المجلة الدولية للعلوم القانونية والاقتصادية والاجتماعية
International Journal of Legal, Economic, and Social sciences
Doi : www.doi.org/10.63585/HQEH9876
Volume 2 Issue 6
N :8 June 2026
ISSN : 3119-6411

الحرب السيبرانية بين حظر التدخل والردع القانوني -قراءة في ضوء ميثاق الأمم المتحدة –

Cyber Warfare Between Non-Intervention and Legal Deterrence

An Analysis in Light of the United Nations Charter

رياض حياة

طالبة باحثة بسلك الدكتوراه، تخصص القانون العام والعلوم السياسية، بكلية العلوم القانونية والاقتصادية والاجتماعية بجامعة القاضي عياض مراكش.

ملخص:

تسعى هذه الدراسة إلى تقييم مدى ملائمة أحكام المادتين (4/2) و(51) من ميثاق الأمم المتحدة في مواجهة تحديات الحرب السيبرانية في ضوء قواعد القانون الدولي العام، وذلك عبر تشخيص الفراغ المعياري الملازم للفضاء السيبراني، مع تتبع محاولات الفقه الدولي الرامية إلى تكييف الهجمات الرقمية ضمن الإطار القانوني القائم. وتتمحور الدراسة حول سؤالٌ قانوني محوري مفاده: متى يَرقى الهجوم السيبراني إلى مستوى "استخدام القوة" على نحو يندرج في نطاق المادة (4/2)، ومتى يبلغ مرتبة "الهجوم المسلح" بما يترتب عليه تفعيل حق الدفاع عن النفس وفقًا للمادة (51)؟ وينعكس هذا التكييف على مدى احترام مبدأ حظر استعمال القوة ومبدأ عدم التدخل بين الدول.

علاوة على ذلك، تختبر الدراسة صرامة شرط" الهجوم المسلح" ومدى كونه في ضوء اشتراط الشدة والأثر قد يُشكل عائقا قانونيا أمام بعض الهجمات السيبرانية، بحيث قد يؤدي عدم بلوغ العتبة إلى تعثر الرد المشروع أو تأخره. كما تقيس الدراسة مدى فاعلية الآلية الجماعية المتمثلة في مجلس الأمن، وتخلص الدراسة إلى أن الممارسة الدولية كثيرا ما تبقى في نطاق التشاور والمناقشات دون التحول إلى تدابير ملزمة وفعّالة، وهو ما يتأكد على سبيل المثال من أول مناقشة مفتوحة حول الأمن السيبراني الصادرة بتاريخ 29 يونيو 2021، بما يفضي إلى ضعف الاستجابة الجماعية وتعميق الفجوة بين خطورة التهديد السيبراني ووسائل الردع المتاحة.

كلمات المفاتيح: الحرب السيبرانية –– حظر استعمال القوة – الدفاع الشرعي -ميثاق الأمم المتحدة.

Abstract

This study seeks to assess the suitability of Articles (2/4) and (51) of the United Nations Charter for addressing the challenges of cyber warfare under the rules of general international law. It does so by identifying the normative gaps inherent in cyberspace and by examining attempts in international legal scholarship to fit digital attacks within the existing legal framework. The study is guided by a central legal question: **when does a cyber attack rise to the level of "use of force" within the meaning of Article (2/4), and when does it reach the threshold of an "armed attack," thereby triggering the right of self-defense under Article (51)?** This legal characterization, in turn, affects how fully the principles prohibiting the use of force and non-intervention between States are respected.

In addition, the study examines the strictness of the requirement of an "armed attack," and whether its emphasis on **severity and effects** may pose a legal obstacle to certain cyber operations. If the threshold is not met, the result may be an inability to mount a lawful response, or at least a delay in doing so. The study also evaluates the effectiveness of the collective security mechanism embodied in the United Nations Security Council. It concludes that international practice often remains confined to consultations and deliberations, without transforming into binding and effective measures. This is exemplified by, among other instances, the first open debate on cyber

security issued on **29 June 2021**, which reflects a weakening of collective responses and a deepening gap between the seriousness of the cyber threat and the deterrent tools available.

مقدمة عامة:

أصبح الفضاء السيبراني اليوم ميدانا استراتيجيا تتقاطع فيه المصالح الوطنية للدول، وتتجلى من خلاله أنماطٌ جديدة من التهديد قد ترقى وفقا لخصوصية الوقائع إلى انتهاكات تمس سيادة الدول وأمنها على نحوٍ غير مألوف. ومن ثم، لم يعد مفهوم الحرب السيبرانية مجرد توصيف لعمليات رقمية، بل صارت ظاهرة قانونية وسياسية تُختبر أمام قواعد القانون الدولي العام، وبخاصة القواعد التي تؤطر حظر استعمال القوة ومنع التدخل بين الدول، إضافة إلى القواعد التي تحدد شروط تفعيل حق الدفاع عن النفس في حالات الهجوم المسلح[663]. الأمر الذي يضعنا أمام إشكالية قانونية وجودية، بحيث تفتقر النصوص التقليدية للقانون الدولي العام لآليات الاستجابة الفورية لطبيعة الأفعال السيبرانية المنفلتة من حدود المادة، مما يولد استعصاءً أو صعوبة في التكييف القانوني. وبالتالي هل يُعتبر الهجوم السيبراني "استخداماً للقوة" وفق منطوق المادة (4/2) من ميثاق الأمم المتحدة؟ ومتى يتجاوز عتبة الضرر التقني ليصبح "هجوماً مسلحاً" يُشرعن حق الدفاع عن النفس بموجب المادة (51) [664] ؟

وفي هذا السياق، تبلورت جملة من المقاربات الفقهية والجهود الدولية الرامية إلى هندسة معالم السيادة في الفضاء الرقمي، حيث برز "دليل تالين" كأهم المحاولات الاجتهادية لجسر الهوة بين جمود النص القانوني التقليدي وديناميكية الفعل السيبراني، عبر تقديم إطار مفاهيمي لتكييف الهجمات الرقمية. وبالتوازي، سعت فرق الخبراء الأمميين إلى إثبات مرونة ميثاق الأمم المتحدة وقابليته للاستيعاب في هذا الفضاء الناشئ. ومع ذلك، تظل هذه المساعي رهينة غياب "توافق دولي ملزم"، إذ يشكل الافتقار إلى معاهدة شمولية ناظمة حالة من الغموض الاستراتيجي في الفضاء السيبراني. وهذا الفراغ التشغيلي لا يحيل الحرب السيبرانية إلى معضلة قانونية فحسب، بل يضع القانون الدولي المعاصر في مواجهة اختبار مصيري لمدى نجاعته وقدرته على مواكبة تصاعد الهجمات العابرة للحدود وتأثيراتها التدميرية.

وفي السياق نفسه، يبرز تفعيل "حق الدفاع الشرعي" في الفضاء السيبراني كأحد أعقد الاستعصاءات القانونية في العصر الراهن، حيث يقف النص الجامد للمادة (51) من ميثاق الأمم المتحدة حائلاً دون استيعاب الخصائص البنيوية للتهديدات الرقمية. وتظهر المعضلة الجوهرية في تعذر تكييف الأفعال السيبرانية كـ "هجوم مسلح" وفق المفهوم الكلاسيكي الذي يشترط جسامة العدوان المادي الملموس. وبما أن معظم العمليات السيبرانية تظل حبيسة "العتبة دون المسلحة"، فإن الدول اليوم تجد نفسها في مأزق "الازدواجية المعيارية"من مُقيدة بصرامة القواعد الآمرة التي أرساها الميثاق، وفي مواجهة حتمية الردع لحماية كينونتها أمام تهديدات سيبرانية قادرة على شلّ مفاصل الحياة دون اللجوء للترسانة العسكرية التقليدية. وهذا ما يُمهد لإعادة صياغة "عقيدة الدفاع عن النفس" لتنتقل من تجلياتها المادية الملموسة إلى فضاء افتراضي يتجاوز حواجز الجغرافيا ويتمرد على نمطية الأسلحة المعهودة[665].

---

663 François DELERUE, La cyberguerre et le droit international, Paris, Pedone, 2023, p. 15

664 المادة 2 من ميثاق الأمم المتحدة في فقرتها 4:

تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية:

- يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة".

المادة 51 من ميثاق الأمم المتحدة على ما 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 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

665 إبراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية -العدد الأول، يناير 2025 ص7

وعلى صعيد آخر يقف مجلس الأمن باعتباره الركيزة الأساسية للأمن الجماعي والملاذ المفترض لردع العدوان، إلا أنه يواجه اليوم حالة من "العجز التنظيمي" أمام الهجمات السيبرانية العابرة للحدود. ويظهر هذا القصور بوضوح في صعوبة تكييف هذه الهجمات كحالات "تهديد للسلم والأمن الدوليين" تحت مظلة الفصل السابع، نتيجة طبيعتها المتخفية وتعقيدات إسنادها لفاعل محدد. هذا الضعف المؤسسي، معطوفاً على الاستقطاب السياسي جعل من الأمن الجماعي خياراً غير عملي، مما دفع الدول للاعتماد على حق الدفاع الشرعي الفردي كآلية أخيرة لحماية كيانها، في ظل منظومة دولية يقيدها الجمود وتفتقر إلى استجابة قانونية حاسمة[666].

وأمام هذا الانسداد في مجلس الأمن، برزت الجمعية العامة للأمم المتحدة كساحة بديلة لمحاولة بناء إجماع دولي، من خلال لجانها وخبراءها، لسد الفراغ التشريعي ووضع قواعد سلوك مسؤولة للدول في الفضاء الرقمي، سعياً لتحويل هذا الفضاء من ساحة صراع منفلتة إلى بيئة تحكمها مبادئ القانون الدولي.

بناء على ما سبق، تتمحور إشكالية هذه الدراسة حول مدى مرونة النص القانوني أمام سيولة الواقع الرقمي المتغير؟، إذ تختبر مدى صمود حظر استخدام القوة المنصوص عليه في المادة (4/2) من ميثاق الأمم المتحدة أمام موجة الهجمات السيبرانية العابرة للحدود. فبين صرامة الميثاق وسيولة الفضاء الافتراضي، يبرز السؤال الجوهري: هل يستوفي هذا العدوان التقني أركان "استخدام القوة"؟ ومتى يتجاوز الهجوم السيبراني حدود المضايقات الرقمية ليرقى إلى مرتبة "الهجوم المسلح"، مما يمنح الدولة المتضررة حقا قانونيا في الدفاع عن النفس وفق المادة (51)؟ فهي محاولة لترسيم الحدود الفاصلة بين الحفاظ على الاستقرار الدولي وبين مخاطر الانزلاق نحو نزاعات سيبرانية منفلتة لا تعترف بقيود الميثاق.

تنطلق هذه الدراسة من فرضيتين أساسيتين الأولى مفادها، كون المادة (4/2) من ميثاق الأمم المتحدة لا تزال تُمثل المرجعية القانونية القادرة على احتواء النزاعات السيبرانية، شريطة الارتكاز على معيار "جسامة الأثر والنتائج المادية" لتكييف القوة الرقمية، بعيداً عن تعقيدات تعديل النصوص. بينما تفترض الثانية كون الافتقار لتعريف دولي جامع للهجوم السيبراني يُؤدي إلى تضارب في التأويل، مما يفرض ضرورة صياغة إطار قانوني متخصص يضع معايير دقيقة تحكم الفضاء الافتراضي، وتنهي حالة "الغموض التفسيري" التي تكتنف طبيعة الهجمات الرقمية.

ترمي هذه الدراسة إلى ضبط مفهوم الحرب السيبرانية في منظومة القانون الدولي العام، عبر فحص مرونة المادة (4/2) من الميثاق في استيعاب الأفعال الرقمية، وبلورة معايير دقيقة تمايز بين "استخدام القوة السيبرانية" و"الهجوم المسلح". كما تسلط الضوء على تعقيدات تكييف العدوان الرقمي في ضوء المادة (51)، لبيان مدى مواءمة حق الدفاع الشرعي مع الطبيعة الافتراضية للفعل السيبراني. وهو ما يضعنا في نهاية المطاف أمام ضرورة الموازنة بين الحفاظ على جوهر الميثاق وبين ابتكار قواعد دولية تواكب التحولات الرقمية، لضمان ألا يظل الفضاء السيبراني ثغرةً قانونية تُهدد استقرار النظام الدولي.

ولمقاربة الموضوع قيد الدراسة والتحليل، سيتم اعتماد تصميم ثنائي يتكون من محورين رئيسيين. سيتم تخصيص **(المحور الأول)** لدراسة المقتضيات القانونية للميثاق المتعلقة باستعمال القوة في مواجهة الحرب السيبرانية، وذلك عبر تحليل المادة 2(4) من ميثاق الأمم المتحدة وتوضيح المعايير التي تُمكّن من تطبيقها على الفعل السيبراني. أما **(المحور الثاني)** فقد خُصِّص لدراسة حق الدفاع الشرعي في الفضاء السيبراني، بوصفه الاستثناء الأوحد الذي يُجيز للدولة اللجوء إلى القوة لرد العدوان، وذلك في ضوء صرامة المادة 51 من الميثاق ومعضلة انطباق وصف "الهجوم المسلح" على الفعل الرقمي.

- **المحور الأول: مبدأ حظر استعمال القوة بين ثبات النص ومرونة الواقع السيبراني**
- **المحور الثاني: حق الدفاع الشرعي في الفضاء السيبراني: بين صرامة المادة 51 ومعضلة "الهجوم المسلح"**

المحور الأول:

666 محمد حسن أحمد جاد حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة، مجلة الدراسات القانونية والاقتصادية – دورية علمية محكمة - المجلد العاشر العدد الرابع -ديسمبر 2024 ص 20 منشور بالموقع الاتي: https://jelc.journals.ekb.eg/article_410585_f00a83408f4a612d05118f5b4e7d0021.pdf تم الاطلاع عليه يوم 2026/04/23.

مبدأ حظر استعمال القوة بين ثبات النص ومرونة الو اقع السيبر اني

لطالما ظل حظر استخدام القوة الركيزة الأساسية لمنع العنف بين الدول، لكن صعود الأسلحة السيبرانية أضفى تعقيداً جديداً على هذا المفهوم. فبسبب طبيعتها غير المادية وصعوبة تتبع مصدرها، تضعنا هذه الهجمات أمام إشكالية قانونية عميقة: هل لا تزال قواعد الميثاق قادرة على تكييف الانتهاكات الرقمية كعطيل شبكات التحكم والاتصالات ضمن مفهوم العدوان؟ وهل يستوعب النص التقليدي واقعاً تكنولوجياً لم يشهده وقت الصياغة؟ وتتضاعف تعقيدات التطبيق عند الانتقال من الفضاء النظري إلى مقتضيات التفعيل القانوني، إذ يظل التكييف القانوني للهجمات السيبرانية رهيناً بتحديد طبيعتها: فهل تُصنَّف ك "استخدام للقوة" أم تندرج ضمن "التدخل غير المشروع"؟ إن حسم هذا الجدل يتوقف على معايير دقيقة توازن بين جسامة الأثر، وحيوية الهدف، ومدى المساس بالسلامة الإقليمية والاستقلال السياسي للدولة. وتصل هذه الإشكالية ذروتها عند محاولة رسم الخيط الفاصل بين الهجمات التي تظل تحت طائلة المسؤولية الدولية، وتلك التي ترقى لمرتبة "العدوان المسلح" بما يشرعن اللجوء إلى حق الدفاع عن النفس.

ومن هذا المنطلق، ولفهم هذا المبدأ فهماً دقيقاً سيتم الانطلاق من حقيقة مفادها أن "الهجوم السيبراني" لم يعد مجرد فعل تقني أو اختراق معلوماتي محض، بل قد يتحول بحسب نتائجه وآثاره إلى ممارسة تُشبه في جوهرها استعمال القوة، أو تُنتج آثاراً خطيرة تمسّ الوظائف الحيوية للدولة. ومن ثمّ يبرز الإشكال في كيفية تكييف الفعل السيبراني قانونياً ضمن قواعد القانون الدولي، وعلى رأسها حظر استعمال القوّة المنصوص عليه في المادة 2(4) من ميثاق الأمم المتحدة.

الفقرة 1: التكييف القانوني للفعل السيبر اني في ضوء المادة 2(4) من الميثاق

لم يعد مفهوم القوة في العلاقات الدولية حبيس الفوهات والمدافع، بل امتد ليتجسد في تدفقات برمجية قد توازي في دمارها الهجمات المادية؛ وهو ما وضع المادة 2(4) من ميثاق الأمم المتحدة أمام اختبار حقيقي حول مدى مرونتها في استيعاب هذه الأنماط المستجدة. لذا، تروم هذه الفقرة تسليط الضوء على الإشكالات القانونية التي تثيرها الهجمات السيبرانية عند قياسها بميزان "حظر استخدام القوة"، مع التمييز بين الأفعال التي تظل في إطار المناوشات الرقمية العادية، وتلك التي ترقى بآثارها إلى درجة العدوان الذي يستنهض آليات الردع القانوني الدولي. كما ينطلق التكييف القانوني للفعل السيبراني من اعتبار مفهوم "القوة" الوارد في المادة 2(4) مفهوماً يتسم بالتطور الذاتي بما يتماشى مع طبيعة المعاهدات المستمرة. وفي ظل غياب سلاح مادي، استقر الإجماع الدولي الناشئ على تبني "النهج القائم على الآثار، وبموجبه يُعد الهجوم السيبراني استخداماً للقوة إذا ترتبت عليه نتائج مادية (كالأضرار في الممتلكات أو الإصابات البشرية) تماثل في جسامتها آثار الهجوم المسلح التقليدي667.

ومع ذلك، يظل هذا الحظر محكوماً بشرط "الإسناد"، حيث يجب إثبات نسبة الفعل إلى دولة ما ليدخل ضمن نطاق العلاقات الدولية التي ينظمها الميثاق، مع استمرار استبعاد الضغوط السياسية والاقتصادية من هذا التوصيف وفقاً للإرادة التاريخية لواضعي الميثاق.

وعلى الرغم من قلة الممارسات الدولية الرسمية حتى عام 2022، بدأت ملامح فقه قانوني جديد تتبلور لدى بعض الدول (مثل فرنسا وهولندا والنرويج) تذهب إلى إمكانية اعتبار العمليات السيبرانية "استخداماً للقوة" حتى دون وقوع تدمير مادي ملموس. ويستند هذا الاتجاه إلى معايير نوعية وكمية، مثل خطورة تعطيل الخدمات الأساسية، ومدى الاختراق، وطبيعة المستهدف (البنى التحتية الحيوية)، وهو ما كرسه "دليل تالين 2.0". وحتى في الحالات التي لا تصل فيها العملية السيبرانية إلى عتبة "استخدام القوة"، فإنها لا تفلت من المساءلة الدولية، إذ قد تُكيف باعتبارها خرقاً لمبدأ "حظر التدخل في الشؤون الداخلية" أو انتهاكاً لسيادة الدولة،

667 عمر أحمد السعدي، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب، مجلة جامعة الامارات للبحوث القانونية 2024 ص 21: منشور بالموقع الاتي:
https://scholarworks.uaeu.ac.ae/cgi/viewcontent.cgi?article=1988&context=sharia_and_law تم الاطلاع عليه يوم 2024/04/23.

مما يضمن وجود حماية قانونية متكاملة ضد التهديدات الرقمية بمختلف مستوياتها 668. وبالرغم أيضا من افتقار المجتمع الدولي لتعريفٍ موحدٍ وجامع لـ"الهجوم السيبراني"، إلا أن الرؤى القانونية المعاصرة باتت تميل نحو مقاربةٍ مرنة تستوعب تحولات التهديد الرقمي؛ فالهجوم لم يعد مجرد اختراقٍ تقني، بل استحال نشاطاً يستهدف تدمير الأصول، وتزييف المعلومات، وشلّ المرافق الحيوية للدولة. وتتجلى خطورة هذا المفهوم في تجاوزه للوسيلة التقنية ليرتكز على "جسامة الأثر"؛ حيث تتفاوت التداعيات بين التجسس الرقمي وصولاً إلى التدمير الشامل، مما يجعل من "النتائج والآثار" المعيارَ الحاسم في تحديد مستوى الاستجابة القانونية والأمنية الكفيلة لمواجهة هذه العمليات 669 .

وفي هذا الصدد نجد الحالة الأوكرانية في المختبر الأكثر ثراءً لتطبيق المادة 2(4) من الميثاق، حيث انتقلت الهجمات السيبرانية من مجرد "إزعاج تقني" إلى "أعمال عدائية" متكاملة الأركان بحيث انتقلت الهجمات السيبرانية من مجرد "إزعاج تقني" إلى "أعمال عدائية" متكاملة الأركان ويتجلى ذلك بوضوح في هجوم "Viasat" عام 2022، الذي استهدف شلّ منظومات الاتصال والقيادة تزامناً مع العمليات العسكرية الميدانية. هذا النموذج قدّم دليلاً قاطعاً على أن "التعطيل الوظيفي الجسيم" للمرافق الحيوية للدولة يُنتج آثاراً استراتيجية وتدميرية توازي القصف التقليدي، مما يفرض تكييفه كاستخدام صريح للقوة بموجب المادة 2(4)، لكونه يتجاوز عتبة التدخل العادي ليمسّ جوهر السيادة والأمن القومي670.

تأسيساً على ما تقدم، يمكن القول إن المادة 2(4) لم تعد مجرد نص تاريخي جامد، بل أضحت إطاراً حيوياً يتمدد لاستيعاب "العدوان الرقمي"؛ حيث لم يعد "السلاح" هو المحدد للفعل، بل "النتيجة" هي التي ترسم معالم الانتهاك. وهذا التحول في المفاهيم يضعنا مباشرة أمام ضرورة البحث عن ضوابط أكثر دقة لتصنيف هذه النتائج، وهو ما سنتناوله في الفقرة الموالية عند فحص المحددات القانونية لإدراج العمليات السيبرانية ضمن مفهوم القوة.

الفقرة 2: معايير إدراج الأفعال السيبرانية في خانة استخدام القوة

لقد شهدت الهجمات السيبرانية طفرةً نوعية وتطوراً مطرداً في طبيعتها وأهدافها، فبعد أن كانت حبيسة نطاق التجسس الرقمي والنشاط الاستخباري التقليدي، تبلورت لتُفصح عن قدرات هجومية فتاكة تتجاوز حدود جمع المعلومات إلى إحداث التعطيل الشامل والتخريب المادي للبنى التحتية. ومن رحم هذا التحول، انبثقت أنماط مستحدثة من الصراعات باتت تُعرف بـ 'الحروب الهجينة'، وهي استراتيجيات تجمع بين التكنولوجيا المتطورة والعمليات الميدانية، وتستهدف شلّ قدرة الخصم والتأثير على مراكز ثقله الحيوية. ويتبدّى هذا التحول الجذري جلياً في الممارسات الدولية المعاصرة، حيث لم تعد الساحة الرقمية مجرد فضاء للمناوشات التقنية، بل أضحت مسرحاً لعمليات عدائية متكاملة الأركان تُعيد صياغة مفاهيم الصراع والردع في العصر الحديث."

وفي هذا الصدد يُعد دليل تالين (Tallinn Manual) وثيقة قانونية استرشاديه غير ملزمة صدرت بمبادرة من مركز التميز التابع لحلف الناتو، بهدف فك الاشتباك القانوني وتوضيح كيفية تطبيق قواعد القانون الدولي على العمليات السيبرانية المعقدة. بحيث يرتكز هذا الدليل في تكييفه للهجوم السيبراني على معيار الأثر المادي؛ فالفعل الرقمي يرقى إلى مستوى 'الهجوم' متى كانت نتائجه المحتملة أو الفعلية تؤدي إلى إصابات بشرية، أو وفيات، أو تدمير مادي للممتلكات، مما يجعل من 'حجم الضرر' المعيار الحاسم للتمييز بين العمليات التقنية العادية وبين الهجمات التي تستوجب رداً قانونياً دولياً 671." ومن هذا المنطلق نجد أن دليل تالين لم

668 https://cyberlaw.ccdcoe.org/wiki/Use_of_force#cite_note-16

669 Karine BANNELIER, Théodore CHRISTAKIS Cyberattaques : Prévention-réactions des acteurs privés et des États rôle p 31. https://www.irsem.fr/storage/file_manager_files/2025/03/cahier-bannelier-christakis-cyberattaques

670 https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

671 Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. (Rule 92 regarding the definition of 'Attack').

المجلة الدولية للعلوم القانونية والاقتصادية والاجتماعية
International Journal of Legal, Economic, and Social sciences
Doi : www.doi.org/10.63585/HQEH9876
Volume 2 Issue 6
N :8 June 2026
ISSN : 3119-6411

يكتفِ بوضع إطار عام، بل اجتهد في تقديم مجموعة من المعايير الاسترشادية (المعروفة بمعايير شميت) لتقييم عتبة "استخدام القوة"، وأبرزها:

أولاً: معيار "الآثار" كشرط لتفعيل الحظر

يُعد معيار 'الآثار' التحول الفلسفي الأبرز في فقه القانون الدولي المعاصر، حيث استطاع بمرونته كسر جمود التفسير التقليدي للمادة 2(4) من ميثاق الأمم المتحدة. فبموجب هذا المنهج، الذي استقر عليه الفقه الدولي لاسيما في "دليل تالين"، لم يعد تكييف الفعل السيبراني كاستخدام غير مشروع للقوة رهيناً بطبيعة الأداة المستخدمة سواء كانت صاروخاً حركياً أو فيروساً إلكترونيا بل بمدى جسامة التداعيات المادية والوظيفية التي يلحقها بالدولة المستهدفة. وبذلك، يُكيف الفعل الرقمي كـ "استخدام للقوة" إذا أسفر عن نتائج مادية ملموسة، كالإصابات البشرية أو تدمير البنية التحتية الحيوية (مثل تعطيل السدود أو المنشآت الصناعية عبر التحكم الرقمي)، مما يجعله يتساوى في ميزان القانون الدولي مع الهجوم المسلح التقليدي في استهدافه المباشر للسيادة الإقليمية للدولة672."

فهذا المعيار قد نجح في سدّ الفجوة بين نصٍّ جامد وواقع سيبرانيٍّ مرن، حيث أقرّ بأن العبرة في تفعيل حظر استعمال القوة تكمن في الأثر التدميري للهجوم (سواء كان بشرياً أو مادياً) لا في الوسيلة التقنية المتبعة. وبذلك، أصبحت الحماية القانونية للسيادة الوطنية غير مرهونة بشكل الاعتداء، بل بمدى تهديده للمصالح الحيوية للدولة، مما يضمن شمولية الحظر لكل فعل رقمي يرقى بآثاره إلى مستوى "العدوان المسلح".

ثانياً: الضوابط التحليلية لتكييف الفعل السيبراني (معايير شميت)

نظراً لصعوبة التمييز بين "المضايقة السيبرانية" و"استعمال القوة"، وضعت الدراسة التي أشرف عليها البروفيسور "مايكل شميت" سبعة ضوابط تساعد على معرفة متى نطبق المادة 2(4) من الميثاق. وإذا كانت شدة الضرر هي الأساس، فإن تفعيل حظر استخدام القوة يتوقف على شرطين لا ينفصلان: "الفورية والمباشرة". فالمباشرة تعني أن يكون هناك رابط واضح ومباشر بين الهجوم الرقمي والضرر الذي وقع، بحيث يكون الهجوم هو السبب الحقيقي للتدمير أو التعطيل، دون وجود أسباب أخرى تُضعف هذا الرابط القانوني. أما الفورية فتتعلق بالزمن، فالهجمات التي تُسبب دماراً سريعاً ومفاجئاً تشبه الهجوم العسكري التقليدي، وهذا ما يَستدعي تحركاً دولياً عاجلاً. هذان الشرطان يعملان كـ "مصفاة قانونية" فهما يستبعدان عمليات التجسس أو الضغط الاقتصادي الرقمي من نطاق المادة 2(4)، لأن آثارها تكون بطيئة أو غير مباشرة، فهذه الأفعال تبقى ضمن انتهاك مبدأ "عدم التدخل" أو "خرق السيادة"، إلا إذا وصلت إلى درجة من التدمير المادي الجسيم تهدد السلم والأمن الدوليين 673 . لكن الواقع السيبراني أثبت أن الأثر قد يسبقه الوعيد. فحين تصبح القدرة التدميرية ورقة ابتزاز، يبرز وجه آخر للحظر "حظر التهديد". فما هي العتبة التي يجب أن يبلغها التهديد الرقمي ليُعدّ خرقاً للسلم الدولي؟"

ثالثاً: عتبة التهديد السيبراني بالاستخدام

لا يقف نطاق الحظر الوارد في المادة 2(4) من الميثاق عند حد التجريم الفعلي لاستعمال القوة، بل يمتد ليشمل تجريم "التهديد" بها، كسياج وقائي استباقي يصون السلم الدولي من الابتزاز. وإذا كان إسقاط هذا المبدأ على الفضاء السيبراني يثير إشكالات بنيوية، فإن تفعيله يقتضي توافر ركنين متلازمين: أولاً، وجود إعلان صريح أو سلوك مادي يكشف عن نية عدائية مقرونة بقدرة تقنية على إيقاع ضرر تدميري حال عدم الإذعان لمطالب معينة؛ وثانياً، أن يتسم هذا التهديد بسمتي "الوشاكة" و"المصداقية"، بحيث يكون تنفيذه، لو وقع، من قبيل الاستعمال غير المشروع للقوة بمعناه التقليدي. غير أن الطبيعة اللامادية للفضاء الرقمي تفرغ هذا الحظر من مضمونه الردعي في كثير من الأحيان. فالتحدي الجوهري لا يكمن في تفسير النص، بل في إثباته؛ إذ تصطدم فكرة

672 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 69, p. 334.

673 Watts, S. (2014). Low-Intensity Cyber Operations and the Principle of Non-Intervention. In J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), Cyber War: Law and Ethics for Virtual Conflicts. Oxford University Press, p. 210

"التهديد" بجدار "الإسناد القانوني" سميك. فكيف يمكن مساءلة دولة عن تهديد صادر من خوادم مجهولة، أو عبر برمجيات خبيثة تتقن التخفي وتغيير بصمتها الرقمية؟ إن هذا الغموض في الإسناد يُحوّل التهديد السيبراني إلى سلاح استراتيجي خفي، يُمارس به الابتزاز وتُقوّض به سيادة الدول دون أن تترك الدولة الفاعلة أثراً قانونياً يمكن الاحتجاج به [674].

وعليه، يظل حظر التهديد السيبراني قاعدة معيارية ذات فعالية منقوصة، معلقة على شرط كشف الأقنعة التقنية. فبدون يقين في الإسناد، لا يجد الميثاق سبيلاً ملموساً لردع الوعيد الرقمي، ويبقى الاستقرار الدولي رهيناً بحسن نية الفاعلين، ما لم يرتقِ التهديد إلى مرتبة "الخطر الداهم" الذي يبرر، بذاته، اللجوء إلى تدابير الدفاع الاستباقي المنصوص عليها في المادة 51.

تُشكّل معايير الشدة والفورية والمباشرة ثلاثية قانونية متكاملة يُستدل بها على بلوغ الهجوم السيبراني عتبة "استعمال القوة" المحظور بموجب المادة 2(4). فإذا كان معيار الشدة يرسم الحد الأدنى من جسامة الضرر اللازم للتكييف، فإن معيار الفورية يُضفي على الفعل طابع العدوان المباغت الذي يستنهض الرد الدولي، بينما يعمل معيار المباشرة كضمانة سببية تقطع الصلة بين الفعل الرقمي وأي عوامل وسيطة قد تُميّع المسؤولية. إن هذه الثلاثية لا تعمل بمعزل عن بعضها، بل تتضافر ك: "مصفاة معيارية" دقيقة، فهي تُخرج من نطاق الحظر كل أشكال الضغط السيبراني منخفض الشدة أو بطيء الأثر أو منقطع السببية كالتجسس والحروب النفسية لتُبقي الباب موصداً إلا أمام تلك الهجمات التي تُحدث، في لحظة خاطفة، تدميراً مادياً مباشراً يُماثل في نتائجه آثار العدوان العسكري التقليدي. وبذلك، يظل تفعيل الحظر رهيناً بتحقق هذه الشروط مجتمعة، كضمانة لعدم التوسع في تفسير "القوة" بما يُهدد استقرار العلاقات الدولية.

المحور الثاني

حق الدفاع الشرعي في الفضاء السيبراني: بين صرامة المادة 51 ومعضلة "الهجوم المسلح"

بعد أن تم الوقوف على المقتضيات القانونية الناظمة لاستخدام القوة في الفضاء الافتراضي، وفهم المعايير والضوابط التي تسمح بتطويع نص المادة 2(4) لاستيعاب الواقع السيبراني المرن، يبرز التساؤل الجوهري حول المآلات العملياتية لهذا التكييف. فإذا كانت القواعد الدولية قد نجحت إلى حد ما في توصيف الفعل السيبراني كعدوان، فإن نقل هذا التوصيف إلى حيز التنفيذ يرتطم بصخرة المادة 51 من الميثاق، مما يضعنا أمام مواجهة حتمية بين صرامة النص التقليدي ومعضلة تصنيف الهجمات الرقمية كـ 'هجوم مسلح'. لذا، يروم هذا المحور استجلاء حدود حق الدفاع الشرعي في البيئة الرقمية، وبحث مدى كفاية الآليات القانونية القائمة لردع التهديدات التي تتخفى وراء شاشات الحواسيب وتستهدف الوجود السيادي للدول."

الفقرة الأولى: صرامة شرط الهجوم المسلح: عائق قانوني أمام مواجهة الهجمات السيبرانية

مما لا شك فيه أن شرط "الهجوم المسلح" يُعدّ العتبة القانونية الحاسمة لقيام الدفاع الشرعي وفق المادة 51 من ميثاق الأمم المتحدة، بما يجعله قيدًا صارمًا على إمكانية إدراج كثير من صور الهجمات السيبرانية ضمن نطاق استخدام القوة. ونتيجةً لطبيعة الهجوم السيبراني التي قد تكون غير تقليدية، وتفاوت آثارها بين التخريب الجزئي والتعطيل العابر، فضلًا عن صعوبة تحديد جسامة الضرر وتكييف الوسيلة والغاية، تتأكد الإشكالية في كيفية مواءمة هذا الشرط مع واقع الهجمات السيبرانية، وهو ما يبرز صرامته بوصفه عائقًا قانونيًا أمام مواجهة تلك الهجمات في الإطار المسموح به دوليًا[675].

وفي هذا الصدد تمثّل المادة 51 من ميثاق الأمم المتحدة الاستثناء الجوهري والأصيل من مبدأ حظر استخدام القوة المقرر في المادة (4/2)، إذ قررت بصورةٍ قاعدية أن حق الدفاع الشرعي هو حق طبيعي للدول. غير أنّ هذا الحق لا يُفهم بوصفه حقًّا مطلقًا، بل يظل مقيدًا بشرطٍ مسبقٍ لا تتقرر آثاره القانونية ما لم يتحقق وقوع "هجوم مسلح ومن ثمّ، فإن التحليل الفقهي للمادة يفضي إلى

674 Katharina Ziolkowski, "Confidence Building Measures for Cyberspace - Legal Implications," in Peacetime Regime for State Activities in Cyberspace, ed. Katharina Ziolkowski (Tallinn : NATO CCD COE Publication, 2013, p553.

675 Tyler VanderMolen, The Next Battlefield is in Cyberspace: Evaluating Cyberattacks under Article 51, Michigan Journal of International Law, 2021. https://www.mjilonline.org/the-next-battlefield-is-in-cyberspace-evaluating-cyberattacks-under-article-51/?utm_source=openai

ركنين حاسمين: ركنٌ عضوي يتعلق بإسناد الهجوم إلى دولة أو كيان محدد على نحوٍ يترتب عليه قانونًا قيام مسؤولية دولية أو على الأقل قابلية الإسناد، وركنٌ مادي يتصل بجسامة الفعل وبلوغ آثاره درجةً تجعل منه هجومًا مسلحًا لا مجرد واقعة اعتداءٍ أقل جسامة[676].

تتجلى المعضلة عند إسقاط هذا التصور على الفضاء السيبراني، بالنظر إلى أن الصياغة التاريخية للمادة 51 قد ارتبطت في تصورها الكلاسيكي بوسائل القوة العسكرية التقليدية، بحيث تُقاس الفاعلية والضرر على أساس أدواتٍ ملموسة كالسلاح والقتال المباشر. أما الهجمات السيبرانية، فقد تستهدف البنى التحتية الرقمية أو تؤدي إلى تعطيل واسع النطاق أو إحداث آثارٍ شديدة الخطورة دون أن يستلزم ذلك إطلاق رصاصة واحدة. وبناءً عليه، يفضي التفسير الضيق للمادة إلى مفاضلة ضمنية بين "وسيلة" العدوان و"نتيجته"، بما يجعل كثيرًا من العمليات السيبرانية على الرغم من دقتها وخطورتها غير قادرة على اجتياز عتبة "الهجوم المسلح" وفق مفهومه التقليدي، فتتسع بالتالي فجوة قانونية تحول دون تمكن الدول المتضررة من الاستناد إلى المادة 51 لردّ تهديداتٍ رقمية تقع في المنطقة الحدّية بين التجسّس والاعتداء المادي ذي الجسامة المعترف بها[677].

وعليه فإن صرامة شرط الهجوم المسلح تكمن في التفرقة الجوهرية التي أرستها محكمة العدل الدولية في قضية نيكاراغوا (1986)، وتحديداً في فقرتيها 191 و195؛ حيث قررت المحكمة أن حق الدفاع الشرعي عن النفس لا ينشأ إلا في مواجهة الأشكال الأكثر خطورة من استخدام القوة. ومن خلال اعتماد معيار 'النطاق والآثار'، وضعت المحكمة عائقاً قانونياً أمام توصيف الهجمات السيبرانية كـ "هجوم مسلح"، إذ تظل معظم هذه العمليات الرقمية رغم ضررها تندرج تحت فئة 'الاستخدام الأقل خطورة للقوة' أو التدخل غير المشروع، مما يحرم الدولة الضحية من التذرع بالمادة 51 لردع الهجمات السيبرانية عسكريا [678].

إن ما تفرضه القيود الصارمة على نطاق الدفاع الفردي يفتح إشكالًا قانونيًا وعمليًا في آنٍ واحد، إذ يوحي منطوق المادة 51 من حيث المبدأ بأن يكون مجلس الأمن هو البديل الجماعي المنوط به تنظيم الاستجابة لوقائع العدوان، بدلًا من أن تبقى حماية الدول رهينة بقدرات كل دولة على حدة. غير أنّ السؤال الأعمق يتعلّق بمدى كفاية "الأمن الجماعي" ليس فقط من الناحية النظرية، بل أيضًا من زاوية الفاعلية زمنَ الأزمات، وآليات اتخاذ القرار، وإمكانية تجاوز العوائق السياسية التي قد تُبطئ التدخل أو تُفرغه من مضمونه. وعليه، تُمثّل هذه الفكرة دعوةً إلى تقييم ما إذا كانت آلية مجلس الأمن قادرة فعلًا على سدّ الفجوة التي يتركها تقييد الدفاع الفردي، وتحويل الحماية القانونية إلى حماية واقعية تضمن ردّ العدوان على نحوٍ عادل وفعّال.

الفقرة الثانية: عجز مجلس الأمن أمام الهجمات السيبرانية

يُنيط ميثاق الأمم المتحدة بمجلس الأمن المسؤولية الرئيسية عن صون السلم والأمن الدوليين، ومن هذا المنطلق واكب المجلس الطبيعة المتغيرة للتهديدات التي تعترض الاستقرار العالمي، فتصدى لجملة من العوامل المستجدة والمركبة التي من شأنها زعزعة كيان الدول أو تعقيد النزاعات القائمة وإطالة أمدها. وقد تجلى ذلك في انعقاد سلسلة من المناقشات المواضيعية المعمقة على مدار السنوات، تناولت مستجدات الأمن الدولي من قبيل تغير المناخ، وإدارة الموارد الطبيعية، وتفشي الأوبئة، وتفاقم المجاعات،

---

676 المادة 51 من ميثاق الأمم المتحدة:

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 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.

677 القاعدة 71 من دليل تالين 2.0:

- نصت على جواز ممارسة الدولة لحق الدفاع الشرعي عن النفس إذا تعرضت لهجوم سيبراني يرق إلى مستوى الهجوم المسلح. ويشترط الدليل أن تماثل آثار الهجوم السيبراني أضرار الهجوم التقليدي، مثل حدوث إصابات بشرية أو أضرار مادية جسيمة بالبنية التحتية
https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

678 https://www.icj-cij.org/fr/node/103143

واستشراء الجريمة المنظمة العابرة للحدود، والاتجار بالمخدرات، والقرصنة البحرية، إلى جانب اجتماعات مخصصة لقضايا بعينها.

على ضوء ما سبق، لا يقتصر الإشكال على تحديد معنى "الهجوم المسلح" بقدر ما يمتد إلى مرحلةٍ لاحقة تتعلق بضمانات الاستجابة الدولية. فمتى تعذر أو ضاق نطاق الدفاع الفردي، يبقى السؤال حاسمًا: إلى أي حدّ يمنح البديل الجماعي الوارد في المادة 51 فعاليةً حقيقية في مواجهة الهجمات السيبرانية ذات الطابع المستعجل والمعقّد؟ وإذا كانت صرامة شرط "الهجوم المسلح" قد ضيّقت نطاق الدفاع الفردي من حيث التكييف والشرعية، فإن الشقّ الثاني من المادة 51 يضيف قيدًا إجرائيًا أكثر حساسية يتمثل في ضرورة تدخل مجلس الأمن بوصفه الضمانة الجماعية. غير أنّ هذا البديل، على الرغم من أهميته النظرية، يصطدم في الواقع بواقع سيبراني شديد الخصوصية: هجمات سريعة ومتعددة المصادر، وأدلة تقنية تستلزم وقتًا للتحقق، فضلاً عن تباين تقديرات الدول وتعارض المصالح السياسية داخل مجلس الأمن. وبهذا يتحول "الأمن الجماعي" من آلية استجابة فعّالة إلى احتمالٍ يعتريه البطء أو يتجمد بفعل ما يُعرف بمعضلة الشلل، فينشأ فراغ زمني وقانوني بين وقوع الاعتداء وبلوغ التدخل الدولي مداه المأمول، الأمر الذي يعيد طرح سؤال الفاعلية: هل يستطيع مجلس الأمن، بآلياته الحالية، مواكبة طبيعة التهديدات السيبرانية دون أن يُفقد المادة 51 مضمونها الحمائي؟

وإن كان الفضاء السيبراني الحر والمفتوح قد شكل رافعة للتنمية وحقوق الإنسان والاستقرار، فإن تنامي الاعتماد عليه واكبه تصاعد في الأنشطة الخبيثة التي تستهدف البنى التحتية الحيوية، بما بات يهدد السلم والأمن الدوليين. وقد أثمرت جهود الأمم المتحدة والمنظمات الإقليمية إطاراً معيارياً متراكماً لسلوك الدولة المسؤول، عبر تقارير الخبراء والاتفاقيات الإقليمية وتدابير بناء الثقة، إلا أن طابعه الطوعي حال دون توفير ردع فعال، فظل الاستقرار السيبراني مرتهناً بالالتزام الأدبي لا بالقوة الإلزامية. فتتجلى المعضلة في" ليست في غياب القاعدة، بل في غياب الإلزام".

ومن هذا المنطلق فقد عقد مجلس الأمن بتاريخ 29 يونيو 2021 أول مناقشة مفتوحة في تاريخه مخصصة كلياً لموضوع الأمن السيبراني تحت عنوان "صون السلم والأمن الدوليين في الفضاء السيبراني. ويكتسي هذا الحدث دلالة رمزية مهمة، إذ يعكس اعترافاً رسمياً من الجهاز الرئيسي المكلف بحفظ السلم والأمن بأن الأنشطة الخبيثة في الفضاء السيبراني باتت تشكل خطراً متنامياً على الاستقرار الدولي. غير أن تحليل أهداف هذه المناقشة يكشف عن محدودية دور المجلس الراهن؛ فقد حصرت أهدافها في "الإسهام في تعزيز فهم أفضل للمخاطر المتنامية" و"إعادة تأكيد التزام الدول بالقانون الدولي وإطار سلوك الدول المسؤول"، دون أن تفضي إلى اعتماد قرار ملزم أو إنشاء آلية تنفيذية خاصة بالردع السيبراني. وبذلك، فإن هذا الاعتراف يبقى اعترافاً تشخيصياً لا علاجياً، مما يؤكد أن البديل الجماعي الذي نصت عليه المادة 51 لا يزال حبيس مرحلة التشاور وتبادل الرؤى، وعاجزاً عن تقديم استجابة عملية وفورية تتناسب مع سرعة الهجمات السيبرانية وطبيعتها العابرة للحدود[679].

وإن مثّلت مناقشة يونيو 2021 سابقةً بوصفها أول معالجة مستقلة للأمن السيبراني في مجلس الأمن، إلا أن حضور الموضوع في أجندته ليس وليد اللحظة. فقد تناوله المجلس سابقاً في اجتماعات غير رسمية وضمن مناقشات أشمل حول السلم الدولي، ما يعكس إدراكاً متنامياً لخطورته. فمنذ ديسمبر 2017 صنّفه الأمين العام خطراً متصاعداً يهدد السلم الدولي (S/PV.8144)، وفي أغسطس 2019 دعت بولندا لبحث آليات الردع السيبراني في الشرق الأوسط (S/2019/643)، كما حذرت مناقشة أبريل 2021 من استهداف البنى الحيوية الطبية (S/2021/415). غير أن هذا التراكم يؤكد أن التهديد السيبراني استقر كهاجس أمني دولي، بينما ظل تعاطي المجلس معه أسير التشاور، بلا ارتقاء إلى فعل ملزم يوازي طبيعته[680].

679 UN Security Council, Open Debate on Cyber Security : Maintaining international peace and security in cyberspace, 29 June 2021, VTC.
https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf?utm_source=openai

680 UN Security Council, Open Debate on Cyber Security Ibid

ويرجع هذا القصور إلى ما يسميه الفقه "معضلة الإسناد"؛ فقد حذرت وزيرة الأمن الداخلي الأمريكي في أواخر 2018 من أن "الهجمات السيبرانية تجاوزت بخطورتها الهجمات المادية"، غير أن القانون الدولي لم يواكب هذا التحول. فالفضاء السيبراني بطبيعته التقنية يسهل إخفاء هوية المهاجم ويعدد مسارات الهجوم، ما يجعل تحديد مصدره بشكل قاطع وسريع أمراً شبه مستحيل، ولأن القانون الدولي يشترط إثبات مسؤولية الدولة قبل السماح بالرد دفاعاً عن النفس، فإن صعوبة الإثبات تقنياً تتحول إلى عائق قانوني يعطل كل آليات الردع، سواء من مجلس الأمن أو من الدولة نفسها. وهكذا تجد الدولة الضحية نفسها بين خيارين أحلاهما مر: إما أن ترد وهي غير متأكدة فتخاطر بإشعال نزاع أوسع، أو أن تصمت فتترك كيانها معرضاً للخطر[681].

وعليه يتضح أن الجمود في تكييف مبادئ الدفاع عن النفس والإسناد مع خصوصية الهجمات السيبرانية المسلحة يفرغ حق الدولة في الدفاع عن كيانها من مضمونه، إذ تغدو الاستحالة التقنية للإسناد الفوري عائقاً قانونياً يحول دون رد مشروع. وإذا كانت التدابير المضادة والالتزام بالعناية الواجبة توفر هوامش للمساءلة غير القسرية، فإنها تظل قاصرة عن موازنة حق الرد عند بلوغ العتبة المسلحة. لذا يغدو تكييف الإطار التقليدي ضرورة لا ترفاً، عبر نموذج مرن يدرج متطلبات الإسناد بحسب جسامة الرد المزمع، بما يصون الأسس القانونية الراسخة، ويكبح مخاطر الإسناد الخاطئ والتصعيد، ويحفز تعاوناً دولياً يرتقي بالمسؤولية السيبرانية من الطوعية إلى الإلزامية. ورغم شيوع الأعمال العدائية ضد الدول، فإن القانون الدولي يمنحها مساحة للرد، لكنه يقيّد هذه المساحة بشروط دقيقة في التوقيت والوسيلة. فالخيارات متاحة، لكن الخطأ في اختيارها قد يحوّل الدولة من ضحية إلى مسؤولة.

كما أن اعتماد المجلس في كثير من الأحيان، على اللغة التحذيرية والاستنكارية دون بناء "معايير تشغيلية" تحسم عتبة التهديد ومتى يُفعَّل الإجراء الملزم، يجعل الجماعية الأمنية أقرب إلى إطار توصيفي منها إلى منظومة استجابة فعّالة، فتحلّ الاستحالة التقنية للإسناد الفوري محلّ عنصر الحسم القانوني، فتتسع الفجوة بين الإقرار بخطورة الهجمات السيبرانية وبين القدرة على ردّ مشروع وسريع.

وبالتالي إنّ التساؤل حول قدرة مجلس الأمن، بآلياته الراهنة، على مواكبة طبيعة التهديدات السيبرانية يفضي إلى نتيجة مفادها أن الإجابة تبدو في كثير من الحالات إلى حدٍّ كبير سلبية ما دام مضمون "الأمن الجماعي" يعتمد على افتراضات لا تَنهض في البيئة السيبرانية. فآلية المجلس كما صُمِّمت تقوم، أولًا، على إمكان تحديد المعتدي وإسناد الفعل في زمن قصير، وثانيًا على توفر إرادة سياسية جماعية قادرة على اتخاذ تدابير رادعة. غير أنّ الهجمات السيبرانية تتسم بطابع لامادي وسريع، وتواجه الدول صعوبة جوهرية في استيفاء معيار "درجة معقولة من اليقين" في الإسناد، بما يجعل الافتراض الأول عمليًا متعثّرًا. وإضافةً إلى ذلك، فإن كثيرًا من النزاعات السيبرانية تمس مصالح الدول دائمة العضوية بصورة مباشرة أو غير مباشرة، الأمر الذي يجعل حق النقض "الفيتو" عاملًا بنيويًا يُفضي إلى شلل المجلس عند لحظة الحسم. وبهذا تتبدّى الفجوة: حين تُعلّق المادة 51 الحماية الجماعية على تدخل مجلس الأمن، قد تتحول الإحالة عمليًا إلى تعليقٍ للحق في الدفاع الشرعي على شروط عسيرة أو شبه مستحيلة التحقق؛ فلا يُستعاد مضمون المادة 51 بوصفه ضمانة حمائية، بل تُفرَّغ من فاعليتها أمام تهديدات الجيل الجديد.

خاتمة :

تقف الحرب السيبرانية عند مفترقٍ دقيق بين قواعد القانون الدولي العام وبين واقعٍ تقني يتسم بالتعقيد وعدم القابلية التامة للضبط. فمن جهة، يظهر مبدأ حظر استعمال القوة بوصفه قاعدةً ثابتة، غير أن تطبيقه في المجال السيبراني يواجه مرونةً مفروضة بحكم طبيعة الأثر والوسائل، بما يفرض إعادة قراءة معيار "القوة" وعتبات التجاوز في بيئة تتبدّل فيها العلامات وتتعاظم فيها فجوة الإثبات، ومن جهة أخرى يتجلى حق الدفاع الشرعي في الفضاء السيبراني بوصفه إطارًا قانونيًا ممكنًا، لكنه لا يعمل بمعزلٍ عن شروطه الصارمة ولا سيما شرط "الهجوم المسلح" وفقًا لمقتضيات المادة51 .فالإشكال لا يتعلق بوجود الحق من حيث

681- https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/ADC0F451A9B560D8A070A753E61E874F?utm_source=openai

المبدأ بقدر ما يتعلق بتكييف الوقائع السيبرانية المسلحة وترجمتها إلى معايير قانونية دقيقة تسمح بالرد دون إخلال بشرط الضرورة والتناسب، ودون أن تتحول الاستثناءات إلى ذريعة .

كما تُبرز معالجة المجلس الأمني للهجمات السيبرانية من خلال قصور البديل الجماعي أن الردع في هذا الميدان لا يتحقق بالشعارات وحدها، بل يحتاج إلى آليات أوضح وأكثر فعالية لتسمية التهديد وتحديد العتبات والإسناد وإعمال الاستجابة. وبهذا المعنى، يتوقف نجاح النظام القانوني في الحد من التصعيد السيبراني على سد الفجوة بين النص القانوني وخصوصية الواقع التقني، وعلى بناء فهمٍ مشترك يوازن بين صون السلم الدولي وضمان حق الدول في حماية كيانها عند تحقق الخطر.

وعليه فإن التصدي للهجمات السيبرانية يتطلب انتقالًا من التأطير النظري إلى البناء الإجرائي، إذ يتضح أن الإشكال لا ينحصر في صون حظر استعمال القوة، بل في كيفية تكييفه داخل واقع سيبراني متقلب يصعب ضبطه، كما يبرز أن حق الدفاع الشرعي يبقى مرهونًا بشرط "الهجوم المسلح" وفقًا للمادة 51 مع ما يرافقه من معضلة في إثبات الإسناد وتحديد عتبة التهديد. وبالتالي فهذه الدراسة توصي بإرساء معايير تشغيلية مشتركة لتحديد متى تَرقى الواقعة إلى مستوى "الهجوم المسلح"، وتعزيز آليات الإسناد والإنذار المبكر لتقليص زمن الاستجابة، فضلاً عن تفعيل بديل جماعي فعّال يترجم التشاور إلى إجراءات واضحة تقلل الفجوة بين مبدأ الردع وبين القدرة العملية على إنفاذه دون الإخلال بالسلم الدولي.

كما تتمثل ملامح سد النقص التنظيمي القائم بالإضافة إلى ما سبق في الانتقال من معالجة الظاهرة عبر التكييف الاجتهادي المتباين إلى بناء قواعد أكثر قابلية للتطبيق والتنبؤ؛ وذلك عبر تطوير تفسير معياري للقواعد القائمة بما يحدّد بدقة عتبة "الهجوم المسلح" وفقًا للمادة 51 ومعايير الضرورة والتناسب، ويضع ضوابط عملية لجمع الأدلة وتيسير الإسناد بما يقلل من أثر التعذر التقني على مشروعية الرد. وفي موازاة ذلك، يُستحسن تفعيل مسار معياري/اتفاقي متخصص يختص بتنظيم النزاعات السيبرانية المسلحة، يقرّ آليات للتعاون وتبادل المعلومات والإنذار المبكر والتحقيق، ويؤسس لإجراءات للحد من التصعيد وتسوية أولية للنزاعات قبل أن تتفاقم إلى مواجهة أشد.

المراجع

أولا باللغة العربية:

- ميثاق الأمم المتحدة 1945
- إبراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية -العدد الأول، يناير 2025
- محمد حسن أحمد جاد حق الدفاع الشرعي في مواجية اليجمات السيبرانية في ضوء ميثاق الأمم المتحدة، مجلة الدراسات القانونية والاقتصادية – دورية علمية محكمة -المجلد العاشر العدد الرابع -ديسمبر 2024
- عمر أحمد السعدي، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب، مجلة جامعة الامارات للبحوث القانونية 2024

ثانيا: باللغة الفرنسية:

- François DELERUE, La cyberguerre et le droit international, Paris, Pedone, 2023
- Karine BANNELIER, Théodore CHRISTAKIS Cyberattaques Prévention-réactions : rôle des États et des acteurs privés2025
- Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 69,

- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. (Rule 92 regarding the definition of 'Attack').
- Molen, The Next Battlefield is in Cyberspace: Evaluating Cyberattacks under Article 51, Tyler Vander Michigan Journal of International Law, 2021.
- UN Security Council, Open Debate on Cyber Security : Maintaining international peace and security in cyberspace, 29 June 2021, VTC.
- Watts, S. (2014). Low-Intensity Cyber Operations and the Principle of Non-Intervention. In J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), Cyber War: Law and Ethics for Virtual Conflicts. Oxford University Press,
- Katharina Ziolkowski, "Confidence Building Measures for Cyberspace - Legal Implications," in Peacetime . Regime for State Activities in Cyberspace, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE Publication, 2013)

ثالثا: المو اقع الالكترونية

- https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/
- https://www.mjilonline.org/the-next-battlefield-is-in-cyberspace-evaluating-cyberattacks-under-article-51/?utm_source=openai
- https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
- https://www.icj-cij.org/fr/node/103143
- https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf?utm_source=openai
- https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/ADC0F451A9B560D8A070A753E61E874F?utm_source=openai
- https://cyberlaw.ccdcoe.org/wiki/Use_of_force#cite_note-16