

تحديات تكيف حق الدفاع الشرعي الدولي في مواجهة العدوان السيبراني

Challenges of Adapting the International Right of Self-Defense against Cyber Aggression

التجاني عبد القهار*

جامعة عمار ثليجي - الأغواط

ak.tidjani@lagh-univ.dz



- تاريخ النشر: 2026/06/05

- تاريخ القبول: 2026/06/04

- تاريخ الإرسال: 2026/05/03

ملخص:

تبحث هذه الدراسة في التحول الجذري والإستراتيجي للنزاعات المسلحة بانتقالها إلى "الفضاء السيبراني" كساحة صراع خامسة وموازية؛ وتكمن الإشكالية في قدرة الهجمات الرقمية العابرة للحدود على استهداف البنى التحتية الحيوية، مما يرفعها إلى مرتبة "العدوان المسلح" ويتجاوز المفهوم التقليدي للسيادة الجغرافية إلى مفهوم "السيادة الرقمية" المستحدث، كما تهدف الدراسة إلى تحليل قصور النصوص القانونية الحالية، وإعادة تكيف قواعد القانون الدولي العام-لاسيما حق "الدفاع الشرعي السيبراني"- مع الواقع التكنولوجي الجديد والمتسارع، وخلصت الدراسة إلى ضرورة سد الفراغ التشريعي الدولي المقلق؛ لضمان حماية الفضاء الرقمي من الهجمات التي تهدد الأمن القومي للدول.

الكلمات المفتاحية: الحرب السيبرانية؛ الدفاع الشرعي؛ العدوان المسلح؛ السيادة الرقمية؛ القانون الدولي.

ABSTRACT:

This study examines the strategic shift of warfare to cyberspace, where cross-border cyberattacks on critical infrastructure escalate to "armed attacks," redefining traditional sovereignty into "digital sovereignty." It analyzes current legislative gaps to readapt international law, especially "cyber self-defense," to rapid technological advancements, emphasizing the urgent need to fill the international legal vacuum to secure the digital realm and protect national security.

Keywords: Cyber Warfare; Self-Defense; Armed Attack; Cyber Sovereignty; International Humanitarian Law.

* - المؤلف المرسل:

مقدمة:

لقد أكدت النزاعات المعاصرة، لاسيما الهجمات السيبرانية واسعة النطاق التي صاحبت الأزمة الروسية الأوكرانية (2022) واستهداف شبكات الطاقة والمرافق الحيوية، أن الفضاء الرقمي بات سلاحاً تدميراً لا يقل خطورة عن الأسلحة التقليدية؛ حيث أثبتت وقائع مثل هجمات "Viasat" و "NotPetya" قدرة العمليات السيبرانية على شل أركان الدولة وتجاوز آثارها العسكرية لتطال المدنيين والأعيان المدنية بشكل مباشر، مما يضع القواعد التقليدية للقانون الدولي العام والإنساني أمام اختبار حقيقي لإثبات كفايتها في كبح جماح هذه التهديدات وضمان السلم والأمن الدوليين.

تتجلى أهمية البحث من الناحية النظرية في إثراء المكتبة القانونية العربية بموضوع يتسم بالحدثة والتعقيد، ومحاولة سد الفجوة البحثية في مجال القانون الدولي السيبراني، أما من الناحية التطبيقية، فتنبع من الواقع الذي يشهد تزايداً في استخدام القدرات الرقمية كأداة في النزاعات، مما يحتم فهم الإطار القانوني لحماية البنية التحتية الوطنية دون انتهاك الشرعية الدولية.

تتمحور الإشكالية الرئيسة لهذا البحث في الغموض الذي يكتنف تطبيق قواعد القانون الدولي العام التقليدية على الظواهر التكنولوجية المستحدثة تحديداً، وتكمن المشكلة في تفسير "حق الدفاع الشرعي" المنصوص عليه في المادة (51) من ميثاق الأمم المتحدة لعام 1945.

ما مدى مرونة هذا النص لاستيعاب "الهجوم السيبراني" واعتباره "هجوماً مسلحاً" يبرر الرد، خاصة في ظل غياب اتفاقية دولية ملزمة تنظم الحرب السيبرانية بشكل صريح وشامل؟.

اعتمدت الدراسة على المنهج الوصفي لاستعراض ماهية الهجمات وتطورها، والمنهج التحليلي لتحليل النصوص القانونية في ميثاق الأمم المتحدة واتفاقيات جنيف، ومحاولة إسقاطها وتكييفها على واقع الهجمات السيبرانية المعاصرة.

تم تقسيم الدراسة إلى مبحثين أساسيين، المبحث الأول: الإطار المفاهيمي وشروط تحقق العدوان السيبراني، والمبحث الثاني: الضوابط القانونية لردع الهجمات السيبرانية.

المبحث الأول: الإطار المفاهيمي وشروط تحقق العدوان السيبراني

يتطلب التطور التكنولوجي المتسارع إعادة النظر في المفاهيم التقليدية التي استقرت عليها قواعد القانون الدولي العام، خاصة تلك المتعلقة باستخدام القوة وشروط تحقق العمل العدائي، ولعل الفضاء السيبراني قد فرض واقعاً جديداً يتطلب تكييفاً قانونياً يتجاوز الطابع المادي الملموس للأعمال العسكرية التقليدية.

وعليه فإن هذا المبحث يسعى إلى تفكيك المضمون القانوني للمادة (4/2) من ميثاق الأمم المتحدة في ضوء الأنشطة الرقمية المستحدثة (المطلب الأول)، تمهيداً لتحديد الأركان المادية والزمنية والمعايير الموضوعية التي يستند إليها لتوصيف الهجمات الرقمية كأعمال عدوانية (المطلب الثاني).

المطلب الأول: قراءة المادة (4/2) من الميثاق في ظل البيئة الرقمية

يهدف هذا المطلب إلى استعراض وتحليل الاتجاهات الفقهية الكبرى التي حاولت تفسير نطاق "القوة المحظورة" في ظل أحكام المادة (4/2) من ميثاق الأمم المتحدة، وذلك من خلال الموازنة بين المقاربة الكلاسيكية الضيقة، والمقاربة الموسعة، وصولاً إلى المقاربة الوظيفية التي تركز على الآثار المترتبة على الهجوم.

الفرع الأول: المقاربة الكلاسيكية (التمسك بالمعيار العسكري المادي)

يبدأ الفقه الدولي في تأصيل حق الدفاع الشرعي من ضرورة إضفاء الصبغة العسكرية على الفعل المادي المكوّن للاعتداء، إذ يُشترط لنشوء هذا الحق الاستثنائي بلوغ الاعتداء عتبة معينة من الجسامّة الموضوعية، واقتترانه بنية عدوانية صريحة لدى الدولة المعتدية، حيث يجد هذا التكييف مرجعيته الأساسية في نص المادة (51)¹ من ميثاق الأمم المتحدة، والتوجه القضائي المستقر لمحكمة العدل الدولية.

تهدف المادة (51) من ميثاق الأمم المتحدة إلى إقامة توازن قانوني دقيق بين إباحة استخدام القوة المسلحة كأداة للدفاع الشرعي، وبين السلوك العدواني الموجب لهذا الرد، وبناءً على القراءة الدقيقة لهذا النص، يتمتع التوسع في تفسير أحكامه عبر القياس القانوني أو تطبيقها على حالات مشابهة لا ترقى موضوعياً إلى مرتبة الاعتداء العسكري المباشر، وذلك لضمان عدم الانحراف بالحق في الدفاع الشرعي عن غايته الاستثنائية.

إذ يقوم هذا التصور على افتراض مفاده أن الأضرار المادية الكبرى لا يمكن تصور حدوثها واقعياً إلا عبر تحريك الجيوش والوسائل القتالية التقليدية².

كما يظهر لنا مما تقدم استبعاد بعض الحالات المشابهة التي لا ترقى موضوعياً إلى مرتبة الاعتداء المسلح العسكري، وهو ما يمكن تفصيله من خلال النماذج والأمثلة التالية³:

أولاً: التدابير القسرية والضغط غير المسلحة ذات الطابع الاقتصادي أو الاجتماعي: حيث لا يترتب على التهديد أو اللجوء إلى وسائل الضغط الاقتصادي أو الاجتماعي نشوء حق الدولة المتضررة في استخدام القوة العسكرية بذريعة الدفاع الشرعي، إذ الأفعال التي تفتقر إلى العنصر المادي المسلح لا تبيح الرد المسلح.

¹ ميثاق الأمم المتحدة لعام 1945 (المادة 51 المتعلقة بحق الدفاع الشرعي).

² د. معمر بن طرية، المسؤولية الدولية عن الهجمات السيبرانية في ظل قواعد القانون الدولي المعاصر، دار الجامعة الجديدة، الإسكندرية، 2023، ص 21.

³ أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، العدد 35 ج 3، 2020، ص 210.

ثانياً: حماية الرعايا المقيمين في الخارج: فالقانون الدولي العام يستند في هذا الشأن إلى مبدأ الإقليمية والسيادة المكانية وليس الشخصية، كما يمتنع على الدولة التدخل عسكرياً لحماية رعاياها في الخارج بذريعة الدفاع الشرعي، إذ إن إجازة مثل هذا السلوك ستؤدي حتماً إلى ذريعة التدخلات العسكرية المفتوحة وإثارة نزاعات مسلحة عشوائية تنتهك سيادة الدول الأخرى.

كما يتضح أن الحق الاستثنائي في استخدام القوة المسلحة للدفاع عن النفس لا ينشأ إلا في مواجهة صور محددة من العدوان العسكري القائم، أما في حال تعرضت الدولة لأعمال عدائية تخلو من الهجوم المسلح المباشر، يمتنع عليها الرد العسكري، ويتعين عليها اللجوء إلى الآليات السلمية ومراجعة مجلس الأمن الدولي لاتخاذ التدابير اللازمة وفقاً للمادة (39)¹ من ميثاق الأمم المتحدة.

الفرع الثاني: المقاربة الموسعة (إدراج الضغوط غير المادية)

إن ممارسة الدولة لحقها الطبيعي في الدفاع عن النفس تستلزم بالضرورة إعمال مبدأي الضرورة والتناسب بما يتوافق مع حجم الضرر الواقع عليها، وتثور في هذا الصدد إشكالية قانونية وعملية بالغة التعقيد، وهي حالة الدولة التي تتعرض لهجوم سيبراني مدمر في حين تفتقر إلى القدرات التقنية اللازمة لصدّه أو الرد عليه بالمثل، ولكنها تمتلك في المقابل ترسانة عسكرية تقليدية كافية لحماية سيادتها وكيانها؛ وهنا يطرح التساؤل القانوني نفسه: هل تجبر الدولة بالوقوف مكتوفة الأيدي وتجرد من حقها في البقاء لعدم تكافؤ الوسائل التقنية؟

والواضح من الناحية الفقهية والقانونية هو أن حق الدفاع عن النفس يمنح الدولة المعتدى عليها مشروعية كاملة في استخدام كافة وسائل الحماية المتاحة لديها والمشروعة دولياً لرد العدوان، والقول بغير ذلك -أي إجبار الدولة على الرد بنفس الوسيلة المستخدمة في الهجوم الأصلي رغم عدم أهليتها التقنية- يترتب عليه تعطيل وتجريد للحق الأصل في الدفاع الشرعي².

الفرع الثالث: المقاربة الوظيفية (معياري النتائج والآثار الموازية)

عند كتابة ميثاق الأمم المتحدة عام 1945، كان الأساس هو منع تكرار مآسي الحرب العالمية الثانية³، لذا نصت المادة (4/2) على حظر "استخدام القوة" أو التهديد بها، والمقصود هنا حتماً القوة المادية العسكرية. لكي يتم تطبيق المقاربة الوظيفية بشكل واضح يمنع الدول من التعسف في استخدام القوة بحجة تعرضها لهجوم سيبراني، وضع الفقه الدولي مجموعة من المعايير المترابطة لقياس الأثر والآثار الموازية:

¹ ميثاق الأمم المتحدة، الفصل السابع، المادة (39).

² د. بوبكر منصور، القانون الدولي السيبراني: دراسة في القواعد المنظمة لاستخدام القوة في الفضاء الافتراضي، دار الكتاب الحديث، الجزائر، 2024، ص33.

³ ميثاق الأمم المتحدة، تم توقيعه في سان فرانسيسكو في 26 حزيران/يونيو 1945، ودخل حيز التنفيذ في 24 تشرين الأول/أكتوبر 1945، المادة (2)، الفقرة (4).

1- معيار الشدة والجسامة: إذا تسبب الهجوم السيبراني في إحداث أضرار مادية ملموسة أو إصابات بشرية أو وفيات، فإنه يُعامل قانونياً معاملة الهجوم العسكري التقليدي تماماً¹، ومثال ذلك إذا تمّ اختراق نظام التحكم في سد مائي وفتح بواباته رقمياً لإغراق القرى المحيطة به، أو اختراق منظومة مراقبة الملاحاة الجوية للتسبب في تصادم الطائرات.

2- معيار الارتباط المباشر: يجب أن يكون الضرر الحاصل نتيجة مباشرة للهجوم السيبراني وليس نتيجة ثانوية أو بعيدة الاحتمال، ومثال ذلك: إذا أدى الهجوم السيبراني على البورصة إلى خسائر مالية فادحة فقط، فهذا ضرر اقتصادي لا يرقى إلى "استخدام القوة".

3- معيار التغلغل والاجتياح: يتعلق بمدى انتهاك الهجوم لسيادة الدولة واختراقه لأمنها الداخلي، وكلما كان النظام المستهدف يمثل عصب السيادة الوطنية (مثل السجلات المدنية، منظومة الدفاع الوطني، أو البنك المركزي)، حيث يتم تكيف الفعل كاعتداء على السيادة يستوجب الرد.

تكمّن ضرورة المقاربة الوظيفية في الربط بين المادتين² (4/2) و(51) من ميثاق الأمم المتحدة.

(1) المادة 4/2 تحظر وتمنع استخدام القوة (وهي دائرة واسعة تشمل التهديد والأفعال الأقل جسامة).

(2) المادة 51 تشترط أساساً للرد بالقوة المسلحة (الدفاع الشرعي) وقوع "هجوم مسلح" وهو عتبة أعلى من مجرد استخدام القوة.

المطلب الثاني: الأركان المادية والزمنية للعمل العدائي الرقمي

ويبحث هذا المطلب في المحددات القانونية لقياس جسامة الهجمات الرقمية وتأثيرها على المنشآت الحيوية، بالإضافة إلى معالجة إشكالية البعد الزمني والعمليات المتراكمة، وصولاً إلى معضلة الإسناد القانوني لتلك الهجمات عندما يتم تنفيذها عبر وكلاء سيبرانيين.

الفرع الأول: عتبة الجسامة والضرر الواقع على البنى التحتية

تعتبر عتبة الجسامة هي المعيار الذي نزن به هذا الأثر، وهي النقطة الحرجة التي يتحول فيها الفعل السيبراني من مجرد "عمل غير مشروع" أو "تجسس رقمي" (والذي يواجه بوسائل سلمية أو تدابير مضادة) إلى "هجوم مسلح" كامل الأركان يمنح الدولة المستهدفة الحق في الرد العسكري المباشر وفقاً لقواعد القانون الدولي³.

أولاً: الضرر المادي المباشر والوفيات (العتبة الواضحة)

¹ د. بن عزوز بن صابر، السيادة الرقمية للدول في ظل تحديات الحروب السيبرانية، دار الهدى، عين مليلة، الجزائر، 2022، ص 42.

² ميثاق الأمم المتحدة لعام 1945 (لا سيما المواد 4/2 المتعلقة بحظر استخدام القوة، والمادة 51 المتعلقة بحق الدفاع الشرعي).

³ د. خالد ممدوح إبراهيم، الحرب السيبرانية والقانون الدولي الإنساني: دراسة في القواعد المنظمة للنزاعات المسلحة الرقمية، دار الفكر الجامعي، الإسكندرية، 2022، ص 53.

يعتبر هذا المستوى الأكثر وضوحاً في القانون الدولي، حيث تترتب على الهجوم السيبراني نتائج مادية تدميرية ملموسة تعادل تماماً نتائج القصف الجوي أو المدفعي¹، ويُكيف هذا الفعل هنا على أنه "هجوم مسلح" بموجب المادة 51 من الميثاق، ويسمح للدولة الضحية بالرد الفوري باستخدام القوة العسكرية المادية لصد هذا التهديد، شريطة الالتزام بقواعد الضرورة والتناسب.

ثانياً: التعطيل الوظيفي الجسيم (العتبة الرمادية)

إذا لم يترتب على الهجوم السيبراني انفجار أو دمار مادي مباشر، إلا أنه أدى إلى شلل كامل ومستمر للبنية التحتية؟ هذا هو التحدي الحقيقي الذي يواجه فقهاء القانون الدولي اليوم.

الفرع الثاني: البعد الزمني وإشكالية الهجمات المتراكمة

أولاً: نظرية "تراكم الآثار" والتكيف القانوني لسلسلة الهجمات المتقطعة

تُعتبر نظرية تراكم الآثار (Needle-prick Theory) الثقل الفقهي الأهم الذي استند إليه القانون الدولي لتفادي القصور في المعايير التقليدية للعدوان المادي عند إسقاطها على البيئة الرقمية، بحيث تنصرف هذه النظرية في جوهرها إلى معالجة تلك الهجمات السيبرانية المتقطعة التي تنفذها دولة ما (أو وكلائها) على فترات متباعدة، بحيث لا تشكل أي عملية منها بمفردها اعتداءً جسيماً يتجاوز عتبة "الهجوم المسلح" ولكنها عند النظر إليها في مجموعها وامتدادها الزمني، يتبين أنها تُحدث أثراً تدميراً تراكمياً يهدد كيان الدولة الضحية ومصالحها الحيوية².

ثانياً: التمييز بين لحظة الاختراق ولحظة التفعيل

تتطلب الطبيعة الافتراضية للهجمات السيبرانية تحدياً زمنياً معقداً يتعلق بتحديد لحظة الخطر الوشيك فالكثير من العمليات الرقمية تبدأ بما يُعرف بـ "الاختراقات الصامتة"³، حيث يتم زرع برمجيات خبيثة أو "قنابل منطقية" نائمة داخل الأنظمة الحساسة للدولة لسنوات دون تفعيلها، وهنا يبرز دور الفقه الدولي حول تكيف هذه اللحظة، هل ينشأ حق الدولة في الدفاع عن نفسها لحظة زرع هذه البرمجية (باعتبارها خطراً وشيكاً يهدد البقاء)، أم يجب عليها الانتظار حتى لحظة تفعيلها الفعلي ووقوع الضرر.

الفرع الثالث: التكيف القانوني لإسناد المسؤولية للوكلاء السيبرانيين

يعتبر الوكلاء السيبرانيون من جماعات القراصنة، أو الأفراد، أو الشركات الخاصة الأذرع الغير رسمية التي تستعين بها بعض الدول لشن هجمات رقمية ضد دول أخرى؛ لكي يتحول العمل السيبراني الصادر عن "فاعل من غير الدول

¹ د. ليلي بن معمر، "تكيف الدفاع الشرعي الرقمي في ظل قصور ميثاق الأمم المتحدة"، مجلة الحقوق والحريات، جامعة المسيلة، الجزائر، العدد 1، 2025، ص 84.

² علي فاضل علي سليمان، "حق الدفاع الشرعي في الهجمات السيبرانية"، مجلة جامعة تكريت للحقوق، المجلد 4، العدد 4، العراق، 2020، ص 70.

³ حمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلبي، كلية القانون جامعة بابل، العراق، 2015، ص 111.

إلى عمل منسوب قانوناً للدولة، استقر الفقه والقضاء الدوليان على اللجوء إلى القواعد العامة للمسؤولية الدولية عن الأفعال غير المشروعة وتحديداً من خلال معيارين رئيسيين وضعتهما محكمة العدل الدولية:

1- معيار السيطرة الفعلية: إتمدت عليه محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة (1986)¹، إذ لا يكفي مجرد قيام الدولة بتمويل الوكلاء السريين أو تزويدهم بالدعم اللوجستي لإسناد المسؤولية إليها، بل يجب إثبات أن الدولة هي من قامت بالتوجيه المباشر والإشراف الفعلي على كل هجوم سرياني محدد قامت به تلك المجموعات ضد البنية التحتية للدولة المستهدفة.

2- معيار السيطرة العامة: تم الإستناد إليه من المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية تاديتش (1999)²، ويعتبر هذا المعيار أكثر مرونة وملاءمة للبيئة الرقمية؛ إذ يكفي بإثبات أن الدولة مارست سيطرة وتوجيهاً عاماً على التنظيم أو المجموعة السريانية (مثل توفير الملاذ الآمن، والدعم المالي المستمر، والأهداف الاستراتيجية)، دون الحاجة لإثبات إصدار أوامر لكل برمجية خبيثة أو هجوم على حدة.

المبحث الثاني: الضوابط القانونية لردع الهجمات السريانية

تصنيف الهجوم السرياني كعمل عدواني يمثل الشق الأول من الإشكالية، أما الشق الثاني والأكثر تعقيداً يكمن في تحديد الوسائل القانونية والتدابير الدفاعية التي تملكها الدولة المتضررة لرد هذا العدوان ووقف آثاره المادية والمعنوية، وتتوزع هذه الوسائل بين آليات الردع العام والخاص التي أقرها القانون الدولي والتشريعات الوطنية، وهو ما يستدعي دراسة مشروعية تفعيل حق الدفاع الشرعي وفقاً لأحكام ميثاق الأمم المتحدة ومدى مواكبة المشرع الجزائري لهذه التدابير (المطلب الأول)، مع تبيان القيود الصارمة التي يفرضها القانون الدولي الإنساني على أي رد عسكري أو سرياني متبادل (المطلب الثاني).

المطلب الأول: الدفاع الشرعي عن النفس بموجب المادة (51) من الميثاق والتشريع الجزائري

ويركز هذا المطلب على دراسة مدى انطباق شروط المادة (51) من ميثاق الأمم المتحدة على حالات الاختراق والتعطيل الرقمي، واستقراء موقف المشرع الجزائري ومدى استيعاب قواعد الإباحة في قانون العقوبات الجزائري لتدابير صد الهجمات الرقمية، وصولاً إلى تبيان مدى الالتزام بضوابط الضرورة والتناسب أثناء الرد.

¹ محكمة العدل الدولية، "قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية)"، حكم ميريتس، 27 جوان 1986، تقارير محكمة العدل الدولية 1986، ص 14.

² المحكمة الجنائية الدولية ليوغوسلافيا السابقة، قضية المدعي العام ضد دوشكو تاديتش، قضية رقم (IT-94-1-A)، حكم غرفة الاستئناف، 15 يوليو 1999، ص 62.

الفرع الأول: شروط تفعيل الدفاع الشرعي في ضوء القانون الدولي

إن إخضاع الهجمات السيبرانية لحكم المادة (51) من الميثاق، والاعتراف بمشروعية الرد عليها، يظل مشروطاً بضبط الفعل العدواني الأصلي لحزمة من المعايير الموضوعية¹ تتمثل فيما يلي.

- 1) جسامته الضرر المادي المعادل للآثار العسكرية.
 - 2) الفورية في إحداث النتائج التدميرية للعمليات الرقمية.
 - 3) تجاوز آثار الهجوم للحدود الوطنية وامتدادها العابر للحدود.
 - 4) وضوح الفعل المادي وإمكانية الربط السببي بين السلوك والنتيجة.
 - 5) حجم الآثار الاستراتيجية المترتبة على الهجوم في الدولة المستهدفة.
- ويُشترط لعدم تجريد الدولة المدافعة من وصف 'الدفاع الشرعي' أن يكون اللجوء إلى الرد الرقمي هو الوسيلة الأخيرة والملاذ الوحيد المتاح لاستعادة سيادتها واستقرارها، وبذلك يقع عليها التزام قانوني بضرورة توجيه الهجوم المضاد نحو أهداف عسكرية وحكومية محددة، مع استثناء الأعيان المدنية والمواطنين؛ بحيث يقتصر الرد على شلّ الأنظمة والمعلومات التابعة للدولة المعتدية.

يُعد مبدأ التناسب في الهجمات السيبرانية الركيزة الأساسية والجوهر الموضوعي لقواعد القانون الدولي الإنساني، ولا سيما اتفاقية جنيف الرابعة لعام 1949م المتعلقة بحماية الأشخاص المدنيين وقت الحرب².

كما يمكن استخلاص وتلخيص المعايير المنهجية لتطبيق المادة (51) من ميثاق الأمم المتحدة على الهجمات السيبرانية؛ إذ يشبّه للدولة المتضررة حق اللجوء إلى الرد الرقمي بوصفه وسيلة دفاع شرعي متى استجمعت الشروط والضوابط التراكمية التالية³:

1. **شرط الضرورة القصوى:** ألا يكون أمام الدولة المتضررة أي بدائل سلمية أو تقنية أخرى لصد العدوان وحماية أمنها القومي سوى اللجوء إلى الرد السيبراني المسلح.
2. **شرط التناسب والنسبية:** أن تتكافأ الآثار والنتائج التدميرية للهجوم السيبراني المضاد مع حجم وجسامته الهجوم الرقمي الأصلي الذي تعرضت له الدولة، دون إفراط أو تجاوز.
3. **شرط التمييز وحماية الأعيان المدنية:** أن يُوجّه الرد السيبراني حصراً نحو الأهداف العسكرية والسيادية التابعة للدولة المعتدية، مع حظر استهداف المدنيين أو ممتلكاتهم ومصالحهم الحيوية.

¹ عفاف محمد إسماعيل المليجي، "الهجوم السيبراني أداة تعيق تشكيل السياسة الخارجية: تحليل الحرب السيبرانية"، المركز الديمقراطي العربي، برلين، ألمانيا، 2018، ص 99.

² اتفاقيات جنيف الأربع لعام 1949 والبروتوكولات الإضافية لها لعام 1977 (الخاصة بالقانون الدولي الإنساني وقواعد النزاع المسلح).

³ د. عبد القادر بوزيد، "المسؤولية الدولية للدولة عن الأفعال السيبرانية الصادرة عن غير التابعين لها"، مجلة البحوث القانونية والسياسية، جامعة الجلفة، الجزائر، المجلد 9، 2024، ص 247.

4. شرط احترام الوجود السيادي للدول: ألا يؤدي الرد السيبراني إلى محو الكيان المادي والسياسي للدولة

المعتدية أو تدمير مقوماتها الأساسية على نحو يعيدها إلى عهد ما قبل البيئة الرقمية.

الفرع الثاني: موقف المشرع الجزائري من تدابير الدفاع الشرعي ضد المخاطر الرقمية

أولاً: الأساس التشريعي التقليدي للإباحة وتحمي تكييف "الحق المعتدى عليه"

ينبني النظام القانوني الجزائري في إقراره لأسباب الإباحة وموانع المسؤولية الجنائية من الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 24-06، حيث تُعد نظرية الدفاع الشرعي إحدى الركائز الأساسية التي ترفع وصف الجريمة عن الفعل متى توافرت شروطها، وتنص المادة 39¹ من قانون العقوبات على أنه: "لا جريمة إذا كان الفعل قد فرضته ضرورة الدفاع المشروع عن النفس أو عن الغير أو عن مال مملوك للشخص أو للغير".

إلا أن هذه النصوص صيغت في أصلها لمواجهة الاعتداءات المادية والجسدية الملموسة، مما يفرض على الفقه والقضاء الجزائري ضرورة إعمال تفسير مرن يتلاءم مع الطبيعة المعنوية للمخاطر الرقمية وينصرف هذا التفسير في المقام الأول إلى استيعاب مفهوم "المال" الوارد في النص ليشمل البيانات الرقمية، والمنظومات البرمجية، والبنى التحتية الحيوية، باعتبارها أموالاً معنوية ذات قيمة اقتصادية وسيادية تستوجب الحماية والإباحة عند رد الاعتداء عنها؛ لاسيما في ظل التعديل الأخير لقانون العقوبات عام 2024، الذي شدد الحماية الجنائية على أنظمة المعالجة الآلية للمعطيات بموجب المواد 394² مكرر إلى 394 مكرر7، مما يجعل من هذه النصوص المرجعية الموضوعية المحددة لـ "عدم مشروعية الاعتداء" الذي يبرر اللجوء إلى الدفاع الشرعي.

ثانياً: انطباق شروط "الخطر الوشيك" ومرونة تقدير "الفورية" في الاعتداء الرقمي

بين المشرع الجزائري لقيام حالة الدفاع الشرعي وفقاً للقواعد العامة أن يكون الخطر حالاً أو وشيك الوقوع³، وهو ما يكتسب طابعاً استثنائياً في البيئة الرقمية؛ حيث إن عنصر "الوشك" يتحقق في أجزاء من الثانية بمجرد إرسال البرمجيات الخبيثة، أو اكتشاف ثغرات أمنية حرجية وبدء استغلالها من قبل المعتدين هذا التسارع التقني يمنح المدافع مبرراً قانونياً للتدخل الفوري لصد الهجوم ومنع تفاقمه دون الانتظار لحين وقوع الضرر الفعلي وتدمير البيانات، استناداً إلى أن محاولات كسر الحماية الرقمية وجدران الأمان الوطنية تُعد قرينة كافية في نظر القانون على قرب وقوع الاعتداء.

¹ المادة 39 من القانون رقم 24-06 المؤرخ في 28 أبريل سنة 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية الجمهورية الجزائرية، العدد 30، الصادرة بتاريخ 30 أبريل 2024.

² المواد 394 مكرر إلى 394 مكرر7، من القانون رقم 24-06، المرجع أعلاه.

³ أحسن بوسقيعة، "الوجيز في القانون الجنائي العام"، دار هومة للنشر والتوزيع، الجزائر، 2022، ص 135 وما بعدها.

ثالثاً: تكامل المنظومة الدفاعية الوطنية والحاجة إلى نصوص تشريعية متخصصة

تنبني الضوابط القانونية الجزائرية في مكافحة المخاطر الرقمية على ردود الأفعال اللاحقة، كما تشمل الوقاية والردع الاستباقي وفقاً لـ القانون رقم 09-04¹ المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يمنح سلطات التحري والتدخل صلاحيات واسعة لضبط الأدلة وإيقاف الهجمات الجارية، كما تتكامل هذه المنظومة مع النصوص التشريعية المتخصصة في حماية البنى التحتية الحساسة للدولة، وعلى رأسها المرسوم الرئاسي رقم 20-05² المتعلق بإنشاء الوكالة الوطنية لأمن الأنظمة المعلوماتية؛ والمرسوم الرئاسي رقم 26-07³ المتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، مما يعطي بعداً سيادياً وأمناً خالصاً على تدابير الدفاع الرقمي، ويجعل من التصدي للهجمات التي تستهدف المنشآت الحيوية دفاعاً عن أمن الدولة ومصالحها العليا وليس مجرد رد جريمة عادية.

الفرع الثالث: أعمال مبدأ الضرورة والتناسب في رد الهجمات

أولاً: المضمون القانوني لمبدأ الضرورة والتحول من صد الاعتداء إلى الردع الاستباقي

يندرج مبدأ الضرورة في الفضاء السيبراني عندما تجد الدولة أو المؤسسة المعتدى عليها نفسها أمام تهديد وشيك يستهدف أنظمتها الحيوية، بحيث لا يترك لها وقتاً كافياً للجوء إلى الوسائل السلمية أو القنوات الدبلوماسية؛ مما يجعل من الاستجابة الدفاعية الفورية لتعطيل الهجوم خياراً حتمياً ووحيداً لحماية السيادة الرقمية ومنع إلحاق أضرار كارثية بالبنى التحتية للدولة⁴، ومن المتعارف عليه قانوناً وفقهياً أن الغاية من الدفاع الشرعي هي "صد الاعتداء" والحد من آثاره، وليس "معاينة المعتدي" أو الانتقام منه، ويفرض مبدأ الضرورة أن يتوقف الرد السيبراني فوراً بمجرد نجاح الجهة المدافعة في تحييد الخطر الرقمي وشل الهجوم الجاري.

ثانياً: التنظيم التشريعي لضوابط الرد والمسؤولية المترتبة على التجاوز

يعتبر هذين المبدأين كضابطين موضوعيين في التشريع الجزائري من خلال المادة 40 من قانون العقوبات التي تمنع صراحة أي عمل دفاعي يفوق في جسامته الخطر المهدد⁵، مما يعني في السياق الرقمي أن أي تدابير تتخذها

¹ القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

² مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441هـ الموافق 20 جانفي سنة 2020م، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية.

³ مرسوم رئاسي رقم 26-07 مؤرخ في 18 رجب عام 1447هـ الموافق 7 جانفي سنة 2026م، يهدف إلى إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في كل مؤسسة وإدارة وهيئة عمومية، الجريدة الرسمية للجمهورية الجزائرية.

⁴ Nicholas T. and Russell B. (Eds) (2015), Research Handbook on International Law and Cyberspace, Elgar.

⁵ أحسن بوسقيعة، المرجع السابق، ص 139.

المؤسسات لصد التهديدات السيبرانية يجب أن تكون موجهة حصراً لقطع الاتصال الهجومي أو تعطيل البرمجيات الخبيثة، أو تحديد مصدر الخطر دون إلحاق أضرار غير مبررة بالأنظمة الأخرى أو بالغير.

المطلب الثاني: قيود الرد في ضوء القانون الدولي الإنساني

لا يعني الاعتراف بحق الدولة في رد العدوان السيبراني إطلاق يدها في اختيار وسائل الرد وأساليبه، بل يظل هذا الحق مقيداً بالقواعد الإنسانية الآمرة التي تحكم النزاعات المسلحة لحماية الأعيان والمدنيين من آثار القتال، ويسعى هذا المطلب إلى تقييم مشروعية استخدام الأسلحة السيبرانية وفقاً للمادة 36 من البروتوكول الإضافي الأول، ومناقشة مدى التزام الأطراف بمبادئ التمييز والتحذير في البيئة الرقمية، وصولاً إلى تحديد المسؤولية الدولية المترتبة على أي تجاوز لتلك الضوابط القانونية.

الفرع الأول: المراجعة القانونية للأسلحة السيبرانية وشرط مارتنز كضابط وقائي

أولاً: الالتزام الوقائي بمراجعة الأسلحة السيبرانية وفقاً للمادة 36 من البروتوكول الإضافي الأول

إن فلسفة القانون الدولي الإنساني تُبنى على حتمية تقييد أساليب ووسائل القتال للحد من الآثار التدميرية للنزاعات المسلحة، وهو ما يمتد بالضرورة إلى البيئة الرقمية والافتراضية المستحدثة، كما تتجسد هذه الرقابة الوقائية في الالتزام الإجرائي الصارم الذي تفرضه المادة (36)¹ من البروتوكول الإضافي الأول لعام 1977، والذي يُلزم الدول المتعاقدة بالتحقق المسبق من مشروعية أي وسيلة أو أسلوب حربي جديد قبل اقتنائه أو استخدامه، ويتمشى هذا التكيف القانوني بصورة مباشرة على الأسلحة والبرمجيات السيبرانية الهجومية؛ فغياب التنظيم الاتفاقي الصريح للحروب الرقمية لا يعفي الدول من مسؤوليتها في إخضاع هذه التقنيات للمعايير الإنسانية العامة.

ثانياً: شرط مارتنز كضابط عرفي لسد الفراغ التشريعي في النزاعات الافتراضية

تجانباً مع التطور المتسارع في الوسائل القتالية وتجنب حدوث أي فراغ قانوني، يستند النظام القانوني الدولي إلى "شرط مارتنز"² العرفي كصمام أمان يحمي المدنيين والأعيان المدنية في الحالات التي لا تغطيها النصوص المكتوبة، وبالرغم من الجدل الفقهي الذي صاحب هذا الشرط بسبب مرونة مصطلحاته كـ "مبادئ الإنسانية" وما يمليه الضمير العام، إلا أن محكمة العدل الدولية في فتاها الصادرة عام 1996 بشأن مشروعية الأسلحة النووية قد حسمت قيمته القانونية، مؤكدة أنه يمثل قاعدة عرفية ملزمة ذات قوة قانونية آمرة وليست مجرد توجيهات أخلاقية اختيارية³.

¹ المادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف المؤرخة في 12 أوت 1949، المتعلق بحماية ضحايا النزاعات المسلحة الدولية، المعتمد في 8 جوان 1977، جنيف، سويسرا.

² جافور اسلام، "شرط مارتنز في مواجهة السلاح النووي"، مجلة الدراسات والبحوث القانونية، الجزائر، 2021، ص 531.

³ محمد عبد المنعم عبد الخالق، الجرائم الدولية: دراسة تأصيلية للجرائم ضد الإنسانية والسلام وجرائم الحرب، ط1، جامعة الزقازيق، الشرقية، مصر، 1989، ص 129.

ثالثاً: الممارسة الدولية والمسؤولية المترتبة على انتهاك القيود الإنسانية للعمليات السيبرانية

تؤكد الفاعلية الإلزامية لشرط مارتنز في تقييد الاستخدامات الهجومية والدفاعية على حد سواء في الفضاء السيبراني، حيث تبرز السوابق الدولية لتعكس خطورة الخروج عن هذه المعايير؛ فالهجمات السيبرانية الشاملة التي تستهدف شل المرافق الحيوية والخدمية (تُعد السلسلة الممتدة من الهجمات السيبرانية التي رافقت الحرب الروسية الأوكرانية (ابتداءً من عام 2022 وما بعدها)¹، ولا سيما الهجوم البرمجي المعروف باسم "ماسح البيانات" (Hermetic Wiper)، تمثل انتهاكاً جسيماً للشرط العرفي، حتى وإن تم التذرع بحق الدفاع الشرعي. فالرد الرقمي يفقد غطاء مشروعيته متى استهدف الأعيان والمرافق المدنية كالمستشفيات والمؤسسات المصرفية.

الفرع الثاني: حماية الأعيان المدنية وتطبيق مبادئ التمييز والتحذير

" أولاً: الالتزام بمبادئ الإنسانية والتمييز في الفضاء السيبراني والمسؤولية المترتبة عليها

يعتبر "مبدأ الإنسانية" في القانون الدولي معياراً آمراً ومجرداً غير قابل للتجزئة أو الانتقاص، ويشكل مع مبدأ التمييز حجر الزاوية لحماية المدنيين والأعيان المدنية من الآثار التدميرية للنزاعات المسلحة²، بما في ذلك العمليات السيبرانية، ويفرض هذا المبدأ التزاماً قانونياً صارماً على الدول يمنعها من توجيه الهجمات الرقمية ضد المنشآت الحيوية التي لا تشكل ضرورة عسكرية ملحة، كما يحظر شن العمليات السيبرانية الهجومية بغرض التهيب أو استعراض القوة وفرض الهيمنة السياسية.

ثانياً: التكيف القانوني للهجمات السيبرانية في ضوء حظر استخدام القوة بموجب ميثاق الأمم المتحدة

توجد إشكالية قانونية بالغة التعقيد حول مدى انطباق المادة (4/2) من ميثاق الأمم المتحدة-التي تحظر التهديد باستخدام القوة أو استخدامها في العلاقات الدولية-على الهجمات والعمليات السيبرانية المعاصرة. ويظهر هذا الخلاف الفقهي نتيجة للغموض التفسيري المحيط بمفهوم "القوة المحظورة"، حيث استقر العرف الدولي على استبعاد تدابير الإكراه الاقتصادي والسياسي والتجسس التقليدي من هذا الحظر.

الفرع الثالث: المسؤولية الدولية الناشئة عن تجاوز حدود الرد

أولاً: الاتجاه المفسر حرفياً لنطاق حظر القوة وحصرها في المظاهر العسكرية المادية

ويحتج هذا الفريق في تأصيله إلى ديباجة الميثاق التي ربطت استخدام القوة بالوسائل العسكرية مستشهدين تاريخياً برفض مؤتمر "سان فرانسيسكو" إدراج وسائل الإكراه والضغط الاقتصادي ضمن نطاق الحظر³، كما يشترط هذا الاتجاه لاعتبار الهجوم السيبراني عملاً غير مشروع يرقى لمرتبة "القوة المحظورة" أن ترتب عليه خسائر بشرية وأضرار

1 هجمات "Wiper" والبرمجيات التدميرية ضد أوكرانيا في فبراير 2022، وبالتزامن مع بدء العمليات العسكرية الميدانية، تعرضت أوكرانيا لهجوم سيبراني تدميري واسع النطاق استهدف مسح البيانات وشل الأنظمة الرقمية للمؤسسات الحكومية، والقطاعات المصرفية، ومنشآت الطاقة، والاتصالات.

2 نبيل أحمد حلمي، القانون الدولي وفقاً لقواعد القانون الدولي العام، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، 1999، ص 65.

3 صلاح الدين جمال، "التفسير الموسع لمفهوم القوة في ظل القانون الدولي المعاصر"، دار الفكر الجامعي، الإسكندرية، 2021، ص 142.

مادية ملموسة تعادل الآثار الناتجة عن النزاعات المسلحة التقليدية وهو ما يلحق معظم الهجمات الرقمية- التي تتسم بطبيعتها غير المادية كأعمال التجسس والإكراه السياسي- بدائرة الأفعال المباحة دولياً أو المسكوت عنها.

ثانياً: التفسير الواسع والشامل لاستيعاب التهديدات والآثار غير المادية

ويبرز هذا الرأي في ربط المشرع الدولي الحظر بالمساس بسلامة الأراضي أو الاستقلال السياسي للدولة المستهدفة، وهو ما يمكن أن تحدثه الهجمات الرقمية المعاصرة بذات الجسامة والخطورة التي تحدثها الهجمات العسكرية المباشرة؛ إذ يفضي كلاهما إلى تقويض سيادة الدول وزعزعة استقرارها المؤسسي¹.

الخاتمة

شهدت النزاعات المسلحة المعاصرة تحولاً جذرياً بانتقالها من الطابع المادي التقليدي إلى البيئة الافتراضية الرقمية، مما فرض تحديات قانونية بالغة التعقيد حول مدى كفاية النصوص الاتفاقية الكلاسيكية لاستيعاب العمليات والأسلحة السيبرانية.

توصلت الدراسة إلى جملة من النتائج والاقتراحات التي نوردتها على النحو الآتي:

أولاً: النتائج

1. يخضع الدفاع الشرعي ضد العدوان السيبراني لشرطي الضرورة والتناسب، وهو ما يتوافق وطنياً مع المادة 39 من قانون العقوبات الجزائري.
2. غياب المعاهدات الصريحة للحروب الرقمية لا يمنع خضوعها للقانون الدولي (كشرط مارتنز)، مما يتقاطع مع فلسفة القانون الجزائري رقم 09-04 لمكافحة الجرائم التكنولوجية.
3. يتطلب استحداث الأسلحة الرقمية مراجعتها دولياً وفق المادة 36 من البروتوكول الأول 1977، وهو ما يوازيه وطنياً تدابير الرقابة بالمرسوم التنفيذي رقم 20-375 لأمن الأنظمة المعلوماتية.
4. يستوجب جمود المادة (4/2) من ميثاق الأمم المتحدة تجاوز المظهر المادي للقوة المحظورة، وتبني معيار "الآثار والنتائج" لتكييف العدوان الرقمي التدميري.

ثانياً: الاقتراحات

1. دعوة المشرع الجزائري لتعديل المواد 394 مكرر وما يليها، لتشديد العقاب على استهداف الأنظمة المعلوماتية للمرافق المدنية الحيوية زمن السلم والنزاع.
2. حث المجتمع الدولي على دمج الهجمات السيبرانية الجسيمة المسببة لشلل البنى التحتية ضمن صور "استخدام القوة" في المادة (2/4).

¹ صلاح الدين جمال، المرجع أعلاه، 2021، ص 143.

3. تفعيل العمل الدبلوماسي لإبرام اتفاقية دولية لـ "قانون الأمن السيبراني"، تمنع احتكار التكنولوجيا وتقويض سيادة الدول.

4. إرساء المسؤولية غير المباشرة للدول عن الهجمات المنطلقة من إقليمها، وهو ما يعززه وطنياً التزام حماية البيانات بموجب القانون الجزائري رقم 07-18

قائمة المصادر والمراجع:

أولاً: النصوص القانونية (الوطنية والدولية)

1- الاتفاقيات والنصوص الدولية:

- اتفاقيات جنيف الأربع لعام 1949 والبروتوكولان الإضافيان لها لعام 1977.
- البروتوكول الإضافي الأول الملحق باتفاقيات جنيف المؤرخة في 12 أوت 1949، المتعلق بحماية ضحايا النزاعات المسلحة الدولية، المعتمد في 8 جوان 1977، جنيف، سويسرا.

• ميثاق الأمم المتحدة لعام 1945.

2- التشريعات والقوانين الجزائرية:

- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024.
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 هـ الموافق 20 جانفي سنة 2020م، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية.
- مرسوم رئاسي رقم 26-07 مؤرخ في 18 رجب عام 1447 هـ الموافق 7 جانفي سنة 2026م، يهدف إلى إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في كل مؤسسة وإدارة وهيئة عمومية، الجريدة الرسمية للجمهورية الجزائرية.

ثانياً: الكتب

1- باللغة العربية:

- أحسن بوسقيعة، "الوجيز في القانون الجنائي العام"، دار هومة للنشر والتوزيع، الجزائر، 2022.
- د. بن عزوز بن صابر، "السيادة الرقمية للدول في ظل تهديدات الحروب السيبرانية"، دار الهدى، عين مليلة، الجزائر، 2022.
- د. بوبكر منصور، "القانون الدولي السيبراني: دراسة في القواعد المنظمة لاستخدام القوة في الفضاء الافتراضي"، دار الكتاب الحديث، الجزائر، 2024.
- د. خالد ممدوح إبراهيم، "الحرب السيبرانية والقانون الدولي الإنساني: دراسة في القواعد المنظمة للنزاعات المسلحة الرقمية"، دار الفكر الجامعي، الإسكندرية، 2022.
- د. سارة كمال، "المسؤولية الدولية عن الهجمات السيبرانية في ضوء مبدأ واجب اليقظة"، دار النهضة العربية، القاهرة، 2023.
- صلاح الدين جمال، "التفسير الموسع لمفهوم القوة في ظل القانون الدولي المعاصر"، دار الفكر الجامعي، الإسكندرية، 2021.

- محمد عبد المنعم عبد الخالق، "الجرائم الدولية: دراسة تأصيلية للجرائم ضد الإنسانية والسلام وجرائم الحرب"، ط1، جامعة الزقازيق، الشرقية، مصر، 1989.
 - د. معمر بن طرية، "المسؤولية الدولية عن الهجمات السيبرانية في ظل قواعد القانون الدولي المعاصر"، دار الجامعة الجديدة، الإسكندرية، 2023.
 - نبيل أحمد حلمي، "القانون الدولي وفقاً لقواعد القانون الدولي العام"، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، 1999.
- 2- باللغة الأجنبية:

- François Delerue (2022), Cyber Operations and International Law, Cambridge University Press.
- Nicholas T. and Russell B. (Eds) (2015), Research Handbook on International Law and Cyberspace, Elgar.

ثالثاً: المقالات

- أحمد سمودي، "حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، 2018.
- جافور إسلام، "شرط مارتنز في مواجهة السلاح النووي"، مجلة الدراسات والبحوث القانونية، الجزائر، 2021.
- حمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلبي، كلية القانون جامعة بابل، العراق، 2015.
- عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، العدد 35، ج3، 2020.
- د. عبد القادر بوزيد، "المسؤولية الدولية للدولة عن الأفعال السيبرانية الصادرة عن غير التابعين لها"، مجلة البحوث القانونية والسياسية، جامعة الخلفة، الجزائر، المجلد 9، 2024.
- عفاف محمد إسماعيل الملبجي، "الهجوم السيبراني أداة تعيق تشكيل السياسة الخارجية: تحليل الحرب السيبرانية"، المركز الديمقراطي العربي، برلين، ألمانيا، 2018.
- علي فاضل علي سليمان، "حق الدفاع الشرعي في الهجمات السيبرانية"، مجلة جامعة تكريت للحقوق، المجلد 4، العدد 4، العراق، 2020.
- د. ليلي بن معمر، "تكييف الدفاع الشرعي الرقمي في ظل قصور ميثاق الأمم المتحدة"، مجلة الحقوق والحريات، جامعة المسيلة، الجزائر، العدد 1، 2025.
- مايكل شميت، "الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب"، المجلة الدولية للصليب الأحمر، جنيف، سويسرا، 2002.
- محمد جلال، "الأبعاد القانونية لاستخدام القوة في الفضاء السيبراني"، مجلة البحوث القانونية والاقتصادية، الجزائر، 2019.