ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

مدى مشروعية الرد العسكري على الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

د، ريم صالح عبيد الزبن
أستاذ القانون الدولي العام المساعد،كلية الحقوق، جامعة الاسراء
د، عبدالله ماجد العكايله
أستاذ القانون الجنائي المشارك، كلية الحقوق، جامعة الاسراء
د.مدين جمال المحاسنة
أستاذ القانون الأداري المشارك كلية الحقوق، جامعة الأسراء
د. اسماعيل محمد الحلالمة
أستاذ القانون الجنائي المساعد، كلية الحقوق، جامعة الاسراء

الملخص
أضحى الفضاء السيبراني ساحة نزاع غير تقليدية تهدد استقرار الأمن الدولي وتضعف منظومة السلم الجماعي المنصوص عليها في ميثاق الأمم المتحدة. فقد أثبتت التجارب الحديثة أن الهجمات السيبرانية قد تلحق أضراراً جسيمة بالبنية التحتية الحيوية والاقتصاد الوطني، وهو ما يضع الدول أمام تحديات قانونية غير مسبوقة تتعلق بمدى مشروعية الرد العسكري وضوابطه. كما أن غياب معايير دقيقة في القانون الدولي لتوصيف هذه الهجمات كـ"أعمال عدوانية" يفتح المجال أمام تفسيرات متباينة قد تستل بصورة تعسفية.
وانطلاقاً من ذلك، برزت الحاجة الماسة إلى تطوير قواعد قانونية واضحة تواكب طبيعة الفضاء السيبراني، وتضمن في الوقت ذاته الالتزام بمبادىء الضرورة والتناسب، وترسخ آليات فعالة للمساءلة الدولية. وفي ضوء النتائج المتوصل إليها، فإن التوصية الأهم تتمثل في تطوير إطار قانوني دولي متكامل يحدد المعايير القانونية للاعتراف بالهجمات السيبرانية كأعمال عدوانية، ويضع حدوداً واضحة للرد المشروع، بما يكفل حماية الأمن الدولي ومنع إساءة استخدام القوة.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
Volume 11 issue 2
N:63 APRIL 2026

The Legitimacy of Military Response to Cyberattacks in Light of the United Nations Charter

Dr. Reem Saleh Obaid Al-Zabe

Assistant Professor of Public International Law, Faculty of Law, Al-Isra University

Dr. Abdallah Majed ALakayleh

Associate Professor of Criminal Law, Faculty of Law, Al-Isra University

Dr.Medyen Jamal Almahasnah

Associate Professor of Administrative Law, Faculty of Law, Al-Isra University

Dr. Ismail Al-Halalmeh

Assistant Professor of Criminal Law, Al-Isra University

Public International Law

ABSTRACT

The cyber domain has become a non-traditional arena of conflict that threatens the stability of international security and undermines the collective peace system stipulated in the United Nations Charter. Recent experiences have demonstrated that cyberattacks may cause severe damage to critical infrastructure and the national economy, placing states before unprecedented legal challenges concerning the legitimacy and constraints of military response. Moreover, the absence of precise standards in international law for characterizing such attacks as "acts of aggression" opens the door to divergent interpretations that may be exploited arbitrarily.

On this basis, there has emerged an urgent need to develop clear legal rules that keep pace with the nature of the cyber domain, while at the same time ensuring adherence to the principles of necessity and proportionality, and establishing effective mechanisms for international accountability. In light of the findings reached, the most important recommendation is to develop a comprehensive international legal framework that defines the legal criteria for recognizing cyberattacks as acts of aggression and sets clear boundaries for lawful response, thereby safeguarding international security and preventing the misuse of force

المقدمة

شـهد العالم في العقود الأخيرة تطوراً هائلاً في تكنولوجيا المعلومات والاتصـالات، وهو ما أوجد واقعاً جديداً سـمح باسـتخدام الفضـاء السـيبراني كأداة فعالة في النزاعات بين الدول، ولم تعد الهجمات السـيبرانية مجرد أعمال تخريبية معزولة أو اعتداءات محدودة الأثر، بل تحولت إلى تهديدات اسـتراتيجية تطال البنى التحتية الحيوية للدول، مثل شـبكات الطاقة، والمنشـآت النووية، والأنظمة المالية، وشبكات الاتصالات. وقد برزت حوادث عملية على هذا التحول، مثل الهجوم الذي طال البرنامج النووي الإيراني عبر البرمجية الخبيثة" سـتكسـنت"، والهجوم المعروف باسـم" نوت بيتيا" الذي خلف أضـراراً اقتصـادية عالمية واسـعة النطاق، لتؤكد أن الفضاء السيبراني أصبح ساحة مواجهة حقيقية تؤثر في استقرار النظام الدولي.

أمام هذا الواقع، يثور التسـاؤل الجوهري حول مدى انطباق أحكام ميثاق الأمم المتحدة، ولا سـيما تلك المتعلقة بحظر اسـتخدام القوة الوردة في المادة الثانية من الفقرة الرابعة، والحق في الدفاع الشـرعي المنصـوص عليه في المادة الحادية والخمسـين، على الهجمات السـيبرانية. فهل يمكن اعتبار الهجوم السـيبراني، الذي قد يتسـبب في تعطيل منشـأة كربائية و شـل نظام مالي أو إحداث

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

أضرار اقتصادية جسيمة، استخداماً للقوة على نحو يستدعي رداً عسكرياً مشروعاً؟ أم أن مثل هذه الهجمات تبقى دون العتبة اللازمة لاعتبارها" هجوماً مسلحاً" وفق المفهوم التقليدي الذي استقر عليه القضاء الدولي؟

أن الجدل الفقهي يتركز على معيار" الشدة"أو "الخطورة"، الذي يجب أن يبلغه الفعل السيبراني كي يرتقي إلى مصاف الهجوم المسلح، وهو المعيار الذي أشار إليه القضاء الدولي في قضايا سابقة تتعلق باستخدام القوة التقليدية. بيد أن خصوصية الفضاء السيبراني، الذي يسمح بإحداث أضرار جسيمة من دون إطلاق رصاصة واحدة أو سقوط ضحايا مباشرين، تجعل مسألة التكييف القانوني أكثر تعقيداً.

وقد حاولت بعض المبادرات الأكاديمية والعملية، مثل" دليل تالين" الصادر عن مجموعة من الخبراء الدوليين، تقديم إرشادات لتطبيق قواعد القانون الدولي على الفضاء السيبراني. غير أن هذه الجهود، على أهميتها، تظل ذات طبيعة تفسيرية وغير ملزمة، وهو ما يبقي الحاجة ماسة إلى بلورة توافق دولي حول المعايير القانونية الضابطة لردود الأفعال على الهجمات السيبرانية، ولا سيما في مسألة مشروعية اللجوء إلى القوة العسكرية كوسيلة ردع أو انتقام.

مشكلة الدراسة:

تتمثل مشكلة هذه الدراسة في غياب التحديد الدقيق لموقع الهجمات السيبرانية ضمن إطار قواعد القانون الدولي العام، ولا سيما ما يتصل بمبدأ حظر استخدام القوة وحق الدفاع الشرعي المنصوص عليهما في ميثاق الأمم المتحدة. فالتطور التكنولوجي أفرز نمطاً جديداً من التهديدات قادراً على إحداث أضرار جسيمة بالبنى التحتية الحيوية للدول، دون أن يصاحبه بالضرورة استخدام الوسائل العسكرية التقليدية أو وقوع خسائر بشرية مباشرة. هذا الواقع أوجد حالة من الغموض القانوني حول ما إذا كانت الهجمات السيبرانية، بمختلف صورها، يمكن أن تعتبر" هجوماً مسلحاً" يبرر اللجوء إلى القوة العسكرية دفاعاً عن النفس. كما أن الطبيعة الخفية للفضاء السيبراني، وصعوبة إسناد الأفعال إلى دولة معينة على وجه اليقين، تثير إشكاليات إضافية بشأن شروط المسؤولية الدولية ومعايير التناسب والضرورة. ومن ثم، تطرح هذه الدراسة إشكالية رئيسية مفادها: إلى أي مدى يمكن اعتبار الرد العسكري على الهجمات السيبرانية مشروعاً في ضوء أحكام القانون الدولي القائم، أم أن الأمر يستدعي تطوير إطار قانوني خاص بالفضاء السيبراني؟

أهمية الدراسة:

تنبع أهمية هذه الدراسة من كونها تسعى إلى توضيح المركز القانوني للهجمات السيبرانية في ضوء ميثاق الأمم المتحدة، بما يساهم في سد الفراغ التشريعي القائم في هذا المجال. كما تكمن أهميتها في إبراز حدود مشروعية الرد العسكري على مثل هذه الهجمات، بما يضمن التوازن بين متطلبات الأمن الدولي واحترام مبادىء الشرعية الدولية. وتزداد قيمة الدراسة لارتباطها المباشر بواقع النزاعات المعاصرة، وما تفرضه من ضرورة وضع معايير دقيقة تحكم سلوك الدول في الفضاء السيبراني.

أهداف الدراسة:

1. بيان مدى انطباق أحكام ميثاق الأمم المتحدة المتعلقة بحظر استخدام القوة وحق الدفاع الشرعي على الهجمات السيبرانية.
2. تحليل الشروط الموضوعية والإجرائية لمشروعية الرد العسكري على الهجمات السيبرانية في إطار قواعد القانون الدولي.
3. تحديد أوجه القصور في القواعد القائمة واقتراح معايير قانونية تراعي خصوصية الفضاء السيبراني.
4. المساهمة في تعزيز الجهود الدولية الرامية إلى بلورة إطار قانوني أكثر وضوحاً لتنظيم سلوك الدول في المجال السيبراني.

الكلمات الافتتاحية:

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

- الهجمات السيبرانية: أفعال عدائية رقمية تستهدف أنظمة أو بنيات تحتية لدولة بهدف إحداث ضرر أو تعطيل، قد يعتبر اعتداءً دولياً.
- الرد العسكري: استخدام القوة المسلحة من قبل الدولة ضد عدوان أو هجوم سيبراني وفقاً لقواعد حق الدفاع الشرعي في القانون الدولي.
- الهجوم المسلح: أي عمل عدواني يحدث أضراراً مادية أو تعطيلات جسيمة على الدولة، ويستدعي حق الدفاع المشروع وفق ميثاق الأمم المتحدة.
- الدفاع الشرعي: حق الدولة في حماية نفسها عند تعرضها لهجوم مسلح، سواء كان تقليدياً أو سيبرانياً، بما يراعي مبدأ الضرورة والتناسب.

أسئلة الدراسة:

1. الى أي مدى يعد الرد العسكري على الهجمات السيبرانية مشروعاً وفق أحكام ميثاق الأمم المتحدة؟
2. ما المعايير القانونية التي تحدد ما إذا كانت الهجمة السيبرانية تصنف كهجوم مسلح يبرر الدفاع الشرعي للدولة؟
3. كيف يمكن إثبات مسؤولية الدولة أو تحديد الجهة المنفذة للهجمات السيبرانية وفق قواعد القانون الدولي؟
4. ما حدود مبدأ الضرورة والتناسب في تبرير الرد العسكري على الهجمات السيبرانية في ظل القانون الدولي؟

منهج الدراسة:

- **المنهج التحليلي**: تعتمد هذه الدراسة على المنهج التحليلي القانوني لدراسة قواعد القانون الدولي المتعلقة بالرد العسكري والهجمات السيبرانية، حيث يتم تحليل النصوص القانونية الدولية، خاصة أحكام ميثاق الأمم المتحدة، ودراسة السوابق القضائية لتحديد مدى مشروعية الرد العسكري على الهجمات السيبرانية وفق قواعد القانون الدولي.
- **المنهج المقارن**: تعتمد هذه الدراسة على المنهج المقارن من خلال مقارنة ممارسات الدول المختلفة وتفسيرات الفقهاء والهيئات الدولية بشأن مشروعية الرد العسكري على الهجمات السيبرانية، بهدف استخلاص المعايير القانونية الأكثر توافقاً مع القانون الدولي.

خطة الدراسة:

تقسيم هذه الدراسة ضمن مقدمة وثلاث مباحث، وهما:

المبحث الأول: الإطار القانوني للهجمات السيبرانية في ضوء ميثاق الأمم المتحدة.

المطلب الأول: مفهوم الهجمات السيبرانية وخصائصها القانونية، ومدى تأثيرها على الأمن الدولي.

المطلب الثاني: أحكام ميثاق الأمم المتحدة المتعلقة بحظر استخدام القوة وحق الدفاع الشرعي.

المبحث الثاني: مدى مشروعية الرد العسكري على الهجمات السيبرانية .

المطلب الأول: تحليل معايير اعتبار الهجمات السيبرانية كـ"هجوماً مسلحاً" يبرر الرد العسكري.

المطلب الثاني: شروط إثبات المسؤولية الدولية للدول المعتدية وسبل تحديد الجهة المنفذة.

المبحث الثالث: الضوابط والمعايير القانونية لتطبيق الرد العسكري على الهجمات السيبرانية.

المطلب الأول: مبدأ الضرورة والتناسب في الرد العسكري على الهجمات السيبرانية.

المطلب الثاني: الحاجة إلى تطوير إطار قانوني دولي يضمن تنظيم سلوك الدول في الفضاء السيبراني وفق ميثاق الأمم المتحدة

المبحث الأول :الإطار القانوني للهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

أصبح الفضاء السيبراني ساحة جديدة للتفاعلات الدولية، حيث يمكن للدول أو الجهات غير الحكومية تنفيذ عمليات عدائية تستهدف البنية التحتية الحيوية للدول الأخرى.هذه العمليات، المعروفة بالهجمات السيبرانية، تتراوح في أثره بين تعطيل الخدمات الرقمية الحيوية إلى التسبب في أضرار اقتصادية جسيمة، مما يثير تساؤلات قانونية حيوية حول مدى انطباق قواعد القانون الدولي عليها، وخصوصاً أحكام ميثاق الأمم المتحدة المتعلقة بحظر استخدام القوة وحق الدفاع الشرعي. الهجمات السيبرانية هي كل فعل عدائي ينفذ عبر شبكات المعلومات بهدف إلحاق الضرر بمصالح دولة أخرى أو تعطيل بنيتها التحتية الحيوية، ومن الناحية القانونية يثير هذا التعريف سؤال مدى إمكانية اعتبار هذه الهجمات" استخداماً للقوة" أو " هجوماً مسلحاً" وفق القانون الدولي؟

ويشير الفقه القانوني إلى أن طبيعة الفضاء السيبراني تجعل تقييم الضرر أكثر تعقيداً مقارنة بالهجمات التقليدية، إذ يمكن تنفيذ هجوم دون وقوع خسائر بشرية مباشرة، مما يضعف من إمكانية تطبيق المعايير التقليدية للقانون الدولي على هذه الحالات. ينص ميثاق الأمم المتحدة في المادة الثانية الفقرة الرابعة على حظر استخدام القوة في العلاقات الدولية، فيما تتيح المادة(51) للدول ممارسة حق الدفاع الشرعي عند تعرضها لهجوم مسلح. تطبيق هذه الأحكام على الهجمات السيبرانية يشكل تحدياً كبيراً، نظراً لصعوبة إثبات نسبة الهجوم إلى دولة معينة، وطبيعة الأضرار التي قد تكون غير مادية مباشرة، مثل تعطيل البنى التحتية الرقمية أو الاختراق الاقتصادي. لذلك يبرز النقاش القانوني حول ما إذا كان يمكن تكييف الهجمات السيبرانية على أنها" هجوم مسلح" يبرر الرد العسكري.[26]

من أبرز التحديات القانونية تحديد المسؤولية الدولية للدول أو الجهات المنفذة للهجمات السيبرانية، وتقييم مدى الضرر الناجم عن هذه الهجمات، كما يظل هناك غموض حول معايير الضرورة والتناسب في الرد العسكري، إذ يتعين على الدولة المدافعة أن توازن بين حماية أمنها وامتثالها لمبادىء القانون الدولي، وقد حاول الفقهاء وضع مبادىء تفسيرية، مثل تلك الواردة في " دليل تالين"، لتوضيح كيفية تطبيق قواعد القانون الدولي في سياق الهجمات السيبرانية، لكنها تظل غير ملزمة، مما يترك المجال واسعاً لتفسير الدول حسب مصالحها .[27]

وعلية سأقوم بتقسيم هذا المبحث إلى مطلبين وهما:

المطلب الأول: تعريف الهجمات السيبرانية وخصائصها القانونية ومدى تأثيرها على الأمن الدولي.

المطلب الثاني: أحكام ميثاق الأمم المتحدة المتعلقة بحظر استخدام القوة وحق الدفاع الشرعي في ضوء الهجمات السيبرانية.

المطلب الأول : تعريف الهجمات السيبرانية وخصائصها القانونية ومدى تأثيرها على الأمن الدولي

تعد الهجمات السيبرانية من أبرز التحديات الحديثة التي تواجه القانون الدولي، نظراً لتطور التكنولوجيا واعتماد الدول على البنية التحتية الرقمية في جميع القطاعات الحيوية، بما في ذلك الدفاع والطاقة والمواصلات والاتصالات المالية.

ووفق الفقه القانوني، يمكن تصنيف الهجمات السيبرانية التي تتسبب في تعطيل البنى التحتية الحيوية أو تسبب أضراراً جسيمة على أنها أعمال قد تندرج تحت خانة" استخدام القوة" أو " هجوم مسلح"، بينما تظل الهجمات الأقل تأثيراً في منطقة قانونية رمادية لا تحفز تلقائياً الرد العسكري، ما يثير إشكالية تطبيق القانون الدولي على هذه الظواهر الحديثة.[28]

تتميز الهجمات السيبرانية بعدة خصائص قانونية تميزها عن الجرائم الإلكترونية التقليدية للهجوم، وهي كالتالي:

أولاً- صعوبة تحديد المسؤولية: إذ غالباً ما ينفذ الهجوم من خلال شبكات متداخلة أو من خلال أطراف غير حكومية، مما يزيد صعوبة إثبات ارتباط الهجوم بدولة بعينها.

---

[26] محمد، عبد الله فوزي، القانون الدولي وحق الدفاع الشرعي في ظل التهديدات السيبرانية، دار النهضة العربية،2020،ص 34-56.

[27] الخطاب، سامي، الهجمات السيبرانية ومسؤولية الدول في القانون الدولي، مركز دراسات الأمن الدولي، 2019، ص 77-110.

[28] رمضان، السيد أحمد، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية، 2025،ص1750-1753.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

ثانياً- القدرة على التسبب بأضرار غير مباشرة للمدنيين: حيث يمكن أن تؤدي الهجمات إلى تعطيل خدمات حيوية مثل الكهرباء والمياه والنقل، دون أن يكون هناك استهداف مباشر للأفراد، ما يثير تساؤلات حول تطبيق قواعد القانون الدولي الإنساني التي تلزم بالتمييز بين الأهداف العسكرية والأهداف المدنية.

ثالثاً- التأثير العابر للحدود: إذ يمكن للهجوم الرقمي أن ينتشر بسرعة عبر الحدود الدولية، مما يعقد من مسؤولية الدولة المعتدية ويثير الحاجة لتنسيق دولي لتحديد المسؤولية ومكافحة الهجمات العابرة للحدود.

رابعاً- السرعة العالية والقدرة على التكرار: ما يجعل من الصعب التصدي لها باستخدام الوسائل التقليدية للرد العسكري أو القانوني.

يشكل تأثير الهجمات السيبرانية على الأمن الدولي أحد أهم الدوافع القانونية لدراسة هذا الموضوع، فقد أظهرت أحداث عالمية عديدة، مثل هجوم البرمجية الخبيثة" ستكسنت" على المنشآت النووية الإيرانية، وأزمة" نوت بيتيا" التي سببت أضراراً مالية جسيمة عالمياً، أن الهجمات السيبرانية قد تتسبب في تعطيل الأنشطة الاقتصادية الحيوية للدول، وتعرض استقرارها السياسي والاقتصادي للخطر، وهو ما يضع القانون الدولي أمام تحد كبير لتحديد نطاق مشروعية الرد العسكري وحقوق الدفاع الشرعي للدول المتضررة.

في ضوء ذلك، يحاول القانون الدولي خاصة أحكام ميثاق الأمم المتحدة، وضع إطار يوازن بين حماية الأمن الدولي وحق الدولة في الدفاع عن نفسها، وبين الالتزام بمبادىء القانون الدولي الإنساني، ومع ذلك تبقى الحاجة ماسة لتطوير قواعد قانونية أكثر تحديداً لتغطية الفضاء السيبراني.[29]

أرى أن الهجمات السيبرانية تمثل تهديداً حقيقياً للأمن الدولي، ويجب التعامل معها ضمن الإطار القانوني الواضح لميثاق الأمم المتحدة، مع مراعاة طبيعتها الخاصة وخصائصها غير المادية، ومن الضروري تطوير معايير دقيقة لتحديد متى يرقى الفعل السيبراني إلى مستوى العدوان الذي يبرر الرد.

المطلب الثاني : أحكام ميثاق الأمم المتحدة المتعلقة بحظر استخدام القوة وحق الدفاع الشرعي في ضوء الهجمات السيبرانية

يكرس ميثاق الأمم المتحدة مبدأ حظر استخدام القوة كأحد أهم القواعد الآمرة في القانون الدولي، حيث نصت المادة (2/4) على التزام جميع الأعضاء بالامتناع عن التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة. ويعد هذا النص حجر الأساس في النظام القانوني الدولي الهادف إلى الحفاظ على السلم والأمن الدوليين ومنع الانزلاق نحو النزعات المسلحة.[30]

ورغم هذا الحظر الصارم، فقد أتاح الميثاق استثناءً وحيداً في المادة(51)، التي أقرت بحق الدول في الدفاع الشرعي الفردي أو الجماعي عند وقوع **" هجوم مسلح"**، شريطة أن يكون الرد ضرورياً ومتناسباً مع حجم العدوان، وألا يستخدم هذا الحق لتجاوز صلاحيات مجلس الأمن في حفظ السلم والأمن الدوليين.[31]

وقد أكدت محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة أن هذا الحق لا يمارس إلا في مواجهة أفعال تبلغ درجة " الهجوم المسلح"، وهو ما يستلزم معياراً موضوعياً لتحديد متى يتحقق هذا الوصف.[32]

وعند إسقاط هذه القواعد على التهديدات الحديثة، تبرز إشكالية الهجمات السيبرانية التي قد تؤدي إلى نتائج كارثية من حيث تعطيل البنية التحتية الحيوية أو الإضرار بالأمن القومي، حيث يرى دليل تالين 2.0 أن معيار التكييف لا يرتبط بوسيلة العدوان،

---

[29] الخطاب، سامي، الهجمات السيبرانية ومسؤولية الدول في القانون الدولي، مرجع سابق، ص 111-113 .

[30] راجع ميثاق الأمم المتحدة، 1945، المادة(2/4).

[31] عبدالله، حسام، الرد العسكري والهجمات السيبرانية في القانون الدولي، دار النهضة العربية، القاهرة، 2020، ص 103-114.

[32] راجع احكام محكمة العدل الولية.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

وإنما بالآثار المترتبة عليه. فإذا بلغت هذه الآثار مستوى الخسائر المادية أو البشرية المماثلة للهجمات المسلحة التقليدية، جاز تفعيل حق الدفاع الشرعي وفقاً للمادة(51).[33]

وبذلك، يظل ميثاق الأمم المتحدة المرجعية الأساسية لتحديد مشروعية الرد على الهجمات السيبرانية. فالقاعدة العامة تقتضي حظر استخدام القوة، بينما يسمح الاستثناء الوحيد- أي الدفاع الشرعي- بالرد العسكري، على أن يكون مقيداً بمبادىء الضرورة، التناسب، والإسناد القانوني الصحيح، بما يمنع التذرع بالهجمات السيبرانية كذريعة لاستخدام غير مشروع للقوة.[34]

يتضح من دراسة الإطار القانوني للهجمات السيبرانية أن هذه الأفعال تمثل تهديداً مستحدثاً يختلف عن العدوان التقليدي في طبيعة الوسائل وطريقة التنفيذ، لكنه قد يحقق آثاراً مادية ومعنوية شديدة على الأمن الدولي، وقد أظهر الفقه أن التعامل مع الهجمات السيبرانية يتطلب فهم خصائصها القانونية الدقيقة، بما في ذلك صعوبة الإسناد، والعبور عبر الحدود، وتأثيرها الاستراتيجي، كما أكدت دراسة أحكام ميثاق الأمم المتحدة، خاصة المادة(2/4) المتعلقة بحظر استخدام القوة والمادة(51) الخاصة بحق الدفاع الشرعي، أن القانون الدولي يوفر إطاراً عاماً للتعامل مع هذه الهجمات، شريطة مراعاة مبادىء الضرورة والتناسب وتحديد حجم الأضرار وتقييم القصد، ويعكس هذا الإطار ضرورة الجمع بين حماية سيادة الدولة ومنع التصعيد العسكري غير المبرر، بما يضمن استقرار السلم والأمن الدوليين في ظل التحديات السيبرانية الحديثة.[35]

أرى أن الهجمات السيبرانية تمثل تهديداً حقيقياً للأمن الدولي، وتتطلب إطاراً قانونياً واضحاً ضمن ميثاق الأمم المتحدة يحدد شروط الرد ومبادىء الدفاع الشرعي. التحدي الأكبر يكمن في إثبات الإسناد وقياس جسامة الضرر، ما يستلزم تطوير معايير دقيقة لتطبيق حق الدفاع الشرعي دون الإخلال بالسلم والأمن الدوليين.

المبحث الثاني : مدى مشروعية الرد العسكري على الهجمات السيبرانية

يثير موضوع مشروعية الرد العسكري على الهجمات السيبرانية جدلاً واسعاً في الفقه والقضاء الدوليين، وذلك لحداثة هذه الظاهرة وتداخلها مع المبادىء التقليدية للقانون الدولي، فالميثاق الأممي أرسى قاعدة عامة تتمثل في حظر استخدام القوة وفق المادة(2/4)، واستثنى من ذلك فقط حالة الدفاع الشرعي المنصوص عليها في المادة(51)[36]، ومن ثم فإن أي رد عسكري على هجوم سيبراني يجب أن يقيم في ضوء هذين النصين، بحيث يتحدد ما إذا كان الهجوم السيبراني يرقى إلى مستوى " الهجوم المسلح" الذي يبرر اللجوء إلى القوة.

يرى الفقه الدولي أن مجرد الهجمات الإلكترونية التي تسبب تعطيلاً محدوداً للأنظمة أو سرقة بيانات لا تكفي لتفعيل المادة(51)، بل لا بد أن تكون آثارها جسيمة تعادل في خطورتها النتائج المترتبة على الهجمات العسكرية التقليدية، مثل تدمير منشآت حيوية أو الإضرار بالبنية التحتية أو التسبب بخسائر بشرية.[37]

ويؤكد هذا الاتجاه دليل تالين2.0 الذي نص على أن معيار" شدة الضرر" هو الأساس في التكييف القانوني للهجوم السيبراني كعدوان مسلح، بصرف النظر عن الوسيلة المستخدمة.

أما من الناحية العملية، فإن مشروعية الرد العسكري على الهجوم السيبراني ترتبط بعدة ضوابط، أهمها الضرورة والتناسب. فالرد يجب أن يكون السبيل الوحيد لدرء الخطر، وألا يتجاوز القدر اللازم لصد العدوان، كما يتعين أن يكون الإسناد القانوني

---

[33] Schmitt, Michael N. (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,Cambridge University Press,2017,pp.65-70 .

[34] سالم، محمد، الالتزامات الدولية للدول في مواجهة الهجمات السيبرانية، دار الإبداع للنشر، القاهرة، مصر، 2021،ص 140-148.

[35] اللجنة الدولية للصيب الأحمر" الهجمات السيبرانية في ضوء القانون الدولي الإنساني .

[36] راجع ميثاق الأمم المتحدة، المادة(51) والمادة(2/4).

[37] محمد، عبد الله فوزي، القانون الدولي وحق الدفاع الشرعي في ظل التهديدات السيبرانية، مرجع سابق، ص 72-74.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

للهجوم واضحاً، بحيث تثبت مسؤولية الدولة المعتدية بشكل لا لبس فيه، إذ إن الغموض في مسألة الإسناد قد يؤدي إلى تصعيد غير مشروع أو إلى تحميل دولة غير مسؤولة نتائج عدوان لم ترتكبه.[38]

وتأسيساً على ما سبق، فإن مشروعية الرد العسكري على الهجمات السيبرانية ليست مطلقة، وإنما مشروطة بمدى تحقق عناصر" الهجوم المسلح" وفقاً للمادة (51) من الميثاق، مع مراعاة القواعد العامة للقانون الدولي، وهذا يفرض على المجتمع الدولي تطوير معايير أكثر وضوحاً لتحديد متى يكون الرد العسكري مشروعاً، بما يمنع إساءة استخدام القوة تحت ذريعة مواجهة الهجمات السيبرانية.[39]

وعليه سأقوم بتقسيم هذا المبحث إلى مطلبين كالتالي:

المطلب الأول: تحليل معايير اعتبار الهجمات السيبرانية كـ"هجوماً مسلحاً" يبرر الرد العسكري.

المطلب الثاني: شروط إثبات المسؤولية الدولية للدول المعتدية وسبل تحديد الجهة المنفذة.

المطلب الأول : تحليل معايير اعتبار الهجمات السيبرانية كـ"هجوماً مسلحاً" يبرر الرد العسكري

يمثل التساؤل حول مدى إمكانية اعتبار الهجمات السيبرانية" هجوماً مسلحاً" بالمعنى المقصود في المادة (51) من الميثاق إحدى أبرز الإشكاليات القانونية المعاصرة. فالميثاق، وإن كان قد حظر استخدام القوة في المادة(2/4)، إلا أنه لم يضع تعريفاً محدداً للهجوم المسلح، تاركاً هذا المفهوم للتفسير الفقهي والقضائي. وقد أسهمت محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة في صياغة هذا المفهوم، مؤكدة أن الهجوم المسلح يتطلب أفعالاً تبلغ درجة من الجسامة تميزها عن صور الاستخدام غير الجسيم للقوة.

وعند محاولة تكييف الهجمات السيبرانية ضمن هذا الإطار، برزت الحاجة إلى تحديد معايير دقيقة يمكن الاستناد إليها. فقد ذهب جانب من الفقه إلى أن معيار شدة الضرر هو الأساس، بحيث لا يعتد بأي هجوم سيبراني إلا إذا خلف آثاراً تماثل نتائج استخدام الأسلحة التقليدية، على سبيل المثال فإن اختراق شبكة الكهرباء الوطنية لدولة ما وتسببه في شلل كامل للبنية التحتية الحيوية أو سقوط ضحايا يمكن أن يعتبر" هجوماً مسلحاً" بالمعنى القانوني.[40]

كما يضاف إلى ذلك معيار القصد والغرض، حيث لا يكفي وقوع الهجوم، بل يجب أن يكون مدفوعاً بنية عدائية تستهدف تقويض سيادة الدولة أو تهديد أمنها القومي، إذ إن العديد من الهجمات الإلكترونية قد تقع بدافع التجسس أو سرقة المعلومات دون أن ترقى إلى مستوى العدوان المسلح.

ويبرز أيضاً معيار الإسناد إلى دولة، وهو من أعقد المعايير في البيئة السيبرانية. فإثبات أن الهجوم تم بواسطة دولة أو بمساندتها المباشرة، يعد شرطاً جوهرياً لاعتباره هجوماً مسلحاً يبرر الرد العسكري، ذلك أن الطابع المجهول للفضاء السيبراني يتيح لجماعات أو أفراد تنفيذ عمليات معقدة قد تنسب خطأ إلى دول، مما يجعل مسألة الإسناد عرضة للتسييس، وقد أوضحت محكمة العدل الدولية في قضية البوسنة ضد صربيا أن مجرد الدعم غير الكافي لا يرتقي لاعتبار الدولة مسؤولة عن هجوم مسلح، بل يجب يثبت وجود سيطرة فعلية.[41]

كما يؤكد دليل تالين 2.0 على معيار النتائج المماثلة، أي أن الحكم على الهجوم لا يتوقف على الوسيلة بل على الأثر. فإذا أحدث الهجوم السيبراني نتائج مدمرة تقارن بالقصف أو التدمير العسكري التقليدي، فإن القانون الدولي يعامله كهجوم مسلح.[42]

---

[38] Hill ,Jonathan E. Cyber Operations and the Use of Force under the UN Charter, Oxford University Press, 2018, PP.110-145

[39] يوسف، نوال، السيطرة على الفضاء السيبراني بين القانون الدولي والأمن الدولي، مكتبة الجامعة الحديثة، الرياض، 2022، ص65.

[40] عبد الكريم، أمل، الهجمات السيبرانية في القانون الدولي، رسالة ماجستير، كلية القانون، جامعة بغداد، 2021، ص 66-67.

[41] أحمد، هبة، المسؤولية الدولية عن الهجمات السيبرانية، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2020، ص 142.

[42] Michael N. Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

وبالنظر إلى هذه المعايير مجتمعة، يتضح أن التوسع في وصف أي هجوم سيبراني بأنه " هجوم مسلح" قد يؤدي إلى تقويض مبدأ حظر استخدام القوة المنصوص عليه في ميثاق الأمم المتحدة. لذا ينبغي أن يظل هذا الوصف محصوراً في الحالات التي تحقق ضرراً جسيماً، يهدد الأمن والسلم الدوليين بصورة ملموسة، مع ضرورة إثبات القصد العدائي والإسناد القانوني بشكل لا يقبل الشك، وهو ما يستدعي تطوير معايير أكثر تفصيلاً، سواء عبر الاجتهاد القضائي أو من خلال اتفاقيات دولية جديدة، لضمان التوازن بين حق الدول في الدفاع الشرعي وضرورة منع إساءة استخدام القوة في العلاقات الدولية.[43]

وترى الباحثة أن تكييف الهجمات السيبرانية كهجوم مسلح لا يجوز أن يبنى على الوسيلة المستخدمة، وإنما على جسامة النتائج المحققة، مع ضرورة توافر القصد العدائي والإسناد الواضح إلى دولة، حتى لا يستغل هذا المفهوم لتبرير استخدام غير مشروع للقوة.

المطلب الثاني : شروط إثبات المسؤولية الدولية للدول المعتدية وسبل تحديد الجهة المنفذة

تعد مسألة إثبات المسؤولية الدولية في مجال الهجمات السيبرانية من أعقد القضايا في القانون الدولي المعاصر، نظراً للطبيعة التقنية المعقدة لهذه العمليات، وما يكتنفها من صعوبة في تحديد الفاعل الحقيقي. فالمسؤولية الدولية للدولة لا تنشأ إلا بتوافر شرطين أساسيين نصت عليهما لجنة القانون الدولي في مشروع المواد الخاصة بالمسؤولية الدولية عن الأفعال غير المشروعة دولياً، وهما: إسناد الفعل إلى الدولة. ومخالفة التزام دولي قائم.

أولاً- شرط الإسناد إلى الدولة: لا يكفي لقيام المسؤولية الدولية مجرد وقوع هجوم سيبراني، بل يجب أن يثبت أن هذا الفعل ارتكب بواسطة أجهزة الدولة أو تحت سيطرتها الفعلية، وقد قضت محكمة العدل الدولية في قضية البوسنة ضد صربيا عام 2007 بأن مجرد تقديم الدعم أو المساندة غير كافٍ لتحميل الدولة المسؤولية، بل يشترط إثبات السيطرة الفعلية أو التوجيه المباشر.

وفي البيئة السيبرانية يزداد الأمر تعقيداً، إذ غالباً ما تستخدم شبكات متعددة الجنسيات أو برمجيات انتحال الهوية، مما يجعل عملية التتبع الرقمي صعبة.[44]

ثانياً- شرط مخالفة الالتزام الدولي: أن الهجمات السيبرانية قد تشكل خرقاً لعدة التزامات دولية، مثل الالتزام باحترام سيادة الدول وعدم التدخل في شؤونها الداخلية، فضلاً عن الالتزام بحظر استخدام القوة. فإذا ثبت أن الهجوم أدى إلى تعطيل المرافق الحيوية أو تهديد السلم والأمن الدوليين، فإنه يعد انتهاكاً واضحاً لالتزامات الدولة بموجب المادة(2/4) من ميثاق الأمم المتحدة.[45]

ثالثاً- سبل تحديد الجهة المنفذة: إحدى أهم التحديات هي التعرف على الجهة المسؤولة عن الهجوم، وقد طرحت عدة آليات لذلك:

1-الأدلة التقنية الرقمية: وهي الوسائل العلمية القائمة على تتبع مصدر البيانات وتحليل الشفرات الإلكترونية، إلا أن هذه الأدلة وحدها لا تكفي لإثبات المسؤولية، نظراً لإمكانية التلاعب بها.

2-الأدلة الاستخبارية والسياسية: حيث تلجأ الدول إلى جمع المعلومات عبر أجهزة الاستخبارات أو التعاون مع أطراف ثالثة، غير أن هذه الأدلة غالباً ما تكون سرية، مما يعيق إمكانية عرضها أمام المحاكم الدولية.

3-الآليات الدولية الجماعية: مثل تفعيل دور مجلس الأمن أو إنشاء لجان تحقيق دولية، وهو ما دعا إليه عدد من الباحثين كوسيلة لتعزيز المصداقية والشفافية.

---

[43] International Court of Justice, Nicaragua v. United States of America (Merits) , ICJ Reports, 1986,pp. 103.

[44] خليل، ندى، المسؤولية الدولية عن الهجمات السيبرانية، رسالة ماجستير، كلية الحقوق، جامعة بيروت العربية، 2021، ص 95-98.

[45] أحمد، هبة، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق،ص 143-145.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

وعليه، فإن إثبات المسؤولية الدولية في المجال السيبراني يتطلب توافر مجموعة من الشروط الصارمة، أبرزها الإسناد المباشر إلى الدولة وتحقق الضرر المخالف للقانون الدولي، إلى جانب اعتماد آليات دقيقة لتحقق من هوية الجهة المنفذة. فغياب هذه المعايير الواضحة يفتح الباب أمام مخاطر التسييس واستخدام الادعاءات السيبرانية كذريعة للعدوان، وهو ما يتعارض مع مقاصد ميثاق الأمم المتحدة في حفظ السلم والأمن الدوليين.[46]

يتضح أن مشروعية الرد العسكري على الهجمات السيبرانية تتوقف على مدى تحقق عناصر الهجوم المسلح وفق المعايير القانونية المعتمدة، بما في ذلك جسامة الضرر، القصد العدائي، والإسناد الواضح إلى الدولة المعتدية، ويظل الالتزام بمبادىء الضرورة والتناسب أساسياً لضمان مشروعية الرد ومنع الانزلاق إلى استخدام القوة غير المشروعة، كما يبرز الحاجة إلى تطوير آليات قانونية وتقنية دقيقة لتحديد المسؤولية الدولية بدقة.[47]

ترى الباحثة أن مشروعية الرد العسكري على الهجمات السيبرانية تظل مقيدة بمجموعة صارمة من المعايير القانونية، أهمها جسامة الضرر، القصد العدائي، والإسناد الواضح، مع الالتزام بمبادىء الضرورة والتناسب لضمان عدم إساءة استخدام القوة.

المبحث الثالث : الضوابط والمعايير القانونية لتطبيق الرد العسكري على الهجمات السيبراني

مع تزايد الهجمات السيبرانية واستهداف البنية التحتية الحيوية للدول، برزت الحاجة إلى تطوير إطار قانوني دولي واضح لتنظيم الرد العسكري على هذه الهجمات، يعتمد هذا الإطار على مبدأين أساسيين: حماية الأمن الدولي ومنع التصعيد غير المشروع، مع ضمان قدرة الدولة على الدفاع عن نفسها وفق القانون الدولي.

أولاً- تطوير إطار قانوني دولي موحد: تشدد الدراسات الحديثة على ضرورة وجود قواعد دولية موحدة لتحديد متى يمكن للدولة الرد العسكري على الهجمات السيبرانية وما هي حدود هذا الرد، بما يضمن الحد من التفسيرات الأحادية للقانون الدولي.

ثانياً- آليات الرقابة والمساءلة الدولية: يشير الفقه الحديث إلى أهمية تفعيل دور المنظمات الدولية مثل الأمم المتحدة، لجان التحقيق المستقلة، والوكالات المتخصصة في الفضاء السيبراني، لتقديم تقييم محايد للهجمات وتحديد المسؤولية. وهذا يعزز من مصداقية الرد العسكري ويحد من استغلال الهجمات السيبرانية كذريعة للعدوان.[48]

ثالثاً- معايير تشغيلية لتقييم المخاطر: ينبغي أن يتضمن الرد العسكري على الهجمات السيبرانية تقييماً مسبقاً للمخاطر، بما في ذلك تقدير حجم الأضرار المحتملة على المدنيين، البنية التحتية الحيوية، والنظام الدولي ككل. كما يجب تحليل الأثر السياسي والدبلوماسي المحتمل قبل تنفيذ أي رد، لضمان توافق مع القانون الدولي والأمن الجماعي.

رابعاً- تعزيز التعاون الدولي وتبادل المعلومات: يشمل الإطار القانوني الفعال أيضاً التعاون بين الدول في تبادل المعلومات عن التهديدات السيبرانية، تنسيق الردود، ومراقبة تطبيق القانون الدولي في الفضاء السيبراني، وبهذه الطريقة يمكن الحد من الاستغلال الفردي للهجمات السيبرانية، وتقليل فرص التصعيد، وضمان استقرار الأمن الدولي.[49]

وعليه سأقوم بتقسيم هذا المبحث إلى المطالب التالية:

المطلب الأول: مبدأ الضرورة والتناسب في الرد العسكري على الهجمات السيبرانية.

المطلب الثاني: الحاجة إلى تطوير إطار قانوني دولي يضمن تنظيم سلوك الدول في الفضاء السيبراني وفق ميثاق الأمم المتحدة.

المطلب الأول : مبدأ الضرورة والتناسب في الرد العسكري على الهجمات السيبرانية

يشكل مبدأ الضرورة والتناسب الركيزة الأساسية في القانون الدولي لتقييم مشروعية الرد العسكري على الهجمات السيبرانية، إذ يحدد إطاراً قانونياً يضمن قدرة الدولة على الدفاع عن نفسها ضمن حدود القانون الدولي، مع منع الانزلاق إلى استخدام القوة

---

[46] يونس، إسراء، الهجمات السيبرانية والمسؤولية الجنائية الدولية، رسالة ماجستير، كلية الحقوق، جامعة الزقازيق، 2021، ص 155-158.

[47] Daniel P.V. O'Connell,The Law of Cyber Operations in International Law, Oxford University Press, 2021, pp.102 , 108 .

[48] عبد الحميد، ريم، القانون الدولي للعمليات السيبرانية، دار المعرفة الجامعية، القاهرة، مصر، 2021، ص 55-70.

[49] عبد الرحمن، عادل، القانون الدولي للفضاء السيبراني: المبادىء والضوابط، دار الفكر العربي، القاهرة، 2021، ص 78-84.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
Volume 11 issue 2
N:63 APRIL 2026

المفرطة أو غير المشروعة، ويستمد هذا المبدأ قوته من ميثاق الأمم المتحدة وخصوصاً المادة(51)، التي تكفل للدول حق الدفاع المشروع عند التعرض لهجوم مسلح، مع الالتزام بالالتزامات الدولية الأخرى.[50]

أولاً- مبدأ الضرورة: يشترط مبدأ الضرورة أن يكون الرد العسكري الخيار الأخير بعد استنفاد جميع الوسائل السلمية والوقائية الممكنة، بما في ذلك الإجراءات الدبلوماسية، التعاون الأمني الدولي، أو استخدام الوسائل التقنية للكشف عن مصدر الهجوم. في السياق السيبراني، تتسم الهجمات بسرعة الانتشار وصعوبة تحديد مصدرها مما يزيد من أهمية تقييم الضرورة بدقة، ويجب مراعاة خطورة الهجوم، طبيعة الأهداف المستهدفة، ومدى الأضرار المحتملة على البنية التحتية الحيوية والأمن القومي والدولي قبل أي رد عسكري. كما يجب التأكد من أن الرد العسكري المقترح هو الوسيلة الوحيدة لتحقيق الهدف المشروع، وأن يكون محدوداً بالقدر اللازم لمنع استمرار الهجوم دون تجاوز الحدود القانونية.[51]

ثانياً- مبدأ التناسب: ينص مبدأ التناسب على أن يكون الرد العسكري متناسباً مع حجم الهجوم وآثاره، بحيث لا تتجاوز التدابير المتخذة حجم الضرر الناتج عن الهجوم الأصلي، ويشمل ذلك تقييم التأثير على المدنيين، البنية التحتية الحيوية، الاقتصاد، والمجتمع، مع مراعاة الأبعاد السياسية والدولية. ويهدف هذا المبدأ إلى منع استخدام القوة المفرطة أو التوسعية، وضمان أن يكون الرد قانونياً، محدوداً، ومتوازناً، بما يحمي حقوق الإنسان ويضمن الالتزام بالقانون الدولي.[52]

ثالثاً- التطبيق العملي لمبادىء الضرورة والتناسب: يتطلب تطبيق هذين المبدأين في الهجمات السيبرانية استخدام أدوات التحليل القانونية والتقنية المتقدمة، ويشمل ذلك إنشاء فرق متخصصة لتقييم طبيعة الهجوم وأثره المحتمل، استخدام الأدلة الرقمية لتحديد مصدر الهجوم بدقة، ودراسة التداعيات السياسية والدولية لأي رد عسكري قبل تنفيذه، تساهم هذه الإجراءات في ضمان أن يكون الرد محدوداً، متوازناً، قانونياً، ويحمي المدنيين والبنية التحتية الحيوية، مع الحفاظ على الأمن الجماعي والنظام الدولي.[53]

رابعاً- المسؤولية القانونية للرد العسكري: الالتزام بالضرورة والتناسب يضمن مشروعية الرد العسكري أمام المجتمع الدولي ويحد من احتمال تحميل الدولة مسؤولية انتهاك القانون الدولي، كما يشجع على وضع سياسات واضحة على المستويين الداخلي والدولي لتنظيم الرد العسكري في الفضاء السيبراني، بما يحمي المدنيين والبنية التحتية الحيوية ويقلل من مخاطر التصعيد الدولي.

أن مبدأ الضرورة والتناسب يشكل الإطار القانوني الرئيسي لتقييم مشروعية الرد العسكري على الهجمات السيبرانية، ويضمن أن يكون الرد محدوداً، متوازناً، قانونياً، ويحقق حماية المدنيين والبنية التحتية الحيوية مع الحفاظ على الأمن الدولي ومنع أي تصعيد غير قانوني.[54]

ترى الباحثة أن الالتزام بمبادىء الضرورة والتناسب يشكل شرطاً قانونياً أساسياً لمشروعية الرد العسكري على الهجمات السيبرانية وفق القانون الدولي، ويضمن تقييد استخدام القوة ضمن الحدود المسموح بها. كما يساهم هذا الالتزام في حماية المدنيين والبنية التحتية ويعزز حفظ النظام الدولي ومنع التصعيد غير القانوني.

---

[50] راجع ميثاق الأمم المتحدة، 1945، المادة(51).

[51] عبد الحميد، ريم، القانون الدولي للعمليات السيبرانية، مرجع سابق، ص 60-65.

[52] محمد، ليلى، التنظيم القانوني للهجمات السيبرانية في القانون الدولي، رسالة دكتوراة، جامعة الإمارات، 2021،ص120-125.

[53] Wolfgang Kerber, Cyber, Security and International Law, Springer, 2020 pp.45-60.,

[54] يونس، إسراء، الهجمات السيبرانية والمسؤولية الجنائية الدولية، مرجع سابق، ص158-159.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

المطلب الثاني : الحاجة إلى تطوير إطار قانوني دولي يضمن تنظيم سلوك الدول في الفضاء السيبراني وفق ميثاق الأمم المتحدة

يمثل الفضاء السيبراني مجالاً جديداً من مجالات التفاعل الدولي لم يضعه المشرع الدولي في الحسبان عند صياغة ميثاق الأمم المتحدة سنة1945. ومع تطور القدرات التقنية واتساع نطاق الاعتماد على البنية التحتية الرقمية، برزت تحديات قانونية معقدة تتعلق بكيفية تنظيم سلوك الدول في هذا المجال، ولا سيما فيما يخص مسألة استخدام القوة، الدفاع الشرعي، والمسؤولية الدولية. ولعل أبرز ما يواجه المجتمع الدولي هو الفراغ التشريعي وعدم وجود قواعد دولية خاصة وملزمة تنظم بشكل مباشر الهجمات السيبرانية، وهو ما يجعل تطبيق قواعد القانون الدولي التقليدي في هذا المجال مسألة مثيرة للجدل وتفتح الباب أمام تفسيرات متباينة.[55]

لقد أظهرت التجارب العملية، مثل الهجمات التي استهدفت بنى تحتية حيوية في دول مختلفة، أن النصوص الحالية في ميثاق الأمم المتحدة، وخاصة المادتين(2/4)و(51)، غير كافية لمعالجة خصوصية الهجمات السيبرانية. فالفضاء السيبراني يتميز بخصائص فريدة كصعوبة إسناد الهجوم لجهة معينة، والقدرة على إحداث آثار واسعة من دون استخدام الأسلحة التقليدية. ولهذا، فإن الحاجة تبدو ملحة إلى تطوير إطار قانوني دولي ينسجم مع مبادىء الميثاق ويعالج هذه الثغرات.[56]

وفي هذا السياق، اتخذت الأمم المتحدة خطوات مهمة من خلال إنشاء مجموعة الخبراء الحكوميين(GGE) وكذلك الفريق العامل مفتوح العضوية(OEWG)، حيث عملت هذه الأطر على دراسة كيفية تطبيق القانون الدولي على الفضاء السيبراني، وقد أكدت تقاريرها أن ميثاق الأمم المتحدة يظل الإطار المرجعي الأساسي، لكنه يحتاج إلى تفسير موسع أو بروتوكولات مكملة لضمان التطبيق الفعال، إلا أن هذه المبادرات لا تزال تفتقر إلى الطابع الإلزامي، مما يضعف فعاليتها أمام التحديات العملية.[57]

كما أن بعض الفقه يرى أن الحاجة باتت ماسة إلى إبرام معاهدات دولية خاصة بالفضاء السيبراني، تنظم سلوك الدول وتضع معايير واضحة للرد على الهجمات، مع مراعاة مبادىء الضرورة والتناسب وحماية المدنيين. ومن شأن مثل هذه المعاهدة أن تضع قواعد أكثر تحديداً فيما يتعلق بالمسؤولية الدولية، وطرق إثباتها، وآليات التعاون الدولي، مما يسد الفراغ التشريعي الحالي ويعزز الاستقرار الدولي.[58]

إلى جانب ذلك، فإن تطوير إطار قانوني دولي جديد يجب أن يأخذ بعين الاعتبار مبدأ الأمن الجماعي، بحيث لا يقتصر الأمر على ردود فعل فردية من الدول، بل يتطلب تعاوناً دولياً تحت مظلة الأمم المتحدة لضمان أن الردود العسكرية أو غير العسكرية على الهجمات السيبرانية لا تؤدي إلى تصعيد غير مشروع للنزاعات الدولية. وهذا يتطلب كذلك تعزيز آليات تبادل المعلومات، وتطوير قدرات التحقيق المشترك، وإيجاد هيئات دولية متخصصة لرصد الهجمات السيبرانية وتقييم مشروعيتها.

إن تطوير إطار قانوني دولي ملزم يضمن سلوك الدول في الفضاء السيبراني يمثل خطوة حتمية لحماية السلم والأمن الدوليين، وتحقيق التوازن بين حق الدول في الدفاع المشروع والالتزام بمبادىء ميثاق الأمم المتحدة. ومن دون هذا التطوير، سيبقى التعامل مع الهجمات السيبرانية رهين التقديرات السياسية للدول الكبرى، بما يهدد بخلق نظام دولي مزدوج المعايير لا ينسجم مع روح العدالة الدولية.[59]

يتضح من خلال هذا المبحث أن تطبيق الرد العسكري على الهجمات السيبرانية يتطلب التزاماً صارماً بمبادىء الضرورة والتناسب، مع وجود إطار قانوني دولي واضح يحكم سلوك الدول في الفضاء السيبراني، كما أن تعزيز التعاون الدولي ووضع

---

[55] الزيد، محمد، القانون الدولي والسيادة الرقمية: قراءة في التحديات المعاصرة، المجلة العربية للدراسات القانونية، العدد2020،12،ص110-122.

[56] علي،محمود، القانون الدولي والحروب الحديثة: التحديات السيبرانية، دار النهضة العربية، القاهرة،2021، 120-130.

[57] يوسف، نوال، الهجمات السيبرانية ومبادىء القانون الدولي، دار الفكر العربي، عمان، 2022، ص 82-88.

[58] رمضان، السيد أحمد، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مرجع سابق ، ص176-178.

[59] الخطيب، لينا، الأمن السيبراني والقانون الدولي العام، المجلة الأردنية للقانون والعلوم السياسية، العدد6، 2020،ص 60-73.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

معايير دقيقة للمسؤولية والرد يضمن حماية المدنيين والبنية التحتية الحيوية، لذلك يشكل تطوير إطار قانوني دولي فعال ركيزة أساسية للحفاظ على الأمن والسلم الدوليين في العصر الرقمي.[60]

ترى الباحثة إن وجود إطار قانوني دولي واضح للفضاء السيبراني يمثل شرطاً أساسياً لممارسة حق الدفاع المشروع، ويحد من الفوضى القانونية ويضمن حماية الأمن الدولي من إساءة استخدام الرد العسكري.

الخاتمة

تشير الدراسة إلى أن الهجمات السيبرانية تمثل تهديداً حقيقياً للأمن القومي والبنية التحتية الحيوية للدول، وقد تصل أحياناً إلى مستوى يبرر الرد العسكري وفق أحكام ميثاق الأمم المتحدة، ويشكل الالتزام بمبادىء الضرورة والتناسب الأساس القانوني لتحديد مشروعية أي رد عسكري، مع حماية المدنيين والنية التحتية ومنع الانتهاكات الدولية.

كما تبين أن الإطار القانوني الدولي الحالي يحتاج إلى تطوير شامل ليواكب التحديات السيبرانية الحديثة، بما يشمل وضع معايير واضحة لتحديد مسؤولية الدول، وتنظيم استخدام القوة، وتعزيز التعاون الدولي في التحقيقات ومساءلة المعتدين. ويهدف هذا الإطار إلى الحد من النزاعات، وضمان التوازن بين حق الدولة في الدفاع المشروع وحماية الأمن الدولي والنظام العالمي.

وباختصار, يمثل الالتزام بالقانون الدولي وميثاق الأمم المتحدة، مع تطوير إطار قانوني دولي متكامل ضرورة أساسية لضمان مشروعية الرد العسكري على الهجمات السيبرانية، وحماية المدنيين والبنية التحتية الحيوية، وتعزيز استقرار النظام الدولي ومنع التصعيد غير القانوني.

وخلصت الدراسة إلى العديد من النتائج والتوصيات نذكرها على النحو التالي:

أولاً- النتائج:

1. الهجمات السيبرانية تشكل تهديداً متزايداً للأمن القومي والبنية التحتية الحيوية للدول، وقد تصل إلى مستوى الهجوم المسلح الذي يبرر الرد العسكري وفقاً لأحكام ميثاق الأمم المتحدة.
2. الإطار القانوني الدولي الحالي يفتقر إلى معايير دقيقة لتحديد متى يعتبر الهجوم السيبراني هجوماً مسلحاً.
3. أن تطبيق مبادىء الضرورة والتناسب على الهجمات السيبرانية يواجه تحديات فنية وقانونية بسبب صعوبة تحديد المصدر وحجم الضرر.
4. غياب آليات فعالة للمساءلة الدولية يتيح للدول المحتملة ارتكاب الهجمات تجنب المسؤولية القانونية بسهولة.
5. أن التعاون الدولي في تبادل المعلومات والتقنيات لمواجهة الهجمات السيبرانية لا يزال ضعيفاً، مما يقلل فعالية الوقاية والاستجابة.

ثانيا- التوصيات:

1. تطوير سياسات وقوانين وطنية ودولية لتقييم الهجمات السيبرانية بشكل فوري وتحديد الرد المشروع وفق أحكام ميثاق الأمم المتحدة، مع مراعاة حماية المدنيين والمرافق الحيوية.
2. تطوير إطار قانوني دولي متكامل يحدد المعايير القانونية للاعتراف بالهجمات السيبرانية كأعمال عدوانية، ويضع حدوداً واضحة للرد المشروع.
3. إنشاء فرق تقييم قانونية وتقنية متخصصة لتقدير الضرر وتحديد مدى استيفاء الرد العسكري لمبدأ الضرورة والتناسب قبل تنفيذه.
4. تطوير آليات دولية للرقابة والمساءلة تشمل توثيق الهجمات السيبرانية، تحديد المسؤوليات، وفرض عقوبات قانونية على الدول المخالفة.

[60] سمير، خالد،الأمن السيبراني والقانون الدولي: المبادىء والتطبيقات، دار الفكر العربي، عمان،2022، ص 83-104.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 2
N:63 APRIL 2026

5. تعزيز التعاون الدولي من خلال اتفاقيات متعددة الأطراف لتبادل المعلومات والخبرات التقنية، وتوحيد السياسات لتنظيم سلوك الدول في الفضاء السيبراني.

المراجع والمصادر:

الكتب القانونية.

- الخطاب، سامي، الهجمات السيبرانية ومسؤولية الدول في القانون الدولي، مركز دراسات الأمن الدولي، 2019.
- سالم، محمد، الالتزامات الدولية للدول في مواجهة الهجمات السيبرانية، دار الإبداع للنشر، القاهرة، مصر، 2021.
- عبدالله، حسام، الرد العسكري والهجمات السيبرانية في القانون الدولي، دار النهضة العربية، القاهرة، 2020.
- عبد الحميد، ريم، القانون الدولي للعمليات السيبرانية، دار المعرفة الجامعية، القاهرة، مصر، 2021.
- عبد الرحمن، عادل، القانون الدولي للفضاء السيبراني: المبادىء والضوابط، دار الفكر العربي، القاهرة، 2021.
- محمد، عبد الله فوزي، القانون الدولي وحق الدفاع الشرعي في ظل التهديدات السيبرانية، دار النهضة العربية،2020.
- يوسف، نوال، الهجمات السيبرانية ومبادىء القانون الدولي، دار الفكر العربي، عمان، 2022.
- يوسف، نوال، السيطرة على الفضاء السيبراني بين القانون الدولي والأمن الدولي، مكتبة الجامعة الحديثة، الرياض، 2022.

الرسائل العلمية والبحوث:

- أحمد، هبة، المسؤولية الدولية عن الهجمات السيبرانية، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2020.
- خليل، ندى، المسؤولية الدولية عن الهجمات السيبرانية، رسالة ماجستير، كلية الحقوق، جامعة بيروت العربية، 2021.
- رمضان، السيد أحمد، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية، 2025.
- الزيد، محمد، القانون الدولي والسيادة الرقمية: قراءة في التحديات المعاصرة، المجلة العربية للدراسات القانونية، العدد12،2020.
- عبد الكريم، أمل، الهجمات السيبرانية في القانون الدولي، رسالة ماجستير، كلية القانون، جامعة بغداد، 2021.
- عبد الكريم، أحمد، الفضاء السيبراني بين ميثاق الأمم المتحدة ومتطلبات الأمن الدولي، مجلة البحوث القانونية، العدد2021،8.
- علي،محمود، القانون الدولي والحروب الحديثة: التحديات السيبرانية، دار النهضة العربية، القاهرة،2021.
- محمد، ليلى، التنظيم القانوني للهجمات السيبرانية في القانون الدولي، رسالة دكتوراة، جامعة الإمارات، 2021.
- يونس، إسراء، الهجمات السيبرانية والمسؤولية الجنائية الدولية، رسالة ماجستير، كلية الحقوق، جامعة الزقازيق، 2021.

ISSN:2509-0291
DOI
https://doi.org/10.63585/WDCG8854
Volume 11 issue 2
N:63 APRIL 2026

المو اثيق والاتفاقيات:

- ميثاق الأمم المتحدة، 1945، المادة(2/4) و المادة(51).
- أحكام محكمة العدل الدولية.
- -اللجنة الدولية للصليب الأحمر.

المراجع الأجنبية:

1. Wolfgang Kerber, Cyber, Security and lnternational Law, Springer, 2020.
2. Daniel P.V. O'Connell,The Law of Cyber Operations in lnternational Law, Oxford University Press, 2021.
3. Schmitt, Michael N. (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,Cambridge University Press,2017.
4. Hill ,Jonathan E. Cyber Operations and the Use of Force under the UN Charter, Oxford University Press, 2018..
5. International Court of Justice, Nicaragua v. United States of America (Merits) , lCJ Reports, 1986.
6. Michael N. Schmitt (ed), Tallinn Manual 2.0 on the lnternational Law Applicable to Cyber Operations, Cambridge University Press, 2017.