفل لهم حماية خاصة ضد كافة أشكال الاعتداء الجسدي أو المعنوي، سواء وقع في سياق مباشر أو غير مباشر. وقد جاءت الاتفاقية تفصيلاً للمبادئ العامة المنصوص عليها في القانون الدولي الإنساني، وأبرزها مبدأ الإنسانية، والتمييز بين المقاتلين وغير المقاتلين، وعدم تعريض الأشخاص المحميين لأي ضرر في حياتهم أو كرامتهم أو أمنهم الجسدي أو النفسي. ومع تطور أنماط النزاعات المسلحة، وانتقال جزء كبير منها إلى الفضاء السيبراني، أصبح من الضروري فقهاً وقانوناً النظر في مدى قابلية الاتفاقية للتطبيق على الهجمات التي تتم عبر الوسائل الرقمية، لاسيما حين تستهدف منشآت أو نظاماً تُعنى بإدارة شؤون أسرى الحرب، أو توفر لهم خدمات أساسية داخل مرافق الاحتجاز.

إن القراءة الموسعة للاتفاقية، وفقاً للتفسير الغائي الذي تأخذ به المادة (٣١) من اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩، تتيح تكييف أحكامها بما يتماشى مع التطورات التكنولوجية^(٢). فالحماية المقررة لأسرى الحرب، كما تنص عليها المواد (١٣) و(١٤) و(١٦) من اتفاقية جنيف الثالثة، لا تنحصر في حمايتهم من العنف المادي المباشر، بل تشمل كل فعل أو تقصير يُعرضهم لخطر أو يُخلّ بكرامتهم الإنسانية. وفي هذا السياق، فإن استهداف نظم المعلومات الإلكترونية الخاصة بتسجيل الأسرى أو إدارة بياناتهم الطبية، أو الهجوم على شبكات الاتصالات الرقمية التي تربطهم بذويهم أو باللجنة الدولية للصليب الأحمر، يعدّ انتهاكاً للحماية التي كفلتها الاتفاقية، لأن هذه الوسائل أصبحت اليوم من مكونات البنية الأساسية لحماية الأشخاص في حالة الأسر.

١ نظر: المادة (٣١) من اتفاقية فيينا لقانون المعاهدات، ٢٣ مايو ١٩٦٩، المادة (٣١)، التي تفرض تفسير المعاهدات بناءً على نصوصها وهدفها، ما يدعم توسيع تطبيق اتفاقية جنيف للتعامل مع التهديدات الرقمية كجزء من سياقها الوظيفي.

٢ ينظر: المادة (٣١) اتفاقية فيينا لقانون المعاهدات، ٢٣ أيار/مايو ١٩٦٩، سلسلة معاهدات الأمم المتحدة.

ويزداد الأمر وضوحاً في حالات الهجمات السيبرانية التي تؤدي إلى تعريض حياة الأسرى للخطر، كما لو تم اختراق نظام التدفئة أو التبريد في مرفق احتجاز ضمن منطقة نزاع، ما يؤدي إلى تعطل البيئة الصحية في الشتاء أو الصيف، أو في حال تدمير السجلات الطبية الرقمية للمرضى من الأسرى، بما يمنع عنهم الوصول إلى العلاج اللازم. وفي جميع هذه الحالات، تتحقق العناصر الموضوعية للانتهاك، حتى وإن لم يكن الضرر ناتجاً عن استخدام القوة التقليدية. فالوسيلة، وإن اختلفت، لا تغير من جوهر الفعل، طالما أن الأثر هو ذات الأثر المحظور بموجب القانون.

وتمثل الهجمات السيبرانية على مرافق احتجاز الأسرى أحد أبرز الأمثلة على استخدام القوة الرقمية في إطار يخالف المبادئ الأساسية لاتفاقية جنيف الثالثة. فقد أظهرت تجارب ميدانية، منها حالات في أوكرانيا وسوريا، أن تعطيل الاتصال أو تعقب نظم الأسرى قد يؤدي إلى انتهاكات جسيمة، كتأخير الإفراج أو الإنكار القسري للوجود، أو إحداث ضرر مباشر بالظروف الإنسانية المحيطة بهم^(١). وفي ظل هذه المخاطر، يصبح من اللازم الاعتراف بأن استهداف نظم المعلومات أو مرافق الرعاية المرتبطة بالأسرى، في ظل نزاع مسلح، يمثل صورة من صور الهجوم المحظور، ويخضع لذات القواعد القانونية التي تحكم الهجمات التقليدية.

ومن ثم، فإن اتفاقية جنيف الثالثة، على الرغم من كونها صيغت بلغة تقليدية، إلا أن مرونتها التفسيرية تجعلها أداة فعالة في تعزيز الحماية من الهجمات السيبرانية متى ما استهدفت الأشخاص الذين تشملهم ولايتهم. وهذه الحماية لا تقتصر على الامتناع عن الاعتداء، بل تشمل أيضاً التزام الأطراف المتنازعة باتخاذ التدابير التقنية والاحترازية لمنع الاختراق أو التسريب أو التعطيل المعتمد للأنظمة الرقمية التي تؤمن حقوق الأسرى وكرامتهم.

رابعاً: اتفاقية جنيف الرابعة: توفر الحماية للمدنيين، بما في ذلك الأراضي المحتلة. إذ نصت اتفاقيات جنيف التي أُعتمدت قبل (١٩٤٩)، على المحاربين فقط، دون المدنيين. وقد أظهرت أحداث الحرب العالمية الثانية العواقب الوخيمة، التي نتجت عن غياب اتفاقية لحماية المدنيين في زمن الحرب. وعليه، أخذت الاتفاقية المعتمدة في عام (١٩٤٩) في عدّها تجارب الحرب العالمية الثانية. وتضم الاتفاقية (١٥٩) مادة ضمنها مادة قصيرة تُعنى بحماية المدنيين عموماً من عواقب الحرب، لكنها لم تتصدّ

١ معهد السلام السيبراني، مستشفيات الحرب السيبرانية في أوكرانيا: ناشطون مدنيون ومواقع محمية، ٢٠٢٣. متاح

على الرابط: <https://cyberpeaceinstitute.org/research/cyber-war-hospitals>

لمسألة الأعمال العدائية في حد ذاتها إلى أن تم مراجعتها في البروتوكولين الإضافيين لعام (١٩٧٧)، وتتناول أغلب مواد الاتفاقية مسائل وضع الأشخاص المحميين ومعاملتهم، ويميز وضع الأجانب في إقليم أحد أطراف النزاع من وضع المدنيين في الإقليم المحتل. وتورد أيضاً التزامات المحتل تجاه السكان المدنيين، وتضم أحكاماً تفصيلية بشأن الإغاثة الإنسانية في الإقليم المحتل. وتضم نظاماً معيناً لمعاملة المعتقلين المدنيين، وملحقات ثلاثة ضمت نموذج الاتفاقية بشأن المستشفيات والمناطق الآمنة، ولوائح نموذجية بشأن الإغاثة الإنسانية، وبطاقات نموذجية^(١).

وتنص اتفاقية جنيف الرابعة أيضاً على إمكانية إنشاء مناطق ومواقع آمنة لحماية المدنيين المعرضين للخطر بشكل خاص من آثار الأعمال العدائية. ورغم أن الاتفاقية أشارت بشكل خاص إلى الجرحى والمرضى والمسنين والأطفال دون سن الخامسة عشرة والأمهات الحوامل وأمهات الأطفال دون سن السابعة، فلا يوجد سبب يمنع جميع المدنيين من البحث عن مأوى في مثل هذه المناطق والمواقع^(٢). وتشير اتفاقية جنيف الرابعة على إمكانية إنشاء مناطق محايدة^(٣). والفرق بين مناطق المستشفيات/السلامة والمناطق المحايدة هو أن الأولى تهدف إلى أن تكون موجودة على مسافة من مناطق القتال، وتشكل ترتيباً أطول أجلاً لفئات معينة من المدنيين المعرضين للخطر بشكل خاص. أما المناطق المحايدة، فهي تقع في مناطق القتال النشط، وتهدف إلى توفير المأوى المؤقت للمقاتلين والمدنيين الجرحى والمرضى والسكان المدنيين بالكامل^(٤).

أما بشأن حماية المناطق التي ينشب فيها نزاع مسلح، فقد تسعى مثل هذه المناطق إلى حماية الأشخاص المحددين فيما يأتي دون تمييز من آثار الحرب، وهم: الجرحى والمرضى من المقاتلين وغير المقاتلين، والمدنيون الذين لا يشاركون في أعمال عدائية ولا يؤدون عملاً ذا طبيعة عسكرية، في أثناء إقامتهم في هذه المناطق، ويمكن لأطراف النزاع، والدول المحايدة أو المنظمات الإنسانية أن

١ اللجنة الدولية للصليب الأحمر، تاريخ الزيارة ٢٠٢٤/٨/١٤، الساعة ٦،٠٠، متاح على الرابط: <https://ihl-databases.icrc.org/ar>

٢ ينظر: المادة (١٤) اتفاقية جنيف الرابعة عام ١٩٤٩.

٣ ينظر: المادة (١٥) اتفاقية جنيف الرابعة عام ١٩٤٩.

٤ ايمانويلا كييارا جيلارد، تعزيز أمن المدنيين في حالات النزاع، ورقة بحثية، رقم الوثيقة الرقمية:

٩٧٨١٧٨٤١٣٦٠٣١/١٠٠٥٥٣١٧

تبادر إلى إقامة منطقة محايدة، ويجب على أطراف النزاع عقد وتوقيع اتفاق كتابي يحدّد بداية مدة تحديد المنطقة، فضلاً عن تفاصيل موقعها الجغرافي، والإدارة، والموادّ الغذائية، والإشراف.^(١)

وفي حين أن اتفاقية جنيف الرابعة تفعل ذلك من خلال إنشاء مناطق يمكن للمدنيين والجرحى والمرضى الانتقال إليها، فإن المناطق منزوعة السلاح التي نص عليها البروتوكول الإضافي الأول تعزل مناطق معينة عن العمليات العسكرية لحماية جميع المدنيين. ويتعين على الطرف الذي ينشئ منطقة منزوعة السلاح أن يضمن عدم استخدامها في أنشطة عدائية — بالمعنى الواسع للمصطلح — وإذا اعترف بالمنطقة، فيتعين على خصمه أن يمتنع عن توسيع العمليات العسكرية، وهو مفهوم واسع أيضاً، لتشمل المنطقة. وحتى الآن لم تنشأ أي مناطق من هذا القبيل. وفيما يتصل بالنزاعات المسلحة غير الدولية، لا تشير المادة المشتركة الثالثة لاتفاقيات جنيف، وكذلك لا يشير البروتوكول الإضافي الثاني إلى أي نوع من المناطق المحمية. وهذا ليس ذا أهمية، إذ لا يوجد ما يمنع الأطراف من إبرام اتفاقيات ذات تأثير مماثل. والواقع أن هذه الاتفاقيات من بين أنواع الاتفاقيات الخاصة، التي تقترح المادة المشتركة الثالثة (٣) أن الأطراف قد تعتمد إلى ابرامها، لإدخال أحكام أخرى من الاتفاقيات حيز النفاذ.^(٢)

وبما أن القانون لا يشترط إنشاء مناطق بعينها، فقد أنشأت المناطق على أساس ما هو مطلوب وقابل للتحقيق في ظل الظروف القائمة، وليس على أساس النماذج المنصوص عليها في اتفاقيات جنيف والبروتوكول الإضافي الأول. وقد استوعبت هذه المناطق الفئات الأكثر ضعفاً من الناس — عادة الجرحى والمرضى، و في حالات المناطق، التي أنشئت في دكا في عام ١٩٧٥، ونيقوسيا في عام ١٩٧٤، وسايجون في عام ١٩٧٥، وأوسيك في عام ١٩٩١. وكانت هذه المناطق تقع في مناطق القتال النشط أو العنف، وكانت تستضيف أعداداً صغيرة نسبياً من الناس.

وعلى نحو مشابه، وعلى الرغم أن هذا النوع من الترتيبات لم يُشر إليه صراحةً في معاهدات القانون الدولي الإنساني في أثناء حرب فوكلاند/ مالفيناس في عام ١٩٨٢، فقد اتّفتت المملكة المتحدة والأرجنتين على إنشاء منطقة محايدة في أعالي البحار إذ يمكن للسفن الطبية من كلا الجانبين العمل بأمان. وكانت هذه المنطقة، التي أطلق عليها صندوق الصليب الأحمر، عبارة عن منطقة يبلغ قطرها

١ ينظر: المادة (٥) من اتفاقية جنيف الرابعة لعام ١٩٤٩.

٢ ايمانويلا كيبارا جيلارد، تعزيز أمن المدنيين في حالات النزاع، ورقة بحثية، رقم ٠١، الوثيقة الرقمية: ٩٧٨١٧٨٤١٣٦٠٣١/١٠٠٥٥٣١٧.

نحو ٢٠ ميلاً بحرياً، إذ كانت أربع سفن طبية بريطانية، وثلاث سفن أرجنتينية متمركزة. وكانت هذه السفن قادرة على استقبال الجرحى وتوفير العلاج دون إعاقة العمليات العسكرية، وكان القرب بين مجموعتي السفن يسمح بتبادل المرضى بسهولة. وقد سمح هذا الترتيب بعلاج مئات الضحايا البريطانيين والأرجنتينيين.^(١)

يمكن للأطراف المتحاربة إنشاء مناطق محمية، ولكن ما لم يعترف بها الخصم، فإن هذه المناطق لا تستفيد من حماية خاصة. ومع ذلك، فإن غياب مثل هذا الاعتراف لا يحرم هؤلاء الأشخاص الذين يحتّمون في هذه المناطق من الحماية، التي يحق لهم الحصول عليها بموجب القانون الدولي الإنساني بوصفهم مدنيين أو أشخاص عاجزين عن القتال.

و أن المناطق المحمية تثير تساؤلات حول قانون اللاجئين، وفي بعض الحالات، كانت الدعوات إلى إنشائها مدفوعة برغبة في منع أو وضع حد لتدفقات السكان عبر الحدود، أو لتعزيز عودة اللاجئين في وقت لم تكن فيه الظروف على الأرض تبرر ذلك.

ينص القانون الدولي الإنساني على أن المناطق المحمية تنشأ بموجب اتفاق بين الأطراف المتحاربة. وفي العقود الأخيرة، كانت هناك حالات قليلة تم فيها إنشاء مناطق محمية بموجب قرارات مجلس الأمن التابع للأمم المتحدة أو على أساسها، وتشمل هذه الحالات الملاذات الآمنة التي أنشئت في شمال العراق في عام ١٩٩١؛ والمناطق الآمنة في البوسنة والهرسك في عام ١٩٩٣ والمناطق الإنسانية الآمنة في رواندا في عام 1994.

فضلاً عن الاعتبارات المتعلقة بالقانون الدولي الإنساني، فإن إنشاء مناطق محمية على هذا النحو يثير تساؤلات بشأن قواعد القانون الدولي المتعلقة باللجوء إلى القوة، فوجود القوات المسلحة لدولة ما على أراضي دولة أخرى دون موافقة هذه الأخيرة يشكل انتهاكاً للحظر المفروض على استخدام القوة، ما لم يكن هذا الوجود مرخصاً به من قبل مجلس الأمن، أو يشكل دفاعاً عن النفس فردياً أو جماعياً "وهو أمر غير ذي صلة في الحالات، التي أنشئت فيها مناطق آمنة حتى الآن".

١ إيمانويلا كيأرا جيلارد، تعزيز أمن المدنيين في حالات النزاع، ورقة بحثية، رقم ٠١، الوثيقة الرقمية:

لقد انشأت ملاذات آمنة في شمال العراق في عام ١٩٩١ عندما فر مئات الآلاف من الأكراد العراقيين إلى الجبال في مواجهة القمع من قبل نظام صدام حسين. وقد أذن قرار مجلس الأمن رقم ٦٨٨ (١٩٩١) القمع وطالب العراق بالسماح الفوري للمنظمات الإنسانية بالوصول إلى كل من هم في حاجة إلى المساعدة. ولم ينشئ القرار هذه المناطق؛ ولم تكن موافقة الحكومة واضحة تمامًا. ومع ذلك، كان القرار هو الأساس لعملية متعددة الجنسيات بقيادة الولايات المتحدة، التي نفذت عمليات إنزال جوي، ونشرت قوات على الأرض لحماية النازحين وبناء المخيمات.^(١)

وقد تشكل اتفاقية جنيف الرابعة لعام ١٩٤٩ الإطار الأكثر شمولاً لحماية المدنيين والمناطق المحمية في النزاعات المسلحة، حيث كرّست مجموعة من القواعد التي تمنع المساس بحياة المدنيين أو ممتلكاتهم أو المنشآت الحيوية التي تقدم خدمات إنسانية. وقد صيغت هذه الاتفاقية في أعقاب الفظائع التي ارتكبت بحق المدنيين خلال الحرب العالمية الثانية، لتؤكد على حظر استهدافهم أو الإضرار بهم بأي وسيلة كانت. ورغم أن الاتفاقية لم تكن آنذاك على دراية بالتهديدات السيبرانية، فإن مبادئها الجوهرية لا تزال ذات صلة وثيقة بالتحديات الحديثة، ولا سيما استخدام الفضاء الإلكتروني كأداة للعدوان في النزاعات المسلحة.

تقر الاتفاقية، لاسيما في المواد (١٤)، (١٧)، و(١٨)، حماية المنشآت المدنية التي تقدم خدمات إنسانية، كالمستشفيات ومناطق الإيواء والإغاثة، وتُلزم أطراف النزاع بعدم استهدافها أو تعطيل وظيفتها بأي شكل، سواء ماديًا أو رقميًا. وقد أكدت المادة (١٤) تحديدًا جواز إنشاء "مناطق استشفاء وأمان" تستثنى تمامًا من العمليات العدائية، شرط الاتفاق المتبادل بين الأطراف^(٢). وتمنح هذه المواد حماية "وظيفية" للمنشآت، ما يعني أن أي إضعاف لقدرتها التشغيلية — حتى لو تم عبر اختراق رقمي — يمثل خرقًا صريحًا لأحكام الاتفاقية.

ويُعد الهجوم السيبراني الذي استهدف "خدمة الصحة العامة الأيرلندية" (HSE) في مايو ٢٠٢١ نموذجًا واقعيًا على مدى خطورة هذا النوع من الهجمات. فقد تسبب الهجوم — الذي استُخدمت فيه برمجية الفدية Conti — في تعطيل شامل للأنظمة الرقمية للمستشفيات، مما أدى إلى إلغاء مئات

١ إيمانويلا كيারা جيلارد، تعزيز أمن المدنيين في حالات النزاع، ورقة بحثية، رقم ٥١، الوثيقة الرقمية:

٩٧٨١٧٨٤١٣٦٠٣١/١٠.٥٥٣١٧

٢ ينظر: المادة (١٤) من اتفاقية جنيف الرابعة لعام ١٩٤٩

المواعيد والعمليات وتأخير العناية بالحالات الحرجة، رغم أنه لم يقع ضمن نزاع مسلح^(١). إلا أن تكرار مثل هذا النمط من الهجمات في سياقات نزاع فعلي — كما في أوكرانيا أو غزة — يُمكن أن يؤدي إلى تكييفها قانونيًا كأفعال عدائية غير مشروعة، إذا استهدفت مناطق محمية أو مستشفيات ضمن مناطق نزاع نشطة^(٢).

وبالاستناد إلى التفسير الغائي للنصوص القانونية، المنصوص عليه في المادة (٣١) من اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩، فإن الهجمات السيبرانية التي تؤدي إلى تعطيل تقديم الرعاية في مناطق محمية، مثل المستشفيات أو مراكز الإغاثة أو مناطق الإيواء، ينبغي أن تُصنف ضمن “الهجمات” المحظورة بموجب القانون الدولي الإنساني^(٣). إذ إن الحماية لا تتعلق فقط بالوسيلة، بل بالأثر النهائي الواقع على المدنيين.

وفي ضوء ذلك، فإن اتفاقية جنيف الرابعة تفرض التزامات مزدوجة على أطراف النزاع: الامتناع عن استهداف المناطق المحمية بالوسائل الرقمية، واتخاذ تدابير احترازية لحمايتها من الاختراق، مثل تأمين أنظمة المستشفيات وتشفير قواعد بيانات المرضى. إن الإخفاق في ذلك قد يُعدّ تقصيرًا في توفير الحماية المنصوص عليها دوليًا.

لذلك، لم تعد الهجمات السيبرانية مجرد تهديد نظري، بل تمثل تحديًا حقيقيًا للقانون الدولي الإنساني. ويجب أن يتوسع الفقه القانوني ليعترف بأن المساس بالوظيفة الإنسانية لمرفق محمي — ولو عبر الوسائل الرقمية — يُعدّ خرقًا للمبادئ الأساسية، ويستوجب المساءلة القانونية وفق قواعد اتفاقية جنيف الرابعة

الفرع الثاني

البروتوكولان الإضافيان لعام ١٩٧٧

خلال العقدَيْن اللذين عقبا اعتماد اتفاقيات جنيف شهد العالم زيادة في عدد النزاعات المسلحة غير الدولية وحروب التحرير الوطني. وكرد فعل على ذلك اعتمد بروتوكولان إضافيان لاتفاقيات جنيف

١ جهاز الخدمات الصحية الأيرلندي (HSE)، “تحديث بشأن الهجوم السيبراني”، ٢٠٢١،

<https://www2.hse.ie/services/cyber-attack>

٢ معهد السلام السيبراني، مستشفيات الحرب السيبرانية في أوكرانيا: الناشطون المدنيون والمواقع المحمية، ٢٠٢٣،

<https://cyberpeaceinstitute.org/research/cyber-war-hospitals>

٣ ينظر: المادة (٣١) من اتفاقية فيينا لقانون المعاهدات، ٢٣ أيار/مايو ١٩٦٩، سلسلة معاهدات الأمم المتحدة.

الأربع لعام (١٩٤٩) في (١٩٧٧). ويعزز البروتوكولان الحماية الممنوحة لضحايا النزاعات المسلحة الدولية -البروتوكول الأول- وغير الدولية -البروتوكول الثاني- و يفرضان قيوداً على طريقة خوض الحروب، وكان البروتوكول الثاني هو أولى المعاهدات الدولية المكرسة بالكامل لحالات النزاع المسلح غير الدولي.^(١)

إن اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين اللاحقين لها لعام ١٩٧٧ أساس أو محور القانون الدولي الإنساني. وتبين هذه الاتفاقيات، التي اعتمدت كرد فعل على الأفعال الفظيعة التي ارتكبت في الحرب العالمية الثانية، وتقنين أحكام القانون الكثيرة للنزاع المسلح، التي جرى التأكيد عليها في اتفاقيات سابقة، وقد وصلت هذه المعاهدات إلى مرحلة التوثيق العالمي تقريباً. وفي عام ١٩٧٧، جرى الاعتماد على بروتوكولين إضافيين لتأمين حماية مضاعفة لضحايا الصراع المسلح، ومع أن هذين البروتوكولين ليسا إجباريين غير أنهما قد حصلا على مصادقة ثلاثة أرباع دول العالم بشكل تقريبي.

ويوجد تفريق مصطنع يتم في العادة بين قطاعين من القانون الإنساني: الأحكام المنظمة للحرب (اتفاقية لاهاي ١٨٩٩ و ١٩٠٧) أما الثانية فهي التي تعمل على تنظيم نشاطات الإغاثة في مدة الصراع أو المنازعات المسلحة (اتفاقيات جنيف).

وفي الحقيقة، فإنه يُلقى على عاتق اتفاقيات جنيف والبروتوكولين الإضافيين، الذين يلحقان بها مهمة تفوق تقنين أحكام تقديم المساعدة للمدنيين وتقديم الحماية لهم. فهي تؤكد الحق في إغاثتهم إلى جانب مبادئ السلوك خلال الاعتداءات ما زالت تقوم بتنظيم بعض أساليب الحرب، وتؤكد مسؤولية الأطراف المتنازعة.

أولاً: البروتوكول الإضافي الأول لاتفاقيات جنيف المؤرخة ١٢ آب/أغسطس ١٩٤٩، المتعلق بحماية ضحايا النزاعات المسلحة الدولية (البروتوكول الأول)، ٨ حزيران/يونيه 1977

أشارت المادة (١-٤) على أن النزاعات المسلحة، التي تقاتل فيها الشعوب ضد الهيمنة الاستعمارية أو الاحتلال الأجنبي أو الأنظمة العنصرية تُعد نزاعات دولية.

وأشير في المادة (١) في الفقرة (٢) منها في البروتوكول الإضافي الأول عام ١٩٧٧ إلى حماية المدنيين والتمييز بينهم وبين المقاتلين، إذ يبقى المقاتلون والمدنيون في الحالات، التي تنص عليها

١ اللجنة الدولية للصليب الأحمر، تاريخ الزيارة ١٤/٨/٢٠٢٤، الساعة ٤،٠٠، متاح على الرابط:

<https://www.icrc.org/ar/law-and-policy/geneva-conventions-and-their-commentaries>

الاتفاقيات الأربعة والبروتوكول تحت سلطة وحماية مبادئ القانون الدولي، مثلما يستقر عليها العرف وما يمليه الضمير العام ومبادئ الإنسانية.^(١)

وأخذ الجزء الثاني (المواد من ٨ إلى ٣٤) قواعد اتفاقيتي جنيف الأولى والثانية بشأن الجرحى والمرضى والغرقى، وقد وسع نطاق الحماية، التي توفرها الاتفاقيات لتشمل أفراد الخدمات الطبية المدنيين والمعدات والإمدادات والوحدات المدنية ووسائل النقل، ويتضمن أحكاماً مفصلة بشأن النقل الطبي.

أما الجزء الثالث وعدد من فصول الجزء الرابع (المواد ٣٥-٦٠) فقد أخذ سير الأعمال العدائية، أي: المسائل، التي كانت تنظمها حتى الآن اتفاقيات لاهاي لعامي (١٨٩٩ و ١٩٠٧) والقانون الدولي العرفي. وإعادة تأكيد هذه الاتفاقيات وتطويرها أمر مهم في ضوء اتفاقيات لاهاي والدول الجديدة التي لم يكن لها دور في صياغتها. وتعطي المادتان (٤٣-٤٤) تعريفاً جديداً للقوات المسلحة والمقاتلين. ومن بين أهم المواد تلك المتعلقة بحماية السكان المدنيين من آثار الأعمال العدائية. وهي تتضمن تعريفاً للأهداف العسكرية وحظر الهجوم على الأشخاص المدنيين والأهداف المدنية. وتتناول المواد الأخرى (٦١-٧٩) حماية منظمات الدفاع المدني، وأعمال الإغاثة، ومعاملة الأشخاص الخاضعين لسلطة أحد أطراف النزاع.^(٢)

وبالنسبة للمادة (٣٦) فقد ألزمت أطراف التعاقد عند تطوير الدراسة أو امتلاك أداة حرب أو سلاح جديد أو اتباع أسلوب الحرب أن يتحقق فيما إذا كان ذلك محظوراً في جميع الأحوال بحسب أي قاعدة من قواعد القانون الدولي أو البروتوكول الذي يلتزم بها الطرف المتعاقد. وأشارت المادة (٤٨) من البروتوكول الإضافي الأول إلى ضرورة أن يميز أطراف النزاع المسلح بين المدني والمقاتل إذ أشارت المادة إلى أن أطراف النزاع تعزل على التمييز بين المقاتلين والمدنيين، وبين أعيان المدينة والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية.^(٣)

١ اللجنة الدولية للصليب الأحمر، البروتوكول الإضافي الأول الملحق ب اتفاقيات جنيف ١٢/٨/١٩٤٩ ص ١١.

٢ اللجنة الدولية للصليب الأحمر، تاريخ الزيارة ١٤/٨/٢٠٢٤، الساعة، ٢٠،٠٠، متاح على الرابط: <https://ihl-databases.icrc.org/ar>

٣ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص ٥٧.

وعرفت الفقرة الأولى من المادة ٤٩ من البروتوكول الإضافي الأول لعام ١٩٧٧، الذي الحق باتفاقيات جنيف الأربعة عام ١٩٤٩ الهجمات بأنها أعمال عنف هجومية و دفاعية ضد الخصم ^(١)، و لا يمكن فصل هذه الفقرة عن باقي فقرات البروتوكول إذ يحكم أعمال العنف و التسلح أمران الأول: أن يكون بشكل مباشر و تلحق أذى بطبيعتها في الأعيان المدنية أو العسكرية. والثاني أن تكون غير مباشرة بعد أن يقع الهجوم مهما كانت الطريقة أو الوسيلة. ومن هنا يجب التركيز على نوع الآثار الناتجة عن الهجوم فمثلاً سيتأثر الناس نتيجة هجوم عسكري سيبراني مثل استهداف منظومات السيطرة والتحكم الإلكتروني لمفاعل نووي يولد الطاقة الكهربائية ^(٢).

وعرفت المادة (٥١) من البروتوكول الإضافي الأول عام ١٩٧٠ الهجوم المسلح بطريقتين: الأول في الفقرة (١/٥) إذ أشارت إلى الوسيلة القتالية بأنها الهجوم قصفاً بالقنابل مهما كانت الوسائل والطرق .. ، والرأي الثاني، فقد أشارت إلى طريقة القتال في الفقرة (٥/ب) بأنه الهجوم الذي بالإمكان أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضرار بالأعيان المدنية . ^(٣)و إذ جاء في الفقرة (٢) من المادة (٥١): لا يجوز أن يكون السكان المدنيون محلاً للهجوم ، و تحظر أعمال العنف و التهديد به، التي ترمي إلى بث الذعر بين السكان المدنيين . ^(٤)

وفي المادة (٥٧) في الفقرة (ب/٢) تمت الإشارة على أنه يعلق أو يُلغى أي هجوم في حال اتضح أن الأهداف المقصودة ليست أهداف عسكرية، أو أنه مشمول بحماية خاصة، أو من المتوقع أن يلحق إصابات في المدنيين أو تصيبهم خسائر في أرواحهم أو يلحق ضرراً بالأعيان المدنية أو يحصل خلط بين الأضرار والخسائر بشكل عرضي، تفرط في تجاوز ما ينتظر أن يسفر عن هذا الهجوم من ميزة عسكرية مباشرة. ^(٥)

وأكد في الفقرة الرابعة من ذات المادة على عدم جواز استخدام طرق ووسائل القتال، التي يمكن أن تؤدي إلى هجمات عشوائية، ومن بينها:

١- الهجمات التي لا توجه إلى أهداف عسكرية معينة.

١ ينظر: المادة (٤٩) من البروتوكول الإضافي الأول.

٢ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص ١٩.

٣ يُنظر: المادة (٥١) من البروتوكول الإضافي الأول.

٤ أحمد عبيس الفتلاوي، المصدر السابق، ص ١٩.

٥ اللجنة الدولية للصليب الأحمر، بخصوص البروتوكولات الملحقات باتفاقيات جنيف الأربعة، ١٩٤٩/٨/١٢ ص ٤٢.

٢- الهجمات التي تستعمل وسيلة أو طريقة القتال، لا يمكن توجيهها إلى هدف عسكري معين.

٣- الهجمات التي تستعمل وسيلة أو طريقة للقتال ليس بالإمكان أن تحصر آثارها بالشكل الذي

يتطلبه هذا البروتوكول، التي من شأنها إصابة الأشخاص المدنيين أو الاهداف العسكرية أو

الأعيان المدنية دون تمييز. (١)

أما المناطق التي يحظر فيها على أطراف النزاع القيام بعمليات عسكرية، أو استعمال هذه المناطق لأي هدف يرتبط بسير العمليات العسكرية، ويؤكد القانون الإنساني على أنها غير محمية بهدف منع حدوث القتال هناك. والهدف هو حماية السكان المدنيين والممتلكات المدنية الموجودة فيها، وعليه يحظر على أطراف النزاع مهاجمة مثل هذه المواقع بأي وسيلة كانت. (٢)

ويخضع تحديد موقع منطقة غير محمية والعلامة المميزة لها لأنظمة مفصلة. (٣) ويجب على أطراف النزاع الاتفاق على علامات تميّز مثل هذه المواقع عند إنشائها، أما المناطق والمواقع التي تقام على أراضي طرف من أطراف النزاع أو على أرض محتلة بهدف حماية الجرحى والمرضى من أفراد القوات المسلحة، فضلاً عن أفراد الخدمات الطبية المعيّنين في كل منطقة، من آثار الحرب. ويجب تمييز مناطق المستشفيات والمناطق الآمنة بعلامات حمراء داكنة على خلفية بيضاء وتعلق على المباني والأبنية الخارجية لها. وهذا شعار مميّز تحميه اتفاقيات جنيف وأن استغلاله بطريقة مشينة أو عدم احترامه يُعدّ خرقاً فاضحاً للمعاهدات وبذلك تُعدّ جرائم حرب. (٤) وأخيراً، يجب وضع علامة صليب أحمر (هلال أحمر أو أسد أحمر أو شمس حمراء) على خلفية بيضاء فوق المناطق المخصصة حصرياً للجرحى والمرضى.

ويجب أن تحدّد هذه المناطق في اتفاقية صريحة، تبرم إما في وقت سلام أو بعد اندلاع العمليات العدائية. ويمكن أن تكون اتفاقية شفوية أو مكتوبة، وتبرمها أطراف النزاع مباشرة أو من خلال وساطة دولة حامية أو منظمة إنسانية محايدة. ويجب وضع علامة واضحة على منطقة منزوعة السلاح إلى الحدّ الممكن بعلامات يجري الاتفاق عليها مع الطرف الآخر. (٥)

١ اللجنة الدولية للصليب الأحمر الملحقان البروتوكولات الإضافيان لاتفاقيات جنيف المعقود في ١٢/٨/١٩٤٩، جنيف، سويسرا، ١٩٩٤، ص ٤٣.

٢ يُنظر: المادة (٥٩) من البروتوكول الأول، لعام ١٩٧٧.

٣ يُنظر: المادة (٩/٥٧) (٩/٥٩) من البروتوكول الأول لعام ١٩٧٧.

٤ يُنظر: المادة (٨٥) من البروتوكول الإضافي الأول، لعام ١٩٧٧.

٥ يُنظر: المادة (٦٠) من البروتوكول الإضافي الأول، لعام ١٩٧٧.

وقضت الفقرة (٢) من المادة (٥٢) على إن الهجمات يجب أن تكون مقتصرة على الأهداف العسكرية فقط وحصر الأهداف العسكرية فيما يتعلق بالأعيان على الأهداف، التي لها مساهمة فعالة في الأعمال العسكرية، على حد سواء إن كان ذلك في استخدامها أو موقعها أو طبيعتها أو غايتها، التي يحقق التدمير الجزئي أو الكلي لها أو الاستيلاء عليها في المعروف، التي تكون سائدة وقتها ميزة عسكرية عظيمة. (١)

وأما بشأن المناطق المنزوعة السلاح لا يجوز لأي طرف من أطراف النزاع أن يلغي من طرف واحد وضع منطقة منزوعة السلاح، ما لم يفشل أحد أطراف النزاع في احترام هذه الشروط أو يستخدم المنطقة لأغراض ترتبط بإدارة العمليات العسكرية. وفي مثل هذه الحالات، يُعفى الطرف الآخر من التزاماته بموجب اتفاقية أولية، وفي مثل هذه الحالة، تفقد المنطقة وضعها، ولكنها تظل متمتعة بالحماية التي توفرها قواعد القانون الإنساني. (٢)

و جاء في المادة (٨٦) من البروتوكول الإضافي الأول عام ١٩٧٧

١- إن أطراف النزاع والأطراف المتعاقدة يجب أن تعمل على قمع الانتهاكات الكبيرة، ويجب أن تتخذ الإجراءات، التي تلزم من أجل تمنع جميع الانتهاكات للاتفاقيات والبروتوكولين الإضافيين الناجمة عن التقصير في أداء واجبهم.

٢- إن رؤساء أي مرؤوس غير معفيين من المسؤولية التأديبية أو الجنائية في حال كان لديهم معلومات بالانتهاك، ولن يقوموا باتخاذ ما بوسعهم من أجل أن يمنعوا ذلك الانتهاك. (٣)

إن نطاق المناطق المحمية المحتملة يتوسع أكثر بموجب البروتوكول الإضافي الأول، الذي ينص على إمكانية إنشاء مناطق منزوعة السلاح. (٤) والهدف من هذه المناطق مماثل لهدف المناطق المحايدة: وضع المناطق وسكانها غير المقاتلين خارج مسرح الحرب، والفرق يكمن في النهج المتبع في القيام بذلك.

ثانياً: البروتوكول الإضافي الثاني لاتفاقيات جنيف المؤرخة ١٢ آب/أغسطس ١٩٤٩، المتعلق بحماية ضحايا النزاعات المسلحة غير الدولية (البروتوكول الثاني)، ٨ حزيران/يونية ١٩٧٧

١ اللجنة الدولية للصليب الأحمر، المادة ٥٢ من البروتوكول الإضافي الأول، لعام ١٩٧٧.

٢ يُنظر المادة: (٦/٦٠ و ٧/٦٠) من البروتوكول الإضافي الأول، لعام ١٩٧٧.

٣ أحمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية، مصدر سابق، ص ٧٦-٧٧.

٤ ينظر: المادة (٦٠) من البروتوكول الأول لعام ١٩٧٧. وتنص المادة (٥٩) من البروتوكول الأول المعدل أيضاً على إمكانية إنشاء مناطق غير مسلحة.

أشير في ديباجة البرتوكول الإضافي الثاني عام ١٩٧٧ إلى انطباق مبدأ التمييز بين المدنيين و المقاتلين على النزاعات المسلحة غير الدولية، إذ نصت الديباجة على: و إذ تذكر أنه في الحالات التي لا تشملها القوانين السارية، يظل شخص الإنسان في حمي المبادئ و ما يمليه الضمير العام.^(١) والبرتوكول الإضافي الثاني هو القرار النهائي، الذي صدر عام ١٩٧٧ لاتفاقيات جنيف المتعلقة بالحماية تسبب في تورط المسلحين غير الدوليين. وهو يحدد بعض القوانين الدولية، التي يوجد بها توفير حماية أفضل للضحايا والمسلحة الداخلية، التي تدور داخل حدود دولة واحدة. ونطاق هذه القوانين أكثر محدودية من نطاق اتفاقية جنيف، التي تعترف بالحقوق السيادية وواجبات المرأة الوطنية.

إن موضوع التمييز بين المدنيين والمقاتلين في الهجمات السيبرانية هو موضوع صعب ومعقد، إذ إن المهاجم سيكون غالباً بعيد عن أمكنة المستهدفين من الهجوم ولمسافات بعيدة، الأمر الذي يعني أن موضوع التمييز بين المدنيين والمقاتلين مستحيل وغاية في الصعوبة، وهذا الأمر دفع المحامين الدوليين بمطالبتهم بتطبيق مبدأ التمييز هذا على الهجمات، التي تقوم بها الطائرات بدون طيار، وخير مثال على ذلك هو تحميل روسيا مسؤولية الهجمات السيبرانية على أستونيا سنة ٢٠٠٧، لأنها لم تميز بين المدنيين والمقاتلين.

وفي هذا الموضوع كان هناك دعوة من قبل فقهاء القانون مثل (مارك روسيني) المحامين لكي يتحركوا من أجل أن يبحثوا في مدى توافق الطابع السري الذي يميز الهجمات السيبرانية تحت مظلة القانون الدولي الإنساني وبشكل خاص مبدأ سلوكيات الحرب لا سيما بعد أن تزايد ادعاء الدول بأنها تتعرض إلى هجمات مجهولة المصدر.^(٢)

تاريخياً يعني الفصل الدولي للصراعات المسلحة إعلانا للحرب التقليدية بين الدول. وعندما تم تحديث اتفاقيات جنيف في عام ١٩٤٩، بعد الحرب العالمية الثانية، سعى المندوبون إلى تحديد معايير إنسانية دنيا معينة للمواقف، التي تحمل كل خصائص الحرب، دون أن تكون حرباً خارجية.^(٣)

١ أحمد عبيس الفنلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص ٦٥.

٢ المصدر نفسه، ص ٥٩.

٣ جان بيكتيه، القانون الدولي الإنساني تطوره ومبادئه، معهد هنري دونان، جنيف، سويسرا، ١٩٨٤، ص ١٥.

وقد أسفرت هذه المفأوضات عن المادة الثالثة المشتركة بين المعاهدات الأربعة الأساسية لاتفاقيات جنيف ١٩٤٩. وتطبق المادة الثالثة من الداخل على التأمين المسلح، التي لا تتميز بطابعة جزئية فقط، ولكنها محصورة ضمن نطاق دولة واحدة، وهي توفر محدودية للضحايا، بما في ذلك: يجب أن تشمل الأشخاص الذين لا يشاركون بشكل عضوي في الأعمال العدائية الشهيرة (بما في ذلك الأعضاء الذين توقفوا نتيجة المرض أو الاحتجاز) يجب جمع الجرحى والمرضى ورعايتهم.

والهدف من هذا البروتوكول هو توسيع نطاق القواعد الأساسية لقانون النزاعات المسلحة لتشمل الحروب الداخلية. ولقد أدى الخوف من أن يؤثر البروتوكول على سيادة الدول، ويمنع الحكومات من الحفاظ على القانون والنظام داخل حدودها بفعالية، وأن يُستعان به لتبرير التدخل الخارجي، إلى اتخاذ المؤتمر الدبلوماسي في دورته الرابعة قراراً بتقشير وتبسيط البروتوكول. وبدلاً من المواد السبع والأربعين التي اقترحتها اللجنة الدولية للصليب الأحمر، اعتمد المؤتمر (٢٨) مادة فقط. ومع ذلك، فقد تم الإبقاء على الجوهر الأساسي للمشروع. وبينما حُذِف الجزء الخاص بأساليب ووسائل القتال، فقد تم الاحتفاظ بالحظر الذي يفرض عدم إبقاء أي ناجين في المادة (٤) الضمانات الأساسية، وظلت ست مواد مخصصة لحماية السكان المدنيين الجزء الرابع (السكان المدنيون) المواد من (١٣ إلى ١٨). وسوف يؤدي التعريف التقليدي لمجال التطبيق المادي في المادة (١) إلى أن يكون البروتوكول الثاني قابلاً للتطبيق على نطاق أصغر من النزاعات الداخلية مقارنة بالمادة (٣) المشتركة بين اتفاقيات ١٩٤٩. (١)

المطلب الثاني

دور القضاء الجنائي الدولي في تعزيز الحماية للمناطق المحمية

أولى القضاء الجنائي الدولي اهتماماً كبيراً في الحد من الانتهاكات للقانون الدولي الإنساني في أثناء النزاعات المسلحة وخصوصاً الجرائم الدولية، وو أولى اهتماماً في تعزيز الحماية للمناطق المحمية من خلال كم هائل من القرارات والآراء القضائية ذات الصلة، وسنبحث هذا الموضوع عبر فرعين، في الفرع الأول دور المحاكم الدولية المؤقتة وفي الفرع الثاني دور المحاكم الدولية في تعزيز الحماية للمواقع المحمية.

١ اللجنة الدولية للصليب الأحمر، تاريخ الزيارة ٢٠٢٤/٨/١٤، الساعة: ٠٦:٠٧ متاح على الرابط: <https://ihl->

الفرع الأول

دور المحاكم الدولية المؤقتة

تتقسم المحاكم الجنائية الدولية المؤقتة على محاكم عسكرية دولية، ومحاكم جنائية دولية خاصة وستأول كل محكمة على حدا فيما يأتي:

أولاً: المحاكم العسكرية الدولية (محكمتي نورمبرغ وطوكيو):

تعالت نداءات دول الحلفاء في أثناء الحرب العالمية الثانية بضورة تعقب ومحاكمة مرتكبي جرائم الحرب، في حال انتهاء الحرب لصالحهم، وبالفعل صدرت عدة تصريحات في هذا الخصوص، كان من بينها تصريح سان جيمس في ١٩٤٢ الذي صدر باسم الدول المتحالفة والحكومات الالاجئة في لندن، إذ تم التأكيد فيه على ضرورة تقديم المسؤولين على الجرائم التي ارتكبت في أثناء العمليات الحربية، للمثول أمام محاكم جنائية لمعاقبتهم عما ارتكبوه من جرائم احتلال وجرائم ضد الإنسانية، واتباعهم وسائل القسوة والوحشية ضد المدنيين، تلك الوسائل، التي لم تكن تملحها أية ضرورات عسكرية، ولم يكن لها أية علاقة بمفهوم الأعمال الحربية، وفي عام ١٩٤٣ صدر تصريح موسكو، الذي أشار إلى الجرائم التي ارتكبتها الألمان على أقاليم البلاد المحتلة، التي تدخل في إطار جرم الحرب، والحرب ضد الإنسانية، و شكلت في تشرين الأول ١٩٤٣ لجنة الأمم المتحدة لجرائم الحرب من ممثلين عن ١٧ دولة، تحت رئاسة القانوني البريطاني هيرست للقيام بالتحقيقات، وتقصي الحقائق عن جرائم الحرب التي ارتكبتها الألمان، تحت حماية ودعم دول الحلفاء.^(١)

وبموجب اتفاقية لندن لعام ١٩٤٥ توصلَ إلى تأسيس محكمة عسكرية دولية في نورمبرغ، التي كانت مهمتها القيام بالمحاكمة، إذ أشارت المادة الأولى من الاتفاقية إلى تشكيل المحكمة العسكرية الدولية بعد مشاورة المجلس المعني بالرقابة في المانيا-لمحاكمة مجرمي الحرب الذين تخطت جرائمهم الحدود الجغرافية المعينة، بغض النظر إن كانوا مهتمين بصفة شخصية أو بصفتهم أعضاء منظمات أو هيئات، أو بكتلي الصفتين. ورغبة في تحقيق التجانس في المبادئ القانونية، التي جاءت بها هذا الاتفاقية المرفقة بها فقد أصر مجلس الرقابة في ألمانيا القانون رقم ١٠ في ٢٠ يناير ١٩٤٥، بغية محاكمة المسؤولين على اقتراف جرائم الحرب الذين لم يُقدّموا إلى محكمة العسكرية الدولية، وأصدر القائد الأعلى للقوات المسلحة لدول الحلفاء في ١٩٤٦ اعلاناً مماثلاً بشأن محاكمة أبرز مجرمي

١ عادل عبد الله المسدي، المحكمة الجنائية الدولية الاختصاص وقواعد الإحالة. ط٢، دار النهضة العربية، القاهرة،

الحرب في الشرق الأقصى أمام المحكمة العسكرية الدولية في طوكيو، بما لا يختلف فحواه عما جاء في اتفاقية لندن واللائحة الملحقة بها.^(١)

وهذا وقد عملت محكمة نورمبرغ على محاكمة (٢٢) شخصاً من بين (٢٤) اتهمهم المحكمة من كبار مجرمي الحرب بصفتهم الشخصية، إذ حكم على (١٢) منهم بالإعدام، الحكم على ثلاثة بالسجن المؤبد، والحكم على اثنين بالسجن لمدة (٢٠) عاماً، والحكم على شخص واحد بالسجن لمدة (١٥) عاماً، والحكم بالسجن لمدة (١٠) سنوات على شخص واحد، والحكم ببراءة ثلاثة مهتمين.^(٢) أما عن محكمة طوكيو فقد جه الادعاء الاتهام إلى (٢٨) منهم من بين كبار المسؤولين السياسيين والعسكريين اليابانيين، أصبحوا فيما بعد (٢٥) بسبب وفاة وجنود الآخرين، عوقب منهم (٧) بالإعدام شنقاً، و(١٦) منهم بالسجن مدى الحياة واثنين بالسجن المؤقت، أحدهم لسبع سنوات والآخر (٢٠) عام.^(٣)

وعلى الرغم من المشاكل القانونية والانتقادات المتمثلة أساساً في مشكلة القانون الواجب التطبيق، ومشكلة شرعية الجرائم والعقوبات، إلا أن هذه المحاولات الدولية الجنائية لم تنتهك أحكام القانون الدولي الإنساني تُعد درساً واقعياً لكل من يحاول في المستقبل أن يرتكب جرمًا مخالفًا للقانون وأعراف الحرب.

لقد وضعت محاولات نورمبرغ وطوكيو سابقة قانونية وإجرائية من أنها أن تكون رادعاً في الحروب التي قد تنشأ مستقبلاً. فقد أفرزت هذه المحاولات عدداً كبيراً من الأحكام، التي أسهمت بدرجة كبيرة في تشكيل القانون المتعلق بالمسؤولية الجنائية الفردية الدولية، ولقد كانت التجربة القضائية لنومبرغ وطوكيو بداية لعملية تدريجية لصياغة دقيقة، وتجميع للمبادئ والقواعد عملت عليها الدول والمنظمات (بالتحديد هيئة الأمم المتحدة واللجنة الدولية للصليب الأحمر) من خلال مبادرات لإنجاز التقنين عبر اعتماد المعاهدات، ومنذ ١١ كانون الثاني ١٩٤٦ كانت الجمعية العامة للأمم المتحدة قد اعتمدت بإجماع الأصوات القرار ذي الرقم (٩٥) بعنوان تأكيد مبادئ القانون الدولي، التي أقرها ميثاق نورمبرغ، وبعد أن أخذت الجمعية العامة علماً باتفاقية لندن واللائحة المرفقة بها والوثائق المتعلقة بمحاكمة طوكيو، فقد اتخذت خطوتين مهمتين، إذ أكدت الجمعية العامة مبادئ القانون الدولي،

١ محمد فهاد شلالدة، القانون الدولي الإنساني. منشأة المعارف، الإسكندرية، ٢٠٠٥، ص ٣٥٨-٣٥٩.

٢ عبد الرحيم صدقي، دراسة للمبادئ الأصولية للقانون الدولي الجنائي. المجلة المصرية للقانون الدولي. الجمعية المصرية للقانون الدولي، المجلد (٤٠)، العدد (٤٠)، القاهرة، ١٩٨٤، ص ٢٩.

٣ علي وهبي ديب، المحاكم الجنائية الدولية-تطورها ودورها في قمع الجرائم الدولية. ط١، منشورات الحلبي للنشر والتوزيع، بيروت، ٢٠١٥، ص ٤٧.

التي أقرها ميثاق نورمبرغ وأحكامها، أما الثانية فكانت التزاماً بأن تقوم لجنة القانون الدولي وهي هيئة منبثقة عن الجمعية العامة للأمم المتحدة بتقنين هذه المبادئ، وعن طريق هذا القرار أكدت الأمم المتحدة أن هناك عدداً من المبادئ العامة تنتمي إلى القانون العرفي، التي اعترف بها ميثاق نورمبرغ وأحكامها.^(١)

ثانياً: المحاكم الجنائية الدولية الخاصة (محكمتي يوغسلافيا سابقاً ورواندا)

أثارت الانتهاكات الجسيمة التي حدثت في يوغسلافيا قلق الدول الأوروبية والإسلامية مما قامت به القوات الربية من ارتكاب جرائم تطهير عرقي بحق الأغلبية من السكان المسلمين في حرب البوسنة عام ١٩٩٢، مما دفع مجلس الأمن إلى إصدار القرار (٧٨٠) عام ١٩٩٢ القاضي بإنشاء لجنة تقصي الحقائق، التي حددت الانتهاكات والجرائم ضد الإنسانية وجرائم الحرب وجرائم الإبادة الجماعية المرتكبة في يوغسلافيا، التي تعد انتهاكاً جسيماً لاتفاقيات جنيف لعام ١٩٤٩، وبرتوكولاتها الإضافيين لعام ١٩٧٧، نتيجة لذلك أصدر مجلس الأمن في عام ١٩٩٣ القرار رقم (٨٠٨)، الذي أنشأ بموجبه المحكمة الجنائية الدولية الخاصة بيوغسلافيا سابقاً لمحاكمة الأشخاص، الذين ارتكبوا جرائم على الأراضي اليوغسلافية.^(٢) وبعد إصدار مجلس الأمن لهذا القرار، تم تكليف الأمين العام للأمم المتحدة بمهمة تحضير مشروع هذه المحكمة الدولية، وأعطيت له مهلة ٦٠ يوماً من تاريخ صدور هذا القرار، لتقديم هذا المشروع إلى مجلس الأمن، وتنفيذاً لذلك أصدر الأمين العام تقريراً ضمن مشروع النظام الأساسي للمحكمة وتعليقاً على مواده.

وبعد ذلك أصدر مجلس الأمن، في عام ١٩٩٣ القرار رقم (٨٢٧) المتضمن إنشاء المحكمة وأقر مشروع الأمين العام دون تعديل، ومن ثم اكتسب المحكمة وجودها القانوني في ٢٥ أيار ١٩٩٣ بمقرها لاهاي، وفي ١٥ أيلول تم انتخاب القضاة، وباشر المدعي العام للمحكمة مهامه عام ١٩٩٤، وأطلق على المحكمة اسم المحكمة الجنائية الدولية ليوغسلافيا سابقاً.^(٣)

وعلى الرغم من العراقيل، التي وضعتها جمهورية يوغسلافيا الاتحادية، أمام عمل المحكمة واضطلاعها بوظائف، سواء فيما يتعلق بالتحقيقات وجمع الأدلة أم تسليم المتهمين، إلا أنها تمكنت من

١ محمد فهاد شلالدة، مصدر سابق، ص ٢٦٣-٢٦٤.

٢ بلال علي النصور ورضوان محمود المجالي، الوجيز في القانون الدولي الإنساني- ما بين الاعتبارات القانونية والسياسية جوانب نظرية وتطبيقية، ط ١، الأكاديميون للنشر والتوزيع، عمان، ٢٠١٢، ص ٢٠٠.

٣ محمود شريف بسيوني، المحكمة الجنائية الدولية- نشأتها ونظامها الأساسي. دار النهضة العربية، القاهرة، ٢٠٠٢، ص ٥٥.

القبض على العديد من كبار المسؤولين في يوغسلافيا سابقا ممن ثبت اتهامهم بارتكاب أو الأمر بارتكاب أي من الجرائم الداخلة في اختصاص المحكمة، على رأسهم الرئيس اليوغسلافي السابق: سلفودان ميلوزوفيتش، الذي سُلِّمَ إلى المحكمة ومثولَ أمامها بعد هزيمته في الانتخابات الرئاسية، وقد استمرت إجراءات محاكمته حتى وفاته في لاهاي في ١١ آذار عام ٢٠٠٦^(١)، وقد نجحت المحكمة منذ انطلاقتها، وحتى أواخر ٢٠١٠ في إنجاز ١٢٦ محاكمة من أصل ١٦١ إتهام قامت بتوجيهه ضد كبار المسؤولين الحكوميين والعسكريين.^(٢)

أما بالنسبة للأزمة الرواندية للمدة من ١٩٩٠ - ١٩٩٣ التي ترجع إلى النزاع المسلح، الذي نشب بين القوات الحكومية وميليشيات الجبهة الوطنية الرواندية، على أثر عدم السماح بمشاركة كل القبائل في نظام الحكم، وبصفة خاصة قبيلة التونسي، إذ كان الحكم بيد قبيلة الهوتو، وقد انتهت محاولات الوساطة، التي قامت بها الدول الأفريقية ومنظمة الوحدة الإفريقية إلى توقيع اتفاق آروشا في ١٩٩٣، فبموجب هذا الاتفاق كان يفترض أن يجري وقف الأعمال القتالية، يتم اقتسام السلطة من قبليتي الهوتو والتوتسي، لكن رغم هذا الاتفاق استمر النزاع المسلح على وتيرته، ولم يظهر في الأفق بوادر تنفيذ بنوده، مما أدى إلى استمرار أعمال العنف.^(٣)

وعلى الرغم من أن الأدلة على ارتكاب أعمال الإبادة في رواندا كانت جلية وواضحة إلا أن مجلس الأمن كان بطيئاً في اتخاذ إجراءاته، فهو طلب من الأمين العام تشكيل لجنة لتزويده بالأدلة على الانتهاكات الخطيرة للقانون الدولي الإنساني، وأعمال الإبادة المرتكبة في رواندا، التي أنشأت بموجب القرار رقم (٩٣٥) الصادر عام ١٩٩٤، التي قدمت تقريرها النهائي مؤكدة فيه على ارتكاب انتهاكات خطيرة للقانون الدولي الإنساني ولا سيما المادة الثالثة المشتركة من اتفاقيات جنيف لعام ١٩٤٩ والبروتوكول الإضافي الثاني لعام ١٩٧٧ الملحق بها من قبل طرفي النزاع المسلح، وأكدت على ارتكاب جرائم ضد الإنسانية وأعمال إبادة، على أثر ذلك قام مجلس الأمن في ٨ شباط من عام ١٩٩٤ بإصدار قراره ذي الرقم (٩٥٥) تحت الفصل السابع من ميثاق الأمم المتحدة الذي أقر بموجبه إنشاء المحكمة الجنائية الدولية الخاصة برواندا.^(٤)

١ عادل عبد الله المسدي، مصدر سابق، ص ٥٣.

٢ علي وهبي ديب، مصدر سابق، ص ٨٠.

٣ علي عبد القادر القهوجي، القانون الدولي الجنائي. ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠١، ص ٢٩٥.

٤ علي وهبي ديب، مصدر سابق، ص ٨٣-٨٤.

أما بالنسبة لمحكمة رواندا فإن غياب الدعم من قبل الحكومة الرواندية أدى إلى تأخير في انطلاق أعمال المحكمة بشكل فعال، هذا فضلاً عن عدد من العوائق اللوجستية والإدارية والمالية، ففي الوقت، الذي كانت فيه محكمة رواندا تركزها على كبار المسؤولين المخططين والمحرضين على ارتكاب الجرائم، كان ٧٥٠٠٠ رواندي أصبحوا معتقلين في السجون الرواندية منذ تغيير نظام الحكم فيها.^(١) لكن رغم ذلك أصدرت محكمة رواندا العديد من الأحكام على الأشخاص المتورطين في ارتكاب جرائم الإبادة والجرائم ضد الإنسانية، ففي أوائل ٢٠١٤ كانت المحكمة قد أصدرت أحكام نهائية بالإدانة في ٣٨ قضية، وحكمت بالبراءة في ٨ قضايا وكانت ١٩ قضية لا تزال منظورة أمام الدائرة الاستئنافية، في حين كان هناك ١٠ قضايا لا تزال في مرحلة المحاكمة، وقضية واحدة في انتظار الإجراءات، ومن أمثلة هذه الأحكام الحكم النهائي بالسجن المؤبد على جون بول أكايسو في ٢ تشرين الأول ١٩٩٨، والحكم النهائي الصادر بالسجن المؤبد ضد الفريد موسيما في ١٦ كانون الأول ٢٠٠١، والحكم بالسجن لمدة ١٥ عام على سيمون بيكيندي في ٢ كانون ٢٠٠٨.^(٢)

وقد وجه انطونيو كاسيزي انتقادات للمحكمة لتبنيها معيار السيطرة الفعالة في القرار الذي أصدرته بخصوص الإبادة الجماعية، وقال عنه بأنه معيار غير واقعي من الإثبات. وفيما يخص المسؤولية الدولية عن الهجمات السيبرانية، أشار كرامر وماركوف إلى أن معيار السيطرة الفعالة فعال في تحديد جزء من المسؤولية الدولية، وليس كلها، ويُعتمد على ذلك من خلال تبني اتفاقيات دولية تكون كل من روسيا وأمريكا أطراف فيها من أجل تحديد المسؤولية التي تنشأ عن الهجمات السيبرانية. ومن أجل تأكيد ضرورة الملاحقة الجنائية والمحاكم الجنائية ضد من يرتكب الهجمات السيبرانية وبشكل خاص حين يتعلق بحفظ الأمن والسلام الدوليين أشار القاضي ستين جولبيرج إلى أن عدم وجود محاكم جنائية أو دولية تختص بملاحقة الأشخاص أو الدول المسؤولة عن ارتكاب جرائم الهجمات السيبرانية الشديدة الخطورة على الصعيد الدولي معناه أن عدداً كبيراً من منفعدي الهجمات السيبرانية الخطيرة سيكونون بعيدين عن العقاب.^(٣)

١ علي وهبي ديب، مصدر سابق، ص ٩٥-٩٦.

٢ عادل عبد الله المسدي، مصدر سابق، ص ٦٢.

٣ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص ٧٢.

عندما تبرم اتفاقيات متعددة الأطراف تقوم بحظر تقديم الدعم إلى الجماعات المسلحة من قبل الدول الأطراف، أمر يمهّد الطريق نحو محاكم جنائية دولية من أجل أن تتحرك وتلاحق المتهمين عندما يرتكبون انتهاكات خطيرة تتسبب بها الهجمات السيبرانية.^(١)

ونستخلص مما سبق: إن المحاكم الجنائية الدولية الخاصة (محكمتي يوغسلافيا ورواندا) تمثل واحدة من أهم الآليات القانونية للقضاء الدولي الجنائي، على الرغم من أنها لا تخلو من السلبيات إذ تتأثر بالاعتبارات السياسية، و أنها تتبع مجلس الأمن، بحكم طبيعتها فهي تُعد واحدة من الأجهزة الفرعية التابعة للمجلس، الأمر الذي قد يؤدي إلى عدم الحيادية والاستقلال القضائي، ولا سيّما وأن مجلس الأمن تحتكره الدول الأعضاء الخمسة، إلا أنها -المحاكم- تُعد انعطافة مهمة في تاريخ القانون الدولي الجنائي، وذلك من خلال اعترافها بالعديد من المبادئ القانونية، وتقنينها للجرائم الدولية، ومحاولتها لمنتَهكي القواعد القانونية للنزاعات المسلحة ومعاقبته، وهذا قد مهد الطريق إلى إنشاء محكمة جنائية دولية دائمة.

يتضح لنا: من خلال تتبع التجارب التاريخية للمحاكم الدولية المؤقتة، مثل المحكمة الجنائية الدولية ليوغسلافيا السابقة والمحكمة الجنائية الدولية لرواندا، أنها أسهمت في تأسيس مرجعية قانونية وقضائية مهمة لمساءلة الأفراد عن انتهاكات القانون الدولي الإنساني، بما في ذلك الاعتداء على الممتلكات الثقافية والدينية. وعلى الرغم من أن اختصاص هذه المحاكم ركّز في المقام الأول على الجرائم ضد الإنسانية وجرائم الحرب والإبادة الجماعية، فإنها أرست مبادئ قانونية مهمة، من بينها عدم جواز استهداف الأعيان المدنية والمواقع المحمية، وأكدت على أن تدمير هذه المواقع لا يُعد انتهاكاً لقواعد السلوك في الحرب فحسب، بل قد يكون جزءاً من استراتيجية تطهير ثقافي أو ديني. وقد أدت هذه المحاكم دوراً تمهيدياً في بناء الفقه الدولي المتعلق بحماية الممتلكات الثقافية والدينية، وأسهمت في تفسير بعض المواد في اتفاقيات جنيف والبروتوكولات الإضافية، بل وشكّلت تمهيداً لإنشاء المحكمة الجنائية الدولية الدائمة، التي أولت لاحقاً اهتماماً أكبر بهذا النوع من الجرائم. غير أن محدودية اختصاص هذه المحاكم زمانياً ومكانياً، وعدم امتداد صلاحياتها إلى نزاعات لاحقة أو مناطق أخرى، قلّل من الأثر العملي المستدام لدورها في حماية المواقع المحمية، لا سيّما في ظل النزاعات المتصاعدة بعد مدة عمل هذه المحاكم.

١ أحمد عبيس الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق ، ص ٧٥-٧٦.

يرى الباحث: أن المحاكم الدولية المؤقتة أدت دوراً تأسيسياً مهماً في تطوير مفاهيم الحماية القانونية للمواقع المحمية في أثناء النزاعات المسلحة، وأسهمت في تحويل الانتهاكات، التي كانت تُعد في الماضي أفعالاً هامشية أو أضراراً جانبية إلى جرائم موصوفة تستوجب المساءلة. وقد أظهرت هذه المحاكم، من خلال اجتهاداتها القضائية، أن الاعتداء على الممتلكات ذات الطابع الثقافي أو الديني لا يقل خطورة عن الاعتداء على الأرواح، لأنه يمثل استهدافاً مباشراً لهوية الجماعات ووجودها التاريخي والمعنوي. وأن أهمية هذه المحاكم لا تكمن فقط في القضايا التي نظرت فيها، بل أيضاً في الرسائل القانونية والسياسية، التي أرسلتها للعالم، والمتمثلة في أن الإفلات من العقاب لم يعد ممكناً مهما طال الزمن، وأن القانون الدولي قادر على ملاحقة مرتكبي الانتهاكات حتى في سياقات معقدة. ومع ذلك، فإن الباحث لا يغفل التحديات، التي رافقت عمل هذه المحاكم، مثل تأخر تأسيسها، وتعقيد الإجراءات، ومحدودية التمثيل الجغرافي، وغياب آليات تنفيذ قراراتها في بعض الأحيان. وأن هناك حاجة لاستثمار إرث هذه المحاكم وتطويره، سواء من خلال تضمين مبادئها في أنظمة المحكمة الجنائية الدولية الدائمة، أم من خلال التفكير في إنشاء آليات مؤقتة متخصصة في النزاعات الحديثة، تهتم تحديداً بجرائم تدمير المواقع المحمية، بما ينسجم مع تطور طبيعة النزاعات واتساع رقعة الانتهاكات الموجهة ضد التراث الثقافي والديني. وأن حماية المواقع المحمية لا تتحقق فقط من خلال النصوص، بل تتطلب أجهزة قضائية فعالة، تملك الإرادة والقدرة على المساءلة، وهو ما أظهرته المحاكم المؤقتة رغم محدودية اختصاصها، مما يسوّغ الحاجة إلى توسيع هذا النموذج، وتكييفه مع المتغيرات الدولية الراهنة.

الفرع الثاني

دور المحاكم الدولية في تعزيز الحماية للمواقع المحمية في الهجمات السيبرانية

في ظل تصاعد وتيرة النزاعات المسلحة المعاصرة، تبرز أهمية الحماية القانونية الدولية للمناطق المحمية بموجب أحكام القانون الدولي الإنساني كآلية أساسية لحفظ الكرامة الإنسانية وضمان الحد الأدنى من متطلبات الحماية في زمن الحرب. وتختلف هذه المناطق جوهرياً عن مفهوم المناطق المحمية البيئية، إذ تركز الحماية هنا على المناطق المدنية والعسكرية المحظورة، التي أقرتها المواثيق الدولية، كالمستشفيات والمناطق الآمنة والمواقع الثقافية، على وفق نظام قانوني متكامل تضمنته اتفاقيات جنيف الأربع ١٩٤٩ وبروتوكولاتها الإضافية ١٩٧٧.

تشكل المحاكم الدولية ركيزة أساسية في تفعيل الحماية القانونية لهذه المناطق من خلال ثلاث مستويات: تفسيرية من خلال توضيح نطاق الحماية المقررة، ورقابية عبر محاسبة الانتهاكات، وتطويرية بإرساء سوابق قضائية تعزز المنظومة الحمائية. وتتجلى هذه الأدوار في اجتهادات محكمة العدل الدولية في القضايا الاستشارية المتعلقة بالحماية، وأحكام المحكمة الجنائية الدولية في مقاضاة جرائم الحرب المرتكبة ضد المناطق المحمية. تواجه المنظومة القضائية الدولية تحديات جسيمة في هذا المجال، أبرزها إشكالية الإثبات في النزاعات المعاصرة، وتعارض الاختصاصات القضائية، والتنازع بين مبدأ السيادة الوطنية والالتزامات الدولية، وتظهر معضلة التطبيق العملي للأحكام في ظل تعدد الفاعلين غير الدوليين في النزاعات الحديثة.

أولاً: المحكمة الجنائية الدولية: كانت هناك محاولات سابقة لإنشاء محكمة جنائية دولية دائمة من قبل عصبة الأمم ١٩١٩، ومنظمة الأمم المتحدة ١٩٤٥ إلا أنها باءت بالفشل، واستمر هذا الأمر حتى نهاية الحرب الباردة، وبشكل خاص عام ١٩٨٩ عندما طلبت الجمعية العامة للأمم المتحدة من لجنة القانون الدولي التابعة لها دراسة مشروع إنشاء محكمة جنائية دولية دائمة، فتكرر الطلب لأكثر من سنة حتى ظهور المحاكم الجنائية الدولية الخاصة، فقامت لجنة القانون الدولي بعرض مشروع إنشاء المحكمة الجنائية الدولية عام ١٩٩٤.^(١)

أنشأت الجمعية العامة للأمم المتحدة في عام (١٩٩٤) لجنة متخصصة تقوم باستعراض القضايا الرئيسية الفنية والإدارية، والنظر في الترتيبات اللازمة لعقد اتفاقية دولية حول إنشاء المحكمة الجنائية الدولية، وفي ١٩٩٥ قررت الجمعية العامة إنشاء لجنة تحضيرية لإجراء المزيد من المناقشات حول الموضوع. وفي ١٩٩٦ قررت الجمعية العامة أن يعقد مؤتمر دبلوماسي للمفوضين عام ١٩٩٨ بغرض اعتماد اتفاقية دولية بشأن المحكمة الجنائية الدولية. وقد انتهت اللجنة التحضيرية من إعداد مشروع الاتفاقية المتعلقة بإنشاء المحكمة الجنائية الدولية، وإحالة إلى المؤتمر في ١٩٩٨. اجتمع المؤتمر في مقر منظمة الأمم المتحدة للأغذية والزراعة في روما، وقد شاركت في المؤتمر وفود ١٦٠ دولة، وقد حضر بصفة مراقب ممثلو المنظمات الحكومية وغير الحكومية. واعتمد المؤتمر في ١٩٩٨ النظام الأساسي للمحكمة، وفتح باب التوقيع عليه حتى ٢٠٠٠، فتح التصديق عليه وبلغ عدد

١ بلال علي النصور ورضوان محمود المجالي، الوجيز في القانون الدولي الإنساني-ما بين الاعتبارات القانونية والسياسية، ط١، الأكاديميون للنشر والتوزيع، الأردن، ٢٠١٢، ص ٢٠٠-٢٠٤.

الدول الموقعة والمصدقة على نظام روما الأساسي للمحكمة الجنائية الدولية ١٣٩ توقيعاً و ٩٤ تصديقاً، الذي دخل حيز النفاذ بتاريخ ٢٠٠٢ عندما بلغ عدد الدول المصدقة ٦٠ دولة.^(١)

عرفت المادة الأولى من النظام الأساسي للمحكمة الجنائية الدولية تلك المحكمة بأنها هيئة دائمة لها السلطة لممارسة اختصاصها على الأشخاص بإزاء أشد الجرائم خطورة محل الاهتمام الدولي، وتكون المحكمة مكملة للولايات القضائية الجنائية الوطنية، وتخضع اختصاصها، وأسلوب عملها لأحكام هذا النظام الأساسي، من خلال التعريف يمكن استفتاء خصائص تلك المحكمة المتمثلة في:

١. **المحكمة الجنائية الدولية:** هي هيئة قضائية دولية أنشئت بموجب معاهدة دولية بغض التحقيق ومباشرة الإجراءات القضائية كاملة ضد المهتمين لذين يرتكبون أشد الجرائم خطورة. وللمحكمة صفة الدوام، وليست منشأة، لغرض خاص أو لمدة زمنية محددة و هو الحال في المحاكم.

تضطلع المحكمة الجنائية الدولية بدور محوري في تعزيز الحماية القانونية للمناطق المحمية في أوقات النزاعات المسلحة، ويزداد هذا الدور أهمية مع التحول البنوي الذي طرأ على طبيعة العمليات العدائية، لا سيما مع اتساع نطاق استخدام الوسائل السيبرانية في الحروب. وعلى الرغم من أن الهجمات السيبرانية لم تُذكر صراحة في نصوص نظام روما الأساسي لعام ١٩٩٨، فإن التطورات التقنية المتسارعة والآثار المترتبة على هذه الهجمات، خصوصاً حين تستهدف مستشفيات أو مراكز إغاثة أو مناطق منزوعة السلاح، أوجبت تأويلاً موسعاً لنطاق الجرائم الدولية، بحيث تشمل الأفعال التي تؤدي من خلال الوسائل الرقمية إلى ذات النتائج التي تتجم عن الأفعال المادية التقليدية، وذلك استناداً إلى القاعدة الفقهية بأن الحظر القانوني في القانون الجنائي الدولي ينصرف إلى النتيجة لا إلى الوسيلة المستخدمة لتحقيقها.

إن المعيار الحاكم في تقييم مدى خضوع الهجمات السيبرانية لاختصاص المحكمة لا يتعلق فقط بوسيلة الاعتداء، بل بمدى تحقق الأثر المحظور قانوناً. وهذا ما أكدته المادة الثامنة من نظام روما، التي تنص على أن تعدد شن هجمات ضد المباني المخصصة للأغراض الإنسانية، كالمستشفيات ومراكز الإغاثة، يُعد جريمة حرب، متى لم تُستخدم تلك المنشآت في أعمال عسكرية^(٢). وعلى وفق التفسير الغائي لهذه المادة، فإن هجوماً سيبرانياً يعطل أجهزة الرعاية الطبية، أو يؤدي إلى حرمان المدنيين من خدمات إنسانية أساسية، يعد عدواناً محظوراً، حتى وإن لم يخلف دماراً مادياً ظاهراً. وقد أيدت المدعية العامة

١ محمد فهاد شلالدة، مصدر سابق، ص ٣٧-٣٧٣.

٢ ينظر: المادة: (٢/٨) نظام روما الأساسي للمحكمة الجنائية الدولية.

السابقة للمحكمة، فاتو بنسودا، هذا التوجه في بيان رسمي صدر عام ٢٠١٩، حين أكدت أن "الأفعال السيبرانية التي تقع في سياق نزاع مسلح، وتُفْضي إلى آثار مدمرة تمس المدنيين أو البنى التحتية الحيوية، قد تُشكّل جرائم تدخل ضمن ولاية المحكمة"^(١).

ومن النماذج الواقعية الدالة على خطورة الهجمات السيبرانية على المناطق المحمية، ما شهده النظام الصحي في الولايات المتحدة خلال عام ٢٠٢٠ من هجوم واسع ببرمجية الفدية المعروفة باسم Ryuk، والذي أدى إلى تعطيل مستشفيات وتأجيل عمليات طبية، بل وسُجّلت وفيات ناتجة عن شلل الخدمات^(٢). ورغم أن هذا الهجوم وقع في سياق سلمي، فإن تكراره في بيئة نزاع مسلح، كالمناطق المحتلة أو مناطق النزاع الأهلي، سيستوجب إخضاعه لقواعد القانون الدولي الإنساني، وقد يُكَيّف بوضوح كجريمة حرب، طالما استهدفت منشآت محمية وأدت إلى نتائج جسيمة بحق السكان المدنيين. أما من حيث الولاية القضائية، فتملك المحكمة الجنائية الدولية صلاحية النظر في الجرائم السيبرانية متى وقعت في دولة طرف، أو ارتكبتها مواطن من دولة طرف، أو إذا أُحيلت إلى المحكمة من قبل مجلس الأمن. وقد تناولت مجموعة خبراء الأمم المتحدة بشأن الأمن السيبراني في تقريرها لعام ٢٠٢١ مدى إمكانية مساءلة الدول والأفراد عن الأفعال السيبرانية العدائية التي تؤثر على المدنيين في سياق النزاع^(٣). وتشمل هذه الصلاحية الجرائم غير التقليدية، طالما أمكن إثباتها بالأدلة الرقمية، وهو ما يتطلب تطوير آليات الإثبات، كتتبع المصدر الرقمي (IP attribution)، وربط الفعل بمخرجاته الجنائية.

وإلى جانب المسؤولية الفردية التي تطل القراصنة أو مسؤولي الأنظمة العدائية، قد تُفَعّل المحكمة مبدأ المسؤولية القائية إذا ثبت أن قادة عسكريين أو سياسيين خططوا أو غصّوا الطرف عن هجمات سيبرانية ضد مناطق محمية. وقد أيدت المحكمة هذا النوع من المسؤولية في قضية باندا وجيروبو بشأن

1 Original Title : "Statement by the Prosecutor of the International Criminal Court, Ms Fatou Bensouda, on Cyber Warfare and International Criminal Law "

2 NPR, "Ransomware Attack Hits U.S. Hospitals," National Public Radio, October 29, 2020.

متاح على الرابط : <https://www.npr.org/2020/10/29/929105788/ransomware-attack-hits-u-s-hospitals>

3 United Nations Group of Governmental Experts (UN GGE), "Report on Developments in the Field of Information and Telecommunications in the Context of International Security," A/76/135, July 20215 <https://undocs.org/A/76/135> متاح على الرابط

دارفور، إذ أُدين المتهمان عن أفعال ارتكبتها مرؤوسوهم دون اتخاذ تدابير فعالة لمنعها أو معاقبة مرتكبيها^(١).

تؤكد هذه التطبيقات أن المحكمة الجنائية الدولية تُعد جهازاً قضائياً قادراً من الناحية المفاهيمية والوظيفية على مساءلة مرتكبي الجرائم السيبرانية ضد المناطق المحمية. إلا أن هذا الدور لن يكتمل إلا بتطوير أدوات التحقيق، وتعزيز التعاون مع الجهات التقنية المتخصصة، وتضمين الهجمات الرقمية في لائحة الجرائم الدولية الجسيمة. ورغم غياب سوابق قضائية نهائية حتى اللحظة في هذا المجال، فإن التوجهات الحديثة والبيانات الرسمية والممارسات القضائية المتنامية تؤسس جميعها لإمكانية التوسع القضائي النوعي، بما يتماشى مع متطلبات الحرب الرقمية المعاصرة، ويضمن فعالية الحماية المقررة للمناطق المحمية بموجب القانون الدولي الإنساني

في تطور نوعي يعكس تعاظم أهمية الفضاء السيبراني في سياق النزاعات المسلحة الحديثة، أكد المدعي العام للمحكمة الجنائية الدولية، السيد كريم خان، أن مكتبه يُجري حالياً تحقيقاً رسمياً في الهجمات السيبرانية التي استهدفت البنية التحتية المدنية الحيوية داخل أوكرانيا، وذلك في إطار النظر في مدى إمكانية تكيف تلك الأفعال كجرائم حرب تخضع لاختصاص المحكمة^(٢).

ويستند هذا التوجه إلى قاعدة راسخة في القانون الدولي الإنساني، مفادها أن الهجمات التي تُوجه ضد الأعيان المدنية، أو تُحدث آثاراً مادية أو إنسانية جوهريّة على السكان المدنيين، قد ترقى إلى مستوى الانتهاك الجسيم، لا سيما حين تكون متعمدة، وتهدف إلى تعطيل خدمات أساسية كالمياه والكهرباء والمرافق الصحية. وبحسب التقارير الصحفية الموثوقة، فقد شملت التحقيقات استهداف أنظمة الكهرباء، ومحطات معالجة المياه، وشبكات الاتصالات المدنية، وهي منشآت تدرج صراحة ضمن الأعيان المحمية بموجب المواد ٥٢ و ٥٤ و ٥٥ من البروتوكول الإضافي الأول لعام ١٩٧٧ لاتفاقيات

1 International Criminal Court (ICC), Prosecutor v. Banda and Jerbo, ICC-02/05-03/09,

متاح على الرابط <https://www.icc-cpi.int/cases/uganda/darfur/banda-jerbo> 2014

٢ Euractiv.com (بالتعاون مع Reuters)، "المحكمة الجنائية الدولية تحقق في الهجمات السيبرانية على البنية التحتية الأوكرانية بوصفها جرائم حرب محتملة"، ٢٠٢٤.

<https://www.euractiv.com/section/global-europe/news/icc-probes-cyberattacks-in-ukraine-as-possible-war-crimes>

جنيف، والتي تحظر أي هجوم من شأنه حرمان السكان المدنيين من الوسائل الضرورية لبقائهم على قيد الحياة^(١).

ويرى الباحث: قد تكتسب هذه التحقيقات أهمية خاصة لكونها تمثل أول محاولة من نوعها لتوسيع نطاق المساءلة الجنائية الدولية ليشمل الهجمات السيبرانية التي تُفرض على البيئة الإنسانية. وإذا ثبت توافر القصد الجنائي والركن المادي وفق المادة ٨ من نظام روما الأساسي، فإن مرتكبي هذه الأفعال قد يخضعون للمساءلة بصفتهم مسؤولين عن ارتكاب جرائم حرب، بصرف النظر عن الوسيلة المستخدمة – سواء أكانت تقليدية أم رقمية.

إن هذا التوجه يعكس تحولاً قضائياً في فهم طبيعة "الاعتداء" في القانون الدولي، من كونه فعلاً مادياً محضاً إلى كونه سلوكاً ضاراً متى ما استهدف الكيانات أو الأشخاص المحميين، ونتج عنه أثر إنساني جسيم. كما يمكن أن يشكل ذلك سابقة قضائية تتيح لاحقاً محاكمة الأفراد أو الجهات الفاعلة من غير الدول التي تمارس هذا النوع من العدوان السيبراني على المناطق المحمية.

٢. المحاكم الجنائية المؤقتة: ينعقد للمحكمة اختصاص محدد بنوع من الجرائم ذات خطورة إجرامية شديدة وورد حصرها في النظام الأساسي للمحكمة، وهي جريمة الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب وجريمة العدوان.

ويأتي دور المحكمة الجنائية الدولية مكمل للنظم القضائية الوطنية في ممارسات اختصاصات المحكمة، إذ إن الاختصاص الجنائي الوطني دائماً ما يكون له الأولوية على اختصاص المحكمة الجنائية الدولية، إلا أن المحكمة الجنائية الدولية تستطيع ممارسة اختصاصها في حالتين فقط هما: انهيار النظام القضائي الوطني، وعدم رفض أو فشل النظام القضائي الوطني في القيام بالتزاماته القانونية بالتحقيق ومحاكمة الأشخاص المشتبه في ارتكابهم إحدى الجرائم، التي تدخل في اختصاص المحكمة.^(٢)

ومن أهم القضايا التي أُحيلت للمحكمة الجنائية الدولية بخصوص الانتهاكات الموجهة للمناطق المحمية، هي قضية أوغندا إذ أحال الرئيس الأوغندي في أوغندا إلى المحكمة الجنائية الدولية عام ٢٠٠٣، تلك الإحالة التي تم الاعلان عنها بشكل علني من جانب الرئيس الأوغندي والمدعي العام

١ ينظر: المواد (٥٢ و ٥٤ و ٥٥،) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧، المتعلقة بحماية الأعيان المدنية والبيئة الطبيعية في النزاعات المسلحة. انظر أيضاً: **International Committee of the Red Cross (ICRC), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva, 1987**.

٢ أشرف محمد لاشين، النظرية العامة للجريمة الدولية. منشأة المعارف، الإسكندرية، ٢٠٢٠، ص ٦٦٧ .

للمحكمة الجنائية الدولية في ٢٠٠٤، وبناء على ما سبق أحال رئيس المحكمة الجنائية الدولية الوضع في أوغندا إلى الدائرة التمهيدية الثانية.^(١)

فضلاً عن هذه القضية المحالة على المحكمة الجنائية الدولية بخصوص انتهاك المناطق المحمية، فقد أُحيلت عديد من القضايا على المحكمة الجنائية الدولية لانتهاكها للمناطق المحمية ومنها الوضع في جمهورية الكونغو الديمقراطية، الوضع في جمهورية إفريقيا الوسطى والوضع في دولة مالي، أيضاً، فضلاً عن الحالة في كل من دارفور - السودان وليبيا، وذلك قيام المدعي العام من تلقاء نفسه بفتح التحقيق في الجرائم والانتهاكات، التي ارتُكبت في كل من كينيا وكوت ديفوار.

أما مؤخراً في العام ٢٠٢٤ أصدرت المحكمة الجنائية الدولية قراراً يقضي باعتقال رئيس وزراء الكيان الصهيوني بنيامين نتنياهو ووزير حربه يوآف غالانت بناءً على المطالبات الداعية إلى تحرك المحكمة الجنائية والدعوى المقدمة من قبل جمهورية جنوب إفريقيا، مما جعل المدعي العام في المحكمة بتقديم طلبات لاستصدار أوامر قبض لاعتقال المتهمين آنفي الذكر من الدائرة التمهيدية الأولى في ٢٠ أيار/ مايو ٢٠٢٤ وان هذه القرارات قد صدرت على خلفية العدوان، الذي يقوده الكيان الصهيوني ضد قطاع غزة منذ السابع من تشرين الأول/ أكتوبر من عام ٢٠٢٣، الذي أودى بحياة الكثيرين ممن هم محميون بموجب القانون الدولي الإنساني خلال النزاعات المسلحة.

وعلى وفق نظام روما الأساسي وملحقاته اتاحت المحكمة للدول الأعضاء فيها وخبراء القانون الدولي تقديم المداخلات والملاحظات حول الطلبات التي قدمها المدعي العام واختصاص المحكمة فيما يخص العدوان على غزة والجرائم المرتكبة فيه، واستقبلت المحكمة كثيراً من الطلبات في هذه السياق وقدمت المحكمة دفوعها القانونية، ومن أبرز الطلبات، التي قدمت هي الطعن في اختصاص المحكمة، وأخرى دعت إلى إشعار الكيان الصهيوني ثانيةً ببدء التحقيقات، التي تسير بها المحكمة وإيقاف أوامر اعتقال نتنياهو وغالانت. وفي ٢١ تشرين الثاني/ نوفمبر من عام ٢٠٢٤ صدر عن الدائرة التمهيدية الأولى في المحكمة ذاتها قرارين بالإجماع وإصدار مذكرة اعتقال بالصيغة السرية^(٢)، ضم القرار الأول بيان السبب الذي دعا المحكمة الجنائية إلى رفض الطعونات، التي قدمت حول اختصاصها بالنظر في هذا النزاع، بينما اشتمل القرار الثاني على الرد على طلب الكيان الصهيوني بإشعار جديد من المحكمة،

١ عادل عبد الله المسدي، مصدر سابق، ص ٢٩٥-٢٩٦.

٢ المركز العربي للأبحاث ودراسة السياسات، وحدة الدراسات السياسية، أوامر الاعتقال بحق نتنياهو وغالانت الصادرة عن المحكمة الجنائية الدولية: السياقات والتداعيات، قطر، ٢٠٢٤، ص ١.

يعنى بالإجراءات التي ستتخذها بغية إيقاف الإجراءات القانونية -طلب الاعتقال- بحق نتنياهو وغالانت على وفق المادتين (١٨ - ١٩) من نظام روما الأساسي.

كان مضمون القرارات الصادرة عن المحكمة الجنائية الدولية بان قررت المحكمة في القرار الأول أن موافقة إلكيان الصهيوني لولاية المحكمة لم يكن ضرورياً، لأن المحكمة لها صلاحية ممارسة اختصاصها على وفق الاختصاص الإقليمي لفلسطين بصفتها دولة عضو في هذه المحكمة والتي ارتكبت على أراضيها جرائم تدخل ضمن اختصاصها، أما القرار الثاني قد بيّن أن المدعي العام في المحكمة قد أخطر إلكيان الصهيوني قبل أن تبدأ المحكمة بالتحقيق عام ٢٠٢١، وهذا ما ينفي الضرورة إلى اشعار إلكيان الصهيوني مرة أخرى بخصوص الإجراءات، التي ترى المحكمة ضرورة اتخاذها أو سبب لإيقاف أوامر الاعتقال.

وصنف أمرا القبض (بالسرية) حماية للشهود وضماناً لسير التحقيقات، وأقرّت المحكمة أن سلوك ممثلي إلكيان الصهيوني الاجرامي يقع من اختصاصها، واختصاصها هذا يطول غزة والضفة الغربية حتى القدس الشرقية، فضلاً عن ذلك أن المحكمة وجدت أسباباً دامغة جعلتها تعتقد أن نتنياهو وغالانت هما المسؤولان استناداً إلى موقعيهما في سلسلة المسؤولية عن اصدار القرار عن الجرائم الآتية معتبرة إياهم مشاركين في الجناية مع الآخرين:

بجريمة الحرب، التي تمثلت في تجويع المدنيين كأسلوب من أساليب الحرب، وشن هجوم ضد المدنيين من السكان وجرائم ضد الإنسانية متمثلة في القتل والاضطهاد، وغيرها من الاعمال اللاإنسانية وقصف المستشفيات واعتقال الطواقم الطبية وقصف دور العبادة.

ثانياً: محكمة العدل الدولية

إن محكمة العدل الدولية كانت تسعى دائماً إلى توطيد وتثبيت مبادئ القانون الدولي الإنساني، التي انشأها ميثاق الأمم المتحدة مانحاً إياها الصفة القضائية وعدّها الجهاز القضائي الرئيسي، الذي يعرض أمامه قضايا الدول الأطراف، ويكون الفصل في النزاعات الدولية التي تعرض عليها على وفق مبادئ القانون الدولي والاتفاقيات الدولية سواء أكانت خاصة أو عامة وكذلك بإمكانها الركون إلى العرف الدولي على لأنه من الممارسات العامة، بصفته قانوناً بحسب ما نصت عليه المادة (١/٣٨) من النظام الأساسي للمحكمة. وأن الزامية قرارات المحكمة بين أعضائها المتنازعين في قضية ما معروضة عليها، إذ إن أحكامها نهائية وملزمة ولا تقبل الاستئناف، وفي حال تبين لدولة ما أن لها مصلحة ما في القضية المنظورة من قبل المحكمة جاز للدولة أن تسأل المحكمة السماح لها أن تتدخل

في تلك القضية وذلك عبر طلب تقدمه للمحكمة، وعلى المحكمة أن تثبت بهذا الطلب، وللمحكمة أن تبدي رأياً استشارياً في مسألة قانونية بناءً على أي طلب من قبل جهة مخولة بتقديم الطلب بموجب ميثاق الأمم المتحدة.

وتجدر الإشارة إلى أن لمحكمة العدل الدولية اصدار نوعين من القرارات، الأول يتمثل بالقرارات القضائية وعند عدم الاستجابة لتنفيذها تتحمل الدولة، التي صدر القرار ضدها الاثار التي ترتبها المسؤولية الدولية، والثاني يتمثل بالآراء الاستشارية إبتدي المحكمة الدولية رأيها، وتقدم وجهة نظرها حول موضوع أو نزاع معين ولا يشترط لهذا النوع من القرارات تنفيذه، ولكنه يستخدم كوسيلة ضغط سياسية يمكن أن تحقق منفعة أو مصلحة مستقبلاً^(١).

وحرصت المحكمة في كثير من آرائها الاستشارية في العديد من القضايا المعروضة امامها على التذكير بضرورة احترام المبادئ الإنسانية، التي يعنى بها قانون النزاعات المسلحة، مثلما جاء بأول حكم صدر عنها في قضية (قناة كورفو)، وأنها سعت للحفاظ على الالتزامات الواجبة على جميع الدول عبر الكثير من احكامها التي تطرقت لها في احكام مختلفة ارتبطت بالقانون الدولي الإنساني كالحقوق الإنسانية الأساسية وحق الشعوب في ان تقرر مصيرها وحظر التهديد بالقوة أو استخدام القوة، إذ إن أول ما أشارت إليه المحكمة هي الالتزامات الضرورية الواجبة التي تلزم الجميع فيما يتعلق بالإبادة الجماعية، إذ أوردت في أحد آرائها الاستشارية حول تحفظها على اتفاقية منع جرائم الإبادة الجماعية ومعاقبة مرتكبيها المؤرخة في ٢٨ آيار/ مايو ١٩٥١، إذ إنها أقرت ضمناً وأشارت إلى طبيعة الاتفاقية الخاصة بأن حظر جريمة الإبادة الجماعية، هو من الواجبات التي تلزم الجميع^(٢).

وأن قرارات محكمة العدل الدولية القضائية هي ملزمة وترتب على عدم الالتزام بها مسؤولية دولية بينما النوع الثاني، والذي هو رأي استشاري للمحكمة بناءً على طلب من دولة ما حول مسألة ما أو خلاف ما وعلى اقتراح من الجمعية العامة للأمم المتحدة، وليس لقرار المحكمة الاستشاري قوة إلزام تنفيذية، لكنه قد ينفذ كوسيلة ضغط سياسية لينتفع منها في تحقيق بعض المكاسب مستقبلاً.

وقد طلبت الجمعية العامة للأمم المتحدة من محكمة العدل الدولية أن تبدي رأيها الاستشاري بخصوص الوضع القانوني للجدار الفاصل الذي بنته إلكيان الصهيوني في فلسطين المحتلة في ٩ تموز

١ النظام الأساسي لمحكمة العدل الدولية.

٢ ياسمين أحمد إسماعيل صالح، دور المحكمة العدل الدولية في تطوير قواعد القانون الدولي الإنساني وضمان الالتزام بمبادئه، مجلة كلية السياسة والاقتصاد، جامعة بنى سويف، العدد (٣)، مصر، ٢٠١٩، ص ١٨٠.

٢٠٠٤، صدر قرار محكمة العدل الدولية بأغلبية الأصوات أن هذا الجدار قد خالف القانون الدولي وطالبت المحكمة الكيان الصهيوني بإزالته من الضفة الغربية وحتى القدس الشرقية، وعليها ان تعوض المتضررين الفلسطينيين جراء هذا الجدار، وأن القرار لم يشر إلى المسجد الأقصى صراحة وإنما تتأول بعض العبارات كعبارة المقدسات في أكثر من موضع، إذ أكدت الفقرة ١٢٨ و ١٤٧ من القرار على ضرورة تمكين الوصول الحر للاماكن المقدسة والمباني والمواقع الدينية مؤكداً على حرية العبادة. (١)

ومن القضايا الأشهر، التي عرضت أمام محكمة العدل الدولية خلال الحرب الفلسطينية ضد الكيان الصهيوني في غزة هي الدعوى التي رفعتها جنوب افريقيا في كانون الأول/ ديسمبر ٢٠٢٣ ضد الكيان الصهيوني لانتهاكاته اتفاقية جنيف الأربع لعام ١٩٤٩ وإلى جانب مطالبة المحكمة باستصدار حكماً نهائياً على الاعمال الكيان الصهيونية في غزة، قدمت جنوب افريقيا طلباً ايضاً يقتضي بفرض تدابير مؤقتة في أثناء ذلك الوقت نظراً للمخاوف الإنسانية الطارئة، وفي كانون الثاني/ يناير ٢٠٢٤ قضت المحكمة بالزام الكيان الصهيوني بتنفيذ بعض هذه الإجراءات، التي تضمنها طلب جنوب افريقيا، التي كانت معنية بسماع وصول المعونات الإنسانية، ومنع سلوك التطرف فيما يخص التحريض على الإبادة الجماعية على الفلسطينيين وقضايا مشابهة. بالمقابل لم ترفض الكيان الصهيوني ان تقدم تقارير مباشرة إلى المحكمة توضح التزامها بأوامر المحكمة، لكن مع الملاحظة أنه لم تنشر هذه التقارير.

واستدركت جنوب افريقيا لاحقاً بأن قدمت طلبات ثلاثة أخرى لفرض تدابير مؤقتة إضافية واجراء التعديلات على التدابير القائمة لما قامت به الكيان الصهيوني من هجمات عسكرية أثر اجتياحها رفح وغيرها من الأحداث الجديدة. بينما المحكمة رفضت الطلبات مسببةً ذلك أن الكيان الصهيوني امتثالاً إلى طلب الإبلاغ الأصلي. وبعد قضية جنوب افريقيا أقامت نيكارغوا إجراءات مشابهة ضد المانيا معتبرةً إياها قد خالفت الالتزام المنصوص عليه في اتفاقية جنيف الأربع ١٩٤٩ ببذل كل ما بوسعها لمنع ارتكاب الإبادة الجماعية، وشددت دعواها على الدعم السياسي والمالي والعسكري، الذي تمده المانيا إلى الكيان الصهيوني، طالبت نيكارغوا المحكمة بأن تتخذ تدابير مؤقتة ضد الكيان الصهيوني،

١ محمد يوسف، تحليل الوضع القانوني والمسؤولية الدولية للاحتلال الإسرائيلي في القدس: رؤية مستقلة، مجلة دراسات بيت المقدس، جامعة انقرة، العدد (١) الجزء (٢٤)، تركيا، ٢٠٢٤، ص ٦١-٦٣.

لكن المحكمة أصدرت قراراً في نيسان/ أبريل ٢٠٢٤ يقضي بعدم الضرورة باتخاذ هكذا تدابير، لأنها اتخذت أساساً في القضية المقامة من قبل جنوب إفريقيا.^(١)

وبما إن محكمة العدل الدولية تعد أداة قضائية فاعلة في فرض المسؤولية الدولية على الدول التي تُباشِر أفعالاً رقمية تمسّ المناطق المحمية، ولا سيما حين ترتبط هذه الأفعال بوقوع ضرر فعلي يؤثر بشكل مباشر على السكان المدنيين. وقد أظهرت تجربة النزاع الروسي-الأوكراني تطوراً نوعياً في زحزحة الخط الفاصل بين الاعتداءات التقليدية والهجمات السيبرانية التي تُحدث أثراً إنسانياً ملموساً في زمن النزاع المسلح.

ففي ١٦ آذار/مارس ٢٠٢٢، قدّمت أوكرانيا دعوى أمام محكمة العدل الدولية ضد الاتحاد الروسي، استناداً إلى أحكام اتفاقية منع جريمة الإبادة الجماعية لعام ١٩٤٨. وقد طلبت أوكرانيا إصدار تدابير مؤقتة تتضمن منع "الإجراءات الرقمية" التي تعطل البنية التحتية المدنية الحيوية وتعرض حياة المدنيين للخطر. وقد أصدرت المحكمة قراراً بأغلبية ١٣ من أصل ١٥ قاضياً، يلزم روسيا بـ "وقف فوري لأي عمليات عسكرية أو إلكترونية تهدد سلامة المدنيين في أوكرانيا"^(٢). وقد وردت الإشارة إلى "الإجراءات الإلكترونية" ضمن منطوق القرار، ما يعكس إدراك المحكمة لخطورة الهجمات السيبرانية كأداة قد تُحدث أضراراً لا تقل فداحة عن وسائل الحرب التقليدية.

وعلى الرغم من أن المحكمة قضت في قرارات لاحقة صادرة في شباط/فبراير ٢٠٢٤ بعدم اختصاصها بشأن بعض عناصر الدعوى المرتبطة بالفعل المباشر للقوات الروسية، فإنها تركت على حالها التدابير المؤقتة المنصوص عليها في المادة ٤١ من النظام الأساسي، والتي تنص على اتخاذ ما يلزم لمنع "الضرر غير القابل للإصلاح" الذي قد يلحق بالأشخاص أو الكيانات المحمية^(٣). ويعد هذا الموقف تطوراً مهماً في تفسير المحكمة لأثر الفعل الرقمي على المناطق المحمية.

١ ألكسندر لونجاروف، إسرائيل ومحكمة العدل الدولية: مقارنة قضايا المحكمة الدولية خلال حرب غزة، مقال منشور على الموقع الإلكتروني الخاص بمعهد واشنطن، ١٩ يونيو ٢٠١٤، على الرابط

<https://www.washingtoninstitute.org/ar/policy-analysis/asrayyl-wmhmkt-aldl-aldwlyt-mqarnt-qdaya-almhmkt-aldwlyt-khlal-hrb-ghzt>

٢ محكمة العدل الدولية، "قضية أوكرانيا ضد الاتحاد الروسي (بشأن تطبيق اتفاقية منع جريمة الإبادة الجماعية)

متاح على الرابط: <https://www.icj-cij.org/case/182>

٣ محكمة العدل الدولية، "قرار بشأن الدفوع الأولية"، ٢ شباط/فبراير ٢٠٢٤، الفقرة ٤٤. متاح على الرابط:

<https://www.icj-cij.org/public/files/case-related>

و أوضحت المحكمة، بصورة ضمنية، أن الانقطاعات الواسعة في التيار الكهربائي أو المياه نتيجة أعمال رقمية (سواء عبر تعطيل برمجيات التحكم أو استهداف الكوابل أو البنية الرقمية) تُعدّ أفعالاً مشمولة بالحماية. وكرّست هذا التفسير ضمن إطار "المحافظة على الوضع الراهن"، بما يعنيه من ضرورة الامتناع عن القيام بأي فعل مادي أو إلكتروني قد يغيّر من طبيعة الحماية الممنوحة للسكان أو المنشآت المدنية^(١).

إن هذا التكييف القضائي للهجمات السيبرانية كأداة محتملة لانتهاك الحماية القانونية للمناطق المدنية المحمية، يمثّل إرساءً لتوسيع مفهوم "العدوان" و"الضرر غير المشروع" ليشمل الوسائل الرقمية، كما يفتح الباب أمام تعويضات قانونية مستقبلية في حال تحقق عنصر الضرر المرتبط بالسلوك العدائي السيبراني. ومن شأن هذه الممارسات القضائية أن تمهد لتطورات تشريعية دولية تعترف رسمياً بخصوصية "الاعتداءات الرقمية" في القانون الدولي الإنساني، وتخضع مرتكبيها لأحكام المسؤولية الدولية سواء أمام القضاء الدولي أو عبر آليات تسوية الأضرار

ويتضح مما تقدم: من خلال استعراض وتحليل دور المحاكم الدولية في تعزيز الحماية القانونية للمواقع المحمية في أثناء النزاعات المسلحة، يتبيّن أنها قد شكّلت، على الرغم من التحديات، ركيزة مركزية في تطبيق وتطوير مبادئ القانون الدولي الإنساني. فقد أسهمت هذه المحاكم في تحويل النصوص القانونية من مجرد التزامات دولية عامة إلى قواعد قابلة للتنفيذ من خلال مساءلة الأفراد عن الانتهاكات التي تطل المواقع الثقافية والدينية والأثرية. وأن أحكام المحاكم الجنائية، ولاسيّما في قضايا مثل قضية تمبكتو في مالي، أثبتت أن انتهاك حرمة هذه المواقع لا يُعد فقط مساساً بمكان مادي، بل هو اعتداء على هوية شعوب وذاكرتها الثقافية، وهو ما يمنح هذه الجرائم بعداً إنسانياً وقانونياً بالغ الأهمية. وفي السياق ذاته، كشفت التجارب في العراق وسوريا وفلسطين عن حجم الخطر الذي يهدد المواقع المحمية في ظل النزاعات المعاصرة، ولا سيّما مع تنامي النزاعات غير الدولية وتصاعد دور الفاعلين من غير الدول، مما يجعل من الحماية القضائية الدولية ضرورة أكثر من أنها خياراً. وأن المحاكم الدولية قد نجحت جزئياً في ترسيخ قواعد الحماية القانونية للمواقع المحمية، من خلال تصنيف بعض الاعتداءات عليها كجرائم حرب، وربطها بالمسؤولية الجنائية الفردية. غير أن هذا النجاح ما زال محدوداً من حيث الانتشار

١- ينظر: المادة (٤١) من النظام الأساسي لمحكمة العدل الدولية تنص على إمكانية إصدار تدابير لحماية الحقوق محل

النزاع من الضرر غير القابل للإصلاح. انظر أيضاً: ICJ, LaGrand (Germany v. United States of

America), Order of 3 March 1999, ICJ Reports 1999, pp. 9–16.

والفاعلية، إذ إن معظم القضايا التي تتأولت الاعتداء على المواقع المحمية تبقى حالات استثنائية، ولم تتحول إلى نمط دائم في الممارسة القضائية الدولية. وهذا يعود إلى عدة أسباب، من بينها قصور في تفعيل ولاية المحاكم الدولية، وضعف التعاون بين الدول، فضلاً عن عدم إعطاء هذه القضايا الأولوية السياسية والإعلامية الكافية.

في ختام هذا الفصل نستخلص مما تقدم:

إن الهجمات السيبرانية أصبحت تمثل تحدياً بنوياً غير تقليدي في مجال النزاعات المسلحة، وذلك بالنظر إلى طابعها الخفي، وقدرتها على إحداث أضرار موازية أو تفوق تلك الناجمة عن الأسلحة التقليدية، مع استغلال ضعف البنية التشريعية الدولية في هذا المجال. وقد برزت الحاجة الملحة لتأطير هذه الهجمات ضمن قواعد القانون الدولي الإنساني، لا سيما من حيث قابلية تطبيق المبادئ الأساسية عليه، مثل التمييز، والتناسب، والاحتياط. و أن الدراسة بيّنت أن قواعد المسؤولية الدولية، وإن كانت في أصلها صالحة للتطبيق من حيث المبدأ على الهجمات السيبرانية، إلا أن هناك فراغاً تنظيمياً حقيقياً في مستوى الممارسة، يستدعي مزيداً من الوضوح في تعريف الفاعل المسؤول، وتحديد صفة النزاع، والتمييز بين الأضرار المشروعة، وتلك التي تمثل انتهاكاً صريحاً للقانون الدولي الإنساني.

يرى الباحث: إن الهجمات السيبرانية باتت تشكل إحدى أبرز الإشكاليات القانونية في النزاعات المسلحة المعاصرة، نظراً لما تطرحه من تعقيدات تتعلق بطبيعة الفاعلين، وتحديد المسؤولية، وآثار الفعل العدائي في سياق لا تُستخدم فيه القوة بشكلها المادي التقليدي. فهذه الهجمات قد تُعطّل منشآت حيوية كالمستشفيات، ومحطات الطاقة، وأنظمة الاتصالات، بما يمس مباشرة المدنيين، ويعرض حياتهم وسلامتهم للخطر، دون أن تُطلق فيها رصاصة واحدة.

ويؤكد الباحث: إن قواعد القانون الدولي الإنساني، بما تحمله من مبادئ عامة، قادرة على احتواء مثل هذه الأفعال من حيث التأطير الأخلاقي والقانوني، إلا أن التحدي الرئيسي يكمن في القدرة على التطبيق العملي لهذه القواعد في الفضاء السيبراني. ففي غياب تعريفات دقيقة لماهية الهجوم السيبراني على وفق المعايير الدولية، وغياب إجماع حول عتبة الضرر التي تستوجب تطبيق القانون الدولي الإنساني، يصعب في كثير من الحالات تحديد ما إذا كان الفعل يُشكّل خرقاً فعلياً يترتب عليه مسؤولية دولية. وأن إسناد المسؤولية الدولية في هذا السياق يواجه معوقات عملية تتعلق بصعوبة التتبع الفني للهجوم، وإمكانية استخدام أدوات تضليل تقنية تُخفي هوية الفاعل الحقيقي (مثل تقنيات الـ Proxy servers، والـ VPN، والتلاعب بسجلات المصدر الرقمي). وهو ما يؤدي إلى وجود ما يُسمى بالمناطق الرمادية في الفضاء

السيبراني، إذ يمكن تنفيذ هجمات مؤثرة دون إمكانية توجيه الاتهام القانوني المباشر. وأن معالجة هذه الإشكالية تتطلب جهوداً قانونية وتقنية مزدوجة. فمن الناحية القانونية، ينبغي على المجتمع الدولي تطوير قواعد صريحة ضمن بروتوكولات ملحقه باتفاقيات جنيف، أو ضمن معاهدات خاصة، تُعرّف الهجمات السيبرانية التي ترتقي إلى مستوى الأعمال العدائية، وتحدد معايير المسؤولية الدولية عنها، سواء كانت من قبل الدول أم الفاعلين من غير الدول. أما من الناحية التقنية، فيجب دعم إنشاء هيئات دولية فنية متخصصة في التحقيقات السيبرانية ذات الطابع العدائي، تمتلك صلاحيات التعاون الدولي وتبادل الأدلة الرقمية.

أن هناك حاجة أيضاً لتحديث أدوات الردع القانونية، بحيث لا تقتصر العقوبات أو التدابير على الهجمات المسلحة التقليدية، بل تشمل كذلك الهجمات الرقمية، التي تحدث آثاراً إنسانية مباشرة، كتخريب أنظمة المياه، أو التلاعب بالبيانات الصحية، أو قطع الاتصالات في مناطق النزاع. ومن المهم أن تُدرج هذه الأفعال ضمن لائحة الجرائم، التي يُمكن للمحكمة الجنائية الدولية أو الآليات الدولية الخاصة أن تحقق فيها وتحاكم مرتكبيها. وأن حماية الفضاء السيبراني يجب أن تُعد جزءاً لا يتجزأ من نظام الحماية الذي يراعى القانون الدولي الإنساني، وأن تطوير هذا المجال هو مسألة أمن إنساني بامتياز، لا يمكن تأجيلها، لا سيما مع تسارع استخدام هذا النمط من الهجمات في النزاعات الدولية والإقليمية الراهنة، بما في ذلك ما شهده العالم في حالات أوكرانيا، غزة، وإثيوبيا.

الخاتمة

توصلنا من خلال بحثنا الموسوم: (أثر الهجمات السيبرانية على المناطق المحمية - دراسة في ضوء أحكام القانون الدولي الإنساني) إلى جملة من الاستنتاجات والمقترحات :

الاستنتاجات

١ إن الهجمات السيبرانية أنشطة عدائية مُنظمة تُمارس عبر الفضاء الإلكتروني، تستهدف الأنظمة التقنية وشبكات المعلومات، والبنى التحتية الرقمية للدول أو المؤسسات أو الأفراد، باستخدام وسائل تكنولوجية تهدف إلى التدمير أو التعطيل أو التجسس أو التأثير النفسي والمعلوماتي. لها بعد عسكري، فالهجمات السيبرانية تُعد أحد أشكال الحروب غير التقليدية، إذ تُستخدم لتحقيق أهداف استراتيجية دون اشتباك مادي مباشر، وغالباً تكون جزءاً من عمليات عسكرية هجينة تهدف إلى إضعاف الخصم أو شل قدراته الدفاعية والاقتصادية. ومن ناحية البعد القانوني، تطرح الهجمات السيبرانية تحدياً للقواعد التقليدية للقانون الدولي، لاسيما فيما يتعلق بمبدأ السيادة، وعدم التدخل، واستخدام القوة.

٢ قد تتنوع الهجمات السيبرانية، وكثرت غايتها فمنها ما عُرفت بحرب المعلومات الشخصية (التجسس الإلكتروني)، وحرب المعلومات بين الشركات والمؤسسات، و حرب المعلومات العالمية (الحرب السيبرانية).

٣ إن خطورة الهجمات السيبرانية لا تكمن فقط في تنوعها وأساليبها المتطورة فحسب، بل في تجاوزها للحدود الجغرافية والقانونية التقليدية، ما يجعل التصدي لها يتطلب نهجاً تكاملياً يشمل البعد التقني والقانوني والسياسي.

٤ إن اعتماد الدول المتزايد على الفضاء السيبراني في إدارة شؤونها الحيوية جعل من هذه الهجمات أداة فاعلة في الصراعات الدولية.

٥ إن المناطق المحمية مساحات جغرافية محددة تُنشأ بموجب اتفاقات صريحة أو قواعد عرفية في سياق النزاعات المسلحة، بهدف تأمين الحماية للأشخاص أو الممتلكات أو المواقع التي تتأثر بشدة من آثار الأعمال العدائية. ويُمنع داخل هذه المناطق أي نشاط عسكري، هجومي أو دفاعي، مع احترام مبدأ الحياد التام، وتخضع هذه المناطق لضوابط قانونية صارمة ومراقبة إنسانية أو دولية عند توفر الإمكانيات. ويمثل هذا المفهوم أداة تنفيذية رئيسية من أدوات القانون الدولي الإنساني، الغاية منها تقليل الأذى الناتج عن الحرب على الفئات الضعيفة أو الممتلكات الحيوية ذات الأهمية الإنسانية أو الثقافية أو البيئية.

٦ تمثل المناطق المحمية إحدى أهم أدوات المجتمع الدولي في الحفاظ على البيئة والتنوع البيولوجي، و أنها تكتسب طابعاً خاصاً من الحماية القانونية يركز على مصادر متعددة في القانون الدولي، تشمل الاتفاقيات الدولية البيئية، الأعراف، المبادئ العامة للقانون، وأحكام القضاء الدولي. وقد تطور النظام القانوني للمناطق المحمية ليشمل ليس فقط الحماية في أوقات السلم، بل امتد أيضاً ليغطي بعض أشكال الحماية في أثناء النزاعات المسلحة، على وفق ما نص عليه القانون الدولي الإنساني.

٧ إن الطبيعة القانونية للمناطق المحمية تشهد تطوراً نوعياً في القانون الدولي، يُظهر التفاعل المتزايد بين القانون الدولي البيئي والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ويؤكد أن هذه الطبيعة القانونية لا تقتصر على البعد البيئي فحسب، بل تشمل أبعاداً سيادية، إنسانية، وتنموية، تفرض على الدول والمجتمع الدولي التزامات متزايدة لا تقف عند حدود التراضي أو الإرادة المنفردة.

٨ إن الهجمات السيبرانية أصبحت تمثل أحد أبرز التهديدات المعاصرة للأمن الدولي، وقد تجاوزت في آثارها الحدود التقليدية للنزاعات المسلحة.

٩ إن دليل تالين، بنسختيه الأولى والثانية، جاء ليسد فراغاً قانونياً في كيفية تطبيق القانون الدولي، ولا سيما القانون الدولي الإنساني، على الفضاء السيبراني. فقد قدم الدليل محاولة تفسيرية غير ملزمة، لكنها رائدة في تأطير المبادئ القانونية النازمة لاستخدام القوة في الفضاء السيبراني، ومعايير التمييز، والتناسب، والحماية، وحقوق وواجبات الدول بإزاء الهجمات السيبرانية. ومع أن الدليل لا يعد نصاً قانونياً ملزماً، إلا أنه يعد مرجعاً مهماً لصانعي السياسات ومطوري العقيدة العسكرية والقانونية للدول، ولا سيما في ظل تزايد الاعتماد على الفضاء السيبراني في المجالات العسكرية والمدنية على حد سواء.

١٠ إن الهجمات السيبرانية أصبحت تُشكل أحد أبرز ملامح النزاعات المسلحة المعاصرة، مما يستدعي إخضاعها لأحكام القانون الدولي الإنساني، ولا سيما لمعيار التمييز في تحديد الأهداف العسكرية المشروعة. وقد أكدت العديد من الوثائق التفسيرية، مثل دليل تالين الصادر عن مجموعة خبراء القانون الدولي بشأن الفضاء السيبراني، أن الهجمات السيبرانية، التي ترتقي إلى حد النزاع المسلح تُخضع أطراف النزاع لواجبات قانونية من أبرزها عدم استهداف المدنيين أو الأعيان المدنية.

١١ إن الهجمات السيبرانية، حينما تُنفذ في سياق نزاع مسلح دولي أو غير دولي، قد ترقى إلى مستوى الأعمال العدائية، التي تُخضع أطراف النزاع للقيود التي يفرضها القانون الدولي الإنساني. فالهجوم السيبراني، وإن كان لا يحدث دماراً مادياً ظاهراً دائماً، إلا أن أثره على الأهداف العسكرية أو المدنية قد يكون بالغاً، ولا سيما إذا استهدف بنى تحتية حيوية كشبكات الكهرباء، وأنظمة الاتصالات، والمنشآت الصحية، أو تسبب في شلل مؤسسات الدولة. ومن ثم، فإن هذه الهجمات تخضع للضوابط القانونية ذاتها التي تنطبق على الوسائل والأساليب التقليدية في القتال، وعلى رأسها مبادئ التمييز والتناسب والاحتياطات الممكنة. وأن بعض الهجمات السيبرانية، التي تحدث آثاراً مدمرة وتستهدف السكان المدنيين أو تعطل الخدمات الأساسية، قد تُشكّل جرائم حرب تستوجب المساءلة الدولية.

١٢ إن القانون الدولي الإنساني لا ينطبق خارج سياق النزاع المسلح، ولكن إذا حدث هجوم سيبراني سبب أو من المحتمل أن يتسبب في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص يمكن أن ترقى هذه الهجمات السيبرانية إلى وصف نزاع مسلح، قياساً على الهجمات العدائية الحركية، التي ترقى إلى نزاع مسلح ويطبق عليها القانون الدولي الإنساني.

١٣ إن الجمعية العامة للأمم المتحدة في كافة قراراتها، التي أصدرتها تدعو إلى إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات، ووضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في عدها عواقب الهجوم السيبراني، وبذلك يتضح أن للجمعية العامة للأمم المتحدة دوراً إيجابياً للحد من آثار الهجمات السيبرانية وتوفير الحماية للمناطق المحمية في أثناء النزاعات المسلحة.

١٤ إن الجهود الدولية وإن كانت لا ترقى إلى مستوى تنظيمي دولي شامل، إلا أنها تظهر مدى الاهتمام الدولي المتزايد لوضع أطر تنظيمية للتصدي للهجمات السيبرانية، وفضلاً عن ذلك تعد الخطوة الأولى نحو اتفاقية متعددة الأطراف تنظم استخدام هذه الهجمات، وتقلل من آثارها الجسيمة على البشر.

١٥ إن اتفاقية جنيف الثالثة لعام ١٩٤٩ لم تشر أو تورد نصاً يُعنى بالمناطق المحمية، إذ إنها جاءت لتعالج قضايا أسرى الحرب، على نقيض ما جاء بالاتفاقيات الثلاث الأخريات اللائي تتأولن المناطق المحمية على اختلاف أنواعها.

١٦ المحاكم الجنائية الدولية الخاصة (محكمتي يوغسلافيا ورواندا) تمثل واحدة من أهم الآليات القانونية للقضاء الدولي الجنائي، على الرغم من أنها لا تخلو من السلبيات إذ تتأثر بالاعتبارات السياسية، وأنها تتبع مجلس الأمن، بحكم طبيعتها فهي تُعد واحدة من الأجهزة الفرعية التابعة للمجلس، الأمر الذي قد يؤدي إلى عدم الحيادية والاستقلال القضائي، ولا سيّما أن مجلس الأمن تحتكره الدول الأعضاء الخمسة، إلا أنها -المحاكم- تعد انعطافة مهمة في تاريخ القانون الدولي الجنائي، وذلك من خلال اعترافها بالعديد من المبادئ القانونية، وتقنينها للجرائم الدولية، ومحاولتها لمنتَهكي القواعد القانونية للنزاعات المسلحة ومعاقبتهم، وهذا قد مهد الطريق إلى إنشاء محكمة جنائية دولية دائمة.

١٧ إن دور المحاكم الدولية في تعزيز الحماية القانونية للمواقع المحمية في أثناء النزاعات المسلحة، يتبيّن أنها قد شكّلت، على الرغم من التحديات، ركيزة مركزية في تطبيق وتطوير مبادئ القانون الدولي الإنساني.

١٨ أسهمت المحاكم الدولية في تحويل النصوص القانونية من مجرد التزامات دولية عامة إلى قواعد قابلة للتنفيذ من خلال مساءلة الأفراد عن الانتهاكات، التي تطال المواقع الثقافية والدينية والأثرية.

١٩ إن أحكام المحاكم الجنائية، لاسيّما في قضايا مثل قضية "تمبكتو" في مالي، أثبتت أن انتهاك حرمة هذه المواقع لا يُعد فقط مساساً بمكان مادي، بل هو اعتداء على هوية شعوب، وذاكرتها الثقافية، وهو ما يمنح هذه الجرائم بعداً إنسانياً وقانونياً بالغ الأهمية.

٢٠ كشفت التجارب في العراق وسوريا وفلسطين ولبنان عن حجم الخطر الذي يهدد المواقع المحمية في ظل النزاعات المعاصرة، ولا سيّما مع تنامي النزاعات غير الدولية وتصاعد دور الفاعلين من غير الدول، مما يجعل من الحماية القضائية الدولية ضرورة أكثر من كونها خياراً.

٢١ إن المحاكم الدولية قد نجحت جزئياً في ترسيخ قواعد الحماية القانونية للمواقع المحمية، من خلال تصنيف بعض الاعتداءات عليها كجرائم حرب، وربطها بالمسؤولية الجنائية الفردية. غير أن هذا النجاح ما زال محدوداً من حيث الانتشار والفاعلية، إذ إن معظم القضايا التي تتأولت الاعتداء على المواقع المحمية تبقى حالات استثنائية ولم تتحول إلى نمط دائم في الممارسة القضائية الدولية. وهذا يعود إلى عدة أسباب، من بينها قصور في تفعيل ولاية المحاكم الدولية، وضعف التعاون بين الدول، فضلاً عن عدم إعطاء هذه القضايا الأولوية السياسية والإعلامية الكافية.

المقترحات

- ١ نوصي بأن تُقنن حماية المناطق المحمية من الهجمات السيبرانية صراحةً بمفهوم أوسع و أدق تتبناه الأمم المتحدة والمنظمات الأخرى المعنية بهذا الشأن خلافاً لما هو عليه الحال الآن.
- ٢ لا بد من تعزيز الفضاء السيبراني في المناطق المحمية مما يوفر بيئة آمنة في حال حدوث هجوم سيبراني، من خلال اتخاذ تدابير وقائية وإجراءات استجابة سريعة.
- ٣ نرى أن الدول للضرورات الأمنية أن تولي أهمية كبرى لتعزيز وتطوير قدراتها في صد ومكافحة الهجمات السيبرانية، لتتمكن من حماية المناطق المحمية سيبرانياً بما ينسجم وقواعد القانون الدولي الانساني في حماية المناطق المحمية.
- ٤ ضرورة التعاون الدولي لمكافحة الهجمات السيبرانية، من خلال تبادل المعلومات والتنسيق فيما بينها.
- ٥ نرى أن من الضروري تكاتف المجتمع الدولي إلى تطوير خبرات العاملين على الذكاء الاصطناعي من خلال ٦ عقد ندوات أو ورش أو مؤتمرات على صعيد دولي تتبناها الأمم المتحدة بغرض صد الهجمات السيبرانية المُستهدفة للمدنيين والمناطق المحمية المطورة بوساطة الذكاء الاصطناعي.
- ٧ لا بد أن تُمنح المحكمة الجنائية قوة الزامية للأعضاء فيها أو حتى لمن هم ليسوا أعضاءً فيها لتنفيذ قراراتها وذلك حمايةً لمن يلجؤون إليها ممن تضرروا من النزاعات.
- ٨ نرى أن ضرورةً تُرتجى لفرض عقوبات أو جزاءات على الدولة العضو في المحكمة الجنائية مالم تنفذ أوامرها، لأن ذلك سيضعف سلطانها، وتزداد الانتهاكات الإنسانية.
- ٩ ندعو الدول إلى جعل قوانينها الداخلية متوائمة مع قواعد القانون الدولي الإنساني.
- ١٠ ندعو المنظمات الدولية الإنسانية إلى ملاحظة الهجمات السيبرانية، التي تقع على المدنيين والاعيان والمناطق المحمية وتسبب ضرراً إلى توثيقها، فهي جرائم من الممكن أن تكون ضد الإنسانية إذا ما سُنت الهجمة السيبرانية على مجموعة من السكان المدنيين أو على منطقة محمية.
- ١١ ينبغي عقد اتفاقيات دولية، ودولية إنسانية تُعنى تحديداً بتحديد وتعريف الهجمات السيبرانية التي توجه إلى المناطق المحمية، وتجريمها بصفقتها اعتداءً على منطقة محمية ومحاكمة منتهكيها.

١٢ دعوة الدول العربية إلى الانضمام للاتفاقيات الدولية المعنية بالهجمات السيبراني و الأمن السيبراني، وتشريع قوانين وطنية تعنى بالأمن السيبراني.

١٣ نرى لا بد اجراء تغييرات جوهرية على اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الاضافيين لعام ١٩٧٧ لغرض تنظيم، وتجريم الهجمات السيبرانية ضد المدنيين والمناطق المحمية.

١٤ ضرورة انشاء مناطق محمية في أثناء النزاعات المسلحة مع الاشارة إلى أن الهجمات السيبرانية على هذه المناطق هي جريمة ضد الإنسانية.

١٥ توسيع نطاق قاعدة التجريم للاتفاقيات، التي عالجت الهجمات السيبرانية لتشمل كل سلوك يتعدى حدود الضرورات الحربية.

١٦ الالتزام بالمبادئ والقواعد التي تضمنتها الصكوك الدولية في الاستخدام النوعي للهجمة السيبرانية في أثناء النزاعات المسلحة.

١٧ العمل على تعزيز تقنيات ومهارات القوات المسلحة الرسمية بغية التعامل مع التهديدات السيبرانية إذ يتحقق ذلك من خلال الممارسة والتدريب لفئات خاصة من المهندسين العاملين في تلك القوات، الأمر، الذي من شأنه أن يحقق أرضية سيبرانية آمنة.

١٨ على الدول العظمى أن تستثمر تطويرها التكنولوجي بما يخدم التعاون الدولي والانسان بصورة خاصة عوضاً عن توجيهها في الصراعات والحروب.

١٩ توفير برنامج حماية إلكتروني يهدف إلى تعزيز ثقة القطاع الخاص والعام بصرف النظر إن كان أجنبياً أو محلياً لحماية القطاعات الاقتصادية والتجارية، وكذلك المناطق المحمية في الدولة.

المصادر والمراجع

❖ القرآن الكريم

أولاً: الكتب

١. علي محمد كاظم الموسوي ، المشاركة المباشرة للهجمات السيبرانية ، ط١، المؤسسة الحديثة للكتاب ، بيروت ، ٢٠١٩.
٢. ابن منظور، لسان العرب، باب حما، دار المعارف، القاهرة، ج١٧، المجلد الثاني.
٣. أحمد خضر شعبان، الحماية الدولية والشرعية لضحايا النزاعات المسلحة-دراسة مقارنة، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥.
٤. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، مكتبة زين الحقوقية والأدبية، لبنان، بيروت، ٢٠١٨.
٥. أحمد لطفي السيد مرعي، نحو تفعيل الإنقاذ الجنائي الوطني لأحكام القانون الدولي الإنساني، ط١، دار الكتاب الجامعي للنشر والتوزيع، الرياض، ٢٠١٦.
٦. اسراء صباح الياسري، التنظيم الدولي للمناطق المحمية دراسة في ضوء القانون الدولي الإنساني، ط١، المركز العربي للدراسات والبحوث العلمية، القاهرة، مصر، ٢٠١٨.
٧. أشرف عبد العزيز الزيات، المسؤولية الدولية لرؤساء الدول، ط١، دار النهضة العربية، القاهرة، 2010.
٨. أشرف محمد لاشين، النظرية العامة للجريمة الدولية. منشأة المعارف، الإسكندرية، ٢٠٢٠.
٩. إيهاب خليفة، القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنت، ط١، العربي للنشر والتوزيع، مصر، ٢٠١٧.
١٠. بلال علي النصور و رضوان محمود المجالي، الوجيز في القانون الدولي الإنساني-ما بين الاعتبارات القانونية والسياسية جوانب نظرية وتطبيقية، ط١، الأكاديميون للنشر والتوزيع، عمان، ٢٠١٢.
١١. جان بيكتيه، القانون الدولي الإنساني تطوره ومبادئه، معهد هنري دونان، جنيف، سويسرا، ١٩٨٤.
١٢. جعفر عبد السلام، مبادئ القانون الدولي. ط٢، دار النهضة العربية، مصر، ١٩٨٦.

١٣. جمال عبد الفتاح عثمان، المسؤولية الدولية عن عمليات البث المباشر العابر للحدود في ضوء أحكام القانون الدولي، دار الكتاب القانوني، مصر، ٢٠٠٩.
١٤. حامد سلطان، القانون الدولي العام وقت السلم، دار النهضة العربية ، القاهرة ، ١٩٦٥.
١٥. خالد طعمة صغفك الشمري، القانون الجنائي الدولي، ط٢، الكويت، ٢٠٠٥.
١٦. ذياب البدانية، الأمن وحرب المعلومات. دار الشروق للنشر والتوزيع، الأردن، ٢٠٠٣.
١٧. رشاد محمد جواد الليثي، حظر وتقييد استخدام الأسلحة في القانون الدولي العام، مصر، ٢٠١٠.
١٨. زازة الخضر، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام. دار الهدى، الجزائر، ٢٠١١.
١٩. سالم عبد الخالق، المسؤولية والعقاب على جرائم الحرب مع دراسة تطبيقه على جرائم الحرب في البوسنة والهرسك. دار الجامعة الجديدة للنشر، مصر، ٢٠٠٤.
٢٠. سمير محمد فاضل، المسؤولية الدولية عن الأضرار الناتجة عن استخدام الطاقة النووية وقت السلم، عالم الكتب للطباعة والنشر، القاهرة، ١٩٧٦.
٢١. السيد أبو عطية، الجزاءات الدولية بين النظرية والتطبيق. مؤسسة القافة الجامعية، مصر، 2013.
٢٢. شريف عتلم، دور اللجنة الدولية للصليب الأحمر في إنماء وتطوير قواعد القانون الدولي الإنساني، منشورات اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠١٥.
٢٣. شريف عتلم، وخالد غازي، دليل تدريب القضاة على أحكام القانون الدولي الإنساني ط١، القاهرة، مصر، ٢٠٠٩.
٢٤. شهاب مفيد، دراسات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر بعثة القاهرة، دار المستقبل العربي، لبنان، ٢٠٠٠.
٢٥. صلاح الدين بو جلال، الحق في المساعدات الإنسانية، ط١، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٨.
٢٦. صلاح الطائي، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديث، مصر، ٢٠٠٩.
٢٧. عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، ط٢، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩.

٢٨. عادل عبد الله المسدي، المحكمة الجنائية الدولية الاختصاص وقواعد الإحالة. ط٢، دار النهضة العربية، القاهرة، ٢٠١٤.
٢٩. عصام العطية، القانون الدولي العام. ط١، المكتبة القانونية، بغداد، ٢٠١٠.
٣٠. عصام جميل العسلي، دراسات دولية. اتحاد كتاب العرب، سوريا، ١٩٩٨.
٣١. علي إبراهيم، الحقوق والواجبات الدولية في عالم متغير. دار النهضة العربية، القاهرة، ١٩٩٧.
٣٢. علي زعلان نعمة وآخرون، القانون الدولي الإنساني. مكتبة السيستان، العراق، ٢٠١٥.
٣٣. علي عبد القادر القهوجي، القانون الدولي الجنائي. ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠١.
٣٤. علي وهبي ديب، المحاكم الجنائية الدولية-تطورها ودورها في قمع الجرائم الدولية. ط١، منشورات الحلبي للنشر والتوزيع، بيروت، ٢٠١٥.
٣٥. عماد خليل إبراهيم، مسؤولية المنظمات الدولية عن أعمالها غير المشروعة. ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣.
٣٦. عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، ط١، منشورات زين الحقوقية، لبنان، ٢٠١٧.
٣٧. عمر مكي، القانون الدولي الإنساني في النزاعات المسلحة المعاصرة، اللجنة الدولية للصليب الأحمر، سويسرا، ٢٠١٧.
٣٨. غسان الجندي، المسؤولية الدولية. ط١، مطبعة التوفيق، الاردن، ١٩٩٠.
٣٩. غسان الجندي، حق التدخل الإنساني، ط١، دار وائل للطباعة والنشر والتوزيع، عمان، الأردن، 2003.
٤٠. فاضل عبد الزهرة الغراوي، المهجرون والقانون الدولي الإنساني، ط١، مطبعة الحلبي الحقوقية، بيروت ٢٠١١.
٤١. فرانسواز بوشيه سولنييه، القاموس العلمي للقانون الإنساني، ترجمة محمد سعود، مراجعة عامر الزمالي ومديحة مسعود، ط١، دار العلم للملايين، لبنان، ٢٠٠٦.
٤٢. كامران الصالحي، قواعد القانون الدولي الإنساني والتعامل الدولي، مؤسسة موكرياني للطباعة والنشر، أربيل، العراق، ٢٠٠٨.

٤٣. ماركو ساسولي وآخرون، كيف يوفر القانون الحماية في الحرب. مختارات من القضايا الخاصة بممارسات معاصرة في القانون الدولي الإنساني، ط١، ICRC، المركز الإقليمي للأعلام، القاهرة، ٢٠١١.
٤٤. المجلس الاقتصادي والاجتماعي، الدورة الموضوعية ٢٠١٠، نيويورك، البند ١٣ (ب) من جدول الأعمال المؤقت والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي ومجتمع المعلومات على الصعيدين الإقليمي والدولي.
٤٥. محمد حافظ غانم، المسؤولية الدولية. ط١، معهد الدراسات العربية، مصر، ١٩٦٢.
٤٦. محمد حافظ غانم، المسؤولية الدولية، دراسة لأحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية، (محاضرات معهد الدراسات العربية العالية)، جامعة الدول العربية، مصر، ١٩٦٢.
٤٧. محمد سعادي، المسؤولية الدولية للدولة في ضوء تشريع والقضاء الدوليين. دار الجامعة الجديدة، الإسكندرية، ٢٠١٣.
٤٨. محمد صابر، المحميات في الوطن العربي إدارة التنوع الأحيائي وتنميتها، ط١، مؤسسة زايد الدولية للبيئة، الإمارات، ٢٠٢٠.
٤٩. محمد طلعت الغنيمي، الوسيط في القانون السلام. منشأة المعارف، الإسكندرية، ١٩٨٢.
٥٠. محمد طي، شرعية التصدي لقرارات مجلس الأمن الدولي: حق الدول وولاية القضاء، المركز الاستشاري للدراسات والتوثيق، بيروت، ٢٠١٣.
٥١. محمد عبد الرحمن الدسوقي، قانون المنظمات الدولية: منظمة الأمم المتحدة ووكالاتها المتخصصة، الجزء الثاني، القاهرة، دار النهضة العربية، ٢٠٠٢.
٥٢. محمد غازي ناصر الجنابي، التدخل الإنساني في ضوء القانون الدولي العام، ط١، منشورات الحلبي الحقوقية، ٢٠١٠.
٥٣. محمد فهاد شلالدة، القانون الدولي الإنساني. منشأة المعارف، الإسكندرية، ٢٠٠٥.
٥٤. محمد وليد سكاف، حق استخدام القوة ودوره في العلاقات الدولية، دار النهضة العربية، القاهرة، ٢٠٠٥.
٥٥. محمود شريف بسيوني، المحكمة الجنائية الدولية- نشأتها ونظامها الأساسي. دار النهضة العربية، القاهرة، ٢٠٠٢.

٥٦. المركز العربي للأبحاث ودراسة السياسات، وحدة الدراسات السياسية، أوامر الاعتقال بحق نتنياهو وغالانت الصادرة عن المحكمة الجنائية الدولية: السياقات والتداعيات، ٢٠٢٤، قطر.
٥٧. مصطفى سيد عبد الرحمن، القانون الدولي العام. دار النهضة العربية، مصر، ٢٠٠٣.
٥٨. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، لبنان، ٢٠١٧.
٥٩. منير البعلبكي، المورد الحديث: قاموس انكليزي-عربي، ط٣، دار العلم للملايين، بيروت، ٢٠١٣.
٦٠. موجز الأحكام والفتاوى الصادرة عن محكمة العدل الدولية ٢٠٠٧ - ٢٠٠٣، منشورات الأمم المتحدة، ٢٠٠٨.
٦١. نوال أحمد بسيح، القانون الدولي الانساني وحماية المدنيين والاعيان المدنية في زمن النزاعات المسلحة، ط١، منشورات الحلبي الحقوقية، ٢٠١٠.
٦٢. نيلس ميلزر، دليل التفسير لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٠.
٦٣. هديل صالح الجنابي، مسؤولية المنظمة الدولية. ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٢.
٦٤. هشام محمد فريجة، القضاء الدولي الجنائي وحقوق الإنسان، دار الخلدونية، الجزائر، ٢٠١٢.
٦٥. إبراهيم عبد الحميد عمر، مسؤولية الأفراد أمام القضاء الجنائي الدولي: دراسة قانونية في ضوء أحكام المحكمة الجنائية الدولية والإقليمية (القاهرة: دار النهضة العربية للطباعة والنشر، ٢٠٢٠).

ثالثاً: الرسائل والاطاريح.

١- الاطاريح .

١. خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، اطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، الجزائر، ٢٠١٣.
٢. صلاح الدين بودربالة، استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر، ٢٠١٠.

٣. صوفيا شراد، تطبيق قواعد المسؤولية الدولية في أحكام المحكمة الدولية لقانون البحار-دراسة تطبيقية لمبدأ التعويض عن الضرر. أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خضير، الجزائر، ٢٠١٣.

٢- الرسائل.

١. أحمد طوزان، قانون النزاعات المسلحة، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠.
٢. إيمان حمدان، التكنولوجيا الجديدة والقانون الدولي الإنساني -الحرب السيبرانية دراسات معمقة في القانون الدولي لإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠.
٣. حسام جاسم الدليمي، التطور التكنولوجي وأثره في سيادة الدول. رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الأنبار، العراق، ٢٠١٨.
٤. رشيد مجيد الربيعي، مبدأ حسن النية في تنفيذ الالتزامات الدولية. رسالة ماجستير، كلية القانون والسياسية، جامعة بغداد، ١٩٨٣.
٥. زقار منية العمري، الدفاع الشرعي في القانون الدولي العام، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، الجزائر، ٢٠١١.
٦. زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة، كلية القانون، النجف الاشرف، العراق، ٢٠١٦.
٧. سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٨.
٨. عبد القادر مرزق، استخدام القوة في إطار القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، ٢٠١٢.
٩. مالك منسي صالح الحسيني، الحماية الدولية للأهداف المدنية- دراسة في ضوء القانون المدني، رسالة ماجستير، المعهد العالي للدراسات السياسية الدولية، جامعة المستنصرية، بغداد، ٢٠٠٥.

١٠. محمد صنيتان الزعبي، المسؤولية الدولية عن الأضرار التي تسببها النفايات النووية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٠.
 ١١. مريم ناصري، فعالية العقاب على الانتهاكات الجسيمة لقواعد القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الحاج الخضر، الجزائر، ٢٠٠٩.
 ١٢. نادية محتالي، حماية حقوق الإنسان تحت الاحتلال، رسالة ماجستير، كلية الحقوق، جامعة باجي مختار، الجزائر ٢٠١٢ ١٢٩.
 ١٣. نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير، الجامعة الافتراضية السورية، سوريا، ٢٠٢١.
 ١٤. ياسر كلزي، النظرية العامة في القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ٢٠٢٠.
- ثالثاً: البحوث والدراسات.
١. ابراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية، المجلد ٦٧، العدد الأول، ٢٠٢٥.
 ٢. أحمد أبو الوفا، شروط المسؤولية الدولية. مجلة الدبلوماسية، معهد الدراسات الدبلوماسية، العدد (١٣)، المملكة العربية السعودية، ١٩٩٠.
 ٣. أحمد سيف الدين، المسؤولية الدولية: ماهيتها وآثارها وأحكامها، مجلة الجيش اللبناني، العدد ٣١٨، لبنان، ٢٠١١.
 ٤. أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكيف الهجمات السيبرانية في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونية والسياسية، المجلد (٤٤)، العدد (١)، كلية القانون والعلوم السياسية، جامعة الكوفة، النجف الاشرف، العراق، ٢٠٢٠.
 ٥. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية السياسية، جامعة بابل، كلية القانون، المجلد ٨، العدد ٤، العراق، ٢٠١٦.
 ٦. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠.

٧. باية فتحية، التعويض في القانون الدولي العام، مجلة القانون والتنمية المحلية، محور القانون والتنمية المحلية، ادرار- الجزائر المجلد (١) العدد (٢)، الجزائر، ٢٠١٩.
٨. بهاء عدنان السعيرى، عماد عيد خضير، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٧٢، العدد ٤، ٢٠١٩.
٩. جون ماري هنكرتس، دراسة حول القانون الدولي الإنساني العرفي-إسهام في فهم واحترام حكم القانون في النزاع المسلح، المجلة الدولية للصليب الأحمر، العدد ٨٥٧، ٢٠٠٥.
١٠. جون-ماري هنكرتس ولويس دوزوالد-بك، القانون الدولي الإنساني العرفي، المجلد الأول: القواعد، القاهرة، ٢٠٠٧، (دراسة اللجنة الدولية للقانون العرفي)، القاعدتان ٧٠ و ٧١.
١١. حسن بن أحمد الشهري، الإرهاب الالكتروني - حرب الشبكات، المجلة العربية الدولية للمعلوماتية، (المجلد ٤، العدد ٨)، ٢٠١٥.
١٢. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي، المجلد ٧٩، العدد ٧٩، مصر، ٢٠٢٣.
١٣. حسن فياض، الهجمات السيبرانية في منظور القانون الدولي الإنساني، مجلة الدفاع الوطني اللبناني، العدد ١١٤، بيروت، ٢٠٢٠.
١٤. حسين شيخة الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، جامعة الشارقة، المجلد ١٧، العدد ١، الإمارات العربية المتحدة، ٢٠٢٠.
١٥. حمزة بن فهم السلمي، الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي، مجلة الجامعة العراقية، العدد (٥٩) الجزء (١)، العراق، ٢٠٢٣.
١٦. درويش سعيد، الحرب السيبرانية وأثرها على حقوق الإنسان: دراسة في ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤، عدد ٥، الجزائر، ٢٠١٧.
١٧. عبد الرحمن العتيبي، دور الامن السيبراني في تعزيز الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، ٢٠١٧.
١٨. سوداني نور الدين، المناطق المحمية بموجب القانون الدولي الإنساني، وآليات محاكمة منتهكيها أمام القضاء الدولي الجنائي، مجلة أبحاث، المجلد ٦، العدد الأول، ٢٠٢١.

١٩. صابر محمد محمود المزعل وياسمين محمد حسن يونس، القانون الدولي والنزاعات المسلحة، المجلة الدولية لنشر البحوث والدراسات، عمان، الأردن، المجلد ٦، العدد ٦٢، ٢٠٢٤.
٢٠. طلال ياسين العيسى، وعدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. مجلة الزرقاء والدراسات الإنسانية، جامعة عجلون الوطنية، المجلد (١٩)، العدد (١)، الأردن، ٢٠١٩.
٢١. عادل أحمد الطائي، المسؤولية الدولية عن الأفعال المحظورة دولياً. مجلة بيت الحكمة، العدد (٣)، العراق، ٢٠٠٠.
٢٢. عبد الرحيم صدقي، دراسة للمبادئ الأصولية للقانون الدولي الجنائي. المجلة المصرية للقانون الدولي. الجمعية المصرية للقانون الدولي، المجلد (٤٠)، العدد (٤٠)، ١٩٨٤.
٢٣. فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمي: الصين نموذجاً، المجلة الجزائرية للأمن الإنساني. جامعة باتنة، المجلد (٥)، العدد (١)، الجزائر، ٢٠٢٠.
٢٤. ماريا عبد الرؤوف الدباس، حماية الأعيان المدنية على وفق القانون الدولي الإنساني (المناطق المحمية - المنشآت ذات الطاقة الخطرة - المرافق الإعلامية - البيئة الطبيعية)، مجلة الحكمة، المجلد ٤١، العدد ٧٤، سوريا، ٢٠١٠.
٢٥. مايكل ن، شमित، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، العدد ٢٠٠٢، ٨٦٤، ٢٠٠٢.
٢٦. التقنيات الإلكترونية والحرب، بعد عشرين عاماً القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، المجلة الدولية للصليب الأحمر، 2020.
٢٧. محمد يوسف، تحليل الوضع القانوني والمسؤولية الدولية للاحتلال الكيان الصهيوني في القدس: رؤية مستقلة، مجلة دراسات بيت المقدس، جامعة انقرة، العدد (١) الجزء (٢٤)، ٢٠٢٤.
٢٨. محي الدين محمود قواس، الإدارة المستدامة للمراعي الطبيعية عند العرب (نظام الحمى)، مجلة بحوث، جامعة حلب، سوريا، العدد ١٢، ٢٠١٧.
٢٩. موسى بن تغري، "الحرب السيبرانية والقانون الدولي الإنساني"، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد ١٢، العدد ٢٢، الجزائر، ٢٠٢٠.

٣٠. هاني محمد خليل الغزاوي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والاحصاء والتشريع، العدد ٥٤٩، القاهرة، مصر، ٢٠٢٣.
٣١. ياسمين احمد إسماعيل صالح، دور المحكمة العدل الدولية في تطوير قواعد القانون الدولي الإنساني وضمان الالتزام بمبادئه، مجلة كلية السياسة والاقتصاد، جامعة بنى سويف، العدد (٣)، مصر، ٢٠١٩.
٣٢. يحيى ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية، جامعة يحيى فارس، المجلد ٤ ، العدد ٤ ، الجزائر، ٢٠١٨.
٣٣. دوريجي، كوردولا، لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، جامعة كامبريدج مجلد ٩٤ العدد ٨٨٦، الولايات الامريكية المتحدة، ٢٠١٢.
٣٤. سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، مجلة حوليات جامعة الجزائر ١، الجزء الثاني، العدد ٢٩، الجزائر ٢٠١٨.
٣٥. لبكي، جورج: "المعاهدات الدولية للإنترنت: حقائق وتحديات"، مجلة الدفاع الوطني، العدد ٨٣، بيروت، ٢٠١٣.
٣٦. عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد ٣٢، مكتبة الإسكندرية، مصر، 2016.
٣٧. مايا شوكت صطفي، نجاح محمد ماهر الدفاق، اللجنة الدولية للصليب الأحمر، مجلة العلوم الاقتصادية والقانونية، جامعة تشرين، المجلد ٤٤، العدد الأول، سوريا، ٢٠٢٢.

رابعاً: الاتفاقيات والقرارات

١. إعلان سان بيترسبرغ بغية حظر استعمال قذائف معينة في زمن الحرب، سان بيترسبرغ، ٢٩ تشرين الثاني/نوفمبر - ١١ كانون الأول/ديسمبر ١٨٦٨.
٢. اتفاقية لاهاي ١٩٠٧.
٣. اتفاقية جنيف الأربع لعام ١٩٤٩.
٤. اتفاقية جنيف الأولى لعام ١٩٤٩.
٥. المواد (٢٢، و ٣٤) من اتفاقية جنيف الثانية لتحسين حالة الجرحى والمرضى والغرقى من القوات المسلحة في البحار، ١٢ أغسطس ١٩٤٩. وينص التفسير الخاص بالمادة (٢٢) على أن الحماية تشمل حالة عدم تحميل السفينة مرضى، وتظل محمية في جميع الظروف، ما لم تُستخدم في أعمال عدائية، وهذا يشير إلى شمول هذه الحماية لأية أدوات قد تُشَلّ وظائفها الإنسانية بما في ذلك الهجمات السيبرانية.
٦. اتفاقية فيينا لقانون المعاهدات، ١٩٦٩.
٧. المادة (٣١) اتفاقية فيينا لقانون المعاهدات، ٢٣ أيار/مايو ١٩٦٩، سلسلة معاهدات الأمم المتحدة.
٨. اتفاقية فيينا لقانون المعاهدات، ٢٣ مايو ١٩٦٩، المادة (٣١)، التي تفرض تفسير المعاهدات بناءً على نصوصها وهدفها، ما يدعم توسيع تطبيق اتفاقية جنيف للتعامل مع التهديدات الرقمية كجزء من سياقها الوظيفي.
٩. قرار رقم (٢٦٧٥) الصادر عن الجمعية العامة للأمم المتحدة بتاريخ ١٩٧٠.
١٠. قرار (٢٥/٢٦٧٥) الصادر عن الجمعية العامة للأمم المتحدة، لعام ١٩٧٠.
١١. البروتوكول الإضافي الأول لعام ١٩٧٧.
١٢. البروتوكول الإضافي الثاني لعام ١٩٧٧.

١٣. قرار هافانا ١٩٩٠ المنبثق عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا في ٢٧ آب/ اغسطس - ٧ أيلول/ سبتمبر ١٩٩٠، جاء مقننا للجرائم المعلوماتية.
١٤. محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى، ٨ تموز/ يوليو ١٩٩٦.
١٥. مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوروبية رقم ١٨٥ بودابست، عام ٢٠٠٠.
١٦. اتفاقية بودابست الصادرة عن المجلس الأوروبي في ٢٣ تشرين الثاني/ نوفمبر ٢٠٠١ لمكافحة الجرائم المعلوماتية.
١٧. القرارات الصادرين عن مجلس الأمن رقم (١٦٧٤، و ١٧٣٨) لعام ٢٠٠٦.
١٨. اتفاقية التعاون في مجال ضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون، يكاترينبورغ، ١٦ حزيران/يونيو ٢٠٠٩ (اتفاقية منظمة شنغهاي للتعاون)، ترجمة غير رسمية في وزارة الدفاع في الاتحاد الروسي.
١٩. قرارات المؤتمر العالمي لتنمية الاتصالات، ٢٠١٧ (wtcd-١٧) مؤتمر المندوبين المفوضين دبي، الامارات، اكتوبر - نوفمبر، ٢٠١٨، الاتحاد الدولي للاتصالات.

خامساً: المواقع الالكترونية

١. أحمد علو، مقال منشور على موقع الجيش اللبناني، متاح على الرابط: <https://www.lebarmy.gov.lb/ar/content>.
٢. أرشيف محكمة العدل الدولية، ملخص قضية نيكاراغوا ضد الولايات المتحدة الأمريكية، متاح على الرابط: <https://www.icj-cij.org/case/70>.
٣. ألكسندر لونجاروف، إلكيان الصهيوني ومحكمة العدل الدولية: مقارنة قضايا المحكمة الدولية خلال حرب غزة، متاح على الرابط: <https://www.washingtoninstitute.org/ar/policy-analysis/asrayl->

٤. الأمم المتحدة لحقوق الإنسان، اتفاقية جنيف بشأن حماية الأشخاص المدنيين في وقت الحرب
١٩٤٩، متاح على الرابط: <https://www.ohchr.org/>
٥. أنصر سفاح كريم، الحروب الإلكترونية وأثرها على الأمن القومي، متاح على الرابط:
<https://www.alnahrain.iq/post/1031>
٦. القاموس العملي للقانون الإنساني، متاح على الرابط: <https://ar.guide-humanitarian-law.org/>
٧. إيلينا بليكسيديا، التعليق على البروتوكول الإضافي الثاني لاتفاقية الجريمة الإلكترونية، متاح على
الرابط: <https://www.icann.org/ar/blogs/details/feedback-on-the->
٨. إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية،
متاح على الرابط: <https://cutt.ly/rkpu3>
٩. جان جاك روسو، العقد الاجتماعي، متاح على الرابط: <https://cutt.ly/WkpNp5Y>
١٠. غيث علّو، الهجمات السيبرانية أكبر من حرب نووية بوسائل إلكترونية، متاح على الرابط:
<https://jadehiran.com/archives/16835>
١١. فأوستو بوكار، متاح على الرابط: www.un.org/law/aval
١٢. القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، متاح على الرابط:
<https://www.icrc.org/ar/document/international-humanitarian-law-and->
١٣. القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية
أو استخدامها، متاح على الرابط: www.icrc.org
١٤. قانون النزاعات المسلحة: عناصر أساسية، متاح على الرابط:
<https://www.icrc.org/ar/document/law-armed-conflict-essentials>
١٥. اللجنة الدولية للصليب الأحمر، متاح على الرابط:
<https://www.icrc.org/ar/publication/0173-geneva-conventions-august-1>
١٦. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات
المسلحة، متاح على الرابط: www.icrc.org/ara/document/international-humanitarian-law-and-cy

١٧. لجنة القانون الدولي، الدورة الثالثة والخمسين حول المسؤولية الدولية ٢٠٠١، متاح على الرابط: <https://legal.un.org/ilc/sessions/53/>
١٨. لوائح الاتصالات الدولية: الوثائق الختامية للمؤتمر الإداري العالمي للبرق والهاتف، الاتحاد الدولي للاتصالات/ متاح على الرابط: <https://www.itu.int/osg/spu/intset/>
١٩. بعد عشرين عاماً: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية في أثناء النزاعات المسلحة، متاح على الرابط: <https://international-review.icrc.org>
٢٠. مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، مجموعة المعاهدات الأوروبية، متاح على الرابط: <https://cutt.ly/YkpJX>
٢١. محمد عدنان البخت، الحمى والمحميات ودورها في الإسلام، متاح على الرابط: https://www.aleqt.com/2009/11/02/article_296139.html
٢٢. محمد غنايم، الحظر الجوي على شمال العراق، متاح على الرابط: www.aliazeera.net/specialcoverage
٢٣. منظمة أطباء بلا حدود، القاموس العملي للقانون الإنساني، متاح على الرابط: <https://ar.guide-humanitarian-law.org/content/article/5/mntq-wmwq-mhmyw/>
٢٤. وكالة فارس للأخبار، "إحباط عملية تخريب في منشأة فوردو النووية"، متاح على الرابط: <https://www.farsnews.ir/>
٢٥. مكتب التدقيق الوطني، "التحقيق: هجوم WannaCry الإلكتروني وهيئة الخدمات الصحية الوطنية"، حكومة المملكة المتحدة، متاح على الرابط: <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs>
٢٦. مجموعة ميرسك، "ميرسك: تكلفة الهجوم السيبراني تصل إلى ٣٠٠ مليون دولار أمريكي"، في التقرير السنوي لعام ٢٠١٧، متاح على الرابط: <https://www.maersk.com/>

٢٧. تيك، إنيكين؛ كاسكا، قدرى؛ فيهل، ليز. الهجمات السيبرانية ضد جورجيا: تحديد الدروس القانونية. مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي ((CCDCOE، 2008. متاح على الرابط: <https://ccdcoe.org>
٢٨. حكمة العدل الدولية، "قرار بشأن الدفوع الأولية"، ٢ شباط/فبراير ٢٠٢٤، الفقرة ٤٤. متاح على الرابط: <https://www.icj-cij.org/public/files/case-related>
٢٩. محكمة العدل الدولية، "قضية أوكرانيا ضد الاتحاد الروسي (بشأن تطبيق اتفاقية منع جريمة الإبادة الجماعية، متاح على الرابط: <https://www.icj-cij.org/case/182>
٣٠. بشأن التدابير المؤقتة، أوكرانيا ضد الاتحاد الروسي، تقارير محكمة العدل الدولية ٢٠٢٢، متاح على الرابط: <https://www.icj-cij.org/case/182>
٣١. تقرير "مستشفيات حرب أوكرانيا السيبرانية: القرصنة المدنيين والمواقع المحمية"، الصادر عن Cyber Peace Institute عام ٢٠٢٣، يتناول أثر العمليات السيبرانية على البنى التحتية الصحية في أوكرانيا متاح على الرابط: <https://blogs.icrc.org/law-and>
٣٢. وزارة الأمن الداخلي الأمريكية، وكالة الأمن السيبراني وحماية البنية التحتية، تحذير: أنشطة برمجات الفدية التي تستهدف قطاع الصحة العامة والرعاية الصحية، تشرين الأول/أكتوبر ٢٠٢٠. متاح على الرابط: <https://www.cisa.gov>
٣٣. وزارة الأمن الداخلي الأمريكية، متاح على الرابط: <https://www.cisa.gov>
٣٤. معهد السلام السيبراني، "مستشفيات الحرب السيبرانية في أوكرانيا: ناشطون مدنيون ومواقع محمية"، ٢٠٢٣ متاح على الرابط: https://cyberconflicts.cyberpeaceinstitute.org/?utm_source=chatgpt.com
٣٥. وزارة العدل الأمريكية - بيان الاتهام الرسمي، متاح على الرابط: https://time.com/4270728/iran-cyber-attack-dam-fbi/?utm_source=chatgpt.com

● المصادر باللغة الأجنبية:

1. Abel S. Knottnerus, "International Law and the Use of Armed Force by States", Global Perspective, Springer Fachmedien Wiesbaden, 2016.
2. Chimni, Incarceration of victims Deconstructing safety zones. In, N. Al. Nauimi and R. Meese, international legal issues Arsing under the united nations decade of international law, Netherlands, 1995.
3. GA. Res. 55/63, 121/56 UN. Doc. No, A/RES/55/63 (Jan, 22, 2001),
4. Gervais, Michael: "Cyber Attacks and The Laws of War", Berkeley Journal of International Law, Volume 30, Issue 2, Article 6, 2012.
5. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", Journal of National Security Law and Policy, Vol.4, 2010
6. Ibid, comment (18) on Rule (38).
7. ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts, forthcoming.
8. International. Law association, report 34conference. 1926.
9. Junaidu Bello Marshall and Mua'zu Abdullahi, "Cyber- Attack: The Legal Response", International Journal of International Law, Vol.1, Issue 2, 2011.
10. Kelsen, State Responsibility and the Abnormally Dangerous Activity, Columbig jolumbig journal of international Law, vol (2), 1972.
11. Knopová, Eva: New IHL Framework for Cyber Warfare, Faculty of Law (Department of International Law), Charles University in Prague, Thesis Supervisor: Dr. Martin Faix, 2016.
12. Kutnayeva, Nuria: "Cybersecurity in Central Asia", Unipath-Magazine, United States Central Command (CENTCOM), August 20, 2015.
13. Lül, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, Working Paper, Vol.3, No3, IFHV, Ruhr University Bochum, Germany, 2013.

- 14.ICJ, LaGrand (Germany v. United States of America), Order of 3 March 1999, ICJ Reports 1999.
- 15.Maonga, Sharon Kerubo: "A Case of Incapacity: The Interrogation of International Humanitarian Law as A Satisfactory Regulator of Cyber Warfare", Strathmore University, Strathmore Law School ,2017.
- 16.Marie Baezner, Patrice Robin, Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), 2018.
- 17.Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", The Yale Journal of International Law, Vol.36, 2011.
- 18.Mccormack, Tim: International Humanitarian Law and The Targeting of Date, Volume 94, International Law studies, U.S. Naval War College, United States, 2018, PP223-240, P227.
- 19.Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal.
- 20.Michael N. Schmitt ed Tallinn Mnnual on The International Law Applicable to Cyber Warfare, 2013.
- 21.Michael N. Schmitt, "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law, Iss, 37, No. 3, 1999.
- 22.Michael Schmitt, (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, Comment (3) On Rule (29).
- 23.Miranda Grange, Cyber Warfare and The Law of Armed Conflict, Research Paper, Faculty of Law, Victoria University of Wellington, 2014.
- 24.Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School, United States of America, Vol. 100:817, 2012.
- 25.Priyanka R. Dev, " Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", Texas International Law Journal, Vol. 50, Issue 2, 2015.

26. Rene Vark, "The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force", Baltic Defence Review, No.10. Vol.2, 2003.
27. Report of the Group of Governmental Experts on Developments in (the Field of Information and Telecommunications in the Context of International Security, Sixty-eighth session, document (A/68/98), 2013.
28. Rousseau (Ch.) (: La responsabilité internationale, cours de droit international public de la faculté de droit, Paris, 1959, 1960.
29. SC. Res. 2341, UN. Doc. No, S/RES/2341(2017) (February, 13, 2017),
30. Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009)
31. Sophie Barnett, "Applying Jus Ad Bellum in Cyberspace", (1 September, 2016), E-International Relations Studies.
32. Titiriga Remus, "Cyber-Attacks and International law of Armed Conflicts; a "Jus ad Bellum" perspective", Journal of International Commercial Law and Technology, Issue 8, No. 3, 2013.
33. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, 2001, Articles 1–2, 4–8
34. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017).
35. United Nations Audiovisual Library of International Law, General Resolution 3314, Defining aggression.
36. Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies, U. S. Naval war college, Vol 89, 2013.

Abstract

This thesis examines "The Impact of Cyber Attacks on Protected Zones" within the framework of International Humanitarian Law (IHL), addressing the growing significance of cyberspace as a new domain in contemporary armed conflicts. As cyber-attacks increasingly target critical civilian infrastructure, fundamental legal questions arise concerning the adequacy of traditional IHL rules in providing effective protection for protected zones against cyber operations, and whether the existing legal framework can address the unique challenges posed by the intangible and unconventional nature of such attacks .

The study establishes a conceptual foundation for cyber-attacks by analyzing their legal characteristics and distinguishing features from conventional military operations. These include the anonymity of attackers, difficulties in attribution, and their transnational impact without the use of physical force. It further explores the concept of protected zones under IHL, which includes hospitals, medical facilities, cultural property, and vital civilian infrastructure, along with the corresponding legal obligations during armed conflicts .

The research analyzes contemporary challenges through case studies such as the 2015 cyber-attack on Ukraine's power grid and attacks on healthcare systems during the COVID-19 pandemic that disrupted critical medical services. These cases are examined to determine whether such cyber operations qualify as "attacks" under the Geneva Conventions and Additional Protocols, thereby triggering IHL protections and obligations for parties to conflict .

A key focus is the application of the principles of distinction and proportionality in cyberspace, particularly given the challenges of distinguishing military objectives from civilian assets in interconnected digital networks. The study also examines the implications of non-material effects from cyber-attacks, such as depriving civilians of essential services without causing physical destruction, which raises important questions about interpreting terms like "harm," "attack," and "direct military advantage" in the context of digital warfare .

The thesis further investigates the complexities of attributing legal responsibility for cyber-attacks, considering how modern technologies enable anonymity and the use of non-state proxies, complicating accountability under IHL. This

underscores the need for enhanced digital forensic capabilities and evidence analysis mechanisms adapted to the nature of cyberspace .

In conclusion, the study demonstrates that cyber-attacks present significant challenges to traditional IHL concepts of humanitarian protection in armed conflicts. The findings highlight the urgent need to adapt and interpret IHL principles to address technological developments while maintaining the fundamental values of this legal framework, particularly given the rapid evolution of cyber capabilities and their expanding role in modern warfare.

Republic of Iraq

Ministry of Higher Education & Scientific Research

AL- Alamein Institute for Higher Education



**The Impact of Cyber Attacks on Protected Areas: A
Study in Light of the Provisions of International
Humanitarian Law**

A thesis submitted by the student

Abbas Thair Sahib

Submitted to: the council of the Institute of
Al-Alamein for Graduate Studies As partial
fulfillment of the requirements for the Phd
degree in Public Law.

Under the supervision of

Assistant Professor Dr.

Fadhil Abd Al-Zahra Fadhil Al-Gharawi

Professor of International Law.