مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

مبدأ التناسب في الدفاع الشرعي ضد الهجمات السيبرانية

الدكتور: أحمد بن علي بن عبد الله الدباسي
أستاذ مساعد بقسم الأنظمة، بكلية الشريعة والدراسات الإسلامية، جامعة القصيم
aaldibasi@qu.edu.sa

ملخص البحث

تناولت هذه الورقة مسألة تحقيق ضابط التناسب عند استخدام حق الدفاع الشرعي الدولي ضد العدوان غير المشروع باستخدام الهجمات السيبرانية وذلك في ثلاثة مباحث رئيسة. إنه من المعلوم وفق القوانين والأعراف الدولية ثبوت حق الدولة في الدفاع عن نفسها بأي وسيلة مشروعة ضد أي عدوان مسلح غير مشروع عليها، فجاء المبحث التمهيدي في هذه الورقة ببيان هذا المفهوم والحق الثابت للدولة وأنه لا مراء فيه. ثم بيّنت الورقة في نفس المبحث التمهيدي مفهوم التناسب في الدفاع الشرعي وكذلك مفهوم الهجمات السيبرانية الذي قد تختلط معه بعض المفاهيم المشابهة. وقد تناول المبحث الأول توضيح العلاقة بين الهجمات السيبرانية وجريمة العدوان كون الأخيرة قد يتم استخدامها في الإضرار بأهداف حيوية، أو بنية تحتية، أو اختراق خصوصية، أو أضرار على المدنيين أو المرافق الحيوية كالمستشفيات ودور الرعاية أو محطات الكهرباء أو الغاز وغيرها لدى الدولة المعتدى عليها. إضافةً لما سبق، جاءت هذه الورقة لتوضيح مفهوم العدوان والاعتداء المسلح والذي قد يتجاوز المفهوم السائد باقتصاره على الأسلحة التقليدية ليشمل غيرها من الأسلحة الحديثة، ومنها الأسلحة الإلكترونية باستخدام الهجمات السيبرانية. ثم بعد ذلك، أوضح المبحث الثاني من هذه الورقة مدى أحقية الدولة في الدفاع عن نفسها ضد هذه الهجمات السيبرانية باعتبارها داخلة تحت مفهوم العدوان المسلح؛ وعليه، فيحق للدولة المعتدى عليها أن تدافع عن نفسها وفق ما جاءت به المادة الواحدة والخمسون من ميثاق الأمم المتحدة. وأخيرًا، اختتمت الورقة توضيحها للخلاف الدائر حول مسألة تطبيق التناسب في الدفاع الشرعي ضد الهجمات السيبرانية حيث لا يشترطه البعض بينما أكدت الورقة على أهمية تطبيق هذا المبدأ – مع صعوبة تطبيقه عمليًا – مع وجوب مراعاة بعض العوامل المهمة التي تم تناولها في ثنايا هذا البحث.

الكلمات المفتاحية: التناسب، هجمات سيبرانية، العدوان، الدفاع الشرعي، الأمم المتحدة، القوة المسلحة

مجلة العلوم الشرعية
جامعة القصيم، - المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

مبدأ التناسب في الدفاع الشرعي ضد الهجمات السيبرانية

المقدمة

الحمدالله والصلاة والسلام على أشرف خلقه وخاتم رسله، نبينا المصطفى محمد ﷺ، أما بعد: فلقد خلق الله الناس شعوبًا وقبائل ليتعارفوا، وأرسل رسلًا ليهتدي الناس بهديهم ويتبعوا سنّتهم، ولقد جاءت شريعتنا الغراء بمنهج قويم سارت عليه أمتنا منذ أن أشرق نور الهداية من مكة المكرمة قبل أربعة عشر قرنًا وحتى عصرنا الحاضر. ومن أعظم ما جاءت به هذه الشريعة السمحاء المقصد العظيم في حفظ النفس بتنميتها وإحيائها حسًّا ومعنًى، وكذلك الحفاظ عليها عن كل ما يعتريها من تهديدات تعترضها فتُذهب بعض منافعها أو تزهقها كلها؛ وقد شرع الله العديد من الأحكام المتعلقة بحفظ النفس بتنميتها كإباحة الزواج لقصد النسل، والأكل والشرب والتداوي، وكذلك الحفاظ على النفس من إهلاكها كتحريم القتل العمد، وتشريع القصاص، وغيرها من الأحكام ذات الصلة. ومن تلك المقاصد أيضًا: الحفاظ على النفس بإباحة أو وجوب الدفاع عنها عند تعرضها للخطر، فقد قال النبي ﷺ:(ومَن قُتِلَ دون نفسه فهو شهيد)، وهذا على المستوى الشخصي. أما على مستوى الجماعة؛ فقد أباح الله ﷻ رد الاعتداء عند التعرض لما يهدد سلامة الناس من تهديدات أو اعتداء، فقد قال ﷻ:﴿وَقَاتِلُوا فِي سَبِيلِ اللَّهِ الَّذِينَ يُقَاتِلُونَكُمْ وَلَا تَعْتَدُوا إِنَّ اللَّهَ لَا يُحِبُّ الْمُعْتَدِينَ﴾، وقال ﷻ: ﴿فَمَنِ اعْتَدَى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ﴾، وقال ﷻ: ﴿وَجَزَاءُ سَيِّئَةٍ سَيِّئَةٌ مِثْلُهَا فَمَنْ عَفَا وَأَصْلَحَ فَأَجْرُهُ عَلَى اللَّهِ إِنَّهُ لا يُحِبُّ الظَّالِمِينَ﴾ فهنا قد أباح الشارع الحكيم الدفاع عن النفس بالرد على الاعتداء بمثله مع اشتراط عدم التجاوز والتعدي في الرد. وهذا مبدأ راسخ في الشريعة السمحة واتفقت كثير من النظم القانونية المعاصرة مع هذا المنهج، ومن أبرزها القانون الدولي الحديث، وهو ما ستتناوله هذه الورقة بمزيد تفصيل.

إن مسألة سيادة الدولة على أراضيها مسألة محسومة في القانون الدولي. ولأجل استقرار وتثبيت هذا المبدأ جعلت الدول تسابق نفسها في التسلح وتقوية أساطيلها العسكرية بشتى أنواع الأسلحة المكتشفة والحديثة، ولعل منها الأسلحة التقنية الجديدة وذلك لاستخدامها إما في عدوانها ابتداءً أو حتى في الدفاع عن نفسها ضد خصومها. ومن المستقرّ في قواعد القانون الدولي أن التهديد باستخدام القوة فضلًا عن استخدامها يعدّ من الأمور المحظورة والمندّد بها باتفاق أمميّ جامع. وفي نفس السياق، فإن من المتفق عليه أن للدولة أو الكيان أو الشعب المعتدى عليه حق الدفاع عن نفسه بأي وسيلة مشروعة وفق ما جاءت به المادة الواحدة والخمسون من الميثاق التأسيسي لهيئة الأمم المتحدة لعام ١٩٤٥م. وفي ضوء هذه الحق المقطوع به برزت العديد من المشاكل والثغرات القانونية في مجال القانون الدولي وكذلك القانون الدولي الإنساني نظرًا للتقدم التقني الهائل والمتزايد في قطاع التكنولوجيا الحربية، ويأتي على رأسها الهجمات السيبرانية التي يكون الهدف منها تدمير أو إلحاق الضرر

مجلة العلوم الشرعية
جامعة القصيم، - المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

بالمصالح الوطنية الأساسية للدول، والتي يمكن أن تتضمن القدرة على التجسس، والاختراق، والتخريب، وخروقات البيانات، وهجمات البنية التحتية، وغيرها.

مشكلة البحث:

تناقش هذه الورقة مشكلة ما إذا كان من الممكن تطبيق ضابط مبدأ التناسب عند استخدام حق الدفاع عن النفس ضد العدوان الناتج عن الهجمات السيبرانية. وللإجابة عن هذا التساؤل؛ لا بد من معرفة الإجابة عن الأسئلة الفرعية التالية:

- ما مفهوم الدفاع الشرعي والهجمات السيبرانية؟
- وما العلاقة بين الهجمات السيبرانية وجريمة العدوان؟
- وهل تنطبق المادة الواحدة والخمسون المتعلقة بأحقية الدولة في الدفاع عن النفس على الهجمات السيبرانية؟

وأخيرًا، هل يمكن تطبيق مبدأ التناسب في الرد عند الدفاع عن النفس على الهجمات السيبرانية؟

أهداف البحث:

يهدف هذا البحث إلى:

- بيان مفهوم الدفاع الشرعي والهجمات السيبرانية.
- توضيح العلاقة بين الهجمات السيبرانية وجريمة العدوان.
- التعرّف على مدى انطباق المادة الواحدة والخمسون المتعلقة بأحقية الدولة في الدفاع عن النفس ضد الهجمات السيبرانية.
- التحقّق من إمكانية تطبيق مبدأ التناسب في الرد عند الدفاع عن النفس ضد الهجمات السيبرانية.

أهمية البحث:

إن الهجمات السيبرانية تعدّ مجالًا كبيرًا وجديدًا على الساحة الدولية، وإن التعاطي الدولي والقانوني معها يعتبر قليل نسبيًا نظرًا لضخامة ما يترتب عليها من آثار وتبعات قانونية وسياسية لم يتناولها القانون الدولي الحديث في تنظيمه الجديد الذي تبلورت أركانه وترسخت مبادئه في أعقاب الحرب العالمية الثانية أي ما يقارب الثمانية عقود. فالقانون الدولي الجديد الذي قامت عليه هيئة الأمم المتحدة كان يتعاطى وفق المعطيات الحربية السائدة في ذلك الوقت حيث لم يدر بخلد واضعي قواعد القانون الدولي والاتفاقيات الدولية هذا المستوى التقني الهائل الذي وصلت إليه البشرية. فالقواعد الدولية المتعلقة بجريمة العدوان وتفعيل

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

خيار حق الدولة في الدفاع عن نفسها كانت مصممة وفق مفهوم الأسلحة التقليدية السائدة في ذلك الوقت؛ ولذلك نشأت قواعد قانونية دولية تتناول ضوابط الدفاع عن النفس تجاه الهجمات المسلحة، ومنها مبدأ التناسب بين الفعل (جريمة العدوان) وردة الفعل تجاه هذا العدوان. وهذا المبدأ كان مقتصرًا على طبيعة ونوع القوة المسلحة التقليدية. ولكن نوع الأسلحة تغير مع مرور الوقت والتطور التقني الحاصل في العقود الأخيرة؛ ولأجل هذا استلزم الأمر دراسة للأسلحة العسكرية الجديدة المتمثلة بالهجمات السيبرانية وما يترتب عليها من التبعات القانونية والذي يأتي في مقدمتها طريقة الدفاع الشرعي ضدها وضوابط استخدام هذا الحق القانوني الدولي والذي يعرف بمبدأ التناسب في الدفاع الشرعي.

منهجية البحث:

نهجت هذه الورقة بدايةً المنهج الوصفي حيث بدأت بتوضيح بعض المفاهيم عن ماهية الدفاع الشرعي ومبدأ التناسب وفق قواعد القانون الدولي العام، ثم بدأت بوصف طبيعة الهجمات السيبرانية ومخاطرها. بعد ذلك أكملت الورقة توصيفها لمفهوم وشروط تحقق جريمة العدوان.

وفي الشق الأخير من الورقة اقتضى الأمر الأخذ بالمنهج التحليلي وذلك ببيان مدى إمكان تطبيق المادة الواحدة والخمسين من ميثاق الأمم المتحدة على الهجمات السيبرانية، ثم تحليل ما إذا كان مبدأ التناسب في الدفاع الشرعي قابلٌ للتطبيق ضد الهجمات السيبرانية.

الدراسات السابقة:

١. **الدفاع الشرعي في القانون الدولي العام في مواجهة الهجمات الالكترونية،** (رسالة ماجستير)، جمال عواد عبد الله العظامات، ٢٠١٤، جامعة آل البيت، العراق.

تناولت هذه الورقة ماهية الدفاع الشرعي في القانون الدولي العام ومشروعية استخدام القوة في القانون الدولي العام، ثم بعد ذلك تطرقت إلى الهجمات الإلكترونية ومشروعية الدفاع الشرعي ضدها.

والفرق بين هذه الدراسة والبحث هنا هو أن هذه الدراسة تناولت موضوع الدفاع الشرعي ضد الهجمات السيبرانية من صفة عامة ولم تتكلم عن التناسب بشكل مستقل.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

٢. **موقف القانون الدولي من الهجمات الإلكترونية**، ليث ناجح حميد، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، المجلد ٧، العدد ٢٤، ٢٠١٨.

تطرقت هذا البحث إلى ماهية الهجوم الإلكتروني واعتباره بمثابة القوة المسلحة وإلى آلية الرد على الهجمات الإلكترونية.

وتفترق هذه الدراسة عن البحث الحالي كونها لم تتطرق إلى مبدأ التناسب إلا بشكل عرضي ولم تستغرق كافة المفاهيم والعناصر المندرجة تحت مفهوم التناسب، وكذلك لم تتطرق إلى مفهوم جريمة العدوان وشروط تحقق الجريمة.

٣. **حق الدفاع الشرعي ضد الهجمات السيبرانية**، علي فاضل سليمان، مجلة جامعة تكريت للحقوق، جامعة تكريت، العراق، المجلد ٤، العدد ٤، ٢٠١٩.

ناقش هذا البحث مسألة الدفاع الشرعي ضد الهجمات السيبرانية وإمكانية تطبيق حق الدفاع الشرعي ضدها، لكنها تفترق عن البحث الحالي في عدم مناقشة مبدأ التناسب بصورة شافية، وكذلك لم تغطِّ حقيقة تطبيق شروط جريمة العدوان على الهجمات السيبرانية.

٤. **الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني**، د. يحيى ياسين سعود، المجلة القانونية، جامعة القاهرة، كلية الحقوق (فرع الخرطوم)، المجلد ٤، العدد ٤، ٢٠١٨.

ناقشت هذه الدراسة آلية تعاطي القانون الدولي الإنساني مع الهجمات السيبرانية وكيفية خضوع هذه الهجمات السيبرانية لقواعد القانون الدولي الإنساني.

ولكن هذه الدراسة تفترق عن البحث الحالي من ناحية عدم التطرق لكيفية الدفاع الشرعي في حال وجود الهجمات السيبرانية فضلًا عن عدم مناقشة آليات وضوابط الدفاع الشرعي.

٥. **حق الدفاع عن النفس نتيجة الهجمات السيبرانية في ضوء قواعد القانون الدولي العام**، رزق أحمد سمودي، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ديسمبر ٢٠١٨.

مجلة العلوم الشرعية
جامعة القصيم، - المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

مبدأ التناسب في الدفاع الشرعي ضد الهجمات السيبرانية

تناولت هذه الدراسة ما يتعلق بمدى ملاءمة تطبيق القواعد القانونية التقليدية الخاصة باستخدام القوة في الدفاع عن النفس على الهجمات السيبرانية، وذلك باستصحاب كل ما يتعلق بشروط الدفاع عن النفس في الأعراف العسكرية التقليدية وتطبيقها على الهجمات السيبرانية. وكان التركيز الأكبر في مدى اعتبار الهجمات السيبرانية يُعد استخدامًا للقوة أم لا.

وتختلف هذه الدراسة عن الورقة الحالية في كونها ركزت بصورة أدق حول شرط التناسب في الدفاع الشرعي ضد الهجمات السيبرانية ولم تستغرق طويلًا في الحديث حول ما إذا كان الهجمات السيبرانية تعد من قبيل استخدام القوة أم لا، حيث تم تناول ذلك في بداية هذه الورقة وبيان أن الهجمات السيبرانية تُعد من قبيل استخدام القوة باعتبارها جريمة عدوان.

خطة البحث:

تم تقسيم هذا البحث إلى مقدمة، ومبحث تمهيدي، ومبحثين رئيسين، وخاتمة.

وقد جاء التقسيم كما يلي:

المبحث التمهيدي: **مفهوم الدفاع الشرعي والهجمات السيبرانية**

المطلب الأول: **ماهية الدفاع الشرعي في القانون الدولي العام**

المطلب الثاني: **تعريف التناسب في الدفاع الشرعي**

المطلب الثالث: **مفهوم الجريمة السيبرانية**

المطلب الرابع: **مفهوم الهجمات السيبرانية**

المبحث الأول: **الهجمات السيبرانية وعلاقتها بجريمة العدوان**

المطلب الأول: **مخاطر الهجمات السيبرانية**

المطلب الثاني: **مفهوم وشروط تحقق جريمة العدوان**

المطلب الثالث: **العلاقة بين الهجمات السيبرانية وجريمة العدوان**

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

المبحث التمهيدي: مفهوم الدفاع الشرعي والهجمات السيبرانية، وفيه أربعة مطالب

المطلب الأول: مفهوم الدفاع الشرعي في القانون الدولي العام

وردت عدة تعريفات لبيان المقصود بحق الدفاع الشرعي في منظور الدولي الدولي العام، فبعض هذه التعريفات تناولت مفهومًا واسعًا لحق الدفاع المشروع، والبعض الآخر على النقيض شدّد في منح هذا الحق للدولة في استخدام الدفاع المشروع إلى أضيق الحدود. وتستند تقريبًا أغلب التعريفات الواردة في بيان مفهوم الدفاع الشرعي على نص المادة ٥١ من ميثاق الأمم المتحدة التي أكدت على أنه من حق أي دولة أن تدافع عن نفسها وفق شروط معينة بينتها المادة، والتي تنص على أنه من: "... 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 فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه."(١)

ويبقى هنا معرفة المفهوم الدقيق حول كلمة (الدفاع الشرعي) كون الأفعال التي تدخل تحت هذا المفهوم لا يمكن حصرها. فقد ورد تعريف الدفاع الشرعي في قاموس المصطلحات على أنه: "أنه ردّ فعلٍ مباشرٍ وعفويّ تقوم به الدولة، على مسؤوليتها الخاصة، مستخدمةً طرقاً قد تكون في ذاتها مخالفةً للقانون الدولي، ويكون ذلك ردًا منها على أعمال قوةٍ غير مشروعة قامت بها أو سمحت بالقيام بها دولة أخرى فجوبهت برد الفعل المشار إليه الذي يجد تبريره في القانون، وهو تبرير استثنائي، في أن الطرق المستخدمة فيه والمتناسبة مع متطلبات الموقف قد أملتها ضروراتٌ ملحةٌ أو حاسمةٌ."(٢)

فوفقًا لهذا التعريف، يتضح أن هناك أركانٌ أو شروطٌ أربعة لاستخدام الدفاع الشرعي وفق منظور القانون الدولي، وهي:

---

(١) ميثاق الأمم المتحدة، المادة ٥١، https://www.un.org/ar/about-us/un-charter/full-text?gclid=Cj0KCQjwnP-ZBhDiARIsAH3FSRfMT4N9DmVgZFYQwAlVzgnwB8YiSQ4oZIHlXg0d-LhAL-4aIlr00lMaAvCsEALw_wcB

(٢) عشوش، د. أحمد عبد الحميد، الوسيط في القانون الدولي العام، مؤسسة الجامعة الاسكندرية ١٩٩٨، ف، ص ٥١٤.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

١– البدء باستخدام قوةٍ غير مشروعة.
٢– الردُّ على تلك القوة باستخدام عمل أو قوة غير مشروعة.
٣– أن يكون الرد متناسبًا مع الفعل غير المشروع الذي حصل ابتداءً.
٤– وجود ضرورة ألجأت للقيام بالردّ.(٣)

فهذا التعريف أعطى حدودًا للدفاع الشرعي بحيث أنه لا يمكن اللجوء إليه إلا في حالات ضيقة.

وفي جانب آخر، تناول بعض الفقهاء الدوليين مفهوم الدفاع الشرعي من منظور واسع حيث اعتبر بعضهم أن مفهوم الدفاع الشرعي ممن الممكن أن يطبق على أي اعتداء "بصفة مطلقة وأياً كان مصدره طالما أنه اعتداء غير مشروع فكل أنواع الدفاع التي تناولها الفقهاء أو التي نصت عليها القوانين الدولية ينطبق على هذا التعريف."(٤)

وقال بعضهم: من الممكن اعتبار الدفاع الشرعي أنه هو "الحق الذي يقرره القانون الدولي الجنائي لدولة أو مجموعة دول باستخدام القوة لصد عدوان مسلح حال يرتكب ضد سلامة إقليمها او استقلالها السياسي شريطة ان يكون استخدام القوة هو الوسيلة الوحيدة لدرء ذلك العدوان ومتناسبا معه."(٥)

ومما يجلي الغموض في التفاوت في بيان مفهوم الدفاع الشرعي بين التعاريف السالفة الذكر الإشارة إلى أنه قد يكون هناك خلط في استخدام مفهوم الدفاع الشرعي ومفهوم استخدام القوة كما هو واضح في التعريف الأخير حيث أن بين هذين المفهومين عموم وخصوص سنحاول إيضاحه فيما يلي. إن استخدام القوة أو مجرد التهديد بها يعتبر محظورًا وفقًا للمادة ٢ (٤) من ميثاق الأمم المتحدة والتي أكدّت على حظر "التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة".(٦) فمبدأ حظر استخدام القوة أو التهديد باستخدامها في

(٣) الكبار، محمد بحر، حق الدفاع الشرعي في القانون الدولي، مجلة جامعة الزيتونة، ٢٠١٦ ع ١٩، ٢٢٥–٢٤٠.
(٤) قاسم، د. يوسف، نظرية الدفاع الشرعي في الفقه الجنائي الإسلامي والقانون الجزائي الوضعي، دار النهضة. العربية، القاهرة، ١٩٧٩.ص ٨٨.
(٥) خلف، محمد محمود، حق الدفاع الشرعي في القانون الدولي الجنائي، الطبعة الأولى، القاهرة، مكتبة النهضة المصرية، (١٩٧٣)، ص ١٦.
(٦) ميثاق الأمم المتحدة، المادة ٢ (٤)، https://www.un.org/ar/about-us/un-charter/full-text?gclid=Cj0KCQjwnP-ZBhDiARIsAH3FSRfMT4N9DmVgZFYQwAlVzgnwB8YiSQ4oZIHlXg0d-LhAL-4aIlr00lMaAvCsEALw_wcB

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

العلاقات الدولية يعتبر مبدأً من مبادئ القانون الدولي والذي تحول فيما بعد إلى عرفٍ دولي عندما أكدت ذلك محكمة العدل الدولية في نظرها لقضية (النشاطات العسكرية وشبه العسكرية في وضد نيكاراغوا) في عام ١٩٨٦م.(٧) وعليه، فقد أصبح استخدام القوة أو مجرد التهديد بها محظورًا في القانون الدولي نظرًا لمنافاته الصريحة في تحقيق الأمن والسلم الدوليين اللذان يعتبران من مرتكزات السياسة الدولية التي لا يمكن المساس بها وفق رؤية وميثاق الأمم المتحدة.

ولكن هذا الأمر ليس على إطلاقه، فهناك استثناءان لاستخدام القوة يمكن استنتاجهما صراحةً أو ضمنًا من نصوص ميثاق الأمم المتحدة؛ فالحالة الأولى يمكن فهمها ضمنًا من نص المادة ٢ (٤) من نصوص ميثاق هيئة الأمم المتحدة والتي توحي إلى أنه من الممكن استخدام القوة فيما لا يخالف مبادئ الأمم المتحدة، أما الحالة الثانية — وهي المعنيّة في هذه الورقة – فهي إمكانية استخدام القوة في حال الدفاع الشرعي وفق ما دلت عليه صراحةً المادة ٥١ من الميثاق.(٨) فقد بيّنت هذه المادة أنه في حال "اعتدت قوة مسلحة" على دولة ما فإن للدولة المعتدى عليها خيار استخدام القوة للرّد على هذا الاعتداء. فالدفاع الشرعي وفق المادة ٥١ مشروط بوقوع اعتداء مسلح والذي يعتبر — أي الاعتداء المسلح – وفق قرار محكمة العدل الدولية في قضية نيكاراغوا أخطر شكل من أشكال استخدام القوة.(٩) وفي نفس السياق فقد أوضحت المحكمة أن الاعتداءات والمناوشات الطفيفة التي تحدث عادة بين الدول على المناطق الحدودية لا ترقى في خطورتها إلى مستوى الاعتداء المسلح الذي يتيح للدولة تفعيل حقها في الدفاع عن النفس حسبما نصت عليه المادة ٥١.(١٠) وعليه، فلا يمكن تطبيق أن النزاعات البسيطة التي تحدث

---

(٧) Judgment of the *International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States*), ١٩٨٦, I.C.J. ١٤, ٩٦-٩٧; See also, Malcolm Shaw, International Law, (٧th edition, ٢٠١٤), Cambridge University Press; Yoram Dinstein, War, Aggression and Self-defence (٣ed edition ٢٠١١).

(٨) Khan ،Kamal Ahmad, Use of Force and Human Rights under International Law, Athens Institute for Education and Research, Conference Paper Series BLE ٢٠١٧- .٢٢٠٥.

(٩) سمودي، رزق أحمد، حق الدفاع عن النفس نتيجة الهجمات السيبرانية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية المجلد ١٥ العدد ٢، ديسمبر ٢٠١٨م، ص ٣٤١.

(١٠) ICJ, case concerning *Military and Paramilitary Activities in and Against Nicaragua*) Nicaragua v. United States) , Reports ١٩٨٦, para. ١٩١.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

بين الدول على الحدود أو في المناطق البحرية أو التجارب والمناورات العسكرية التي تجريها الدول في بعض الأحيان أنها ترقى إلى خطورة ومستوى الاعتداء المسلح الذي يفعل خيار الدفاع عن النفس وإن كانت تندرج تحت مفهوم استخدام القوة.

إن الخط الفاصل بين خيار استخدام القوة أو تفعيل خيار الدفاع عن النفس يعتريه نوع من الغموض في تطبيقه، فليس كل استخدام للقوة يرقى إلى مستوى الاعتداء المسلح، وهذا ما جعل المجتمع الدولي يعجز عن الاتفاق على تعريف واضح ومحدد لجريمة العدوان (الاعتداء المسلح)؛ فقد أتى قرار الجمعية العامة لأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤م الخاص بتعريف العدوان باشتراط وجود «الخطورة الكافية» كأحد متطلبات الهجوم العسكري.(١١) وهذا القرار لم يحدّد ماهي الخطورة الكافية التي تستوجب تفعيل خيار الدفاع عن النفس. وقد اشترط بعض الفقهاء الدوليين عددًا من المعايير لاعتبار فعلٍ ما اعتداءً مسلحًا وهي: النطاق والشِّدَّة والمدّة الزمنية.(١٢)

وفي ذات السياق، أورد النظام الأساسي لمحكمة الجنايات الدولية جريمة العدوان أنها من ضمن الجرائم الداخلة في اختصاص المحكمة إلا أنه لم يُفرِد لها مادةً مستقلة تبين تفاصيلها على غرار ما فعله النظام مع الجرائم الأخرى وذلك لاستمرار عدم التوافق الأممي حول تعريف هذا المصطلح الشائك.(١٣) وهذا الأمر كان هو السائد في بداية عمل المحكمة إلى أن تم تعديل نظام المحكمة في ٢٠١٠م، وهو ما سيتم تناوله في مبحث قادم. إن عدم تعريف ما يمكن اعتباره جريمة عدوان لعدة عقود هو ما أدّى ولا يزال يقود إلى وجود تباين كبير في دلالة مفهومي استخدام القوة والاعتداء المسلح؛ ويمكن استنتاج أن كل اعتداء مسلح يُعد بطبيعة الحال استخدامًا للقوة بينما لا يمكن اعتبار أن أي استخدامٍ للقوة داخل في نطاق النزاع المسلح؛ فالاعتداء المسلح أعمّ وأشمل من استخدام القوة.(١٤)

---

(١١) UN General Assembly Res. ٣٣١٤ (XXIX), Definition of Aggression, Adopted ١٤ December ١٩٧٤.

(١٢) سمودي، رزق أحمد، مرجع سابق، ص ٣٤٢. ستتطرق الورقة عن هذه المفاهيم عند الحديث عن موقف دليل تالين من علاقة الهجمات السيبرانية بالهجوم المسلح وذلك في المطلب الثاني من المبحث الثاني

(١٣) أبرز الدول المعارضة لإدراج جريمة العدوان ضمن اختصاص المحكمة هي الولايات المتحدة الأمريكية ودولة الكيان الصهيوني، انظر: أ. كينة محمد لطفي، مفهوم جريمة العدوان في نظام المحكمة الجنائية الدولية الدائمة، مجلة دفاتر السياسة والقانون، العدد ١٤، يناير ٢٠١٦، ص ٢٩٤-٢٩٥.

(١٤) سمودي، رزق أحمد، مرجع سابق، ص ٣٤٢.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

إن الحديث عن مفهوم الدفاع الشرعي في القانون الدولي قد يتجاوز حدود هذه الورقة؛ وعليه، فلا بد من الاتفاق على أن الدفاع الشرعي يعتبر حقًا قانونيًا للدولة المعتدى عليها وفق منظور العرف الدولي، وكذلك وفق ما جاءت به المادة ٥١ من ميثاق الأمم المتحدة مع مراعاة ضوابط الدفاع الشرعي: الضرورة، والتناسب، والفورية، وهي ما أكّدتها محكمة العدل الدولية في نظرها لقضية (نيكاراغوا ضد الولايات المتحدة الأمريكية) في عام ١٩٨٦م.(١٥) فالضرورة تعني لجوء الدولة المعتدى عليها لاستخدام القوة كونها الوسيلة الوحيدة لرد الاعتداء وذلك بعد أن تكون الطرق السلمية الأخرى لم تعد مجدية.(١٦) أما الفورية، فهي تعني أن الدولة المعتدى عليها لا تمضي مدة زمنية طويلة يفوت من خلالها حقها في الدفاع عن النفس، وذلك لأن ضابط الفورية يحتم الرد السريع على الاعتداء وأن التأخير يفضي إلى منح مجلس الأمن الحق الكامل في رد الاعتداء بعد أن كان ممنوحًا لها على سبيل الاستثناء وفق المادة ٥١.(١٧) وسوف يتناول المبحث التالي الحديث عن التناسب بشكل أوسع.

المطلب الثاني: تعريف التناسب في الدفاع الشرعي ووسائل تحقيقه

يُعدّ الدفاع الشرعي حقًا طبيعيًا للدولة المعتدى عليها إلا أن له طابع مؤقتٌ واستثنائي؛ فالهدف منه وقف العدان وردّه ما استطاعت الدولة إليه سبيلًا وليس المقصود منه الانتقام أو إيقاع العقوبة على المعتدي، فهذا ليس من صلاحيات الدولة حينما تدافع عن نفسها وإنما هو من صلاحيات مجلس الأمن كما دلت عليه نصوص الميثاق. (١٨) فتقدير مضمون وحجم ومدى فعل الدفاع ليس مطلقًا بيد الدولة المعتدى عليها لأن في إعطائها مثل هذه الصلاحيات قد يؤدي إلى عكس نتائج ما تسعى إليه منظومة الأمم المتحدة في تحقيق الأمن والسلم الدوليين؛ ولأجل ذلك فقد حدّد القانون الدولي عددًا من الضوابط لضمان عدم انفراط عقد الأمن والسلم الدوليين واعتبار أن تجاوز هذه الضوابط يعدّ عدوانًا بحدّ ذاته حتى وإن كانت الغاية من نشوء هذا الحق مشروعة. ومن ضمن هذه الضوابط الموضوعة للدفاع الشرعي وفق القانون الدولي: هو مبدأ التناسب.

---

(١٥) ICJ, *supra note ٧*, para. ١٧٦.

(١٦) Stuesser ،Lee, Active Defense: State Military Response to International Terrorism, ١٧, *California Western International Law Journal*, ١٩٨٧, p.٣١.

(١٧) Dinstein ،Yoram, Computer Network Attacks and Self-Defense, ٧٦ U.S. Naval War College of International Law Studies (٢٠٠٢).

(١٨) ميثاق الأمم المتحدة، المادة ٥١، مرجع سابق.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

ويمكن تعريف التناسب في الدفاع الشرعي وفقًا للقانون الدولي على النحو التالي: إنه مبدأ ينص على أن أي استخدام للقوة يجب أن يكون متناسبًا مع الهدف الذي يرمي إليه، ولا يجب أن يتجاوز الحدود التي تكفل الدفاع اللازم والمناسب لحماية النفس أو المصالح المحمية. وبالتالي، يجب أن يكون الاستخدام المشروع للقوة أقل تدميرًا وأقل خطورة على المدنيين والممتلكات المدنية ومن الممكن السيطرة عليه، وأن يكون متناسبًا مع درجة الخطر الذي يتعرض له المدافع وحق المدافع في حماية نفسه ومصالحه.(١٩)

ويعد مبدأ التناسب أحد مبادئ القانون الدولي الإنساني والقانون الدولي العام، ويجب تطبيقه في جميع النزاعات المسلحة وفي الدفاع الشرعي. ويساعد مبدأ التناسب على حماية الأفراد والمدنيين والممتلكات والبنى التحتية الحيوية من الأضرار غير المبررة، ويحمي المجتمع الدولي من الانزلاق إلى دائرة من العنف والتصعيد. إن التناسب في الدفاع الشرعي هو مبدأ قائم على تحقيق التوازن بين الهدف المطلوب من الدفاع والقوة التي تستخدم لتحقيق هذا الهدف. ويتطلب التناسب أن يتم استخدام القوة المناسبة واللازمة والمتناسبة مع الهدف المطلوب من الدفاع، وأن تكون أي أضرار محتملة نتيجة للاستخدام المناسب للقوة أقل بقدر الإمكان.

ومن أجل تقييم مدى التناسب في الدفاع الشرعي، يمكن استخدام عدة وسائل قياس، من بينها:
١- تجنب المزيد من الضرر المتوقع للمدنيين والأهداف المدنية: يتعين على دولة الدفاع أن تقدر المخاطر المتوقعة للمدنيين والأهداف المدنية، ومقارنتها بالمزيد من الفائدة العسكرية المتوقعة من استخدام القوة العسكرية.
٢- مدى الضرر الذي يمكن تفاديه: يتعين على دولة الدفاع اتخاذ إجراءات تفادي الضرر الذي يمكن تفاديه، وتقليل أي ضرر متوقع للمدنيين والأهداف المدنية.
٣- الأهداف العسكرية المحددة: يجب أن يُحدد الهدف العسكري المستهدف بوضوح وبالتفصيل، ويتعين على دولة الدفاع تحقيق الهدف المحدد بأقل قدر من القوة الممكنة.

---

(١٩) International Law Commission, Draft articles on the responsibility of states for internationally wrongful acts, with commentaries, United Nations, ٢٠٠٦. See also, International Committee of the Red Cross, Customary International Humanitarian Law: Volume I: Rules. Cambridge University Press, ٢٠١٦.s. See also, Dinstein, Yoram, The conduct of hostilities under the law of international armed conflict. Cambridge University Press, ٢٠١٦.

مجلة العلوم الشرعية
جامعة القصيم، - المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

٤- وجود خيارات بديلة: يجب على دولة الدفاع تحقيق الهدف العسكري بأقل قدر من القوة الممكنة، وتجنب استخدام القوة العسكرية إذا كانت هناك خيارات بديلة متاحة.

٥- الطوارئ والضرورات القصوى: يجوز لدولة الدفاع استخدام القوة العسكرية بشكل أكبر في الظروف الطارئة والضرورية للدفاع عن نفسها.

كما يجب أن يتم تقييم المدى الذي يتوافق به الدفاع الشرعي مع مبدأ التناسب بموجب الظروف المحددة سالفة الذكر.[٢٠][٢١]

وأورد بعض فقهاء القانون عددًا من المحكات والاختبارات لقياس التناسب في الدفاع الشرعي، منها:

١- اختبار الأضرار المتعددة: يتمثل هذا الاختبار في تحليل الأضرار المحتملة للأطراف المتصارعة والمناطق المحيطة بها، وتحديد ما إذا كان الهجوم أو الرد المرتقب يؤدي إلى أضرار زائدة وغير متناسبة مقارنة بالمصلحة المحمية التي يرمي إليها الهجوم.

٢- اختبار المتانة العسكرية: يتمثل هذا الاختبار في تحليل قدرة الدفاع على مواجهة الهجوم والمحافظة على قدرة الدفاع على البقاء على قيد الحياة والاستمرارية.

٣- اختبار المنفعة العسكرية: يتمثل هذا الاختبار في تحليل قدرة الهجوم على تحقيق أهدافه، ومدى تأثير الرد المرتقب على قدرة الهجوم على تحقيق أهدافه.[٢٢]

٤- اختبار المنفعة الاقتصادية: ويتمثل في تحليل الآثار الاقتصادية والمادية للهجوم والرد المرتقب، وتحديد ما إذا كان الأضرار الاقتصادية والمادية لا تتناسب مع الهجوم المرتقب.

٥- اختبار الإنسانية: ويتمثل في تحليل التأثير المحتمل على المدنيين وحقوق الإنسان، وتحديد ما إذا كان الهجوم أو الرد المرتقب يخل بحقوق الإنسان أو يتسبب في ضحايا مدنيين بشكل غير متناسب.

---

(٢٠) اللجنة الدائمة للعمليات المشتركة للأركان العامة الأمريكية، "الموجه العسكري الأمريكي الجديد لقواعد الاشتباك"، ١٣ يوليو ٢٠١٦. انظر كذلك: ميثاق الأمم المتحدة، المادة ٥١. انظر أيضًا: ميشيل دوريا، القانون الدولي الإنساني: المبادئ الأساسية، المجلس الأعلى للقضاء، ٢٠١١.

(٢١) The UK Government's Legal Opinion on Forcible Measures in Response to the Use of Chemical Weapons by the Syrian Government, (٢٠١٣).

(٢٢) Gardam, J. (٢٠٠٤). *Proportionality and force in international law.* American Journal of International Law, ٩٨(٢), ٢٧٦-٣٠١.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

٦- اختبار الحاجة: ويتمثل في تحليل الحاجة الفعلية للدفاع عن النفس، وتحديد ما إذا كان الهجوم المرتقب يشكل تهديدًا حقيقيًا للأمن والسلامة العامة.(٢٣)

المطلب الثالث: مفهوم الجريمة السيبرانية

قبل البدء في تعريف الهجمات السيبرانية فإنه يستحسن توضيح ما يتعلق بها من مصطلحات مشابهة تمهد للوصول إلى معنى الهجمات السيبرانية. ولعل أبرز المصطلحات التي تتقاطع مع مفهوم الهجمات السيبرانية هو مصطلح "الجرائم السيبرانية". فقد تم إطلاقه دوليًا عن طريق معاهدة بودابست حول الجريمة السيبرانية والمعلوماتية، والتي أقرتها مجموعة من الدول الأوروبية في عام ٢٠٠١م. وتهدف هذه المعاهدة إلى تحديد جرائم تقنية المعلومات وتحديد الإجراءات الجزائية اللازمة لمكافحتها. وتشمل الجرائم السيبرانية في هذه المعاهدة على سبيل المثال لا الحصر: الاحتيال الإلكتروني، والتجسس الإلكتروني، والهجوم على الأجهزة والبرمجيات والبيانات الحساسة، وحملات البريد الإلكتروني غير المرغوب فيه، والتهديد بإيذاء المعلومات والأنظمة الحيوية.(٢٤)

ومن بين التعريفات الأخرى المتداولة للجرائم السيبرانية، يمكن الإشارة إلى التعريف الذي وضعته الشرطة الفيدرالية الأسترالية والذي يصف الجريمة السيبرانية على أنها "الجرائم الموجهة إلى أجهزة الكمبيوتر أو غيرها من تقنيات الاتصالات المعلوماتية، وتشمل الوصول غير المصرح به أو تعديل أو إضعاف أنظمة وشبكات الكمبيوتر، وسرقة المعلومات الموجودة على الأجهزة الإلكترونية وغيرها من الأعمال الإجرامية المرتكبة باستخدام الإنترنت أو وسائل التكنولوجيا الأخرى".(٢٥)

من المهم ملاحظة أن هذه التعريفات ليست ملزمة قانونًا وأن التعريف القانوني الدقيق للجرائم السيبرانية قد يختلف بين الدول والمنظمات الدولية، وبعد استقراء لعدد كبير من الصكوك والاتفاقيات الدولية مثل: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، ومشروع اتفاقية الاتحاد الأفريقي نجد أنها لم تعطِ تعريفاً محددًا للجريمة السيبرانية داخل هذه الاتفاقيات، وفي نفس الوقت، استخدمت بعض الاتفاقيات الدولية مصطلحات مشابهة للجريمة السيبرانية؛ فعلى سبيل المثال: اعتبرت اتفاقية منظمة شنغهاي للتعاون "المعلومات الحاسوبية" أنها قد تستخدم أو يتم "التأثير عليها في المجال

(٢٣) The UK Government's Legal Opinion on Forcible Measures in Response to the Use of Chemical Weapons by the Syrian Government, *supra note* at ٢١.

(٢٤) معاهدة بودابست حول الجريمة الإلكترونية والمعلوماتية (٢٠٠١)، المادة ٢ و٣.

(٢٥) Australian Federal Police ،https://www.afp.gov.au/what-we-do/crime-types/cyber-crime.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

المعلوماتي لأغراض غير مشروعة"[٢٦]، بينما عرفت اتفاقية دول الكومنولث المستقلة حول التعاون في مكافحة الجرائم في مجال المعلومات الحاسوبية الجريمة السيبرانية على أنها "جريمة تتعلق بالمعلومات الحاسوبية" أو أي "فعل إجرامي يستهدف المعلومات الحاسوبية" وذلك بدلًا من مصطلح جريمة سيبرانية.[٢٧]

وبالنظر لما سبق من تناول للتعاريف الواردة حول مفهوم الجريمة السيبرانية فإننا نستطيع القول أن أغلب الصكوك الدولية أو القوانين والتشريعات الداخلية حين تناولها لهذا المفهوم لا تسعى لتعريف دقيق حول الجريمة السيبرانية بقدر محاولتها لتحديد أفعال أو سلة من الأعمال قد تشكل جريمة سيبرانية مع إيجاد وصف دقيق للسلوك الذي يتم تجريمه ، ومع ذلك يمكن القول بأن الجريمة السيبرانية إجمالًا تشمل أي نوع من الأنشطة الإجرامية التي تستخدم تقنيات الحاسوب أو الإنترنت أو الشبكات الأخرى للتسبب في أضرار أو خسائر للأفراد أو المؤسسات أو المجتمعات، وأن عدم وجود تعريف موحد ومقبول عالميًا للهجمات السيبرانية يعد أحد التحديات في تطبيق القانون الدولي تجاه العمليات السيبرانية.

ويتضح مما سبق أن مصطلح "جريمة سيبرانية" لا يمكن تعريفه كمصطلح مفرد وأحادي، ومن الأفضل اعتبار هذا المصطلح على أنه تعبير عن مجموعة من الأفعال أو السلوكيات بدلا من اعتباره فعلا منفردا. ورغم ذلك، فإنه يمكن وصف المضمون الأساسي للجريمة السيبرانية وتقسيم الأفعال المكونة لهذا المصطلح إلى فئات منفردة والتعامل مع كل فعل على أساس أنه جريمة مستقلة يتوافر فيه الأركان الخاصة بالجريمة.

المطلب الرابع: مفهوم الهجمات السيبرانية

إن التعريف الدقيق للهجمات السيبرانية وفقًا للقانون الدولي لم يتوصل إليه بصيغة متفق عليها، وذلك يرجع إلى تعقيد طبيعة الهجمات السيبرانية وصعوبة تحديد حدودها والتعرف عليها بشكل دقيق. القانون الدولي للهجمات السيبرانية لا يزال في مرحلة التطور والنقاش، ولم يتم التوصل بعد إلى تعريف موحد وشامل للهجمات السيبرانية. نعم، توجد بعض المبادئ والقوانين التي تستخدم على نطاق دولي للتعامل مع الجرائم السيبرانية، ولكنها ليست جزءًا من نظام قانوني دولي موحد حتى الآن. منظمات دولية مثل الأمم المتحدة ومجموعة العمل المفتوحة للجرائم السيبرانية (Open-ended Intergovernmental

(٢٦) اتفاق منظمة شنغهاي، الملحق (١).

(٢٧) الاتفاقية المتعلقة بالتعاون بين بلدان كومنولث الدول المستقلة، الفقرة (أ)، المادة الأولى.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

Expert Group on Cybercrime) والاتحاد الدولي للاتصالات (ITU) يعملون على تطوير مبادئ وإطار قانوني دولي للتعامل مع الهجمات السيبرانية. ومع ذلك، لا يوجد حتى الآن تعريف قانوني دقيق للهجمات السيبرانية على المستوى الدولي.

من المهم الإشارة إلى أن الدول تعتمد على التشريعات والقوانين الوطنية للتعامل مع الهجمات السيبرانية التي تستهدفها، وتتعاون أيضًا في إطار القوانين الدولية المعمول بها لمكافحة الجرائم السيبرانية على المستوى الدولي. ومع ذلك، يمكن الإشارة إلى بعض التعاريف العامة للهجمات السيبرانية، والتي تدور في مجملها إلى أنها عمليات تستهدف الأنظمة الإلكترونية وتستخدم الأدوات والتقنيات السيبرانية للوصول إلى البيانات أو تعطيل النظام. فالهجوم السيبراني هو أي محاولة خبيثة للوصول غير المصرح به إلى نظام أو شبكة كمبيوتر، أو لتعطيل أو تعطيل أنظمة أو شبكات الكمبيوتر. يشمل هذا التعريف مجموعة واسعة من الأنشطة الخبيثة، بما في ذلك: القرصنة، والتصيد، وبرامج الفدية، وهجمات رفض الخدمة، وخروقات البيانات، وهجمات البنية التحتية وغيرها.(٢٨)

وقد قدمت بعض المنظمات الدولية والبلدان المختلفة التعاريف الخاصة بها لتحديد طبيعة ومفهوم الهجمات السيبرانية. على سبيل المثال، وصف فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (UNGGE) الهجوم الإلكتروني بأنه "عملية إلكترونية، سواء كانت هجومية أو دفاعية، من المتوقع بشكل معقول أن التسبب في إصابة أو وفاة الأشخاص أو إلحاق الضرر أو تدمير الأشياء". كما ذكر التقرير كذلك التصرفات التي تشكل هجومًا سيبرانيًا. وجاء فيه أن الهجوم السيبراني هو "الاستخدام العدائي لتكنولوجيا المعلومات والاتصالات لإلحاق الضرر بالمصالح الوطنية الأساسية للدول، والتي يمكن أن تتضمن القدرة على التجسس والاختراق والتخريب".(٢٩)

(٢٨) The Law of Cyber-Attack, Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, California Law Review
vol. ١٠٠, No. ٤, ٢٠١٢, pp. ٨١٧-٨٢٠.

(٢٩) United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), ٢٠١٥, paragraph ٣-٨.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

وبالمثل، يُعرِّف دليل تالين وهو دليل شامل للقانون الدولي المطبق على العمليات السيبرانية، الهجوم السيبراني على أنه "عملية إلكترونية، سواء كانت هجومية أو دفاعية، من المتوقع بشكل معقول أن تتسبب في إصابة أو موت أو ضرر أو تدمير".(٣٠)

المبحث الأول: الهجمات السيبرانية وعلاقتها بجريمة العدوان، وفيه ثلاثة مطالب

المطلب الأول: مخاطر الهجمات السيبرانية

تشكل الهجمات السيبرانية تهديدات مختلفة للأفراد والمنظمات والمجتمع ككل. يمكن أن يكون لهذه التهديدات عواقب وخيمة وتتطلب تدابير استباقية للتخفيف من المخاطر. أحد تهديدات الهجمات السيبرانية هو احتمال حدوث خسائر مالية فادحة. فيمكن لمجرمي الإنترنت استهداف المؤسسات المالية والشركات والأفراد للوصول غير المصرح به إلى المعلومات المالية الحساسة، مثل تفاصيل بطاقة الائتمان أو بيانات اعتماد الحساب المصرفي. يمكن أن يؤدي هذا إلى الاحتيال المالي، وسرقة الهوية، والخسائر المالية.(٣١)

ومن ضمن المخاطر هي المساومة على الخصوصية الشخصية والسرية؛ فيمكن أن تؤدي الهجمات السيبرانية إلى الوصول غير المصرح به إلى المعلومات الشخصية والكشف عنها، بما في ذلك البيانات الحساسة مثل أرقام الضمان الاجتماعي أو السجلات الطبية أو المراسلات الشخصية. وقد يترتب على ذلك عواقب وخيمة على الأفراد، بما في ذلك الإضرار بالسمعة والضرر المحتمل لحياتهم الشخصية والمهنية.(٣٢) كما تعد الهجمات السيبرانية أيضًا خطرًا على الأمن القومي. فيمكن للهجمات السيبرانية التي

(٣٠) Schmitt, M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press), ٢٠١٣, ١٠٦-١٠٧.

(٣١) Quinn S., Ivy N., Barrett M., Feldman L., Witte G., Gardner R. Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. ٢٠٢١. https://doi.org/١٠,٦٠٢٨/nist.ir.٨٢٨٦a .

(٣٢) Razaque A., Ajlan A., Melaoune N., Alotaibi M., Alotaibi B., Dias I.et al.. Avoidance of Cybersecurity Threats with the Deployment of a Web-based Blockchain-enabled Cybersecurity Awareness System. Applied Sciences ٢٠٢١;١١(١٧):٧٨٨٠. https://doi.org/١٠,٣٣٩٠/app١١١٧٧٨٨٠ .

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

ترعاها بعض الدول أن تستهدف البنية التحتية الحيوية والأنظمة الحكومية والشبكات العسكرية، مع احتمال تعطيل الخدمات الأساسية، وتعريض المعلومات الحساسة للخطر، وحتى التسبب في أضرار مادية. بالإضافة إلى أنه قد يكون لهذه الهجمات عواقب بعيدة المدى على أمن الدولة واستقرارها.(٣٣)

علاوة على ذلك، يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل الخدمات والأنظمة الأساسية. فعلى سبيل المثال، يمكن لهجمات هجمات الحرمان من الخدمات (DDoS) أن تسحق أو تعطل مواقع الويب أو الخدمات عبر الإنترنت، مما يجعل الوصول إليها غير ممكن للمستخدمين مما قد يؤدي إلى آثار اقتصادية ومجتمعية كبيرة، خاصة بالنسبة للشركات التي تعتمد على منصات الإنترنت في عملياتها أو حتى بالنسبة للدول المتطورة التي تعتمد بكثافة على الأنظمة التقنية الحديثة.(٣٤) بالإضافة إلى ذلك، يمكن أن تؤدي الهجمات السيبرانية إلى انتشار البرامج الضارة واختراق أنظمة الكمبيوتر فيمكن أن تصيب البرامج الضارة أجهزة الكمبيوتر والشبكات؛ مما يتسبب في حدوث خروقات للبيانات وفشل النظام وفقدان المعلومات الهامة وسيؤدي هذا إلى تعطل كبير وتكاليف مالية وإلحاق ضرر بسمعة المنظمة أو الدولة بصفة عامة.(٣٥)

وعلى ضوء ما سبق، تشكل الهجمات السيبرانية تهديدات مختلفة، بما في ذلك الخسائر المالية، وانتهاكات الخصوصية، ومخاطر الأمن القومي، وتعطل الخدمة، واختلالات النظام. ومن الضروري للأفراد والمنظمات والحكومات إعطاء الأولوية لتدابير الأمن السيبراني للتخفيف من هذه التهديدات والحماية من العواقب المحتملة للهجمات السيبرانية.

أما على صعيد القانون الدولي، تمثل الهجمات السيبرانية تهديدات وتحديات قانونية مختلفة. إن وصف الهجمات السيبرانية عبر الإنترنت بأنها أعمال عدوانية أو إرهاب دولي هو لا يزال موضوع نقاش. عزو الهجمات السيبرانية إلى جهات فاعلة محددة يعد

(٣٣) Steyn C., Blaauw D. Towards a Critical Review of Cybersecurity Risks In Anti-poaching Systems. iccws ٢٠٢٣;١٨(١):٥٦٠–٥٦٨. https://doi.org/١٠,٣٤١٩٠/iccws.١٨,١,١٠٩٠ .

(٣٤) Philipsen S., Andersen B., Singh B. Threats and Attacks to Modern Vehicles. ٢٠٢١ IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) ٢٠٢١. https://doi.org/١٠,١١٠٩/iotais٥٣٧٣٥,٢٠٢١,٩٦٢٨٥٧٦ .

(٣٥) Quinn S., *et all, supra note* at ٣١.

معضلة كبرى في إطار لقانون الدولي ويتزامن هذا مع الإدراك المتزايد بأن الهجمات السيبرانية يمكن أن يكون لها عواقب وخيمة وتشكل تهديدًا للسلام والأمن الدوليين.(٣٦)

أحد التهديدات القانونية للهجمات السيبرانية هو انتهاك سيادة الدولة. فيمكن اعتبار الهجمات السيبرانية التي تنشأ من دولة وتستهدف البنية التحتية أو الأنظمة الحيوية لدولة أخرى انتهاكًا للسيادة، ويثير هذا تساؤلات حول الأساس القانوني للتدابير الدفاعية واستخدام القوة للرد على الهجمات السيبرانية.(٣٧)

التهديد القانوني الآخر هو انتهاك القانون الإنساني الدولي وقانون حقوق الإنسان. إن الهجمات السيبرانية التي تستهدف البنية التحتية المدنية أو إلحاق الضرر بالمدنيين من الطبيعي جدًا اعتبارها انتهاكات لهذه الأطر القانونية الدولية. كما يثير استخدام الهجمات السيبرانية في العمليات العسكرية تساؤلات أخلاقية حول استخدام القوة في العلاقات الدولية واحتمالية حدوث أضرار جانبية غير مقصودة.(٣٨)

يؤدي عدم وجود تعريف مقبول عالميًا للجرائم السيبرانية إلى تعقيد الاستجابة القانونية للهجمات السيبرانية، فيمثل تطبيق قوانين الجرائم الإلكترونية ومحاكمة مجرمي الإنترنت عبر الحدود تحديًا كبيرًا في القانون الدولي؛ ومع هذا، فقد حاول عدد من المؤسسات

---

(٣٦) Lobach D. Cyberattacks as a Crime of Aggression and International Terrorism: Legal Qualification Problems. The European Proceedings of Social and Behavioural Sciences ٢٠٢٢. https://doi.org/١٠,١٥٤٠٥/epsbs.٢٠٢٢,٠٦,٧٠, Mazaraki N., ГОНЧАРОВА Ю. Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' Of International Law to Adress Economic Damages. BJES ٢٠٢٢;٨(٢):١١٥–١٢٠. https://doi.org/١٠,٣٠٥٢٥/٢٢٥٦-٠٧٤٢/٢٠٢٢-٨-٢-١١٥-١٢٠, Greco G. Cyber-attacks As Aggression Crimes in Cyberspace In the Context Of International Criminal Law. EJPSS ٢٠٢٠;٤(١). https://doi.org/١٠,٤٦٨٢٧/ejpss.v٤i١,٩٣٧.

(٣٧) Spáčil J. Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations. MUJLT ٢٠٢٢;١٦(٢):٢١٥–٢٣٩. https://doi.org/١٠,٥٨١٧/mujlt٢٠٢٢-٢-٤. See also, Ali S. Legal Framework of Right of Self Defense in Cyber Warfare: Application Through Laws Of Armed Conflict. JDSS ٢٠٢٢;٣(II). https://doi.org/١٠,٤٧٢٠٥/jdss.٢٠٢٢(٣-ii)٩٦.

(٣٨) أخلاقيات الحرب السيبرانية: استكشاف استخدام الهجوم الإلكتروني في العمليات العسكرية، IRJMETS، ٢٠٢٣، https://doi.org/١٠,٥٦٧٢٦/irjmets٣٥٣٨٥.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

والأطر القانونية الدولية للتصدي للتهديدات السيبرانية، ولعبت المنظمات الدولية دورًا حاسمًا في تطوير القانون الدولي في مجال الأمن السيبراني، ومن ذلك: دليل تالين سالف الذكر والذي دعا إلى توفير إرشادات خاصة حول تطبيق القانون الدولي على الحرب السيبرانية. وعلى الرغم من ذلك؛ فلا تزال التحديات القانونية قائمة ومعقدة وذلك لعدم التوصل إلى اتفاق دولي موحد وشامل حول كيفية التعامل مع هذه التهديدات نظرًا لتسارع وتيرة التطور التقني والاكتشافات الهائلة والضخمة في هذا المجال وعدم توافق الرؤى الدولية حيالها.

المطلب الثاني: مفهوم وشروط تحقق جريمة العدوان

نص قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ (XXIX) الذي تم تبنيه في عام ١٩٧٤م على تجريم العدوان. واعتباره جريمة منددًا فيها. فيوفر هذا القرار الأساس لفهم مفهوم العدوان في القانون الدولي.[٣٩] ومع ذلك، فقد ظل هذا المصطلح دون تعريف دولي متفق عليه حتى مع بداية إنشاء محكمة الجنايات الدولية. فقد تم ذكر جريمة العدوان في نظام روما الأساسي للمحكمة الجنائية الدولية ١٩٩٨م ولكن لم يتم تعريف الجريمة بطريقة تفصيلية. فتعريف جريمة العدوان هي إضافة حديثة نسبيًا إلى اختصاص المحكمة الجنائية الدولية، حيث تم وضع تعريف وشروط الجريمة في عام ٢٠١٠ في المؤتمر الاستعراضي لنظام روما الأساسي في كمبالا، أوغندا. قبل ذلك، لم تكن جريمة العدوان معرّفةً تعريفًا صريحًا بأركانها وشروطها وإن كان الاتفاق على أنها جريمة موجودًا بموجب القانون الدولي.[٤٠] وهذا التأخر في تعريف جريمة العدوان يعود إلى عدة أسباب أبرزها هو تنازع الاختصاص بين محكمة الجنايات الدولية ومجلس الأمن الدولي الذي يعنى بشكل أساس في حفظ الأمن والسلم الدوليين وفق ما نص عليه ميثاق الأمم المتحدة؛ وهذا ما تم تجاوزه نسبيًا في التعديل الجديد لنظام محكمة الجنايات الدولية.

فيمكن للمحكمة أن تمارس اختصاصها على جريمة العدوان بمجرد اعتماد حكم وفقًا للمادتين ١٢١ و١٢٣ من نظام روما الأساسي، اللتين تحددان الجريمة وتحددان الشروط التي بموجبها تمارس المحكمة اختصاصها كما يجب أن يكون الحكم متسقًا مع

(٣٩) لوباتش، د. "الجريمة الدولية": مناهج مختلفة لمسألة تعريف المفهوم، (٢٠٢٢م).

(٤٠) سياب، حكيم، مفهوم جريمة العدوان في ظل تطوّر نظام روما الأساسي للمحكمة الجنائية الدولية، مجلة أبحاث قانونية وسياسية، (٢٠١٧)، ٢٢٧.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

الأحكام ذات الصلة من ميثاق الأمم المتحدة.(٤١) فللمحكمة الجنائية الدولية (ICC) اختصاص قضائي على جريمة العدوان منذ ١٧ يوليو ٢٠١٨م، ولكن فقط بالنسبة لتلك الدول التي صادقت على التعديلات الخاصة بجريمة العدوان التي تم تبنيها في مؤتمر كمبالا في عام ٢٠١٠م. ويمكن للمحكمة الجنائية الدولية ممارسة اختصاصها على جريمة العدوان إما بالإحالة من مجلس الأمن التابع للأمم المتحدة، أو بالإحالة من دولة طرف، أو بمبادرة من المدعي العام، مع مراعاة شروط معينة.(٤٢)

وتجدر الإشارة إلى أنه تختلف جريمة العدوان عن مسؤولية الدولة عن العدوان. فبينما يمكن للمحكمة الجنائية الدولية مقاضاة الأفراد على أعمال العدوان، فإن مسؤولية الدولة عن العدوان هي مسألة منفصلة حيث يركز اختصاص المحكمة الجنائية الدولية على المسؤولية الجنائية الفردية فقط. فما يهم في هذا المبحث هو إيضاح التوافق الدولي على تعريف مصطلح جريمة العدوان التي ظلت عددًا من العقود يكتنفها الكثير من الغموض. وقد نصت المادة الثامنة مكررًا، فقرة (٢) من نظام المحكمة الجنائية الدولية على أن جريمة العدوان تعني: "استعمال القوة المسلحة من جانب دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة أي عمل من الأعمال التالية، سواء بإعلان حرب أو بدونه ".(٤٣)

ويقوم الركن المادي للجريمة وفق ما ذكرته المادة الثامنة مكرر، فقرة (١) من نظام روما الأساسي بذكر عدد من الأشكال التي تجسد الصورة الإيجابية لجريمة العدوان وفق ما يلي:

١– استخدام القوة المسلحة: يجب أن يشمل العمل العدواني استخدام القوة المسلحة من قبل دولة ضد دولة أخرى. ويمكن أن يشمل ذلك أعمالًا مثل الغزو أو الاحتلال العسكري أو الهجوم.

---

(٤١) وونغ إم، العدوان ومسؤولية الدولة في المحكمة الجنائية الدولية. ICLQ ٢٠٢١ ؛ ٧٠ (٤): ٩٦١–٩٩٠. https://doi.org/١٠,١٠١٧/s٠٠٢٠٥٨٩٣٢١٠٠٠٣٧٣.

(٤٢) واد، ن. "نظام روما الأساسي: مراجعة نقدية لـ دور Swgca في تحديد جريمة العدوان." بيجيا ١ (٦) (٢٠٢٣)، . https://doi.org/١٠,٥٢٣٣٧/pjia.v٦i١,٧٠٣، انظر أيضًا، الخبر في موقع المحكمة الجنائية الدولية، ١٥ ديسمبر ٢٠١٧، https://www.icc-cpi.int/news/assembly-activates-courts-jurisdiction-over-crime-aggression.

(٤٣) المادة الثامنة مكررًا، فقرة (٢) من نظام روما الأساسي للمحكمة الجنائية الدولية، A/CONF.١٨٣/٩، ١٩٩٨.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

٢- انتهاك ميثاق الأمم المتحدة: يجب أن يكون الفعل انتهاكًا للمبادئ الواردة في ميثاق الأمم المتحدة. كما يحظر الميثاق استخدام القوة في العلاقات الدولية إلا في حالات الدفاع عن النفس أو عندما يأذن بها مجلس الأمن التابع للأمم المتحدة بموجب الفصل السابع.

٣- خطورة الحجم والشخصية: يجب أن يظهر العمل العدواني مستوى من الجدية، من حيث الحجم والشخصية، يمكن مقارنته بالجرائم الدولية الأخرى مثل جرائم الحرب والإبادة الجماعية والجرائم ضد الإنسانية. يضمن هذا المطلب أن أعمال العدوان الخطيرة هي فقط تلك التي تعتبر جرائم بموجب القانون الدولي.

٤- المنصب القيادي: يجب أن يرتكب الفعل شخص في منصب قيادي داخل دولة، مثل زعيم سياسي أو عسكري، الذي يتحكم أو يدير بشكل فعال الجيش أو قوات الأمن. يهدف هذا المطلب إلى مساءلة أولئك الذين في مواقع السلطة عن أعمال العدوان المرتكبة تحت سلطتهم.(٤٤)

المطلب الثالث: العلاقة بين الهجمات السيبرانية وجريمة العدوان

الفرع الأول: موقف القانون الدولي

الهجمات السيبرانية هي شكل سريع التطور من أشكال الجريمة التي ظهرت مع تقدم تكنولوجيا المعلومات والاتصالات. وتعتبر الهجمات السيبرانية وجريمة العدوان في القانون الدولي مفهومان متمايزان من حيث الأصل، ومع ذلك؛ فهناك مناقشات حول تقاطعهما وآثارهما في الإطار القانوني. ويمكن اعتبار هذه الهجمات جرائم عدوان نظرًا لتأثيرها. وقد أقر المجتمع الدولي بالحاجة إلى التنظيم والتعاون الدوليين للتصدي للهجمات السيبرانية كجرائم عدوان.(٤٥) كما أن نظام روما الأساسي للمحكمة الجنائية الدولية يوفر أساسًا قانونيًا لتحديد مسؤولية الدولة عن العدوان إلا أن هناك مناقشات حول ما إذا كان يمكن اعتبار

(٤٤) المادة الثامنة مكررًا، فقرة (١) من نظام روما الأساسي للمحكمة الجنائية الدولية، A/CONF.١٨٣/٩، ١٩٩٨.

(٤٥) The Urgency of International Regulation Regarding Cyber Attack with An Indication of Aggression Crime in Asean. ٢٠٢٣. https://doi.org/١٠,٥٢٧٨٣/rlj.v١١i١,٢٩٣.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

العدوان في سياق الهجمات السيبرانية شكلاً من أشكال قيام المسؤولية الدولية.(٤٦) ولا يزال هناك نقاش مستمر بشأن تصنيف الهجمات السيبرانية على أنها جرائم عدوان.(٤٧)

أدى غياب تعريف "التهديد باستخدام القوة" أو "استخدام القوة" في ميثاق الأمم المتحدة (١٩٤٥م) إلى مشكلة في تفسيره. وقد تم سد هذه الفجوة باعتماد قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ (١٩٧٤م) بشأن تعريف العدوان، عندما وافقت الدول بموجبه بالإجماع على أن "القوة" تعني "القوة المسلحة" فيما يخص المادة ٢، الفقرة ٤ من ميثاق الأمم المتحدة.(٤٨) يعد دليل تالين –الدراسة الأكثر موثوقية وغير الملزمة حول انطباق القانون الدولي على الحرب السيبرانية – وثيقة شاملة توفر إرشادات حول تطبيق القانون الدولي في سياق الحرب السيبرانية، بما في ذلك الهجمات السيبرانية. وفي حين أن دليل تالين لا يتعامل على وجه التحديد مع الهجمات السيبرانية التي تسبب ضائقة نفسية على أنها ترقى إلى مستوى هجوم إرهابي، إلا أنه يوفر إطارًا لتحليل شرعية العمليات السيبرانية فيما يتعلق بالقانون الدولي.(٤٩)

ينعكس هذا المنظور أيضًا في تعريف الهجوم السيبراني الذي قدمه دليل تالين سالف الذكر حيث أشار إلى أنه كي يتم اعتبار الهجوم السيبراني استخدمًا للقوة فإنه يجب أن تكون العملية السيبرانية قابلة للمقارنة من حيث الحجم والتأثيرات لتلك الخاصة بالهجوم الحركي التقليدي.(٥٠) لذلك، عند تقييم ما إذا كانت العملية الحاسوبية تعادل استخدام القوة، فإن في حقيقة الأمر أن استخدام القوة قد تم تنفيذها بالوسائل الحاسوبية ليست ذات صلة. وفي هذا الصدد، أكدت محكمة العدل الدولية في فتواها أن الفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة تنطبق على " أي استخدام للقوة، بصرف النظر عن الأسلحة المستخدمة".(٥١) لذلك، فإن اندراج بعض الهجمات السيبرانية تحت مفهوم القوة المسلحة يسمح لمجلس الأمن التابع للأمم المتحدة بالتصرف

---

(٤٦) أبو القاسم، م. ليلى عيسى، المسؤولية الدولية عن جريمة العدوان بالهجمات السيبرانية في ضوء أحكام القانون الدولي، ٢٠٢١م. https://doi.org/١٠,٢٣٩١٨/ilic٢٠٢١,١٨

(٤٧) Greco G. Cyber-attacks As Aggression Crimes in Cyberspace in the Context of International Criminal Law. EJPSS ٢٠٢٠;٤(١). https://doi.org/١٠,٤٦٨٢٧/ejpss.v٤i١,٩٣٧.

(٤٨) المرجع السابق.

(٤٩) Schmitt, M. N., *Supra note* at ٣٠.

(٥٠) القاعدة ٦٩، دليل تالين ٢,٠ بشأن القانون الدولي المطبق على العمليات السيبرانية، الإصدار الثاني

(٥١) فتوى محكمة العدل الدولية بشأن شرعية التهديد بالأسلحة النووية أو استخدامها لعام ١٩٩٦، ص ٢٢.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

بموجب الفصل السابع من ميثاق الأمم المتحدة وللدول المعتدى عليها كذلك أن ترد دفاعًا عن النفس.(٥٢) الهجمات السيبرانية هي جرائم عبر وطنية تتطلب تعاونًا دوليًا لمعالجتها بفعالية وتطوير نظام دولي يحظى بالقبول والاحترام عالمياً من قبل المجتمع الدولي يعتبر شيئًا ضروريًا لتنظيم الهجمات السيبرانية كجرائم عدوان.(٥٣)

الفرع الثاني: موقف القانون الدولي الجنائي

إن مفهوم الجريمة السيبرانية يشير تقليديًا إلى الأنشطة غير القانونية التي تتم عبر شبكات الكمبيوتر، مثل القرصنة وخرق البيانات والاحتيال المالي. وعلى الرغم من ذلك، فقد أدى التطور والحجم المتزايد للهجمات السيبرانية إلى إثارة مخاوف بشأن إمكانية تسببها في إلحاق ضرر كبير بالدول وسكانها. وقد أدى ذلك إلى دعوات لفهم أوسع للجرائم السيبرانية التي تشمل الهجمات على الأمن القومي والبنية التحتية الحيوية. وقد أدى النقاش حول إمكانية تطبيق القانون الدولي الإنساني إلى الاستنتاج الأساسي القائل بأنه على الرغم من عدم وجود أحكام محددة بشأن القانون الدولي الإنساني، فإن هذه المجموعة من القوانين مرنة بما يكفي لتكون ذات صلة بالعمليات السيبرانية التي تحدث أثناء النزاع المسلح الدولي وكذلك الصراع المسلح غير الدولي. على وجه الخصوص، فإن المبادئ الأساسية للعدالة في الحرب أي مبادئ (التمييز والاحتياط والتناسب) قابلة للتطبيق.(٥٤)

وفي حين أن هذا التطور قد يبدو كتوسيع للقدرة القضائية للمحكمة الجنائية الدولية لمحاكمة الأفراد على جرائم أساسية أخرى، عدد من فقهاء القانون عبروا عن قلقهم من أن جريمة العدوان سيكون لها تطبيق صارم للمفاهيم الحديثة للحرب وذلك بالنظر إلى العديد من القضايا المتعلقة بالهجمات السيبرانية التي بدأت فعليًا بالظهور. فتنص الفقرة ١من المادة ٨ مكرر من نظام روما الأساسي على تعريف جريمة العدوان بأنها "التخطيط أو التحضير أو الشروع أو التنفيذ من قبل شخص ما له وضع يمكِّنه فعلًا من التحكم في العمل السياسي أو العسكري للدولة من القيام بعمل عدواني يشكل بحكم طابعه وخطورته ونطاقه انتهاكًا واضحًا

(٥٢) المادة ٥١ من ميثاق الأمم المتحدة. انظر أيضًا: Greco G., *Supra note* at ٤٨.

(٥٣) Maskun M., Irwansyah I., Yunus A., Safira A., Lubis S. Cyber-attack: Its Definition, Regulation, and Asean Cooperation to Handle with It. home ٢٠٢١;٤(٢):١٣١-١٥٠. https://doi.org/١٠,٢٢٤٣٧/jlj.٤,٢,١٣١-١٥٠ .

(٥٤) Chaumette, A. L. (٢٠١٨). International Criminal Responsibility of Individuals in Case of Cyberattacks. International Criminal Law Review, ١٨, ١-٣٥.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

لميثاق الأمم المتحدة".(٥٥) هذه الصياغة تجعل من المستحيل صراحة على المحكمة الجنائية الدولية لمحاكمة الأفراد الذين يتصرفون بمفردهم أو الذين يمكن أن يقودوا مجموعة من "الفاعلين غير الحكوميين". أبعد من ذلك، من المرجح أن تقوم الدول نفسها بالتوظيف مخترقين من القطاع الخاص لإجراء عمليات الهجمات السيبرانية، حيث يتطلب وجود مهارات تقنية عالية لتنفيذ بعض الهجمات الخطيرة. ومع ذلك، وكما كان متوقعًا، فإن مسألة الإسناد تجعل من الصعب إثبات الصلة بين الدولة التي جندت ذلك الهاكر والهجمات المنفذة. وحتى لو كان هذا ممكنًا، فإن المخترق لا يزال غير مسؤول. أما في حالة الجرائم الثلاثة الأساسية الأخرى، فإذا أدت عملية الاختراق من قبل الهاكر إلى ارتكاب ما يستوجب قيام مسؤولية جنائية فردية وفقًا للمادة ٢٥ من نظام روما الأساسي، فهذا ليس هو الحال مع جرائم العدوان. فتشترط المادة ٢٥، الفقرة ٣ مكررًا، ألا ينطبق هذا الحكم إلا على الأشخاص الذين يتصرفون بصفتهم كقادة. علاوة على ذلك، فإن المادة ٨ مكرر، الفقرة ١، تضع بالفعل معيارًا عاليًا كي تكون الهجمات كافية للمقاضاة وفق نظام المحكمة الجنائية الدولية، حيث يجب أن تشكل انتهاكًا "واضحًا" لميثاق الأمم المتحدة. فمجال تطبيق هذه الصيغة متعمد أن يكون مقيّدًا وذلك لتجنب خضوع بعض الهجمات الطفيفة من الملاحقة القضائية.(٥٦)

المادة ٨ مكرر، الفقرة ٢، من نظام روما الأساسي هي نسخة طبق الأصل من المادتين ١ ٣ من القرار ٣٣١٤ لعام ١٩٧٤م بشأن تعريف العدوان. وهذا يمكن أن يمثل عقبة فيما يخص تطبيق الهجمات السيبرانية على كونها جريمة عدوان وذلك بالنظر إلى أن تعريف العدوان يتعلق فقط بالاستخدام التقليدي للقوة، والذي ينطبق فقط على الدول ويستند إلى المفاهيم التقليدية مثل السلامة الإقليمية للدولية. صياغة العبارات في المادة ٨ مكرر لها عاملان مهمان محددان: أولًا، ترحيل توصيف الجريمة الدولية الى قرار الجمعية العامة للأمم المتحدة لعام ١٩٧٤م – على الرغم من أن أنماط الحرب المعاصرة وأساليبه قد تغيرت وتشابكت وأصبحت أكثر تعقيدًا – إلا أن التعريف الجديد اشتمل فقط على التعريف القديم الذي تبلورت معانيه في أعراف القانون الدولي والمعاهدات الدولية التي حدثت بعده. أيضا، أعمال العدوان تم تعريفها بالطريقة التي تتم بها (النهج الأداتي) أي

(٥٥) المادة الثامنة مكررًا، فقرة (١) من نظام المحكمة الجنائية الدولية.

(٥٦) Greco G. *Supra note* at ٤٨.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

الوسيلة التي ارتكبت من خلالها الجريمة، بدلاً من النظر في عواقبها (النهج التأثيري)، مما يجعل من الصعب إسقاط الهجمات السيبرانية ضمن نطاق المادة.(٥٧)

ومع ذلك، هناك آراء مختلفة حول ما إذا كان ينبغي الاعتراف بالهجمات السيبرانية، بما في ذلك تلك التي تهدد الأمن القومي وتعطل شبكات الاتصال، كجرائم عدوان بموجب القانون الدولي. ويجادل البعض بأن تأثير الهجمات السيبرانية على السيادة والأمن القومي يبرر تصنيف هذه الهجمات كجرائم عدوان. وهم يعتقدون أن المفهوم التقليدي للجريمة السيبرانية يجب تعديله لمواجهة هذه التهديدات المتطورة.(٥٨)

فيجادل بعضهم أن تعريفات مؤتمر كمبالا يمكن تفسيرها بمرونة من قبل قضاة المحكمة الجنائية الدولية لتشمل الهجمات السيبرانية. إلى جانب ذلك، ووفقًا للمادة ٤ من قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ بشأن تعريف العدوان، يمكن لمجلس الأمن التابع للأمم المتحدة تحديد الأعمال الأخرى التي تشكل عدوانًا، وبالتالي من المحتمل أن تندرج الهجمات السيبرانية ضمن هذه الفئة. ويقول بعضهم مستخدمين أيضًا نفس الرؤية العريضة لتفسير جريمة العدوان على الهجمات السيبرانية أنه: "يمكن أن تشكل القوة السيبرانية جزءًا من القوات المسلحة للدولة، ومن السهل جدًا إسقاط الهجمات السيرانية ضمن النطاق القانوني لأفعال جريمة العدوان الواردة في المادة ٨ مكرر للفقرات (أ) و (ب) و (ج) و (د) و (هـ)، وأما ما يتعلق بالفقرة (ز) فإن الهجمات السيبرانية يرتكبها قراصنة يمكن اعتبارهم مرتزقة ".(٥٩)

---

(٥٧) Kocibelli, A., Aggression, From Cyber-Attacks to ISIS: Why International Law Struggles to Adapt. Michigan Journal of International Law, ٢٠١٧, p. ٣٩.

(٥٨) Trahan J. The Criminalization of Cyber-operations Under the Rome Statute. Journal of International Criminal Justice ٢٠٢١;١٩(٥):١١٣٣-١١٦٤. https://doi.org/١٠,١٠٩٣/jicj/mqab٠٦٦.

(٥٩) Papanastasiou, A. Application of International Law in Cyber Warfare Operation, ٢٠١٠, https://dx.doi.org/١٠,٢١٣٩/ssrn.١٦٧٣٧٨٥.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

وقد خلص فريق الخبراء الحكوميين التابع للأمم المتحدة إلى أن الأفعال المرتكبة بوسائل الكمبيوتر يمكن تصنيفها على أنها جرائم حرب كما هو الحال في المادة ٨ من نظام روما الأساسي، ٢٠٠٢م إذا كانت تستوفي وجود الفعل الإجرامي والقصد الجنائي شريطة أن يكون هناك رابط عدواني، أي أن مثل هذه الهجمات جزء من الصراع المستمر.(٦٠)

ومما يجدر بالذكر أن الاعتراف بالهجمات السيبرانية كجرائم عدوان بموجب القانون الدولي سيكون له تداعيات كبيرة. قد يعني ذلك أن بإمكان الدول الاحتجاج بالحق في الدفاع عن النفس أو اتخاذ إجراءات جماعية ضد الهجمات السيبرانية التي تهدد سيادتها أو أمنها القومي. ومع ذلك، هناك تحديات في تعريف الهجمات السيبرانية وعزوها إلى جهات فاعلة محددة، فضلاً عن تحديد آليات الاستجابة والمساءلة المناسبة. (٦١)

وتأكيدًا لما سبق، فلا يزال الوصف القانوني للهجمات السيبرانية على أنها جرائم عدوان بموجب القانون الدولي الجنائي موضوع نقاش مستمر ولا يزال يثير الكثير من الجدل غير المحسوم. وتظل الهجمات السيبرانية باعتبارها جريمة عدوان وفق قواعد القانون الدولي بحاجة إلى مزيد من التطوير والتوضيح نظرًا للطبيعة المتطورة للحرب السيبرانية والتحديات الفريدة التي تطرحها مما يتطلب دراسة وتحليل دقيقين لضمان التنظيم الفعال والاستجابة للتهديدات السيبرانية داخل المجتمع الدولي.

(٦٠) Ambos, K. (٢٠١٥). International criminal responsibility in cyberspace. in Research Handbook on International Law and Cyberspace. Edward Elgar Publishing. See also, Schmitt, M. N. *Supra note* at ٣٠.

(٦١) Schmitt, M. N. *Supra note* at ٣٠.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

المبحث الثاني: علاقة المادة ٥١ من ميثاق الأمم المتحدة بالهجمات السيبرانية، وفيه ثلاثة مطالب

تعتبر المادة ٥١ من ميثاق الأمم المتحدة مادة حاسمة تتناول حق الدولة في الدفاع عن النفس رداً على الهجمات المسلحة. فتمنح الدول حق الدفاع عن النفس، بما في ذلك استخدام القوة، عندما تتعرض لهجمات مسلحة. ولايزال تفسير المادة ٥١ وتطبيقها موضع نقاش وتحليل في الدراسات القانونية.

فيجادل البعض بأن الميثاق يسمح باتخاذ إجراءات قسرية عندما يأذن بها أعضاء مجلس الأمن بالتصرف بشكل جماعي وفقًا للقواعد المعمول بها. فهم يعتقدون أن توسيع المادة ٣٩ [٦٢] لتشمل القضايا التي لم تكن تعتبر تهديدات للسلم والأمن الدوليين عندما تم التوقيع على ميثاق الأمم المتحدة يعتبر أمرًا مشروعا بسبب الحقائق المتغيرة في العالم وفي أساليب الحرب.[٦٣] كما تم فحص النتائج القانونية ونطاق المادة ٥١ في عدة سياقات مختلفة. فقد تم الاحتجاج به لتبرير أعمال الدفاع عن النفس، بما في ذلك ضربات الطائرات بدون طيار، رداً على الهجمات المسلحة. ومع ذلك، يحذر الخبراء من أن مفهوم الدفاع عن النفس "مرن للغاية" وقد لا يتوافق دائمًا مع نطاق المادة ٥١.[٦٤]

ومما يثيره تفسير المادة ٥١ أيضًا هي مشكلة العنف المسلح الذي تسببه جهات فاعلة غير حكومية تقع في أراضي دول ثالثة؛ فيجادل البعض بأن قانون ميثاق الأمم المتحدة الذي يحكم الدفاع عن النفس غير كافٍ لمعالجة هذه الأساليب الناشئة في التسلح العنف. وعلى ذلك، فإن بعض الفقهاء القانونيين يقترحون أطرًا قانونية بديلة، مثل حالة الضرورة، كظرف يستبعد عدم المشروعية،

جاء نص المادة كما يلي: " يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، (٦٢) ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ ٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه."

(٦٣) Binder M., Heupel M. The Legitimacy of the Un Security Council: Evidence from Recent General Assembly Debates. Int Stud Q ٢٠١٤;٥٩(٢):٢٣٨–٢٥٠. https://doi.org/١٠,١١١١/isqu.١٢١٣٤.

(٦٤) Lushenko P., Raman S., Kreps S. Multilateralism and Public Support for Drone Strikes. Research & Politics ٢٠٢٢;٩(٢):٢٠٥٣١٦٨٠٢٢١٠٩٣٤. https://doi.org/١٠,١١٧٧/٢٠٥٣١٦٨٠٢٢١٠٩٣٤٣٣.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

وذلك للسماح بالدفاع عن النفس خارج الحدود الإقليمية ضد الجهات الفاعلة غير الحكومية مع الحفاظ على سيادة الدولة الإقليمية.(٦٥)

تسبب استخدام القوة وتفسير المادة ٥١ في انقسامات أساسية بين الدول. فهناك خلاف حول التفسير الصارم لحظر استخدام القوة وما إذا كان يسمح بالتدخل الإنساني. كما أن هناك أيضًا خلاف حول نطاق الحق في الدفاع عن النفس، وقد أدى الرد على هجمات الحادي عشر من سبتمبر الإرهابية إلى إعادة تقييم جوهرية للقانون في هذا المجال.(٦٦)

وقد تم تفسير المادة ٥١ كذلك وربطها فيما يتعلق بالحرب السيبرانية. فيجادل البعض بأن الهجمات السيبرانية عبر الإنترنت يمكن اعتبارها هجمات مسلحة تؤدي في النهاية إلى حق الدولة في الدفاع عن النفس لأنها تعتبر هجمات مسلحة غير تقليدية، بينما يشكك البعض الآخر في إمكانية تطبيق المادة ٥١ على العمليات السيبرانية. وهذا ما سيتم تغطيته في مطلب لاحق.

المطلب الأول: شروط تطبيق المادة ٥١ من ميثاق الأمم المتحدة

تشترط المادة ٥١ من ميثاق الأمم المتحدة تطبيق حق الدفاع عن النفس رداً على الهجمات المسلحة. ويسمح بفرض قيود مؤقتة على حظر استخدام القوة بموجب المادة ٢ (٤) من الميثاق. يُعترف بالحق في الدفاع عن النفس كحق أصيل للدول؛ فتسمح المادة ٥١ للدولة باللجوء إلى الدفاع الفردي أو الجماعي عن النفس في حالة وقوع هجوم مسلح حتى يتخذ مجلس الأمن تدابير للحفاظ على السلم والأمن الدوليين.(٦٧) وقد جاء نص المادة ٥١ من ميثاق الأمم المتحدة كما يلي:

> "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس

(٦٥) موغولون، م. نداء من الضرورة: إطار معياري مقبول للدفاع عن النفس خارج الحدود الإقليمية ضد الجهات الفاعلة غير الحكومية. IUSETVERITAS، (٢٠٢١م) ، ٦٣ ، ١٥–٣٥. https://doi.org/١٠,١٨٨٠٠/iusetveritas.٢٠٢١٠٢,٠٠١.

(٦٦) Gray C. ٢٠. the Use of Force and The International Legal Order. International Law ٢٠١٨. https://doi.org/١٠,١٠٩٣/he/٩٧٨٠١٩٨٧٩١٨٣٦,٠٠٣,٠٠٢٠.

(٦٧) Chinkin C., Kaldor M. International Law and New Wars. ٢٠١٧. https://doi.org/١٠,١٠١٧/٩٧٨١٣١٦٧٥٩٨٦٨.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه."(٦٨)

ويشترط للدولة عند الحاجة إلى الممارسة القانونية لحق الدفاع عن النفس في القانون الدولي عدة شروط هي كالتالي:

١. **وجود هجوم مسلح**، وهذا يعني أنه يجب أن يكون هناك تهديد حقيقي ووشيك بالهجوم أو الهجوم الفعلي من قبل دولة أخرى. إن وجود هجوم مسلح هو الشرط الأول والأكثر أهمية للممارسة القانونية لحق الدفاع عن النفس في القانون الدولي. وهذا يعني أنه يجب أن يكون هناك تهديد حقيقي ووشيك بالهجوم أو الهجوم الفعلي من قبل دولة أخرى. الجدير بالذكر أنه ليس من السهل تعريف مفهوم "الهجوم المسلح" دائمًا كما أسلفنا؛ فيمكن أن يشمل هذا المصطلح مجموعة واسعة من الأعمال؛ فعلى سبيل المثال:

- استخدام القوة العسكرية، مثل الغزو أو المداهمة بالقنابل؛
- التهديد باستخدام القوة العسكرية، مثل الحشود العسكرية على الحدود؛
- دعم الجماعات الإرهابية التي تخطط لمهاجمة دولة أخرى.

إن المفتاح لتحديد ما إذا كان الفعل يشكل هجومًا مسلحًا هو ما إذا كان من المحتمل أن يتسبب هذا الهجوم في ضرر جسيم للدولة التي تدافع عن نفسها. فإذا كان من المحتمل أن يتسبب العمل في ضرر جسيم، فسيتم اعتباره هجومًا مسلحًا، حتى لو لم يتضمن استخدام القوة العسكرية(٦٩). أما شرط أن يكون الهجوم وشيكًا فيعني أن الدولة التي تدافع عن نفسها يجب أن يكون لها رأي مقبول الاعتقاد بأن الهجوم على وشك الحدوث. وهذا يعني أنه لا يمكن للدولة استخدام القوة دفاعًا عن النفس إذا كان الهجوم مجرد احتمال.(٧٠)

---

(٦٨) ميثاق الأمم المتحدة، المادة ٥١، مرجع سابق.

(٦٩) حميد، علي حسين وهاشم، فراس عباس، الأبعاد الجيوبوليتيكية للدبلوماسية الدفاعية العراقية: نحو مقاربة جديدة في السياسية الخارجية. قضايا سياسية ٢٠٢٢ (٦٩). https://doi.org/١٠,٥٨٢٩٨/٢٠٢٢١٠٢.

(٧٠) مرسلي، د. عبد الحق، ضوابط الدفاع الشرعي في القانون الدولي، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد ٧، العدد ٦،

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

ومعنى شرط أن يكون الهجوم حقيقيًا فهذا يعني أن الدولة التي تدافع عن نفسها لا يمكنها استخدام القوة في الدفاع عن النفس إذا كان الهجوم مجرد نسج من خيالها. فيجب أن يكون لدى الدولة دليل على أن الهجوم يتم التخطيط له أو تم تنفيذه بالفعل. فمسألة وجود هجوم مسلح تعد مسألة قانونية معقدة، ولا توجد طريقة سهلة لتحديد ما إذا كان الفعل يشكل هجومًا مسلحًا. ورغم ذلك، فإن الشروط المنصوص عليها في المادة ٥١ من ميثاق الأمم المتحدة توفر إطارًا مفيدًا لتقييم ما إذا كان استخدام القوة في الدفاع عن النفس قانونيًا.

تجدر الإشارة أنه لم يتم تعريف مصطلح "الهجوم المسلح" في ميثاق الأمم المتحدة، ولكن وفقًا لقواعد القانون الدولي العرفي – وتحديدًا لما يعرف بـ (اختبار كارولين) والذي استمد منه شروط الدفاع الشرعي عند الهجوم المسلح– فإن الهجوم المسلح يعني أنه "عملٌ من أعمال القوة من الخطورة بحيث يشكل انتهاكًا للسلامة الإقليمية أو الاستقلال السياسي لدولة ما، أو تصل إلى حد التهديد باستخدام القوة المسلحة بطريقة مماثلة". وبعبارة أخرى، إن استخدام القوة من قبل الدولة للدفاع عن نفسها يجب أن يكون "فوريًا، وساحقًا، ولا يترك أي خيار للوسائل، ولا لحظة للمداولات". وهذا يعني أن استخدام القوة يجب أن يكون ردًا على تهديد حقيقي ووشيك بالهجوم، ويجب ألا يتأخر.(٧١)

٢. **ضرورة الدفاع عن النفس،** وهذا يعني أن استخدام القوة يجب أن يكون ضروريًا لصد الهجوم أو لمنع حدوثه. فيكون استخدام القوة هو الطريقة الوحيدة لصد هذا الهجوم المسلح. أما إذا كانت هناك وسائل سلمية أخرى متاحة لصد الهجوم؛ فإن استخدام القوة ليس ضروريًا. فضرورة الدفاع عن النفس هي الشرط الثاني للممارسة القانونية لحق الدفاع عن النفس وفق قواعد القانون الدولي. إن ضرورة الدفاع عن النفس شرط شخصي، بمعنى أن الأمر متروك للدولة التي تستخدم القوة لتحديد ما إذا كان استخدام القوة ضروريًا أم لا. ورغم ذلك، يجب أن تكون الدولة قادرة على تبرير استخدامها للقوة، فيجب أن تكون قادرة على إثبات عدم وجود خيارات أخرى متاحة لها.(٧٢)

(٢٠١٨)، ص ٢٦١، https://www.asjp.cerist.dz/en/downArticle/٢٢٢/٧/٦/٦٣٤٧٥ .

(٧١) Forster E., Taylor I. Asking the Fox to Guard the Chicken Coop: In Defense of Minimalism in The Ethics of War and Peace. Journal of International Political Theory ٢٠٢١;١٨(١):٩١-١٠٩. https://doi.org/١٠,١١٧٧/١٧٥٥٠٨٨٢٢٠٩٨٥٨٨٢.

(٧٢) المرجع السابق.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

وقد فسرت محكمة العدل الدولية ضرورة الدفاع عن النفس على أنها تعني أن استخدام القوة يجب أن يكون "الملاذ الأخير"، وهذا يعني أن الدولة يجب أن تكون قد استنفدت جميع الوسائل السلمية الأخرى لحل الموقف قبل استخدام القوة، وأن يقتصر استخدام القوة على ما هو ضروري لصد الهجوم أو منعه من الحدوث.(٧٣)

وتعدُ ضرورة الدفاع عن النفس شرط يصعب تطبيقه في الممارسة العملية، وقد كان موضوع الكثير من النقاش في القانون الدولي. ففي بعض الحالات، قد يكون من الصعب تحديد ما إذا كانت هناك خيارات أخرى متاحة للدولة التي استخدمت القوة. وفي حالات أخرى، قد يكون من الصعب تحديد ما إذا كان استخدام القوة متناسبًا مع الهجوم. إن وجود الضرورة للدفاع عن النفس شرط مهم لاستخدام حق الدفاع عن النفس فهي تساعد على ضمان عدم استخدام القوة في العلاقات الدولية إلا للدفاع عن النفس فقط وليس ذريعة للعدوان.

٣. **تناسبية الرد**. هذا يعني أن استخدام القوة يجب أن يكون متناسبًا مع الهجوم، وألا يتسبب في ضرر أكبر من الهجوم نفسه. فيعدّ التناسب عنصرٌ أساسي في قانون استخدام القوة وقانون النزاعات المسلحة الدولي. ويشير إلى التوازن بين تحقيق الأهداف العسكرية والخسارة البشرية جراء تحقيق المنافع العسكرية. إن اللجوء إلى القوة دفاعًا عن النفس، على النحو الذي تسمح به المادة ٥١، مقيد بشرط القانون الدولي العرفي أن يكون متناسبًا مع العدوان غير القانوني الذي تسبب في تفعيل واستخدام هذا الحق.(٧٤) إن تناسبية الرد شرط يصعب تطبيقه في الممارسة العملية، وقد كان ولا يزال موضوع الكثير من النقاش القانوني بين فقهاء القانون الدولي. ففي بعض الحالات، قد يكون من الصعب تحديد ما هو "المتناسب" في حالة معينة. وفي حالات أخرى، قد يكون من الصعب تحديد ما إذا كان استخدام القوة قد تسبب في ضرر أكبر من الهجوم نفسه.

وقد أقرت قواعد القانون الدولي العرفي أنه يجب تقييم تناسب الرد على أساس كل حالة على حدة، مع مراعاة ما يلي من عوامل:

- طبيعة الهجوم: كلما كان الهجوم أكثر خطورة؛ كان الرد أكثر تناسبًا.

(٧٣) Dinstein Y. The Conduct of Hostilities Under the Law of International Armed Conflict. ٢٠١٥. https://doi.org/١٠.١٠١٧/cbo٩٧٨١٣١٦٣٨٩٥٩١.

(٧٤) Gardam J. *Proportionality and Force in International Law*. Am. j. int. law ١٩٩٣;٨٧(٣):٣٩١–٤١٣. https://doi.org/١٠.٢٣٠٧/٢٢٠٣٦٤٥.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

- فورية التهديد: كلما كان التهديد وشيكًا؛ كانت الاستجابة أكثر تناسبًا.
- احتمال وقوع أضرار جانبية: من المرجح أن يُعتبر استخدام القوة الذي يُرجح أن يتسبب في إلحاق ضرر بالمدنيين أو غيرهم من غير المقاتلين أكثر من الهجوم نفسه غير متناسب.
- توافر الخيارات الأخرى: فإذا كانت هناك خيارات أخرى متاحة للدولة التي تستخدم القوة؛ فمن غير المرجح أن يتم اعتبار استخدام القوة متناسبًا.(٧٥)

كما رأت محكمة العدل الدولية أنه يجب تقييم تناسب الرد من منظور الدولة التي تستخدم القوة في وقت استخدام القوة. وهذا يعني أن الدولة لا تخضع لمعيار الإدراك المتأخر، وأنه ليس مطلوبًا منها التنبؤ بالعواقب الدقيقة لاستخدامها للقوة.

فيما يلي بعض الأمثلة على كيفية تطبيق تناسبية الاستجابة في الممارسة:

- ففي قضية نيكاراغوا ضد الولايات المتحدة؛ رأت محكمة العدل الدولية أن استخدام القوة من قبل الولايات المتحدة ضد نيكاراغوا لا يتناسب مع الهجوم الذي زُعم أن نيكاراغوا قد ارتكبته ضد الولايات المتحدة؛(٧٦)
- وفي قضية الجدار الإسرائيلي؛ رأت محكمة العدل الدولية في فتواها الشهيرة أن بناء جدار الفصل العنصري الإسرائيلي في الضفة الغربية لا يتناسب مع التهديد التي تشكلها الهجمات الفلسطينية؛(٧٧)
- وأما في قضية الإبادة الجماعية في البوسنة؛ فرأت محكمة العدل الدولية أن استخدام القوة من قبل الناتو ضد صربيا كان متناسبًا مع التهديد الذي تشكله القوات الصربية.(٧٨)

---

(٧٥) Forster E., Taylor I., *Supra note* at ٧٣.

(٧٦) شومسكي، نعوم، الولايات المتحدة بين الافراط في القوة وفي السيطرة: الإرهاب، سلاح الأقوياء، الموسوعة البريطانية، https://web.archive.org/web/٢٠١٦٠٣٠٥١٢٠٢٣٩/http://www.mondiploar.com/dec٠١/articles/chomsky.htm. (آخر زيارة للموقع ٢٧ يوليو ٢٠٢٣م).

(٧٧) فتوى محكمة العدل الدولية، لاهاي، هولندا، ٢٠٠٤، ٤٠٠٢/٧/٩.

(٧٨) Dr. Bekker, Peter H.F. and Borgen, Christopher J., World Court Rejects Yugoslav Requests to Enjoin Ten NATO Members from Bombing Yugoslavia, Insights Journal, V. ٤, Issue ٤, ١٩٩٩. https://www.asil.org/insights/volume/٤/issue/٤/world-court-rejects-yugoslav-requests-enjoin-ten-

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

٤. **فورية الرد**. هذا يعني أن استخدام القوة يجب أن يكون فوريًا، ويجب ألا يتأخر. فيعتبر مفهوم الرد الفوري جانبًا مهمًا في تقييم استخدام القوة في الدفاع عن النفس بموجب القانون الدولي. ويشير إلى اشتراط أن يكون استخدام القوة في الدفاع عن النفس فوريًا وألا يتم تأخيره دون داع.

فوفقًا للقانون الدولي العرفي، يجوز للدولة استخدام القوة للدفاع عن النفس إذا كان هناك هجوم مسلح أو تهديد وشيك بهجوم مسلح ضدها. وفي مثل هذه الحالات، يحق للدولة الرد بالقوة لحماية نفسها. فيقر مبدأ الفورية أن استخدام القوة في الدفاع عن النفس يجب أن يكون متناسبًا وضروريًا لصد التهديد الوشيك. وهذا يعني أن الاستجابة يجب أن تحدث على الفور ودون تأخير كبير، مع مراعاة سرعة وضرورة الموقف.

ومع ذلك، من المهم ملاحظة أن تفسير وتطبيق مبدأ الفورية قد يختلف تبعًا للظروف المحددة وطبيعة التهديد الذي تواجهه الدولة. يعتمد تقييم ما إذا كان استخدام القوة فوريًا بدرجة كافية على حقائق وسياق كل حالة على حدة. وبشكل عام، يعمل مبدأ فورية الرد كوسيلة لضمان ألا يكون استخدام القوة في الدفاع عن النفس مفرطًا أو مطولًا بما يتجاوز ما هو ضروري لمواجهة التهديد الوشيك.(٧٩)

المطلب الثاني: مدى إمكان تطبيق المادة ٥١ من ميثاق الأمم المتحدة على الهجمات السيبرانية

تمنح المادة ٥١ من ميثاق الأمم المتحدة جميع الدول الأعضاء في الأمم المتحدة الحق الطبيعي في الدفاع الفردي أو الجماعي عن النفس في حالة وقوع هجوم مسلح ضدها. وتتناول المادة ٥١ الحق الطبيعي في الدفاع عن النفس وتنص على أنه لا يوجد في الميثاق ما يخل بالحق في الدفاع عن النفس إذا وقع هجوم مسلح ضد أحد أعضاء الأمم المتحدة إلى أن يتخذ مجلس الأمن التدابير اللازمة للحفاظ على الأمن والسلام الدولي. إن تعريف "الهجوم المسلح" غير واضح في ميثاق الأمم المتحدة، ولا يوجد إجماع دولي حول ما إذا كانت الهجمات السيبرانية عبر الإنترنت يمكن أن تشكل هجومًا مسلحًا. ويكمن التحدي في الهجمات السيبرانية في أنها قد لا تتناسب دائمًا مع الفهم التقليدي للهجمات المسلحة، والتي تنطوي في المقام الأول على القوة

---

nato-members-bombing.

(٧٩) Forster E., Taylor I., *Supra note* at ٧٣.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

البدنية أو العمل الحركي المباشر. فتتضمن الهجمات السيبرانية عادةً استخدام أنظمة وشبكات الكمبيوتر لاستهداف وتعطيل البنية التحتية الرقمية أو البيانات أو أنظمة المعلومات.

ويشار أيضًا إلى أن محكمة العدل الدولية لم تحسم الجدل بعد بشأن إمكانية تطبيق المادة ٥١ على الهجمات السيبرانية. ورغم ذلك، ففي حكم المحكمة حول شرعية استخدام الأسلحة النووية في قضية نيكاراغوا ضد الولايات المتحدة الأمريكية، ذكرت محكمة العدل الدولية أن مفهوم "الهجوم المسلح" الوارد في المادة ٥١ من الميثاق لا يقتصر على الأعمال التي تقوم بها القوات المسلحة التقليدية.(٨٠) فيشير هذا الرأي إلى أن محكمة العدل الدولية قد تكون منفتحة على احتمال اعتبار الهجمات السيبرانية عبر الإنترنت هجمات مسلحة بموجب المادة ٥١ ولكن لم يتم التصريح بعد بذلك من قبل المحكمة.

وقد اختلفت التوجهات القانونية حول اعتبار الهجمات السيبرانية هجومًا مسلحًا بين فقهاء القانون الدولي. فيجادل بعض الخبراء بأن الهجمات السيبرانية عبر الإنترنت لا تستوفي تعريف الهجوم المسلح بموجب المادة ٥١، ويشيرون إلى حقيقة أن الهجمات السيبرانية عبر الإنترنت لا تنطوي على استخدام القوة المادية والعمل الحركي المباشر، والذي قد لا ينطبق بشكل مباشر على العمليات الإلكترونية. وتتضمن بعض الحجج الرئيسة التي طرحها المعارضون ما يلي:

- **الغموض ومشكلة العزو**: يمكن أن تكون الهجمات الإلكترونية معقدة وصعبة نسبتها إلى جهات فاعلة حكومية معينة على وجه متيقن، وهذا الغموض في إسناد هذه الأفعال إلى فاعل محدد من شأنه أن يخلق صعوبات كبيرة في مساءلة الأطراف المسؤولة عنها وفق إطار الهجوم المسلح على النحو المحدد في المادة ٥١ من ميثاق الأمم المتحدة.(٨١)
- **عدم وجود ضرر جسدي**: قد لا تسبب الهجمات الإلكترونية ضررًا جسديًا أو تدميرًا مباشرًا، وهي سمة مميزة للهجمات المسلحة التقليدية. فيجادل النقاد بأن تطبيق المادة ٥١ على الهجمات السيبرانية يمكن أن يطمس الخط الفاصل بين العمليات السيبرانية والاستخدام التقليدي للقوة. كما يجادلون أيضًا بأن الهجمات السيبرانية ليست مدمرة بطبيعتها،

(٨٠) ICJ, *supra note ٧.*

(٨١) Kreps S., Das D. Warring from the Virtual to The Real: Assessing the Public's Threshold for War Over Cyber Security. Research & Politics ٢٠١٧;٤(٢):٢٠٥٣١٦٨٠١٧٧١٥٩٣. https://doi.org/١٠,١١٧٧/٢٠٥٣١٦٨٠١٧٧١٥٩٣٠.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

ويمكن استخدامها لمجموعة متنوعة من الأغراض، سواء كانت ضارة أو حميدة، فيرون أن الحد الأدنى للهجوم المسلح بموجب المادة ٥١ يجب أن يقتصر على الهجمات الحركية التقليدية.

- **التناسب والرد:** قد لا يكون استخدام القوة ردًا على الهجمات الإلكترونية متناسبًا دائمًا ويمكن أن تؤدي إلى ردود فعل تصعيدية قد يكون لها عواقب وخيمة. فيؤكد بعضهم أن الوسائل غير العسكرية، مثل التدابير الدبلوماسية أو الاقتصادية، هي أكثر ملاءمة لمعالجة الحوادث السيبرانية. وعلى ضوء ذلك؛ فهم يرون أن الهجمات السيبرانية تجب معالجتها فقط من خلال الإجراءات الدبلوماسية والقانونية والتعاونية بين الدول المعنية بدلاً من سلك الردود العسكرية الأحادية.(٨٢)
- **عدم وجود توافق في الآراء:** لا يوجد حاليًا إجماع دولي حول ما إذا كان ينبغي اعتبار الهجمات الإلكترونية عبر الإنترنت – وتحت أي ظروف – هجمات مسلحة تؤدي إلى تفعيل خيار الحق في الدفاع عن النفس. فيرى النقّاد إلى أنه في عدم وجود توافق في الآراء أنه تحدّ كبير في وضع معايير قانونية واضحة للنزاع السيبراني.
- **الحاجة إلى معايير جديدة:** ويجادل بعض المعارضين بأن تعقيدات العمليات السيبرانية تتطلب تطوير أطر قانونية ومعايير جديدة خاصة بالحرب السيبرانية بدلاً من محاولة تطبيق المبادئ القانونية الحالية المصممة للسيناريوهات العسكرية التقليدية.

وعلى النقيض، فيرى خبراء آخرون أن الهجمات السيبرانية يمكن اعتبارها هجمات مسلحة بموجب المادة ٥١، ويشيرون إلى حقيقة أن الهجمات السيبرانية يمكن أن تسبب ضررًا كبيرًا للبنية التحتية الحيوية للدولة، مثل شبكة الكهرباء أو النظام المالي. كما يجادلون بأنه يمكن استخدام الهجمات السيبرانية لتعطيل أو تدمير العمليات العسكرية للدولة. فيجادل البعض بأنه يمكن اعتبار الهجمات السيبرانية على أنها تشكل هجومًا مسلحًا إذا وصلت إلى حد معين من الخطورة والتسبب بضرر كبير أو تشكيل تهديد للمصالح الحيوية للدولة. وهم يؤكدون أن الدول لها الحق في الرد دفاعًا عن النفس على مثل هذه الهجمات السيبرانية بموجب المادة ٥١. في عام ٢٠١٥م، اعتمدت الجمعية العامة للأمم المتحدة قرارًا يؤكد بأنه "يجوز لدولة ما أن تمارس حقها في

(٨٢) Shandler R., Gross M., Backhaus S., Canetti D. Cyber Terrorism and Public Support for Retaliation – A Multi-country Survey Experiment. Brit. J. Polit. Sci. ٢٠٢١;٥٢(٢):٨٥٠-٨٦٨. https://doi.org/١٠,١٠١٧/s٠٠٧١٢٣٤٢٠٠٠٨١٢.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

الدفاع عن النفس ردًا على هجوم سيبراني على نطاق وتأثير كافٍ لتشكيل هجوم مسلح".[٨٣] فيوفر هذا القرار بعض الإرشادات حول كيفية تفسير المادة ٥١ في سياق الحرب السيبرانية.

ويجادل مؤيدو اعتبار الهجمات السيبرانية عبر الإنترنت هجوماً مسلحاً بأن طبيعة العمليات الإلكترونية الحديثة قد تطورت إلى درجة يمكن أن يكون لبعض الهجمات السيبرانية فيها آثار مماثلة للهجمات المسلحة التقليدية. وتتضمن بعض الحجج الرئيسة التي طرحها المؤيدون ما يلي:

- **التأثير الكبير**: فيمكن أن تسبب الهجمات السيبرانية اضطرابات شديدة في البنية التحتية الحيوية، مثل شبكات الطاقة وأنظمة النقل وشبكات الاتصالات. في بعض الحالات، يمكن أن يكون لهذه الاضطرابات تأثيرات مساوية للهجمات الجسدية، مما يدفع المؤيدين إلى القول بأنه ينبغي معاملتهم بالمثل بموجب القانون الدولي.
- **مفهوم النهج القائم على التأثيرات**: يدافع المؤيدون عن مبدأ "النهج القائم على التأثيرات"، وهو يعني التركيز على تأثير الهجوم السيبراني بدلاً من الوسائل المحددة المستخدمة في تنفيذ الهجوم. فهم يجادلون بأن آثار العمليات السيبرانية يجب أن تكون الاعتبار الأساسي في تحديد ما إذا كانت تشكل هجومًا مسلحًا.
- **تطور التكنولوجيا**: يناقش المؤيدون أن التطور والقدرات المتزايدة للأسلحة الإلكترونية بالفعل قد طمس الخطوط الفاصلة بين الهجمات المسلحة التقليدية الهجمات السيبرانية. فهم يجادلون بأن القانون الدولي يجب أن يتكيف ليعكس هذه التطورات التكنولوجية.[٨٤]
- **مسؤولية الدولة**: يجادل المؤيدون بأنه إذا نشأ هجوم سيبراني من أراضي دولة أو تم تنفيذه من قبل جهات فاعلة غير حكومية تعمل تحت سيطرة الدولة، فيجب أن تتحمل تلك الدولة المسؤولية عن الهجوم. يمكن أن توفر معاملة الهجمات السيبرانية على أنها هجمات مسلحة أساسًا قانونيًا للدول لاتخاذ إجراءات دفاعية ضد الدولة المسؤولة.[٨٥]

---

(٨٣) قرار الجمعية العامة للأمم المتحدة ٦٨/٢٤٣ (٢٠١٥م).

(٨٤) Hindy H., Atkinson R., Tachtatzis C., Bayne E., Bures M., Bellekens X. Utilising Flow Aggregation to Classify Benign Imitating Attacks. Sensors ٢٠٢١;٢١(٥):١٧٦١. https://doi.org/١٠,٣٣٩٠/s٢١٠٥١٧٦.

(٨٥) Spáčil J. Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations. MUJLT ٢٠٢٢;١٦(٢):٢١٥–٢٣٩. https://doi.org/١٠,٥٨١٧/mujlt٢٠٢٢-٢-٤.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

- **الحاجة إلى الردع**: يعتقد المؤيدون أن توضيح الإطار القانوني حول الهجمات السيبرانية والاعتراف بإمكانية وقوعها على أنها هجمات مسلحة يمكن أن يكون بمثابة رادع ضد الأنشطة السيبرانية الضارة. ويجب أن ينطبق قانون النزاعات المسلحة على جميع أشكال الحرب، بما في ذلك الحرب الإلكترونية. فيجادل المؤيدون أن قانون النزاعات المسلحة مصمم لحماية المدنيين وغيرهم من غير المقاتلين في أوقات الحرب؛ وعليه، فيجب تطبيق هذا القانون على جميع أشكال الحرب – بما في ذلك الحرب الإلكترونية – من أجل ضمان حماية المدنيين.

الفرع الأول: موقف دليل تالين من علاقة الهجمات السيبرانية بالهجوم المسلح

يقترح دليل تالين أن بعض الهجمات السيبرانية من الممكن أن ترتقي إلى أن تصنّف أنها "هجوم مسلح" مما يقود في النهاية إلى تفعيل خيار حق الدفاع عن النفس. فيعرّف دليل تالين الهجوم المسلح بأنه "عمل من أعمال القوة على درجة معينة من الخطورة ينتهك سيادة الدولة أو سلامتها الإقليمية أو استقلالها السياسي، أو يلحق عمدًا بالدولة أو سكانها ضررًا من الخطورة يصل إلى حد التهديد لبقاء الدولة أو لقيمها الأساسية". ويستند هذا التعريف إلى تعريف الهجوم المسلح الذي طورته محكمة العدل الدولية وغيرها من الهيئات الدولية. وقد عرف الدليل المقصود بالهجوم السيبراني بأنه: "عملية إلكترونية، سواء كانت هجومية أو دفاعية، من المتوقع بشكل معقول أن تتسبب في إصابة أو موت أو ضرر أو تدمير".(٨٦)

ويتناول دليل تالين أيضًا مسألة استخدام القوة في الدفاع عن النفس ردًا على الهجمات السيبرانية؛ فيحدد الدليل عددًا من العوامل التي يمكن أخذها في الاعتبار عند تحديد ما إذا كان الهجوم السيبراني يشكل هجومًا مسلحًا. وتشمل هذه العوامل نطاق وتأثير الهجوم (Scale and Effect)، إسناد الهجوم إلى جهة فاعلة، وارتباط الهجوم السيبراني بالهجوم المسلح، وكذلك هدف الهجوم وحدّة الأثر (Severity)، وأخيرًا نية المهاجم. ويخلص دليل تالين إلى أن نطاق وتأثيرات الهجوم السيبراني هي عوامل مهمة يجب مراعاتها عند تحديد ما إذا كان الهجوم يشكل هجومًا مسلحًا أم لا. وينص الدليل على أنه "يجب تقييم حجم وتأثير العملية السيبرانية في ضوء جميع الظروف، بما في ذلك طبيعة العملية والغرض منها، ومداها، وتأثيرها على الهدف، والسياق الذي تحدث فيه". وقد جاءت هذه المعايير التي ذكرها الدليل كما يلي:

---

(٨٦) Schmitt, M. N., *Supra note* at ٣٠.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

- **النطاق والتأثيرات**: يجب أن تكون آثار الهجوم السيبراني قابلة للمقارنة مع آثار الهجمات المسلحة التقليدية، والتي تنطوي عادةً على خسائر كبيرة في الأرواح أو تدمير مادي أو إلحاق أضرار جسيمة بالممتلكات. إن حجم العملية الإلكترونية وعواقبها حاسمة في تحديد ما إذا كان يمكن تصنيفها على أنها هجوم مسلح. فمن المرجح أن يُعتبر الهجوم السيبراني الذي يؤثر على عدد كبير من الأنظمة أو الشبكات هجومًا مسلحًا وليس هجومًا عاديًا يؤثر على عدد صغير من الأنظمة أو الشبكات.
- **شدة الضرر الناجم عن الهجوم**: من المرجح كذلك أن يتم اعتبار الهجوم السيبراني الذي يتسبب في أضرار جسيمة هجومًا مسلحًا أكثر من كونه هجومًا سيبرانيًا يتسبب في أضرار طفيفة. فخطورة الهجوم السيبراني عامل حاسم في الاعتبار. وهذا يشمل شدة الضرر الناجم، والأهمية العسكرية أو الأمنية للهدف، والأثر العام على الدولة المستهدفة.
- **الإسناد**: من المهم تحديد هوية المهاجم وإثبات أن الهجوم تم تنفيذه من قبل دولة أو جهة فاعلة غير حكومية تعمل تحت إشراف أو سيطرة دولة. ولكن، يمكن أن يكون الإسناد إلى جهة فاعلة محددة عملية معقدة، كونها تشمل وجود مستوى عالي من التقنية والذكاء والتحليل القانوني العميق لمصدر وأبعاد وأثر الهجوم.
- **المباشرة**: يجب أن يكون الهجوم السيبراني مرتبطًا بشكل مباشر باستخدام القوة أو النزاع المسلح. وعليه، فيجب أن يكون هناك ارتباط سببي واضح بين العملية السيبرانية والضرر الناتج.
- **التعطيل الناجم عن الهجوم لعمليات الهدف**: من المرجح أن يُعتبر الهجوم السيبراني الذي يعطل عمليات الهدف هجومًا مسلحًا أكثر من كونه هجومًا سيبرانيًا لا يعطل عمليات الهدف.
- **أثر الهجوم على الأمن القومي للهدف**: قد يتم اعتبار الهجوم السيبراني الذي له تأثير كبير على الأمن القومي للهدف هجومًا مسلحًا وليس هجومًا إلكترونيًا ليس له تأثير كبير على الأمن القومي للهدف. قد يكون من الصعب تقييم تأثير الهجوم السيبراني على الأمن القومي، لأنه يعتمد على مجموعة متنوعة من العوامل، بما في ذلك طبيعة الهجوم وهدف الهجوم وقدرات المهاجم. ومع ذلك، فإن بعض المؤشرات المحتملة للتأثير الكبير على الأمن القومي تشمل:
  - تعطل البنية التحتية الحيوية، مثل شبكات الكهرباء أو إمدادات المياه أو شبكات النقل.
  - سرقة المعلومات الحساسة، مثل الأسرار العسكرية أو المخططات الحكومية.
  - تعطيل العمليات الحكومية، مثل القدرة على تحصيل الضرائب أو تقديم الخدمات الأساسية.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

- انتشار معلومات مضللة أو معلومات مضللة من شأنها زعزعة استقرار الحكومة أو المجتمع.

- **قصد المهاجم**: القصد من المهاجم أيضًا عاملاً يجب مراعاته عند تحديد ما إذا كان الهجوم السيبراني يشكل هجومًا مسلحًا كون الهجوم السيبراني الذي يُقصد به إحداث ضرر أو اضطراب كبير يعتبر هجوماً مسلحاً على عكس هجوم سيبراني لا يُقصد به إحداث ضرر أو اضطراب كبير. فيجب أن يكون لدى المهاجم نية التسبب في إصابة أو وفاة الأشخاص أو إتلاف أو تدمير الأشياء. ويتطلب هذا تقييمًا لأهداف المهاجم ودوافعه والتأثيرات المحددة للعملية الإلكترونية.
- **مبادئ القانون الدولي الإنساني**: يجب مراعاة مبادئ الضرورة، والتمييز، والتناسب، والإنسانية، والتي تعتبر مبادئ أساسية في القانون الدولي الإنساني وذلك عند تقييم ما إذا كان الهجوم السيبراني يرقى إلى مستوى الهجوم المسلح.(٨٧)

ختامًا، من المهم ملاحظة أن تحديد ما إذا كان الهجوم السيبراني يعتبر هجومًا مسلحًا هو تحليل قانوني ووقائعي معقد قد يتطلب النظر في عوامل وظروف إضافية. وقد حاول دليل تالين في توفير إرشادات للدول والممارسين القانونيين في تفسير القانون الدولي الحالي في سياق العمليات الإلكترونية. ومن المرجح أن تكون استنتاجات دليل تالين بشأن حجم وتأثيرات الهجمات السيبرانية مؤثرة في القضايا القانونية المستقبلية التي تنطوي على هجمات إلكترونية. فتوفر استنتاجات الدليل إطارًا لفهم كيفية استخدام نطاق وتأثيرات الهجمات السيبرانية لتحديد ما إذا كانت الهجمات تشكل هجمات مسلحة. ويتناول دليل تالين أيضًا مسألة استخدام القوة في الدفاع عن النفس ردًا على الهجمات السيبرانية، فيخلص الدليل إلى أن استخدام القوة في الدفاع عن النفس يجب أن يكون متناسبًا مع الهجوم الذي تعرض له. وهذا يعني أنه لا يمكن للدول استخدام القوة في الدفاع عن النفس بشكل غير متناسب مع الضرر الناجم عن الهجوم السيبراني. ولذا فإن النقاش القائم فيما إذا كان يمكن تطبيق المادة ٥١ على الهجمات السيبرانية هي مسألة معقدة ولا توجد إجابة سهلة واضحة وحاسمة، ومن المرجح أن تتم مناقشتها لسنوات عديدة قادمة.

---

(٨٧) Schmitt, M. N., *Supra note* at ٣٠.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

المطلب الثالث: تطبيق مبدأ التناسب في الدفاع الشرعي على الهجمات السيبرانية

إن مبدأ التناسب هو مبدأ أساسي من مبادئ القانون الدولي يطبق عند الحاجة إلى استخدام القوة، بما في ذلك استخدام القوة في الدفاع عن النفس. فيتطلب مبدأ التناسب أن يكون استخدام القوة متناسبًا مع التهديد الذي تتم معالجته. أما في سياق الهجمات الإلكترونية؛ فيتطلب مبدأ التناسب أن يكون أي رد على هجوم إلكتروني متناسبًا مع الضرر الناجم عن الهجوم.(٨٨) فعلى سبيل المثال، إذا تسبب الهجوم الإلكتروني في أضرار طفيفة، فإن الاستجابة التي تسبب ضررًا كبيرًا ستُعتبر غير متناسبة. والتناسب مفهوم أساسي في القانون الدولي يهدف إلى منع الاستخدام المفرط أو غير المتناسب للقوة ردًا على العدوان. في عالم الحرب الإلكترونية، يمثل تطبيق مبدأ التناسب تحديًا كبيرًا بسبب الطبيعة المعقدة لعزو الهجمات الإلكترونية إلى فاعل محدد مع غياب اللوائح القانونية الدولية الدقيقة حيال هذه المعضلة. وتكمن الصعوبة كذلك في تحديد المستوى المناسب للرد الذي يتناسب مع الهجوم السيبراني.

يجدر القول بأن مسألة التناسب في الدفاع عن النفس ضد الهجمات الإلكترونية كانت ولاتزال محل نقاش قانوني ساخن. فيجادل البعض بأنه حتى الهجمات الإلكترونية غير المدمرة جسديًا يمكن أن تؤدي إلى نتائج من شأنها أن تشكل هجومًا مسلحًا وفق المنظور القانوني؛ مما يبرر استخدام القوة المسلحة في الدفاع عن النفس. ويؤكد هذا المنظور الضرر النفسي المحتمل الناجم عن الهجمات الإلكترونية، مثل إيذاء المدنيين وتقويض التماسك المجتمعي، ونشر الرعب في المجتمع، واختراق المعلومات الخاصة والحساسة. وفي المقابل، يرى آخرون أن الفهم التقليدي للهجمات المسلحة يتطلب شكلاً من أشكال الضرر أو الإصابة المادية، والتي قد لا تكون موجودة دائمًا في الهجمات الإلكترونية، ويناقشون بأن التناسب يجب أن يستند إلى الضرر الجسدي الناجم عن الهجوم. وعليه، فلا يمكن تطبيق مبدأ التناسب على الأضرار غير الجسدية الناتجة عن استخدام الأسلحة غير التقليدية التي لم يتم النصّ على تجريمها وفق قواعد القانون الدولي.(٨٩) يثير تطبيق مبدأ التناسب في الدفاع عن النفس على الهجمات الإلكترونية تساؤلات حول مسألة الضرر الحال أو الآني (Imminence) حيث يتطلب الحق في استخدام القوة للدفاع عن النفس بموجب المادة ٥١ من ميثاق الأمم المتحدة أن يكون الهجوم المسلح وشيكًا. ومع ذلك، فمن غير الواضح ما إذا كانت الهجمات الإلكترونية عبر الإنترنت يمكنها استيفاء هذا المعيار، سواءً من الناحية النظرية أو العملية. ولكن، يجادل آخرون أنه أدت

(٨٨) Shandler R., *Supra note* at ٨٤.

(٨٩) المرجع السابق.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى الآخرة ١٤٤٥هـ /يناير ٢٠٢٤م)

التطورات التقنية إلى زيادة قدرات الكشف عن الهجمات الإلكترونية حتى قبل حدوثها، مما يجعل استيفاء هذا الشرط ليس صعبًا.(٩٠) وقد ذهب البعض إلى أبعد من ذلك حيث قالوا إن مبدأ التناسب مقيد للغاية وأنه يمكن أن يمنع الدول من الاستجابة بفعالية موازية أو مساوية للهجمات الإلكترونية. ويجادلون بأن الدول يجب أن تكون قادرة على استخدام جميع الوسائل الضرورية للدفاع عن نفسها ضد الهجمات الإلكترونية، حتى لو كان هذا يعني استخدام القوة غير المتناسبة.

فوفقًا للرأي المتوجه حول اعتبار الهجمات السيبرانية هجومًا مسلحًا وأن للدولة الحق في تفعيل خيار الدفاع عن النفس؛ فيعني ذلك أنه يجب أن تكون استجابة الدولة في ردها على هذه الهجمات مصممة وفقًا للتهديد السيبراني المحدد الذي تواجهه. وليس من السهل دائمًا تطبيق مبدأ التناسب من ناحية الممارسة العملية. فهناك عدد من العوامل التي يجب أخذها في الاعتبار، مثل شدة الهجوم ونية المهاجم والسياق الذي حدث فيه الهجوم وغيرها من الأمور. ومع ذلك، فإن مبدأ التناسب هو ضمانة مهمة ضد استخدام القوة المفرطة ردًا على الهجمات الإلكترونية، وهذا يستلزم النظر في العوامل التالية:

- شدة الهجوم السيبراني: يجب أن تكون الاستجابة متناسبة مع شدة الهجوم السيبراني. فإذا تسبب الهجوم السيبراني الأولي في خراب أو ضرر جسيمين؛ فقد يكون هناك ما يبرر الدولة المستجيبة في استخدام تدابير مضادة قوية لتحييد التهديد.
- فورية التهديد: يجب أن تكون الاستجابة في الوقت المناسب وألا تطول بما هو ضروري للتصدي للتهديد بشكل فعال. فالتناسب يأخذ في الاعتبار الطبيعة الفورية للتهديدات السيبرانية والحاجة إلى التصرف بسرعة لمنع المزيد من الضرر.
- التمييز: يتطلب التناسب أن يكون الرد موجهًا إلى الطرف المسؤول أو الأطراف المتورطة في الهجوم السيبراني. ولا ينبغي أن يلحق الضرر بالمدنيين أو غير المقاتلين دون تمييز.
- تقليل الأضرار الجانبية: يؤكد المؤيدون أن مبدأ التناسب يضمن أن أي رد على هجوم إلكتروني مصمم لتقليل الأضرار الجانبية وذلك من خلال النظر في التأثير المحتمل على البنية التحتية المدنية وغير المقاتلين لكي يساعد مبدأ التناسب على منع الضرر غير الضروري والعواقب غير المقصودة.

(٩٠) Stone J. Undervaluing the Right to an Interpreter: How Societal and Judicial Interests Threaten the Fairness of Multilingual Criminal Proceedings. UCLJLJ ٢٠١٧;١(١):٤٠-٦٤. https://doi.org/١٠,١٤٣٢٤/١١١,٢٠٥٢-١٨٧١,١٢٦.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

- ضمان الاستخدام المشروع للقوة: يعتقد المؤيدون أن الالتزام بمبدأ التناسب يضمن أن أي استخدام للقوة رداً على الهجمات السيبرانية مبرر ومشروع، وفي نفس الوقت يمنع الدول من استخدام القوة المفرطة التي تتجاوز ما هو ضروري لمواجهة التهديد.
- الردع: يمكن أن تكون الاستجابات المتناسبة بمثابة رادع للمعتدين المحتملين في الفضاء السيبراني. فيجادل المؤيدون بأن إظهار الالتزام بالتناسب يُظهر أن تدابير الدفاع عن النفس في الدولة محسوبة ومعقولة العواقب، من شأنها أن تثني الخصوم عن الانخراط في مزيد من العدوان السيبراني.
- التدابير غير العسكرية: التناسب يعني أيضًا التفكير في الوسائل غير العسكرية للرد على الهجمات الإلكترونية. فقد تكون الإجراءات الدبلوماسية أو الاقتصادية أو القانونية أكثر ملاءمة في بعض الحالات ويجب تجريبها قبل اللجوء إلى العمل العسكري.
- تجنب مخاطر التصعيد: التناسب يأخذ في الاعتبار مخاطر التصعيد وإمكانية تحول الوضع إلى صراع أكبر. فهنا، يجب على الدول أن تقيِّم بعناية العواقب المحتملة لاستجابتها لتجنب المزيد من التصعيد.
- مصالح الأمن القومي: تتم موازنة التناسب مع حق الدولة المشروع في حماية مصالح أمنها القومي. فيجب أن تهدف الاستجابة إلى ردع التهديد السيبراني وتحييده على نحو فعال.

وفي الختام، نظرًا لتعقيد وتطور طبيعة الهجمات الإلكترونية، فإن تطبيق التناسب في الفضاء السيبراني هو موضوع نقاش وجدال مستمر في مجال القانون الدولي. ومع استمرار الحوادث السيبرانية في فرض تحديات على المجتمع الدولي، فإن إيجاد أرضية مشتركة بشأن الاستخدام المناسب لتدابير الدفاع عن النفس استجابة للتهديدات السيبرانية يظل مسألة بالغة الأهمية.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

الخاتمة

إن مسألة ما إذا كان ينبغي اعتبار الهجمات الإلكترونية عبر الإنترنت هجمات مسلحة هي مسألة نقاش معقد ومستمر. ففي حين أن هناك شبه اتفاق على أن الهجمات الإلكترونية يمكن أن تشكل جرائم حرب أو جرائم ضد الإنسانية، فإن تصنيف الهجمات الإلكترونية على أنها إبادة جماعية أو جرائم عدوان لا يزال موضوعًا للنقاش الساخن بين فقهاء القانون الدولي. إن الإطار القانوني الحالي لا يعالج سوى جزء صغير من الهجمات الإلكترونية المحتملة، وهناك حاجة إلى إطار قانوني دولي جديد للتعامل بفعالية مع التحديات التي تشكلها الهجمات الإلكترونية. مسألة ما إذا كان يمكن اعتبار الهجمات الإلكترونية وشيكة والمصطلحات المستخدمة لوصف إساءة الاستخدام عبر الإنترنت هي أيضًا نقاط الخلاف. وهناك حاجة إلى مزيد من البحث والمناقشة للتوصل إلى توافق في الآراء بشأن هذه الأمور.

ولاتزال هناك حاجة إلى مزيد من البحث والمناقشات لتطوير فهم شامل للتناسب في الدفاع عن النفس مع الهجمات الإلكترونية والتصدي للتحديات القانونية والسياسية المرتبطة بها. ويظل كون التعقيد والتدمير المتزايد للهجمات السيبرانية يعني أن هذه القضية تزداد أهمية، خاصة مع الطبيعة المتطورة للحرب السيبرانية وعدم وجود اتفاقيات دولية شاملة بشأن هذه المسألة، وقد تختلف الإجابة حسب الظروف المحددة للحالة. ولا تزال القضية موضوع مناقشات جارية في المنتديات الدولية، مثل الأمم المتحدة، وفي تطوير المعايير والاتفاقيات الدولية المتعلقة بالأمن السيبراني والحرب السيبرانية. وهناك عدد من العوامل التي يجب أخذها في الاعتبار، بما في ذلك تعريف "الهجوم المسلح"، ومبدأي الضرورة والتناسب، ودور مجلس الأمن حيالها.

النتائج

فيما يلي أبرز النتائج التي توصلت إليها الورقة:

١. هناك خلط في استخدام مفهوم الدفاع الشرعي ومفهوم استخدام القوة كما هو واضح في التعريف الأخير حيث أن بين هذين المفهومين عموم وخصوص.
٢. إن استخدام القوة أو مجرد التهديد بها يعدّ محظورًا في القانون الدولي إلا أن هناك استثناءات لاستخدامها ومنها استخدام القوة في حال الدفاع الشرعي وفق ما دلت عليه المادة ٥١ من ميثاق الأمم المتحدة.

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

٣. إن الهدف من وجود مبدأ حق الدولة في الدفاع عن النفس هو وقف العدان وردّه ما استطاعت الدولة إليه سبيلًا وليس المقصود منه الانتقام أو إيقاع العقوبة على المعتدي، فهذا ليس من صلاحيات الدولة وإنما هو من صلاحيات مجلس الأمن.

٤. التناسب في الدفاع الشرعي ينص على أن أي استخدام للقوة يجب أن يكون متناسبًا مع الهدف الذي يرمى إليه، ولا يجب أن يتجاوز الحدود التي تكفل الدفاع اللازم والمناسب لحماية النفس أو المصالح المحمية.

٥. إن مفهوم الجريمة السيبرانية مختلف من وجوه كثيرة عن الهجمات السيبرانية حيث أن الأولى تعني مجموعة من الأفعال أو السلوكيات الإجرامية التي تهدف إلى الوصول غير المصرح به أو تعديل أو إضعاف أنظمة وشبكات الكمبيوتر، وسرقة المعلومات الموجودة على الأجهزة الإلكترونية على المستوى الفردي سواء من ناحية مرتكب الجريمة أو من الضحية. بينما تعني الهجمات السيبرانية "الاستخدام العدائي لتكنولوجيا المعلومات والاتصالات لإلحاق الضرر بالمصالح الوطنية الأساسية للدول، والتي يمكن أن تتضمن القدرة على التجسس والاختراق والتخريب".

٦. تمثل الهجمات السيبرانية خطرًا كبيرًا في العديد من الأصعدة، على سبيل المثال: تشكيل انتهاك لسيادة الدولة، استهداف المدنيين والبنية التحتية لدى الدول، تمويل الإرهاب والأعمال العدوانية، التجسس واختراق الخصوصيات.

٧. لم تكن جريمة العدوان معرّفةً تعريفًا صريحًا بأركانها وشروطها قبل المؤتمر الاستعراضي لنظام روما الأساسي في كمبالا، أوغندا ٢٠١٠.

٨. أكدت محكمة العدل الدولية في فتواها أن الفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة تنطبق على "أي استخدام للقوة، بصرف النظر عن الأسلحة المستخدمة" وهذا يعني أن الهجمات السيبرانية من المحتمل أن تكون داخلة تحت مفهوم استخدام القوة.

٩. إن الاعتراف بالهجمات السيبرانية كجرائم عدوان بموجب القانون الدولي سيكون له تداعيات قانونية وسياسية كبيرة.

١٠. الهجمات السيبرانية يمكن اعتبارها هجمات مسلحة تؤدي في النهاية إلى حق الدولة في الدفاع عن النفس وفق المادة ٥١ من ميثاق الأمم المتحدة لأنها تعتبر هجمات مسلحة غير تقليدية.

١١. هناك خلاف قوي أنه فلا يمكن للدولة لتفعيل خيار حق الدفاع عن النفس ضد الهجمات السيبرانية لا بد أن تنطوي تلك الهجمات على عدد من المتطلبات، مثل: استخدام القوة المادية والعمل الحركي المباشر، تحديد مصدر الاعتداء لجهة فاعلة محددة، عدم وجود أضرار جسدية، وهذه الشروط غير متحققة في الهجمات السيبرانية. بينما يرى المؤيدون

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

أن كل هذه الشروط متحققة في الهجمات السيبرانية وأن للهجمات السيبرانية في بعض الأحيان تأثير أكبر من الهجمات بالأسلحة التقليدية.

١٢. يوجد خلاف أيضًا متفرع عن مدى اعتبار الهجمات السيبرانية هجمات مسلحة أم لا؛ وهو المتعلق بشرط التناسب في استخدام حق الدفاع عن النفس، فمن يرون أن للدولة تفعيل خيار الدفاع عن النفس اختلفوا في إمكانية تحقيق شرط التناسب في الرد على تلك الهجمات السيبرانية.

التوصيات

وهذه أبرز التوصيات التي تقترحها هذه الورقة:

١. يجب تجلية مفهوم استخدام القوة الذي نص عليه ميثاق الأمم المتحدة حتى لا يكون هناك لبس في المصطلحات الداخلة تحت مضمون هذا المفهوم.
٢. يستحسن الخروج بصياغة قانونية دولية متناسبة حول مفهوم الجريمة السيبرانية وكذلك الهجمات السيبرانية لأن عدم تقييدها يجعل المجال محرجًا وغامضًا سواءً للقضاة الدوليين أو للاعبين الأساسيين في السياسة الدولية.
٣. لا شك أن الدعوة إلى الخروج بصيغة توافقية أممية جامعة لتحرير مفهوم العدوان زيادة على ما تم إلحاقه في عام ٢٠١٠م في نظام محكمة الجنايات الدولية يعدّ أمرًا لازمًا.
٤. يتوجب الاعتراف بقوة الحاجة إلى تعديل ميثاق الأمم المتحدة المتعلق بحق الدولة في الدفاع عن النفس وكذلك في تحرير مفهوم استخدام القوة على نحو يتوافق مع التطورات الحديثة في مجال الأسلحة غير التقليدية.
٥. هناك حاجة إلى إطار قانوني دولي جديد للتعامل بفعالية مع التحديات التي تشكلها الهجمات السيبرانية على وجه التحديد.
٦. ينبغي تصنيف الجرائم السيبرانية تصنيفًا مختلفًا عن الجرائم العسكرية التقليدية من حيث الأركان والشروط؛ بما في ذلك شرط التناسب الذي تشترطه المواثيق الدولية في الدفاع عن النفس حيث أنه من شبه المستحيل أن يتم ضبطه بصورة دقيقة.

مجلة العلوم الشرعية
جامعة القصيم، - المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

مبدأ التناسب في الدفاع الشرعي ضد الهجمات السيبرانية

The Principle of Proportionality in Legitimate Defense against Cyber Attacks

Dr. Ahmed bin Ali bin Abdullah Aldibasi

Assistant Professor, Department of Law, College of Sharia and Islamic Studies, Qassim University

aaldibasi@qu.edu.sa

Abstract

This paper discusses the issue of achieving the proportionality concept when using the right of international self-defense against illegal aggression via cyber-attacks, and this subject is examined in three main chapters. It is known, according to international laws and customs, that the state has the right to defend itself by any legitimate means against any illegal armed aggression, so the introductory topic of this paper explains the concept of international self-defense and clarifies how this concept is beyond doubt. Then, in the same introductory chapter, the paper demonstrates the concept of proportionality when using the right of self-defense as well as the clarification of the precise meaning of cyber-attacks, which may intersect with some similar concepts. The first chapter demonstrates the relationship between cyber-attacks and the crime of aggression since the latter might be used to harm attacked country in its vital targets, infrastructure, breach privacy, and/or harm civilians or vital facilities, such as hospitals, care homes, power or gas stations, etc. In addition to the above, this research clarifies the concepts of aggression and armed-attack, which may go beyond the common limited-concept of conventional weapons to include modern weapons, such as electronic weapons by using cyber-attacks. Then, the second chapter of this paper clarified the state's eligibility of self-defense against these cyber-attacks; as it falls under the concept of armed aggression. Thus, the attacked state has the right to defend itself in accordance with the provisions of Article ٥١ of the United Nations' Charter. Finally, the paper demonstrates the dispute over the issue of applying proportionality to the legitimate defense against cyber-attacks, as some do not even require it. The paper, hence, emphasizes the importance of applying proportionality despite the difficulty of implementing it in practice, with the necessity of considering some important factors that were addressed in this research.

Key Words: Proportionality, cyber-attacks, aggression, legitimate defense, United Nations, armed force

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

قائمة المراجع

المراجع العربية

- أبو القاسم، م. ليلى عيسى، المسؤولية الدولية عن جريمة العدوان بالهجمات السيبرانية في ضوء أحكام القانون الدولي، ٢٠٢١.
- أخلاقيات الحرب السيبرانية: استكشاف استخدام الهجوم الإلكتروني في العمليات العسكرية، IRJMETS، ٢٠٢٣. (غير مترجم) https://doi.org/١٠,٥٦٧٢٦/irjmets٣٥٣٨٥
- حميد، علي حسين وهاشم، فراس عباس، الأبعاد الجيوبوليتيكية للدبلوماسية الدفاعية العراقية: نحو مقاربة جديدة في السياسية الخارجية. قضايا سياسية ٢٠٢٢ (٦٩). https://doi.org/١٠,٥٨٢٩٨/٢٠٢٢١٠٢.
- خلف، محمد محمود، حق الدفاع الشرعي في القانون الدولي الجنائي، الطبعة الأولى، القاهرة، مكتبة النهضة المصرية، ١٩٧٣.
- دليل تالين ٢.٠ بشأن القانون الدولي المطبق على العمليات السيبرانية، الإصدار الثاني.
- رار الجمعية العامة للأمم المتحدة ٢٤٣/٦٨، ٢٠١٥.
- سمودي، رزق أحمد، حق الدفاع عن النفس نتيجة الهجمات السيبرانية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية المجلد ١٥ العدد ٢، ديسمبر ٢٠١٨.
- سياب، حكيم، مفهوم جريمة العدوان في ظل تطوّر نظام روما الأساسي للمحكمة الجنائية الدولية، مجلة أبحاث قانونية وسياسية، ٢٠١٧.
- شومسكي، نعوم، الولايات المتحدة بين الافراط في القوة وفي السيطرة: الإرهاب، سلاح الأقوياء، الموسوعة البريطانية، https://web.archive.org/web/٢٠١٦٠٣٠٥١٢٠٢٣٩/http://www.mondiploar.com/dec٠١/articles/chomsky.htm.
- عشوش، د. أحمد عبد الحميد، الوسيط في القانون الدولي العام، مؤسسة الجامعة الاسكندرية ١٩٩٨.
- فتوى محكمة العدل الدولية بشأن شرعية التهديد بالأسلحة النووية أو استخدامها لعام ١٩٩٦.

- فتوى محكمة العدل الدولية، لاهاي، هولندا، ٢٠٠٤، ٤٠٠٢/٧/٩.
- قاسم، د. يوسف، نظرية الدفاع الشرعي في الفقه الجنائي الإسلامي والقانون الجزائي الوضعي، دار النهضة. العربية، القاهرة، ١٩٧٩.
- الكبار، محمد بحر، حق الدفاع الشرعي في القانون الدولي، مجلة جامعة الزيتونة، ٢٠١٦ ع ١٩.
- اللجنة الدائمة للعمليات المشتركة للأركان العامة الأمريكية، "الموجه العسكري الأمريكي الجديد لقواعد الاشتباك"، ١٣ يوليو ٢٠١٦.
- لوباتش، د. "الجريمة الدولية": مناهج مختلفة لمسألة تعريف المفهوم، ٢٠٢٢. (غير مترجم)
- مرسلي، د. عبد الحق، ضوابط الدفاع الشرعي في القانون الدولي، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد ٧، العدد ٦، ٢٠١٨. https://www.asjp.cerist.dz/en/downArticle/٢٢٢/٧/٦/٦٣٤٧٥ .
- معاهدة بودابست حول الجريمة الإلكترونية والمعلوماتية ٢٠٠١. (غير مترجم)
- موغولون، م. نداء من الضرورة: إطار معياري مقبول للدفاع عن النفس خارج الحدود الإقليمية ضد الجهات الفاعلة غير الحكومية. IUSETVERITAS، ٢٠٢١، (غير مترجم) https://doi.org/١٠,١٨٨٠٠/iusetveritas.٢٠٢١٠٢,٠٠١.
- ميثاق الأمم المتحدة، الأمم المتحدة، ١٩٤٥.
- ميشيل دوريا، القانون الدولي الإنساني: المبادئ الأساسية، المجلس الأعلى للقضاء، ٢٠١١. (غير مترجم)
- نظام روما الأساسي للمحكمة الجنائية الدولية، A/CONF.١٨٣/٩، ١٩٩٨.
- واد، ن. "نظام روما الأساسي: مراجعة نقدية لـ دور Swgca في تحديد جريمة العدوان." بيجيا ١ (٦) ٢٠٢٣. (غير مترجم)
- وونغ إم، العدوان ومسؤولية الدولة في المحكمة الجنائية الدولية، ٢٠٢١ ICLQ؛ ٧٠ (٤). (غير مترجم)

مجلة العلوم الشرعية
جامعة القصيم، – المجلد (١٧)، العدد (٣)، الجزء الثاني ص ص ٣٣٣٣ – ٣٣٨٦ (جمادى االآخرة ١٤٤٥هـ /يناير٢٠٢٤م)

المراجع الأجنبية

- Judgment of the International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), ١٩٨٦, I.C.J. ١٤, ٩٦-٩٧; See also, Malcolm Shaw, International Law, (٧th edition, ٢٠١٤), Cambridge University Press; Yoram Dinstein, War, Aggression and Self-defence (٣ed edition ٢٠١١).
- Khan ،Kamal Ahmad, Use of Force and Human Rights under International Law, Athens Institute for Education and Research, Conference Paper Series BLE ٢٠١٧- .٢٢٠٥.
- ICJ, case concerning *Military and Paramilitary Activities in and Against Nicaragua*) Nicaragua v. United States) , Reports ١٩٨٦.
- UN General Assembly Res. ٣٣١٤ (XXIX), Definition of Aggression, Adopted ١٤ December ١٩٧٤.
- Stuesser, Lee, Active Defense: State Military Response to International Terrorism, ١٧, *California Western International Law Journal*, ١٩٨٧
- Dinstein, Yoram, Computer Network Attacks and Self-Defense, ٧٦ U.S. Naval War College of International Law Studies, ٢٠٠٢.
- International Law Commission, Draft articles on the responsibility of states for internationally wrongful acts, with commentaries, United Nations, ٢٠٠٦.
- International Committee of the Red Cross, Customary International Humanitarian Law: Volume I: Rules. Cambridge University Press, ٢٠١٦.
- Dinstein, Yoram, The conduct of hostilities under the law of international armed conflict. Cambridge University Press, ٢٠١٦.
- The UK Government's Legal Opinion on Forcible Measures in Response to the Use of Chemical Weapons by the Syrian Government, ٢٠١٣.
- Forster E., Taylor I., Asking the Fox to Guard the Chicken Coop: In Defense of Minimalism in The Ethics of War and Peace. Journal of International Political Theory ٢٠٢١;١٨(١). https://doi.org/١٠,١١٧٧/١٧٥٥٠٨٨٢٢٠٩٨٥٨٨٢.
- Gardam, J., *Proportionality and force in international law*. American Journal of International Law, ٩٨(٢), ٢٠٠٤.
- Spáčil J., Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations. MUJLT ٢٠٢٢;١٦(٢):٢١٥-٢٣٩. https://doi.org/١٠,٥٨١٧/mujlt٢٠٢٢-٢-٤.
- Australian Federal Police ،https://www.afp.gov.au/what-we-do/crime-types/cyber-crime.
- The Law of Cyber-Attack, Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, California Law Review, Vol. ١٠٠, No. ٤, ٢٠١٢.

- United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), ٢٠١٥.
- Schmitt, M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press), ٢٠١٣.
- Quinn S., Ivy N., Barrett M., Feldman L., Witte G., Gardner R., *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*. ٢٠٢١. https://doi.org/١٠,٦٠٢٨/nist.ir.٨٢٨٦a.
- Razaque A., Ajlan A., Melaoune N., Alotaibi M., Alotaibi B., Dias I.et al.. Avoidance Of Cybersecurity Threats with the Deployment of a Web-based Blockchain-enabled Cybersecurity Awareness System. Applied Sciences ٢٠٢١;١١(١٧):٧٨٨٠. https://doi.org/١٠,٣٣٩٠/app١١١٧٧٨٨٠.
- Steyn C., Blaauw D. Towards a Critical Review of Cybersecurity Risks in Anti-poaching Systems. iccws ٢٠٢٣;١٨(١) https://doi.org/١٠,٣٤١٩٠/iccws.١٨,١,١٠٩٠.
- Papanastasiou, A.. Application of International Law in Cyber Warfare Operation, ٢٠١٠, https://dx.doi.org/١٠,٢١٣٩/ssrn.١٦٧٣٧٨٥.
- Philipsen S., Andersen B., Singh B., Threats and Attacks to Modern Vehicles. ٢٠٢١ IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) ٢٠٢١. https://doi.org/١٠,١١٠٩/iotais٥٣٧٣٥,٢٠٢١,٩٦٢٨٥٧٦ .
- Lobach D. Cyberattacks as a Crime of Aggression and International Terrorism: Legal Qualification Problems. The European Proceedings of Social and Behavioural Sciences ٢٠٢٢, https://doi.org/١٠,١٥٤٠٥/epsbs.٢٠٢٢,٠٦,٧٠.
- Mazaraki N., ГОНЧАРОВА Ю., Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' Of International Law to Adress Economic Damages. BJES ٢٠٢٢;٨(٢), https://doi.org/١٠,٣٠٥٢٥/٢٢٥٦-٠٧٤٢/٢٠٢٢-٨-٢-١١٥-١٢٠
- Greco G., Cyber-attacks As Aggression Crimes in Cyberspace in the Context Of International Criminal Law. EJPSS ٢٠٢٠;٤(١). https://doi.org/١٠,٤٦٨٢٧/ejpss.v٤i١,٩٣٧.
- Spáčil J., Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations. MUJLT ٢٠٢٢;١٦(٢):٢١٥-٢٣٩. https://doi.org/١٠,٥٨١٧/mujlt٢٠٢٢-٢-٤.
- Ali S., Legal Framework of Right of Self Defense in Cyber Warfare: Application Through Laws of Armed Conflict. JDSS ٢٠٢٢;٣(II). https://doi.org/١٠,٤٧٢٠٥/jdss.٢٠٢٢(٣-ii)٩٦.
- The Urgency of International Regulation Regarding Cyber Attack with An Indication of Aggression Crime in Asean. ٢٠٢٣. https://doi.org/١٠,٥٢٧٨٣/rlj.v١١i١,٢٩٣.
- Maskun M., Irwansyah I., Yunus A., Safira A., Lubis S., Cyber-attack: Its Definition, Regulation, and Asean Cooperation to Handle with It. home ٢٠٢١;٤(٢):١٣١-١٥٠. https://doi.org/١٠,٢٢٤٣٧/jlj.٤,٢,١٣١-١٥٠.

- Chaumette, A. L. (٢٠١٨). International Criminal Responsibility of Individuals in Case of Cyberattacks. International Criminal Law Review, ١٨.
- Kocibelli, A., Aggression, From Cyber-Attacks to ISIS: Why International Law Struggles to Adapt. Michigan Journal of International Law, ٢٠١٧.
- Trahan J., The Criminalization of Cyber-operations Under the Rome Statute. Journal of International Criminal Justice ٢٠٢١;١٩(٥):١١٣٣-١١٦٤. https://doi.org/١٠,١٠٩٣/jicj/mqab٠٦٦.
- Papanastasiou, A., Application of International Law in Cyber Warfare Operation, ٢٠١٠, https://dx.doi.org/١٠,٢١٣٩/ssrn.١٦٧٣٧٨٥.
- Ambos, K., International criminal responsibility in cyberspace. in Research Handbook on International Law and Cyberspace. Edward Elgar Publishing, ٢٠١٥.
- Binder M., Heupel M., The Legitimacy of the Un Security Council: Evidence from Recent General Assembly Debates. Int Stud Q ٢٠١٤;٥٩(٢):٢٣٨-٢٥٠. https://doi.org/١٠,١١١١/isqu.١٢١٣٤.
- Lushenko P., Raman S., Kreps S., Multilateralism and Public Support for Drone Strikes. Research & Politics ٢٠٢٢;٩(٢):٢٠٥٣١٦٨٠٢٢١٠٩٣٤. https://doi.org/١٠,١١٧٧/٢٠٥٣١٦٨٠٢٢١٠٩٣٤٣٣.
- Gray C., ٢٠. the Use of Force and The International Legal Order. International Law ٢٠١٨. https://doi.org/١٠,١٠٩٣/he/٩٧٨٠١٩٨٧٩١٨٣٦,٠٠٣,٠٠٢٠.
- Chinkin C., Kaldor M., International Law and New Wars. ٢٠١٧. https://doi.org/١٠,١٠١٧/٩٧٨١٣١٦٧٥٩٨٦٨.
- Forster E., Taylor I., Asking the Fox to Guard the Chicken Coop: In Defense of Minimalism in The Ethics of War and Peace. Journal of International Political Theory ٢٠٢١;١٨(١):٩١-١٠٩. https://doi.org/١٠,١١٧٧/١٧٥٥٠٨٨٢٢٠٩٨٥٨٨٢.
- Dinstein Y., The Conduct of Hostilities Under the Law of International Armed Conflict. ٢٠١٥. https://doi.org/١٠,١٠١٧/cbo٩٧٨١٣١٦٣٨٩٥٩١.
- Gardam J., Proportionality and Force in International Law. Am. j. int. law ١٩٩٣;٨٧(٣):٣٩١-٤١٣. https://doi.org/١٠,٢٣٠٧/٢٢٠٣٦٤٥.
- Dr. Bekker, Peter H.F. and Borgen, Christopher J., World Court Rejects Yugoslav Requests to Enjoin Ten NATO Members from Bombing Yugoslavia, Insights Journal, V. ٤, Issue ٤, ١٩٩٩. https://www.asil.org/insights/volume/٤/issue/٤/world-court-rejects-yugoslav-requests-enjoin-ten-nato-members-bombing.
- Kocibelli, A., Aggression, From Cyber-Attacks to ISIS: Why International Law
- Struggles to Adapt. Michigan Journal of International Law, ٢٠١٧.
- Kreps S., Das D., Warring from the Virtual to The Real: Assessing the Public's Threshold For War Over Cyber Security. Research & Politics ٢٠١٧;٤(٢):٢٠٥٣١٦٨٠١٧٧١٥٩٣. https://doi.org/١٠,١١٧٧/٢٠٥٣١٦٨٠١٧٧١٥٩٣٠.

- Shandler R., Gross M., Backhaus S., Canetti D., Cyber Terrorism and Public Support for Retaliation – A Multi-country Survey Experiment. Brit. J. Polit. Sci. ٢٠٢١;٥٢(٢):٨٥٠-٨٦٨. https://doi.org/١٠,١٠١٧/s٠٠٧١٢٣٤٢٠٠٠٠٨١٢.
- Hindy H., Atkinson R., Tachtatzis C., Bayne E., Bures M., Bellekens X., Utilising Flow Aggregation to Classify Benign Imitating Attacks. Sensors ٢٠٢١;٢١(٥):١٧٦١. https://doi.org/١٠,٣٣٩٠/s٢١٠٥١٧٦.
- Spáčil J., Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations. MUJLT ٢٠٢٢;١٦(٢):٢١٥-٢٣٩. https://doi.org/١٠,٥٨١٧/mujlt٢٠٢٢-٢-٤.
- Shandler R., Gross M., Canetti D., Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-analysis. Journal of Global Security Studies ٢٠٢٢;٨(١). https://doi.org/١٠,١٠٩٣/jogss/ogac٠٤٢.
- Stone J., Undervaluing the Right to an Interpreter: How Societal and Judicial Interests Threaten the Fairness of Multilingual Criminal Proceedings. UCLJLJ ٢٠١٧;١(١):٤٠-٦٤. https://doi.org/١٠,١٤٣٢٤/١١١,٢٠٥٢-١٨٧١,١٢٦.