ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

معيار الضرر السيبراني المحمي أثناء النزاعات المسلحة: حماية البيانات والبنية التحتية المدنية في ضوء القانون الدولي الإنساني

The Protected Cyber Harm Standard during Armed Conflicts: Civilian Data and Infrastructure under International Humanitarian Law

الباحث الأول: الدكتور عمر بن صالح السعيد

عضو هيئة تدريس، كلية الحقوق، جامعة الملك فيصل، المملكة العربية السعودية

الباحثة الثانية: أمنية طارق أحمد الشاهين

باحثة قانونية

الملخص

يعالج هذا البحث سؤالًا أدق من السؤال الشائع عن مدى انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة، وهو: متى يبلغ الضرر السيبراني حدًّا يجعله ضررًا محميًا، ولا سيما حين يقع على البيانات المدنية أو يعطل بنية تحتية مدنية دون تدمير مادي ظاهر؟ وتنطلق الدراسة من فرضية مؤداها أن الصعوبة لا تكمن في أصل قابلية قواعد القانون الدولي الإنساني للتطبيق، بل في تشغيلها على أضرار رقمية تمس الوظيفة المدنية للنظام أو البيانات أو الخدمات الأساسية. وتعتمد الدراسة منهجًا تحليليًا تأصيليًا، مع إفادة وظيفية محدودة من دليل تالين ومواقف اللجنة الدولية للصليب الأحمر والأمثلة الواقعية والافتراضية المنضبطة. ولا تدعي الدراسة جدة الموضوع في ذاته، وإنما تتمثل مساهمتها في نقل مركز النقاش إلى معيار الضرر السيبراني المحمي بوصفه أداة لتشغيل القواعد القائمة عند المساس بالبيانات أو الوظائف المدنية دون تدمير مادي ظاهر. ويخلص البحث إلى أن المطلوب ليس إعلان عجز القانون الدولي الإنساني، بل تطوير قراءة تفسيرية منضبطة تعترف بالضرر الوظيفي الجوهري متى مس المدنيين أو خدماتهم الأساسية.

الكلمات المفتاحية: العمليات السيبرانية؛ القانون الدولي الإنساني؛ معيار الضرر السيبراني المحمي؛ التعطيل الوظيفي؛ البيانات المدنية؛ البنية التحتية المدنية؛ الأنظمة مزدوجة الاستخدام.

Abstract

This article addresses a narrower enquiry than whether international humanitarian law applies to cyber operations during armed conflicts: when does cyber harm reach a threshold that should be treated as protected harm, particularly where civilian data or civilian infrastructure is impaired without visible physical destruction? It argues that the real difficulty lies not in the abstract applicability of international humanitarian law, but in the operation of its rules in relation to digital harms affecting civilian functions, data and essential services. The article adopts a doctrinal analytical method, drawing in a limited and functional manner on the Tallinn Manual, the positions of the International Committee of the Red Cross, and carefully framed real and hypothetical examples. It does not claim novelty in the general topic itself; rather, its contribution lies in shifting the inquiry towards a protected cyber harm standard for applying existing rules where data or civilian functions are impaired without material destruction. It concludes that the proper response is not to declare international humanitarian law obsolete, but to develop a disciplined interpretation that recognises serious functional disruption as legally relevant harm.

Keywords: cyber operations; international humanitarian law; protected cyber harm standard; functional disruption; civilian data; civilian infrastructure; dual-use systems.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

المقدمة

لم يعد النقاش الجاد في العمليات السيبرانية أثناء النزاعات المسلحة يقف عند السؤال الأولي: هل ينطبق القانون الدولي الإنساني على الفضاء السيبراني؟ فهذا السؤال، على أهميته في مرحلة التأسيس، لم يعد كافيًا وحده لإدارة الإشكال القانوني الأشد دقة. فالمشكلة لا تظهر في الحالة السهلة التي تؤدي فيها عملية سيبرانية إلى انفجار مادي، أو توقف محطة طاقة، أو تعطيل مستشفى بما يفضي إلى موت أو إصابة أو تلف عيني مباشر؛ إذ يسهل عندئذ رد الواقعة إلى قواعد التمييز والتناسب والاحتياطات وحماية الأعيان المدنية. وإنما تظهر الصعوبة في المنطقة الأقل وضوحًا: حين لا يدمر الهجوم شيئًا بمعناه المادي التقليدي، ولكنه يمحو بيانات مدنية، أو يعطل نظامًا صحيًا، أو يفسد سجلات إغاثية، أو يشل وظيفة مرفق حيوي، أو يجعل البنية الرقمية سببًا في إنتاج أثر إنساني لا يقل خطرًا عن كثير من الأضرار المادية.[1]

ولا تنطلق هذه الدراسة من دعوى وجود فراغ كامل في القانون الدولي الإنساني، ولا من اطمئنان مفرط إلى أن القواعد القائمة تكفي في صورتها التقليدية لكل صور الضرر الرقمي. فالقول بالفراغ الكامل يتجاهل أن القانون الدولي الإنساني صيغ، في أصوله الكبرى، ليضبط وسائل الحرب وأساليبها وآثارها الإنسانية، لا ليقصر الحماية على أداة قتالية بعينها. والقول بالكفاية المطلقة يتجاهل أن البيئة السيبرانية تكشف صورًا من الضرر لا تستجيب دائمًا لثنائية التلف المادي وعدم التلف، ولا تنحصر في سؤال: هل تعطل جهاز أو تهدم مبنى؟ وإنما تفرض سؤالًا أدق: هل أصيبت وظيفة مدنية محمية إصابة جوهرية؟ وهل مس الأثر بيانات أو خدمة أو بنية رقمية يعتمد عليها المدنيون في حياتهم وأمنهم وصحتهم وتنقلهم وغذائهم ومياههم؟[2]

وقد عالجت طائفة من الأدبيات العربية موضوع الحرب السيبرانية في ضوء القانون الدولي الإنساني من خلال التعريف بالفضاء السيبراني، وتمييز الحرب السيبرانية عن الحرب التقليدية، والبحث في التكييف القانوني للهجمات السيبرانية بين الجريمة الدولية والحرب السيبرانية، ثم عرض دور اللجنة الدولية للصليب الأحمر ودليل تالين.[3] ولا تنكر هذه الدراسة أهمية ذلك التأسيس، بل تفيد منه بقدر ما يخدم سؤالها. غير أن إضافتها لا تقف عند إعادة تقرير قابلية القانون الدولي الإنساني للانطباق على العمليات السيبرانية، وهي مسألة تناولتها دراسات سابقة، بل تنتقل إلى بناء معيار لتحديد الضرر السيبراني المحمي حين يصيب البيانات أو الوظائف المدنية دون تدمير مادي ظاهر.[4]

وتظهر أهمية هذا التحول إذا استحضرنا أن البنية المدنية المعاصرة لم تعد تقوم على الجدران والآلات وحدها، بل على طبقات رقمية غير مرئية: سجلات المرضى، أنظمة المرور، شبكات المياه والكهرباء، قواعد بيانات الإغاثة، نظم الاتصال والإنذار، منصات الهوية، وتدفقات البيانات التي تجعل المرفق المدني قادرًا على العمل. فاستهداف هذه الطبقات قد لا يحطم المبنى، لكنه قد يعطل وظيفته. وقد لا يتلف الجهاز، لكنه قد يجعله عاجزًا عن إنتاج الخدمة المدنية التي وجد لأجلها. وهنا تحديدًا تتغير

---

1 اللجنة الدولية للصليب الأحمر، "الحرب السيبرانية والقانون الدولي الإنساني"، أسئلة وأجوبة، جنيف، 2013؛ اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، جنيف، تشرين الثاني/نوفمبر 2019، ص 5-3.

2 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, Rules 80-83.

3 يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، مج 4، ع 4، 2018، ص 80-108؛ منزر رابح ودرويش سعيد، "الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول"، مجلة صوت القانون، مج 8، ع 1، 2021، ص 538-557.

4 نورية الساعدي المقريف، "الحرب السيبرانية في ضوء أحكام القانون الدولي العام"، مجلة أبحاث قانونية، جامعة سرت، ع 14، ديسمبر 2022، ص 1-30؛ ياسين محمد أحمد بونة، "الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية"، مجلة شمال إفريقيا للنشر العلمي، مج 1، ع 4، 2023، ص 154-168.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

زاوية النظر: فالمعيار لا ينبغي أن يحبس الضرر في صورة الأثر الحركي وحده، وإنما ينبغي أن يستوعب ما تسميه هذه الدراسة التعطيل الوظيفي الجوهري؛ أي التعطيل أو الإفساد أو الحجب الذي يمس وظيفة مدنية أساسية على نحو غير عابر.[5]

وتزداد المسألة دقة لأن القانون الدولي الإنساني لا يحمي المدنيين من كل انزعاج أو اضطراب أو أثر عابر، كما لا يحظر كل عملية سيبرانية بمجرد اتصالها بمرفق مدني. فالحرب، بطبيعتها، تفرز آثارًا، والقانون الدولي الإنساني لا يلغي الحرب، بل يحد من آثارها الإنسانية. لذلك لا بد من معيار يميز بين مجرد الأثر التقني المحدود، وبين الضرر السيبراني الذي يمس حماية القانون الدولي الإنساني. وليس المقصود بهذا المعيار أن تستبدل الدراسة النصوص القائمة بقاعدة جديدة مصطنعة، بل أن تقترح طريقة في تشغيل القواعد القائمة على وقائع سيبرانية معقدة، بحيث لا تهدر حماية المدنيين بحجة غياب التلف المادي، ولا تتوسع الحماية على نحو يحول كل خلل رقمي أو اختراق معلوماتي إلى انتهاك لقواعد النزاع المسلح.[6]

ولا يغير من ذلك أن السوابق القضائية الدولية المباشرة في تطبيق القانون الدولي الإنساني على العمليات السيبرانية لا تزال محدودة، بل تكاد تكون نادرة في المسائل الدقيقة المتصلة بالبيانات المدنية والضرر الوظيفي. فهذه الندرة لا تعفي البحث من التحليل، وإنما تفرض عليه أن ينطلق من النصوص والمبادئ العامة والمواقف الدولية المعتبرة، وأن يختبرها على أمثلة واقعية وافتراضية منضبطة دون أن يحمل الوقائع أكثر مما تحتمل. ولهذا تستحضر الدراسة بعض الوقائع، مثل هجوم برمجية الفدية "WannaCry" على هيئة الخدمات الصحية الوطنية في المملكة المتحدة، والهجوم على شبكة الكهرباء الأوكرانية، وهجوم شبكة الاتصالات الفضائية Viasat/KA-SAT، لا لتقرير تكييفها النهائي في القانون الدولي الإنساني، بل لاختبار قدرة الضرر السيبراني على الانتقال من مستوى الخلل التقني إلى مستوى تعطيل الوظيفة المدنية.[7]

وعليه تتمثل مشكلة البحث في أن تطبيق القانون الدولي الإنساني على العمليات السيبرانية لا يواجه صعوبة واحدة، بل صعوبتين متداخلتين: الأولى تتعلق بعتبة الانطباق، أي متى تقع العملية السيبرانية في سياق نزاع مسلح أو تبلغ في ذاتها أثرًا يجعل قواعد النزاع المسلح ذات صلة؛ والثانية، وهي الأهم في هذه الدراسة، تتعلق بموضوع الحماية، أي متى يكون الأثر السيبراني الواقع على البيانات أو البنية التحتية المدنية ضررًا ذا اعتبار قانوني إنساني. فإذا بقي التحليل أسير الضرر المادي، ضاقت الحماية عن وقائع تمس المدنيين فعليًا. وإذا توسع التحليل دون ضابط، فقدت القواعد تمييزها بين المجال الإنساني والمجال الأمني أو الجنائي أو السياسي العام.[8]

ومن هذا المنطلق، يسأل البحث: ما المعيار الذي يمكن من خلاله تحديد الضرر السيبراني المحمي في العمليات السيبرانية أثناء النزاعات المسلحة؟ ويتفرع عن هذا السؤال الرئيس ثلاثة أسئلة: ما حدود قصور السؤال التقليدي عن مجرد انطباق القانون الدولي الإنساني؟ وكيف يمكن فهم الضرر السيبراني بين التلف المادي وتعطيل الوظيفة المدنية؟ وكيف تشغل مبادئ التمييز والتناسب والاحتياطات عند استهداف أنظمة مدنية أو مزدوجة الاستخدام تقوم عليها خدمات رقمية أساسية؟[9]

---

5 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 1-3.

6 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, Vol. I: Rules, Cambridge University Press, Cambridge, 2005, Rules 1, 7, 14 and 15.

7 National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*, HC 414, London, 2017; Cybersecurity and Infrastructure Security Agency (CISA), "Cyber-Attack Against Ukrainian Critical Infrastructure", ICS Alert IR-ALERT-H-16-056-01, 2016, last revised 20 July 2021; Council of the European Union, "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union", Press Release, 10 May 2022.

8 Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, Cambridge, 2012.

9 Schmitt (ed.), *Tallinn Manual 2.0*, Rules 92-97.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

وتنطلق الدراسة من فرضية مؤداها أن القانون الدولي الإنساني يملك، من حيث الأصل، قابلية الامتداد إلى العمليات السيبرانية أثناء النزاعات المسلحة، لكن فعالية هذه القابلية تتوقف على قراءة معيارية لا تختزل الضرر في التدمير المادي. فالمعيار المقترح يقوم على خمسة عناصر متكاملة: طبيعة المصلحة المدنية المتأثرة، ووظيفة النظام المستهدف، ودرجة التعطيل، وقابلية الأثر للامتداد، وموقع العملية من النزاع المسلح. ولا يعمل أي عنصر منها منفردًا، بل تتحدد النتيجة من اجتماعها وتفاعلها في الواقعة المعروضة.[10]

وتعتمد الدراسة منهجًا تحليليًا تأصيليًا، يقوم على قراءة قواعد القانون الدولي الإنساني في ضوء طبيعة الضرر السيبراني، مع إفادة وظيفية محدودة من دليل تالين 2.0 بشأن القانون الدولي المنطبق على العمليات السيبرانية بوصفه عملاً صادرًا عن خبراء وغير ملزم، ومن مواقف اللجنة الدولية للصليب الأحمر (ICRC) بوصفها مرجعًا إنسانيًا مؤثرًا في تفسير تحديات النزاعات المسلحة المعاصرة. ولا تستعمل الدراسة الأمثلة الواقعية بوصفها سوابق قضائية أو دراسات حالة مستقلة، بل بوصفها اختبارات وظيفية لعناصر المعيار المقترح، مع بقاء التكييف النهائي لكل واقعة محكومًا بسياقها وأدلتها. كما توظف الدراسة، في حدود ضيقة، بعض المواد التنظيمية السعودية في الأمن السيبراني وحماية البيانات لا كمصدر مباشر لقواعد القانون الدولي الإنساني، وإنما كشاهد على أن حماية البنية الرقمية أصبحت جزءًا من حماية المصالح الحيوية والمدنية في زمن السلم، وهو ما يعزز الحاجة إلى فهم أثرها وقت النزاع المسلح.[11]

وتكمن مساهمة البحث في أمرين متلازمين. أولهما نقل النقاش من سؤال الانطباق المجرد إلى سؤال الضرر المحمي. وثانيهما اقتراح معيار تشغيلي يوازن بين حماية المدنيين من الأثر السيبراني الجوهري، وبين منع التوسع غير المنضبط في وصف كل أثر رقمي بأنه ضرر إنساني محمي. وعلى هذا ينتظم البحث في مبحثين: يخصص الأول للانتقال من سؤال الانطباق إلى معيار الضرر السيبراني المحمي، وذلك ببيان قصور السؤال التقليدي، وتحليل الضرر بين الأثر المادي وتعطيل الوظيفة المدنية، وتحديد موقع البيانات والبنية التحتية المدنية من الحماية. ويخصص الثاني لتشغيل هذا المعيار في ضوء مبادئ القانون الدولي الإنساني، وذلك من خلال التمييز والتناسب والاحتياطات، والأنظمة مزدوجة الاستخدام، والحاجة إلى تطوير تفسيري منضبط لا إلى إعلان عجز القواعد القائمة.[12]

المبحث الأول: من سؤال الانطباق إلى معيار الضرر السيبراني المحمي

يمهد هذا المبحث لبناء معيار الضرر السيبراني المحمي من خلال نقل النظر من سؤال الانطباق المجرد إلى سؤال الأثر القانوني للضرر الرقمي. فلا يكفي، في البيئة السيبرانية، تقرير أن القانون الدولي الإنساني قابل للتطبيق متى وجد نزاع مسلح، بل يلزم بيان نوع الضرر الذي تستطيع قواعده أن تتعرف عليه وتحكمه. لذلك يبدأ المبحث ببيان قصور السؤال التقليدي عن مدى الانطباق، ثم ينتقل إلى تحليل الضرر السيبراني بين الأثر المادي وتعطيل الوظيفة المدنية، لينتهي إلى تحديد موقع البيانات والبنية التحتية المدنية بوصفهما محلًا محتملًا للحماية متى كان المساس بهما مساسًا بوظيفة مدنية جوهرية.

المطلب الأول: قصور السؤال التقليدي عن مدى انطباق القانون الدولي الإنساني

10 Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", *International Review of the Red Cross*, 2020.

11 الهيئة الوطنية للأمن السيبراني، "الضوابط الأساسية للأمن السيبراني ECC-2:2024"، الرياض، 2024؛ الهيئة الوطنية للأمن السيبراني، "ضوابط الأمن السيبراني للأنظمة الحساسة CSCC-1:2019"، الرياض، 2019؛ المملكة العربية السعودية، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم م/19 بتاريخ 9/2/1443هـ، والمعدل بالمرسوم الملكي رقم م/148 بتاريخ 5/9/1444هـ.

12 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC/Martinus Nijhoff, Geneva, 1987, pp. 598-626.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

لا تبدأ صعوبة العمليات السيبرانية من كونها تقع في فضاء غير مادي فحسب، بل من أنها تكشف حدود كثير من الأسئلة القانونية حين تطرح بصيغتها العامة. فمن السهل أن يقال إن القانون الدولي الإنساني ينطبق على العمليات السيبرانية متى وقعت في سياق نزاع مسلح. وهذه العبارة صحيحة في أصلها، لكنها لا تجيب عن الأسئلة التي تهم القاضي أو المستشار القانوني العسكري أو الباحث: هل تعد العملية السيبرانية هجومًا؟ وهل يكون النظام المستهدف عينًا مدنية أم هدفًا عسكريًا؟ وهل تدخل البيانات في نطاق الحماية ذاتها التي تتمتع بها الأعيان المدنية؟ وهل يكفي تعطيل الوظيفة المدنية للقول بوجود ضرر محي؟[13]

وقد ذهبت اللجنة الدولية للصليب الأحمر إلى أن العمليات السيبرانية أثناء النزاعات المسلحة تخضع للقانون الدولي الإنساني، وأن القواعد القائمة، ولا سيما التمييز والتناسب والاحتياطات، تحمي البنية التحتية المدنية من الهجمات السيبرانية. غير أن أهمية هذا الموقف لا تكمن فقط في تقرير الانطباق، بل في التنبيه إلى أن المدنيين والبنية التحتية المدنية والبيانات المدنية قد يتعرضون لضرر سيبراني يستدعي فهمًا أعمق لكيفية عمل هذه القواعد في البيئة الرقمية.[14] فالمسألة، إذن، ليست في أن القانون الدولي الإنساني يدخل الفضاء السيبراني أو لا يدخله، بل في طريقة دخوله، وفي نوع الضرر الذي يتعرف عليه، وفي الحد الذي عنده يتحول الأثر التقني إلى أثر إنساني محي.

ويزداد قصور السؤال التقليدي إذا استحضرنا أن العمليات السيبرانية ليست نوعًا واحدًا. فقد تكون تجسسًا رقميًا لا يفضي بذاته إلى ضرر إنساني مباشر، وقد تكون عملية تمهيدية لجمع معلومات، وقد تكون عملية تضليل أو إرباك، وقد تكون تعطيلًا مؤقتًا لخدمة، وقد تكون هجومًا على نظام تحكم صناعي يؤدي إلى أثر مادي واسع. وبين هذه الصور درجات كثيرة لا يستقيم جمعها تحت عبارة واحدة. لذلك فإن السؤال عن "الحرب السيبرانية" في عمومه يميل إلى إخفاء الفروق الدقيقة التي تقوم عليها الحماية القانونية.[15]

وقد كشفت بعض الوقائع الحديثة، خارج التحليل الحصري لقواعد النزاع المسلح، أن الأثر السيبراني يمكن أن يخرج من نطاق الخلل التقني إلى تعطيل وظيفة مدنية أساسية. فقد أظهر هجوم برمجية الفدية "WannaCry" سنة 2017 على هيئة الخدمات الصحية الوطنية في المملكة المتحدة (NHS) كيف يمكن لبرمجية خبيثة أن تؤثر في تقديم الرعاية الصحية وتؤدي إلى إلغاء مواعيد وخدمات طبية، كما كشفت الهجمات على شبكة الكهرباء الأوكرانية سنة 2015 قابلية أنظمة التحكم الصناعية لأن تتحول إلى نقطة ضغط على خدمة مدنية واسعة.[16] ولا تستدعي هذه الدراسة تلك الوقائع لتكييفها تكييفًا نهائيًا في القانون الدولي الإنساني، وإنما لتوضيح أن الضرر الرقمي قد يمس الوظيفة المدنية للنظام ولو لم يبدأ في صورة قصف أو تدمير مادي ظاهر.

ومن ثم تبدو الحاجة إلى تحرير محل البحث. فليس كل نشاط سيبراني موضوعًا لهذه الدراسة، ولا كل جريمة إلكترونية، ولا كل اختراق يقع في زمن الحرب. محل البحث هو العملية السيبرانية المتصلة بنزاع مسلح، والتي ينتج عنها أو يتوقع أن ينتج عنها أثر يمس المدنيين أو الأعيان المدنية أو الوظائف المدنية الجوهرية. وبهذا التضييق يتجنب البحث خلط القانون الدولي الإنساني بقانون مكافحة الجريمة السيبرانية، أو بقواعد المسؤولية الدولية عن التدخل في شؤون الدول، أو بقواعد الأمن السيبراني الوطني في زمن السلم، مع بقاء إمكان الاستفادة من هذه الحقول في حدودها الوظيفية.[17]

---

13 البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977، المواد 48، 51، 52، 57؛ Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rules 1, 7, 14 and 15.

14 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 1-9.

15 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, pp. 885-937.

16 National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*; CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure".

17 اتفاقية بودابست بشأن الجريمة المعلوماتية، مجلس أوروبا، 2001؛ رابح ودرويش، "الطبيعة القانونية للهجمات السيبرانية"، ص 546-548.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

ولعل أحد أسباب الاضطراب في الأدبيات هو أن تعبير "الحرب السيبرانية" يوحي أحيانًا بأن كل هجوم سيبراني بين دولتين هو حرب، أو أن كل حرب تستخدم وسائل رقمية هي حرب سيبرانية. وهذا التوسع لا يخدم الدقة. فالعملية السيبرانية قد تقع خارج النزاع المسلح، وقد تثير قواعد حظر استخدام القوة أو عدم التدخل أو المسؤولية الدولية، لكنها لا تدخل بالضرورة في القانون الدولي الإنساني. وقد تقع أثناء نزاع مسلح، لكنها لا تكون "هجومًا" بالمعنى الفني إذا لم تبلغ أثرًا معينًا. وقد تستهدف هدفًا عسكريًا، لكنها تثير سؤال التناسب إذا امتدت آثارها إلى شبكة مدنية مترابطة.[18]

إن تحرير هذا التدرج هو المدخل الضروري لمعيار الضرر المحمي. فالضرر السيبراني المحمي ليس مرادفًا لكل اختراق، ولا لكل فقد بيانات، ولا لكل تعطيل عابر. كما أنه لا يقتصر على التلف المادي وحده. إنه يقع في المسافة بين هذين الطرفين: بين التضييق الذي لا يرى الضرر إلا إذا تهدم الشيء، والتوسع الذي يرى الضرر في كل اضطراب تقني. وفي هذه المسافة يعمل المعيار المقترح بوصفه أداة تفسيرية لا قاعدة جديدة مستقلة عن القانون القائم.[19]

ويمكن تقريب ذلك بمثالين متقابلين. فإذا أدت عملية سيبرانية إلى إطفاء نظام التكييف في مبنى إداري مدني لساعات محدودة دون أثر على سلامة الأشخاص أو استمرار خدمة أساسية، فقد يكون الفعل غير مشروع وفق قواعد أخرى، لكنه لا يبلغ بالضرورة مستوى الضرر الإنساني المحمي في القانون الدولي الإنساني. أما إذا أدت عملية مماثلة إلى تعطيل نظام حفظ الأدوية في مستشفى ميداني، أو إلى إفساد سجلات المرضى بما يمنع العلاج، أو إلى تعطيل نظام إنذار مدني في مدينة تتعرض للقصف، فإن غياب التدمير المادي لا ينفي جوهر الضرر. فالاعتبار هنا ليس بما إذا كان الجدار قد تهدم، بل بما إذا كانت الوظيفة المدنية المحمية قد شلت أو تضررت على نحو جوهري.[20]

وبهذا المعنى، فإن سؤال الانطباق يظل لازمًا لكنه غير كاف. فهو يحدد الباب الذي ندخل منه، أما معيار الضرر المحمي فيحدد ما إذا كانت الواقعة التي دخلت الباب تستدعي حكمًا إنسانيًا خاصًا. وهذا التمييز يحفظ للقانون الدولي الإنساني مجاله، ويمنع في الوقت ذاته إفراغ الحماية من مضمونها في بيئة أصبحت فيها الوظيفة المدنية محمولة على أنظمة وبيانات وشبكات قد لا ترى بالعين المجردة.[21]

المطلب الثاني: الضرر السيبراني بين الأثر المادي وتعطيل الوظيفة المدنية

اعتاد التفكير القانوني في النزاعات المسلحة أن يتعامل مع الضرر من خلال آثار ظاهرة: قتل، إصابة، تدمير، إتلاف، أو إلحاق ضرر مادي بالأعيان. وهذه اللغة مفهومة تاريخيًا؛ لأنها نشأت في بيئة كان السلاح فيها يترك أثره على الجسد أو الشيء بصورة مباشرة. غير أن العمليات السيبرانية تجعل الضرر أكثر تركيبًا؛ فقد يكون الأثر المادي حاضرًا، وقد يغيب ظاهريًا مع بقاء أثر وظيفي بالغ الخطورة. وهذا لا يعني إلغاء مركزية الضرر المادي، بل يعني أن معيار الحماية لا ينبغي أن يتوقف عنده كلما كانت الوظيفة المدنية هي محل الإصابة الحقيقي.[22]

فالبيانات، مثلًا، ليست شيئًا ماديًا في ذاتها بالمعنى التقليدي، لكنها قد تكون شرطًا لعمل عين مدنية أو مرفق مدني. سجلات المرضى ليست مجرد معلومات، بل هي شرط للعلاج الصحيح. بيانات توزيع الغذاء ليست مجرد أرقام، بل هي شرط لوصول الإغاثة. نظم التحكم في المياه والكهرباء ليست مجرد برامج، بل هي طبقة تشغيلية تجعل البنية المادية قادرة على أداء وظيفتها.

18 Schmitt, "Computer Network Attack and the Use of Force", pp. 913-925.

19 Schmitt (ed.), *Tallinn Manual 2.0*, Rules 69-71.

20 اللجنة الدولية للصليب الأحمر، "الحرب السيبرانية والقانون الدولي الإنساني".

21 Dinniss, *Cyber Warfare and the Laws of War*, pp. 202-210.

22 البروتوكول الإضافي الأول، المواد 48، 51، 52.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

فإذا أتلفت العملية السيبرانية هذه الطبقة أو عطلتها، فإن السؤال لا يكون: هل تحطم الجهاز؟ بل: هل أصيبت الوظيفة المدنية التي يحميها القانون؟[23]

ومن هنا تقترح الدراسة التمييز بين ثلاثة مستويات من الأثر. المستوى الأول هو الأثر التقني المجرد، كاختراق محدود أو توقف قصير لا يتجاوز نطاقه النظام المستهدف ولا يمس خدمة مدنية جوهرية. وهذا لا يدخل غالبًا في الضرر المحمي، وإن أمكن أن يخضع لقواعد أخرى. والمستوى الثاني هو الأثر الوظيفي، حيث يتعطل النظام أو البيانات على نحو يمس خدمة مدنية أو مصلحة إنسانية، دون أن يتحقق تلف مادي ظاهر. والمستوى الثالث هو الأثر المادي أو البشري، حيث يؤدي التعطيل إلى إصابة أو وفاة أو تدمير أو تلف عيني. والمستوى الثاني هو مجال الإشكال الحقيقي؛ لأنه لا يبلغ وضوح المستوى الثالث، لكنه يتجاوز بساطته المستوى الأول.[24]

ولا يكفي في هذا المستوى الثاني أن يقال إن البيانات محمية دائمًا أو غير محمية دائمًا. فكلا القولين متطرف. البيانات المدنية قد تكون محل حماية حين تكون مرتبطة بوظيفة مدنية جوهرية، أو حين يؤدي إتلافها أو تعديلها أو حجبها إلى أثر إنساني ملموس. لكنها لا تتحول بالضرورة إلى عين مدنية بالمعنى ذاته في كل صورة. لذلك يكون الأجدى أن نتعامل مع البيانات لا بوصفها مفهومًا مجردًا، بل بحسب وظيفتها وسياقها وأثر المساس بها.[25]

وتظهر أهمية الوظيفة المدنية في الأمثلة الافتراضية. فحذف قاعدة بيانات تحتوي على مواعيد داخل مؤسسة ثقافية قد يكون ضررًا إداريًا أو ماليًا، لكنه لا يبلغ غالبًا حد الضرر الإنساني المحمي. أما حذف قاعدة بيانات تحتوي على فصائل دم المصابين أو خريطة توزيع الأدوية أو مواقع ملاجئ المدنيين، فيختلف نوعيًا. فالبيانات هنا لا تحمى لأنها "بيانات" فقط، بل لأنها تحمل وظيفة إنسانية مدنية، ولأن المساس بها ينعكس على حياة المدنيين أو صحتهم أو أمنهم.[26]

وهذا التحليل لا يخرج عن منطق القانون الدولي الإنساني. فالقانون لا يحمي الشيء لذاته دائمًا، وإنما يحميه بحسب طبيعته أو استخدامه أو أثر استهدافه. فالمدرسة، والمستشفى، وشبكة المياه، ومحطة الكهرباء، لا تستمد قيمتها القانونية من مادتها الفيزيائية وحدها، بل من وظيفتها المدنية. وإذا كان ذلك صحيحًا في الأعيان المادية، فلا وجه لأن يستبعد حين تصبح الوظيفة المدنية ذاتها معتمدة على نظام رقمي أو قاعدة بيانات أو شبكة تحكم.[27]

على أن هذا القول يجب أن يبقى منضبطًا. فليس كل تعطيل لوظيفة مدنية ينهض بالضرورة انتهاكًا. لا بد من النظر إلى درجة التعطيل ومدته وسعته وقابليته للتدارك، وإلى ما إذا كان متوقعًا أو مقصودًا أو قابلًا للتوقع، وإلى موقعه من العملية العسكرية. فتعطيل خدمة مدنية لوقت قصير مع بدائل فعالة يختلف عن شل خدمة أساسية في وقت يحتاج فيه المدنيون إليها للبقاء أو الحماية. وهنا تظهر عناصر المعيار المقترح: طبيعة المصلحة، ووظيفة النظام، ودرجة التعطيل، وقابلية الأثر للامتداد، والسياق النزاعي.[28]

وإذا أخذنا مثال المستشفى، وجدنا أن جوهر الحماية لا يتوقف على تدمير جهاز طبي. فلو أدت عملية سيبرانية إلى إفساد نظام فرز الحالات، أو منع الوصول إلى سجلات مرضى العناية الحرجة، أو تعطيل نظام تشغيل أجهزة مرتبطة بحفظ الحياة، فإن

23 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 5-8.

24 Schmitt (ed.), *Tallinn Manual 2.0*, Rule 92 and commentary.

25 Gisel, Rodenhäuser and Dörmann, "Twenty Years On".

26 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 7-8.

27 البروتوكول الإضافي الأول، المادة 52؛ Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rules 7-10.

28 Schmitt (ed.), *Tallinn Manual 2.0*, Rules 100-103.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

الضرر هنا لا يكون افتراضيًا أو معنويًا مجردًا. إنه ضرر وظيفي ينعكس على أشخاص محميين. ولا يكون منطقيًا أن يستبعد القانون الدولي الإنساني هذا الأثر من حساباته لمجرد أن الخادم لم يحترق أو أن الجهاز المادي لم يتلف.[29]

وكذلك الحال في شبكة الكهرباء أو المياه. فالهجوم على نظام التحكم قد لا يكسر الأنابيب أو يحطم المحولات، لكنه قد يمنع الضخ أو التوزيع أو المراقبة أو الإصلاح. وإذا ترتب على ذلك حرمان المدنيين من المياه أو الكهرباء أو الرعاية أو الاتصال، فإن معيار الضرر يجب أن يستحضر النتيجة الوظيفية لا الصورة الخارجية للأثر. فالضرر السيبراني في هذه الحالة لا ينفصل عن أثره على الأعيان أو الوظائف المدنية التي تعتمد على النظام الرقمي.[30]

ومن هذه الزاوية، لا يضيف معيار الضرر السيبراني المحمي حماية غريبة على القانون، بل يكشف الإمكان التفسيري الكامن في قواعده القائمة. فالحماية المدنية في القانون الدولي الإنساني ليست حماية للأحجار والمعادن وحدها، بل حماية للإنسان من آثار الحرب. وإذا أصبحت طبقة رقمية معينة شرطًا لسلامة الإنسان أو استمرار خدمة مدنية أساسية، فإن إقصاء هذه الطبقة من التحليل لا يكون وفاءً بحرف القانون، بل تضييقًا لوظيفته الإنسانية.[31]

المطلب الثالث: البيانات والبنية التحتية المدنية بوصفهما محلًا للحماية

يثير إدخال البيانات المدنية في نطاق التحليل أحد أكثر الأسئلة حساسية في القانون الدولي الإنساني المعاصر. فمن ناحية، لا يريد القانون أن يتحول إلى أداة لتنظيم كل تدفق معلوماتي في زمن الحرب. ومن ناحية أخرى، لم تعد البيانات شيئًا هامشيًا يمكن فصله عن حماية المدنيين. فالمجتمعات الحديثة، في السلم والحرب، تدار ببيانات: الهوية، الصحة، المصارف، الغذاء، التعليم، النقل، الإغاثة، والاتصال. ولذلك فإن إتلاف البيانات أو تعديلها أو حجبها قد ينتج أثرًا لا يقل خطورة عن تدمير بعض الأعيان المادية.[32]

وقد تعامل دليل تالين 2.0 مع العمليات السيبرانية من خلال محاولة إسقاط قواعد القانون الدولي القائمة على الوقائع الرقمية، لكنه بقي، بحكم طبيعته، عملًا صادرًا عن خبراء، لا يمثل اتفاقية دولية ولا رأيًا رسميًا جامعًا للدول. ومع ذلك، تكمن قيمته في أنه كشف حدود الأسئلة التقليدية، ولا سيما عند مناقشة معنى الهجوم، والأعيان، والسيادة، والمسؤولية، والعمليات التي لا تبلغ عتبة القوة المسلحة. غير أن هذه القيمة لا تعني التسليم بكل ما يقرره، بل الاستفادة منه بوصفه أداة حوارية تظهر مواضع الاتفاق والخلاف.[33]

والمسألة الأشد أهمية هي ما إذا كانت البيانات المدنية تعد "عينًا مدنية" بذاتها. لا تتبنى هذه الدراسة جوابًا مطلقًا. فالنصوص التقليدية لم تصغ مفهوم العين المدنية وهي تستحضر البيانات بوصفها محلًا مستقلًا للحماية. ومع ذلك، فإن حصر الحماية في الأشياء المادية على نحو جامد قد يؤدي إلى نتيجة غير مقبولة إنسانيًا: حماية الحاسوب الخادم بوصفه شيئًا ماديًا، وإهمال البيانات التي تجعل المستشفى أو شبكة المياه أو منظومة الإغاثة قادرة على العمل. لذلك تقترح الدراسة طريقًا أضيق وأكثر اتزانًا: لا تعامل كل البيانات المدنية كعين مستقلة دائمًا، لكن يعتد بها حين يكون المساس بها مساسًا بوظيفة مدنية محمية.[34]

---

29 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 5-8.

30 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، جنيف، 2011، ص 40-41.

31 Sandoz, Swinarski and Zimmermann, *Commentary on the Additional Protocols*, pp. 683-688.

32 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 6.

33 Schmitt (ed.), *Tallinn Manual 2.0*, Introduction and Rules 80-97.

34 Gisel, Rodenhäuser and Dörmann, "Twenty Years On".

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

ويختلف الأمر باختلاف نوع البيانات. فهناك بيانات مدنية ذات صلة مباشرة بالحياة والسلامة: السجلات الطبية، بيانات الإسعاف، خرائط الإخلاء، نظم الإنذار، بيانات المياه والطاقة، وبيانات توزيع الغذاء. وهناك بيانات مدنية اقتصادية أو إدارية قد يكون المساس بها ضارًا، لكنه لا يبلغ بالضرورة عتبة الضرر الإنساني. وهناك بيانات مختلطة أو مزدوجة الاستخدام تخدم أغراضًا مدنية وعسكرية في الوقت ذاته. وهنا لا يكفي التصنيف الاسمي، بل يجب البحث في الوظيفة الفعلية والأثر المتوقع.[35]

أما البنية التحتية المدنية، فهي أكثر وضوحًا من البيانات لكنها ليست أقل تعقيدًا. فقد تكون البنية التحتية مادية ورقمية في وقت واحد. محطة الكهرباء ليست مجرد مبنى أو مولدات؛ إنها كذلك أنظمة تحكم، وبرمجيات مراقبة، وشبكات اتصال، وبيانات تشغيل. والمستشفى ليس مبنى وأجهزة فقط؛ إنه سجلات ونظم وجدولة وتكامل معلوماتي. وشبكة المياه ليست أنابيب فحسب؛ إنها أنظمة قياس وضخ وتحكم. لذلك فإن الفصل الصارم بين العين المادية والنظام الرقمي الذي يديرها قد لا يعكس الواقع الوظيفي للبنية المدنية المعاصرة.[36]

ويكشف السياق السعودي، في حدود وظيفية لا استعراضية، عن هذه الحقيقة. فالهيئة الوطنية للأمن السيبراني تعرض الضوابط الأساسية للأمن السيبراني (ECC-2:2024) بوصفها ضوابط محدثة لتعزيز الأمن السيبراني على المستوى الوطني وحماية الأصول المعلوماتية والتقنية للجهات الوطنية، كما تكشف ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) عن تصور تنظيمي يربط الأمن السيبراني بالأنظمة ذات الحساسية العالية والوظائف الحيوية.[37] ولا يعني ذلك أن هذه الضوابط الوطنية تنشئ قواعد في القانون الدولي الإنساني، لكنها تكشف أن البنية الرقمية باتت جزءًا من تصور الحماية المدنية والمؤسسية في زمن السلم، ومن باب أولى لا يجوز تجاهل أثرها حين تكون العمليات السيبرانية جزءًا من نزاع مسلح.[38]

وتبدو أهمية ذلك عند تحليل الأثر الممتد. فالعملية السيبرانية، بخلاف كثير من الأعمال الحركية المحددة، قد تنتقل آثارها عبر شبكات مترابطة، أو تصيب أنظمة لم تكن مقصودة ابتداءً، أو تتفاعل مع اعتماد مدني وعسكري على البنية ذاتها. وهذا الامتداد يجعل التوقع والاحتياط أكثر أهمية. فالمهاجم لا يستطيع أن يكتفي بالقول إنه استهدف وظيفة عسكرية داخل شبكة، إذا كان يعلم أو كان ينبغي أن يعلم أن الشبكة ذاتها تحمل خدمات مدنية أساسية وأن تعطيلها سيصيب المدنيين على نطاق واسع.[39]

ومن هنا فإن معيار الضرر السيبراني المحمي لا يعمل فقط بعد وقوع الأثر، بل ينبغي أن يعمل قبل العملية في تقدير مشروعيتها. فإذا كان النظام المستهدف مدني الوظيفة، أو كان ذا استخدام مزدوج، وكان تعطيله سيؤدي غالبًا إلى حرمان المدنيين من خدمة أساسية، فإن التقييم القانوني يجب أن يبدأ من هذا الأثر المتوقع. أما إذا كان الضرر التقني محدودًا وقابلًا للاحتواء ولا يمس وظيفة مدنية ذات شأن، فإن وصفه بالضرر المحمي سيكون توسعًا غير دقيق.[40]

ويمكن تلخيص المعيار في صيغة عملية: يكون الضرر السيبراني محميًا، في سياق النزاع المسلح، متى أصاب أو كان متوقعًا أن يصيب مصلحة مدنية ذات أهمية إنسانية، من خلال تعطيل أو إتلاف أو تغيير أو حجب نظام أو بيانات أو وظيفة رقمية، على

35 Dinniss, *Cyber Warfare and the Laws of War*, pp. 215-226.

36 اللجنة الدولية للصليب الأحمر، "الحرب السيبرانية والقانون الدولي الإنساني".

37 الهيئة الوطنية للأمن السيبراني، "الضوابط الأساسية للأمن السيبراني ECC-2:2024"، ص 13-25؛ الهيئة الوطنية للأمن السيبراني، "ضوابط الأمن السيبراني للأنظمة الحساسة CSCC-1:2019"، ص 11-13.

38 المملكة العربية السعودية، نظام حماية البيانات الشخصية.

39 Schmitt (ed.), *Tallinn Manual 2.0*, Rules 102-104.

40 Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rules 14-21.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

نحو جوهري غير عابر، مع قابلية الأثر للامتداد إلى أشخاص مدنيين أو أعيان أو خدمات مدنية محمية. وهذه الصيغة لا تزعم أنها قاعدة ملزمة بذاتها، لكنها تقدم إطارًا لتشغيل القواعد القائمة في الوقائع السيبرانية.[41]

المبحث الثاني: تشغيل معيار الضرر السيبراني المحمي في ضوء مبادئ القانون الدولي الإنساني

بعد أن حدد المبحث السابق محل الإشكال في الضرر السيبراني المحمي، ينتقل هذا المبحث إلى اختبار المعيار داخل القواعد العملية للقانون الدولي الإنساني. فالقيمة الحقيقية للمعيار لا تظهر في تعريفه المجرد، بل في قدرته على توجيه تطبيق مبادئ التمييز والتناسب والاحتياطات عند التعامل مع أنظمة رقمية مدنية أو مزدوجة الاستخدام. ومن ثم يعالج المبحث أولًا أثر البيئة السيبرانية في تشغيل هذه المبادئ، ثم يناقش خصوصية البنية التحتية المدنية والأنظمة مزدوجة الاستخدام، قبل أن يخلص إلى أن الحاجة ليست إلى إعلان فراغ القواعد القائمة، بل إلى تطوير تفسيري منضبط يجعل هذه القواعد قادرة على إدراك الضرر الوظيفي الجوهري.

المطلب الأول: التمييز والتناسب والاحتياطات في البيئة السيبرانية

إذا كان معيار الضرر السيبراني المحمي يحدد متى يكون الأثر السيبراني ذا اعتبار إنساني، فإن مبادئ القانون الدولي الإنساني تحدد كيف ينبغي التعامل معه. وأول هذه المبادئ هو التمييز بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية. غير أن تطبيق التمييز في البيئة السيبرانية لا يقف عند تسمية النظام المستهدف، بل يتطلب فهم وظيفته الفعلية. فالخادم أو الشبكة أو نظام التحكم قد يبدو في الظاهر بنية تقنية واحدة، لكنه قد يحمل وظائف مدنية وعسكرية متداخلة. لذلك لا بد من تحليل الاستخدام والوظيفة والأثر، لا الاكتفاء بالموقع أو الملكية أو التصنيف التقني.[42]

والتمييز في هذا السياق يقتضي سؤالين. الأول: هل النظام أو البيانات أو الوظيفة المستهدفة تسهم إسهامًا فعالًا في العمل العسكري؟ والثاني: هل يحقق تعطيلها ميزة عسكرية محددة؟ فإذا لم يكن الجوابان متوافرين، بقيت الحماية المدنية قائمة. وإذا توافرا، لم تنته المسألة؛ لأن الانتقال إلى وصف الهدف العسكري لا يرفع واجبات التناسب والاحتياطات. وهذه نقطة مهمة في العمليات السيبرانية، لأن أثر العملية قد يتجاوز الهدف المحدد إلى خدمات مدنية متصلة به.[43]

أما التناسب فيقتضي موازنة الميزة العسكرية المتوقعة مع الأضرار العرضية المتوقعة على المدنيين والأعيان المدنية. وفي البيئة السيبرانية ينبغي أن تشمل الأضرار العرضية ليس فقط القتل والتدمير المادي، بل كذلك التعطيل الجوهري لوظائف مدنية أساسية متى كان متوقعًا. فإذا كانت عملية سيبرانية ضد نظام عسكري ستؤدي، بسبب بنية الشبكة المشتركة، إلى تعطيل مستشفيات أو شبكات مياه أو نظم إنذار مدني، فلا يصح تجاهل هذا الأثر بحجة أنه غير مادي. معيار الضرر السيبراني المحمي يجعل هذا الأثر جزءًا من حساب التناسب.[44]

ولا يعني ذلك أن كل ضرر وظيفي يحسم عدم المشروعية. فالتناسب بطبيعته موازنة، وقد توجد ميزة عسكرية كبيرة مع أثر مدني محدود وقابل للتدارك. غير أن إدخال الضرر الوظيفي في الحساب يمنع التحايل على الحماية. فلو قصرنا التناسب على الإصابات والتدمير المادي فقط، أمكن لطرف النزاع أن يشل منظومة مدنية كاملة من خلال بياناتها وأنظمتها دون أن يظهر في حسابه ضرر ذو وزن. وهذا يناقض الغاية الإنسانية من القاعدة.[45]

41 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 5-9.

42 البروتوكول الإضافي الأول، المادة 48.

43 البروتوكول الإضافي الأول، المادة 52 (2).

44 البروتوكول الإضافي الأول، المادة 51(5)(ب)؛ Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rule 14.

45 Sandoz, Swinarski and Zimmermann, *Commentary on the Additional Protocols*, pp. 683-688.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

أما الاحتياطات، فهي المجال الذي يظهر فيه معيار الضرر السيبراني المحمي بأوضح صوره. فالطرف الذي يخطط لعملية سيبرانية يجب أن يتحقق من طبيعة النظام المستهدف، وأن يقدر نطاق الاتصال الشبكي، وأن يختبر احتمال انتقال الأثر، وأن يختار الوسيلة الأقل إضرارًا بالمدنيين متى كان ذلك ممكنًا. وفي العمليات الحركية قد يكون نطاق الانفجار أو الإصابة محدودًا نسبيًا بخصائص السلاح والمكان، أما في العمليات السيبرانية فقد تكون الحدود أقل وضوحًا، لأن البرمجية أو الأمر الرقمي قد يتفاعل مع أنظمة غير مقصودة أو ينتقل إلى شبكات أخرى.[46]

ومن ثم ينبغي أن تشمل الاحتياطات أسئلة تقنية وقانونية معًا: هل النظام معزول أم متصل؟ هل يخدم وظيفة مدنية؟ هل توجد بدائل مدنية؟ هل يمكن تقليل مدة التعطيل؟ هل يمكن تصميم العملية بحيث تصيب وظيفة عسكرية محددة دون إتلاف البيانات المدنية؟ هل يمكن عكس الأثر بعد تحقق الميزة العسكرية؟ ولا يعني ذلك أن يحل القانوني محل الخبير الفني، بل أن يكون التقدير القانوني مبنيًا على فهم كاف للتبعية التقنية والامتداد المحتمل للأثر.[47]

وتظهر المسألة في مثال نظام الاتصالات. إذا استخدم جزء من شبكة اتصالات مدنية لدعم عمليات عسكرية، فقد يغري ذلك باستهداف الشبكة كلها. لكن معيار الضرر السيبراني المحمي يفرض تحليلًا أدق: ما الجزء الذي يسهم في العمل العسكري؟ هل يمكن عزله؟ هل تعطيل الشبكة كلها سيحرم المدنيين من الاتصال بالطوارئ أو الإنذار أو الخدمات الطبية؟ هل يوجد توقيت أقل ضررًا؟ وهل الميزة العسكرية المتوقعة من التعطيل الشامل تبرر الأثر المدني؟ بهذا لا يكتفي التحليل بوصف الشبكة بأنها مزدوجة الاستخدام، بل يسأل عن حدود الوظيفة العسكرية داخلها وحدود الضرر المدني المتوقع.[48]

ويصدق ذلك أيضًا على البيانات. فإذا كانت البيانات العسكرية مخزنة داخل منظومة مختلطة تضم بيانات مدنية، فإن استهداف كامل المنظومة بالحذف أو التشفير أو التعطيل قد يثير إشكالًا في التمييز والتناسب والاحتياطات. لا يكفي أن يقال إن وجود بعض البيانات العسكرية يجعل كل البيانات هدفًا عسكريًا. كما لا يصح أن يقال إن وجود بيانات مدنية يحظر كل عملية. الحل في اختبار الوظيفة، والفصل الممكن، والأثر المتوقع، والبدائل المتاحة.[49]

ويكشف هذا عن أن المعيار المقترح لا يحل محل المبادئ، بل يمدها بمادة تحليلية. فالتمييز يحتاج إلى فهم ما الذي يستهدف فعليًا. والتناسب يحتاج إلى تقدير ماذا سيترتب على ذلك. والاحتياطات تحتاج إلى معرفة ما الذي يمكن فعله لتقليل الضرر. وفي كل هذه المراحل، لا يجوز أن يكون غياب الدمار المادي سببًا لاستبعاد التعطيل الوظيفي الجوهري من الاعتبار.[50]

المطلب الثاني: الأنظمة مزدوجة الاستخدام والبنية التحتية المدنية

تعد الأنظمة مزدوجة الاستخدام من أعقد مواضع العمليات السيبرانية؛ لأنها تكشف التداخل بين المدني والعسكري داخل بنية رقمية واحدة. فقد تستخدم شبكة اتصالات مدنية لنقل أوامر عسكرية، أو تعتمد قوة عسكرية على بنية سحابية تجارية، أو تستخدم جهة عسكرية خدمة مدنية في جزء من عملياتها. وفي المقابل، يعتمد المدنيون على الشبكة ذاتها في المستشفيات والتعليم والإغاثة والاتصال. هذا التداخل لا يسمح بتبسيط المسألة إلى حماية مطلقة أو استهداف مطلق.[51]

46 البروتوكول الإضافي الأول، المادة 57؛ Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rules 15-21.

47 Schmitt (ed.), *Tallinn Manual 2.0*, Rule 113.

48 Dinniss, *Cyber Warfare and the Laws of War*, pp. 230-235.

49 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 9.

50 Gisel, Rodenhäuser and Dörmann, "Twenty Years On".

51 Schmitt (ed.), *Tallinn Manual 2.0*, Rules 100-102.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

والقاعدة العامة في القانون الدولي الإنساني أن العين المدنية تفقد حمايتها من الهجوم في حدود تحولها إلى هدف عسكري، أي حين تسهم، بحسب صياغة المادة 52(2) من البروتوكول الإضافي الأول، "إسهامًا فعالًا في العمل العسكري"، ويحقق تدميرها أو تعطيلها أو تحييدها "ميزة عسكرية محددة" في الظروف القائمة.[52] لكن تطبيق هذه القاعدة على الأنظمة الرقمية يتطلب عناية خاصة. فالاستهداف السيبراني قد لا يدمر العين، بل يعطل وظيفة داخلها أو يفسد بيانات أو يمنع الوصول. ومن ثم ينبغي أن يظل وصف الهدف العسكري مرتبطًا بالوظيفة العسكرية المحددة لا بالبنية كلها كلما كان الفصل ممكنًا.

ومعيار الضرر السيبراني المحي يضيف هنا فائدة عملية. فهو يطلب من التحليل أن يحدد الوظيفة المدنية المتأثرة لا أن يكتفي ببيان أن النظام مزدوج الاستخدام. فإذا كان تعطيل جزء من النظام سيصيب خدمة طوارئ مدنية، أو يمنع ضخ المياه، أو يوقف نظام مستشفى، فإن هذا الأثر يدخل في تقدير التناسب والاحتياطات حتى لو كان النظام يخدم وظيفة عسكرية في جانب منه. أما إذا أمكن عزل الوظيفة العسكرية أو تعطيلها مؤقتًا دون المساس الجوهري بالخدمة المدنية، فإن اختيار التعطيل الشامل يصبح أكثر صعوبة في التبرير.[53]

ولا تخفى صعوبة ذلك في الواقع العملي. فالطرف المهاجم قد لا يملك دائمًا معرفة كاملة ببنية النظام، وقد يستخدم الخصم البنية المدنية لإخفاء نشاط عسكري أو لحماية عملياته. غير أن هذه الصعوبة لا تلغي الواجبات. فهي قد تؤثر في تقدير المعقولية والمعلومات المتاحة وقت القرار، لكنها لا تمنح ترخيصًا مفتوحًا. والقانون الدولي الإنساني لا يطلب علمًا يقينيًا بكل الآثار، لكنه يوجب تحققًا معقولًا في ضوء المعلومات المتاحة وقت اتخاذ القرار، واتخاذ الاحتياطات الممكنة لتجنب الأضرار المدنية أو تقليلها.[54]

ويزداد الأمر تعقيدًا في البنية التحتية الحرجة. فشبكات الكهرباء والمياه والاتصالات والصحة والنقل تتداخل فيها المصالح المدنية والعسكرية. ولذلك فإن العمليات السيبرانية ضدها قد تكون مغرية عسكريًا، لكنها شديدة الخطر إنسانيًا. فالعملية التي تعطل الكهرباء في مدينة لا تعطل الإنارة فقط، بل قد تعطل المستشفيات، ومحطات المياه، وأنظمة الاتصال، وسلاسل الغذاء والدواء. والعملية التي تضرب الاتصالات لا تمنع أوامر عسكرية فقط، بل قد تمنع المدني من طلب الإسعاف أو تلقي إنذار أو الوصول إلى معلومات إخلاء.[55]

وتقدم واقعة Viasat/KA-SAT مثالًا صالحًا لاختبار هذا التحليل دون تحميلها تكييفًا قضائيًا نهائيًا. فقد أعلن الاتحاد الأوروبي أن هجومًا سيبرانيًا استهدف شبكة الاتصالات الفضائية Viasat/KA-SAT قبل ساعة تقريبًا من بدء الغزو الروسي لأوكرانيا في 24 فبراير 2022، وأنه أدى إلى اضطرابات اتصالات أثرت في سلطات عامة وشركات ومستخدمين في أوكرانيا وعدد من الدول الأوروبية.[56] ولا يراد من استحضار هذه الواقعة تقرير كل آثارها القانونية، وإنما بيان أن استهداف بنية اتصالات ذات استخدامات متداخلة قد يثير في الوقت ذاته أسئلة الهدف العسكري، والضرر المدني، وقابلية الامتداد، وصعوبة عزل الوظيفة العسكرية عن الوظائف المدنية. فهنا لا يكفي السؤال عما إذا كانت البنية محل الاستهداف ذات قيمة عسكرية، بل يلزم أيضًا فحص الوظائف المدنية التي تحملها، ودرجة التعطيل، وقابلية امتداد الأثر إلى مستخدمين مدنيين خارج النطاق العسكري المقصود.

---

52 البروتوكول الإضافي الأول، المادة 52 (2).

53 Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rules 7-10 and 14-21.

54 Sandoz, Swinarski and Zimmermann, *Commentary on the Additional Protocols*, pp. 680-688.

55 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 4-6.

56 Council of the European Union, "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union", Press Release, 10 May 2022.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

ومن ثم لا يصح أن ينظر التناسب إلى كل خدمة منفصلة عن غيرها. في البيئة السيبرانية، الضرر قد يكون شبكيًا ومركبًا. تعطيل خدمة واحدة قد يؤدي إلى سلسلة آثار في خدمات أخرى. وهذا ما يجعل قابلية الأثر للامتداد أحد عناصر معيار الضرر السيبراني المحمي. فكلما كان النظام مترابطًا، وكانت آثار تعطيله قادرة على الانتقال إلى وظائف مدنية متعددة، ارتفعت الحاجة إلى تحقق أدق واحتياطات أقوى.[57]

وفي هذا السياق، لا بأس من استحضار التجربة السعودية بوصفها مؤشرًا على مركزية حماية الأنظمة الحرجة. فالضوابط الوطنية للأمن السيبراني في المملكة تميز بين الضوابط الأساسية والضوابط الخاصة بالأنظمة الحساسة، وتؤكد الصمود، واستمرارية الأعمال، وحماية الأصول المعلوماتية والتقنية. وهذه اللغة التنظيمية، وإن كانت تعمل في زمن السلم وداخل نطاق وطني، تكشف منطقًا مهمًا: أن الخطر الرقمي لا يقاس دائمًا بمجرد الاختراق، بل بقدرته على تعطيل وظائف حيوية. وهذه الفكرة ذاتها تساعد، على مستوى القانون الدولي الإنساني، في فهم لماذا ينبغي إدخال الوظيفة المدنية في معيار الضرر السيبراني المحمي.

لكن يجب أن يبقى هذا التوظيف محدودًا. فالقانون الوطني للأمن السيبراني لا يحدد مشروعية الهجوم في النزاع المسلح الدولي، ولا يغير قواعد التمييز أو التناسب أو الاحتياطات. وإنما يقدم شاهدًا على أن الدول نفسها، في تنظيمها الداخلي، لم تعد ترى الأمن السيبراني شأنًا تقنيًا منعزلًا، بل شأنًا مرتبطًا بالمصالح الحيوية والخدمات الأساسية. وهذا يعزز الحجة المنهجية للبحث دون أن يحول الدراسة إلى بحث في النظام السعودي للأمن السيبراني.[59]

وتظهر قيمة المعيار أيضًا عند التعامل مع الشركات التقنية والجهات المدنية التي تدير بنى يعتمد عليها أطراف النزاع والمدنيون معًا. فقد تكون البنية مملوكة لقطاع خاص، لكنها تؤدي وظيفة مدنية أو عسكرية أو مختلطة. الملكية، هنا، ليست حاسمة. العبرة بالوظيفة والأثر. وهذا يتفق مع منطق القانون الدولي الإنساني الذي لا يجعل الحماية المدنية قائمة على مالك العين فحسب، بل على طبيعتها واستخدامها ومساهمتها في العمل العسكري.[60]

وقد يقال إن توسيع الاعتداد بالوظيفة المدنية سيقيد العمليات العسكرية السيبرانية على نحو مبالغ فيه. والجواب أن المعيار لا يحظر الاستهداف المشروع، بل يمنع تجاهل الأثر المدني. فإذا كان النظام يسهم فعلًا في العمل العسكري، وكانت الميزة العسكرية محددة، وكانت الأضرار المدنية المتوقعة غير مفرطة، واتخذت الاحتياطات الممكنة، فقد لا تكون العملية غير مشروعة لمجرد وجود أثر مدني محدود. أما إذا كان الضرر المدني الوظيفي واسعًا أو متوقعًا أو قابلًا للامتداد، فلا يصح إسقاطه من الحساب لأنه لم يتحول إلى ركام مادي.[61]

ويبدو هذا التوازن هو الأقرب إلى طبيعة القانون الدولي الإنساني. فهو لا يطلب من أطراف النزاع الامتناع عن كل عملية ذات أثر مدني، لكنه يلزمهم بأن يجعلوا المدنيين ووظائفهم الأساسية حاضرين في قرار الاستهداف. ومعيار الضرر السيبراني المحمي لا يفعل أكثر من ترجمة هذا الالتزام إلى لغة تصلح للفضاء السيبراني، حيث يمكن للضرر أن يظهر في صورة توقف وظيفة أو فقد بيانات أو انقطاع خدمة قبل أن يظهر في صورة تدمير شيء.[62]

المطلب الثالث: من فراغ القواعد إلى الحاجة إلى تطوير تفسيري منضبط

---

57 Schmitt (ed.), *Tallinn Manual 2.0*, Rule 113 and commentary.

58 الهيئة الوطنية للأمن السيبراني، "الضوابط الأساسية للأمن السيبراني ECC-2:2024"؛ الهيئة الوطنية للأمن السيبراني، "ضوابط الأمن السيبراني للأنظمة الحساسة CSCC-1:2019".

59 الهيئة الوطنية للأمن السيبراني، "الضوابط الأساسية للأمن السيبراني ECC-2:2024"، ص 13-25.

60 البروتوكول الإضافي الأول، المادة 52؛ Schmitt (ed.), *Tallinn Manual 2.0*, Rule 100.

61 Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rule 14.

62 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 8-9.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

تنتهي بعض الكتابات إلى القول إن الحرب السيبرانية تكشف حاجة القانون الدولي الإنساني إلى اتفاقية جديدة. وهذه النتيجة قد تبدو جذابة؛ لأنها تعد بحل واضح لمشكلة معقدة. غير أن الجزم بها على إطلاقه لا يخلو من تعجل. فالمشكلة ليست أن القواعد القائمة لا تصلح أبدًا، بل أن تشغيلها في البيئة السيبرانية يحتاج إلى تفسير أدق، وإلى مواقف دولية أكثر وضوحًا، وإلى تطوير تدريجي يراعي خصوصية الضرر الرقمي دون أن يهدم البنية العامة للقانون الدولي الإنساني.[63]

فالقول بالحاجة إلى تطوير لا يعني القول بالفراغ. والقول بقابلية القواعد القائمة للتطبيق لا يعني الاكتفاء بتكرارها دون اجتهاد. بين هذين الطرفين يقع الخيار الأكثر اتزانًا: تطوير تفسيري منضبط. والمقصود به قراءة القواعد القائمة، ولا سيما التمييز والتناسب والاحتياطات وحماية الأعيان المدنية، قراءة تستوعب البيانات والوظائف الرقمية والبنية التحتية الشبكية، من غير أن تدعي إنشاء قواعد جديدة خارج النصوص والعرف والمبادئ العامة.[64]

وتتجلى الحاجة إلى هذا التطوير في ثلاث مسائل. الأولى هي تحديد معنى "الهجوم" في البيئة السيبرانية. فإذا قصر الهجوم على العمليات التي تحدث دمارًا ماديًا، خرجت صور خطيرة من التعطيل الوظيفي. وإذا وسع ليشمل كل عملية رقمية، فقدت القاعدة معناها. لذلك يكون الأجدى أن يربط التحليل بين الهجوم والأثر المتوقع على الأشخاص أو الأعيان أو الوظائف المدنية الجوهرية.[65]

والمسألة الثانية هي وضع البيانات المدنية. لا يكفي أن يترك الأمر لعبارة عامة عن الأعيان، ولا أن يفترض أن كل البيانات محمية كالأشياء المادية. المطلوب موقف أكثر تدرجًا: البيانات قد تكون محلًا لاعتداد قانوني خاص حين يكون المساس بها مساسًا بوظيفة مدنية محمية أو حين يؤدي إلى أثر إنساني جوهري. وهذا لا يلغي الفروق بين البيانات والأعيان، لكنه يمنع أن تكون الفروق الشكلية ذريعة لإهدار الحماية.[66]

أما المسألة الثالثة فهي الاحتياطات التقنية. فالقانون الدولي الإنساني يطلب احتياطات عملية ممكنة، وفي البيئة السيبرانية تتطلب الإمكانات العملية معرفة تقنية وتقييمًا لاحتمالات الانتشار والتعافي والبدائل. ولذلك ينبغي أن تتطور ممارسات التخطيط القانوني والعسكري بحيث لا ينفصل المستشار القانوني عن الخبير التقني. فالتحقق من الهدف في عملية سيبرانية لا يكون بالنظر إلى خريطة فقط، بل بفهم شبكة واتصالات وتبعيات وبيانات ووظائف.[67]

وتسند فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها هذا الاتجاه في حدودها العامة لا بوصفها قضية سيبرانية. فقد أكدت الفتوى أهمية المبادئ الأساسية للقانون الدولي الإنساني عند النظر في وسائل وأساليب حرب غير مألوفة، وهو ما يدعم منهجيًا عدم تجميد قواعد الحماية عند الوسائل التقليدية. ولا تفيد هذه الفتوى في حسم المسائل السيبرانية بذاتها، وإنما تفيد في دعم الفكرة المنهجية الأوسع، وهي أن مبادئ القانون الدولي الإنساني لا تتجمد عند وسيلة قتالية معينة.[68]

وقد يسهم مشروع تالين 3.0، ومواقف الدول، ووثائق اللجنة الدولية للصليب الأحمر، في تعميق هذا التطوير. غير أن القيمة الحقيقية لا تكون في انتظار وثيقة واحدة تحسم كل شيء، بل في تراكم فهم قانوني أكثر دقة. فالفضاء السيبراني يتغير بسرعة،

63 سعود، "الحرب السيبرانية"، ص 100-108.

64 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، جنيف، 2011؛ النظام الأساسي لمحكمة العدل الدولية، المادة 38.

65 Schmitt (ed.), *Tallinn Manual 2.0*, Rule 92.

66 "Gisel, Rodenhäuser and Dörmann, "Twenty Years On.

67 Schmitt (ed.), *Tallinn Manual 2.0*, Rule 113.

68 International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, para. 86.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

وأي اتفاقية تفصيلية قد تصبح ناقصة أمام التقنية التالية. ولذلك يبدو أن الجمع بين القواعد العامة الراسخة والتفسير الوظيفي المنضبط أكثر قدرة على الاستمرار من الاكتفاء بالدعوة إلى صك جديد بوصفه الحل الوحيد.[69]

ولا يعني ذلك استبعاد الحاجة المستقبلية إلى قواعد إضافية أو إعلانات تفسيرية أو مواقف دولية مشتركة. فقد تكون هناك حاجة إلى توضيح حماية البيانات المدنية، وإلى ضبط واجبات الحذر في الأنظمة المترابطة، وإلى تأكيد عدم جواز استهداف الخدمات المدنية الأساسية بعمليات سيبرانية تؤدي إلى آثار إنسانية واسعة. لكن هذه الإضافات ينبغي أن تبنى على القانون القائم لا أن تبدأ من فرضية عجزه الكامل.[70]

وهنا تظهر ثمرة معيار الضرر السيبراني المحمي. فهو لا يقدم نفسه بديلًا عن الاتفاقيات ولا عن العرف، بل أداة تفسيرية تساعد في اختبار الوقائع. فإذا عرضت واقعة تتعلق بتشفير بيانات مستشفى، أو تعطيل نظام إنذار، أو إفساد نظام توزيع المياه، فإن المعيار يوجه الأسئلة: ما المصلحة المدنية؟ ما وظيفة النظام؟ ما درجة التعطيل؟ هل الأثر عابر أم جوهري؟ هل يمتد إلى مدنيين أو خدمات أخرى؟ هل العملية مرتبطة بالنزاع المسلح؟ وكيف تدخل هذه العناصر في التمييز والتناسب والاحتياطات؟[71]

وبهذا المعنى، لا يعود البحث إلى السؤال التقليدي في خاتمته، بل يتجاوزه. فالإجابة ليست: نعم، ينطبق القانون الدولي الإنساني، أو لا، لا ينطبق. الإجابة الأشد دقة هي أن القانون ينطبق متى توافرت شروطه، لكنه لا يعمل بفعالية إلا إذا استطاع أن يتعرف على الضرر الرقمي في صورته الوظيفية. وإذا أخفق في ذلك، فلن يكون سبب الإخفاق بالضرورة قصور النصوص، بل قصور القراءة التي ظلت تبحث عن آثار مادية تقليدية في بنية حرب رقمية معاصرة.[72]

ولذلك فإن منهج هذه الدراسة يرفض الانحرافين معًا: انحراف الاطمئنان الذي يكرر المبادئ العامة دون اختبار، وانحراف القطيعة الذي يعلن انتهاء صلاحية القانون القائم. والبديل هو قراءة معيارية وظيفية تظل وفية لبنية القانون الدولي الإنساني، لكنها لا تنكر أن حماية المدنيين اليوم تمر عبر طبقات رقمية أصبحت شرطًا لسلامتهم وخدماتهم وكرامتهم في زمن النزاع.

الخاتمة

انطلقت هذه الدراسة من ملاحظة أن النقاش حول العمليات السيبرانية والقانون الدولي الإنساني لا يزال، في جانب معتبر منه، يدور حول سؤال عام عن مدى الانطباق، مع أن الصعوبة العملية الأشد لا تكمن في أصل هذا الانطباق وحده، بل في تحديد الضرر السيبراني الذي يستحق أن يعامل بوصفه ضررًا محميًا. ولذلك أعادت الدراسة ترتيب محل النزاع من أساسه: من سؤال "هل ينطبق القانون؟" إلى سؤال "كيف يتعرف القانون على الضرر الرقمي حين يمس البيانات والبنية التحتية المدنية دون تدمير مادي ظاهر؟".

وقد خلصت الدراسة إلى أن القانون الدولي الإنساني يملك، من حيث الأصل، قابلية معتبرة للتطبيق على العمليات السيبرانية أثناء النزاعات المسلحة، ولا سيما من خلال مبادئ التمييز والتناسب والاحتياطات. غير أن هذه القابلية لا تكفي بذاتها إذا ظل الضرر محصورًا في التصور المادي التقليدي. فالبيئة السيبرانية تفرض الاعتداد بالتعطيل الوظيفي الجوهري؛ أي التعطيل

69 NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual 3.0 Project", Tallinn, launched 2021. 2017 ويلاحظ أن المشروع مشروع تحديث لطبعة . وليس صكًا نهائيًا منشورًا وقت كتابة هذه الدراسة

70 اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية"، ص 9.

71 Dinniss, *Cyber Warfare and the Laws of War*, pp. 215-235.

72 Geneva Academy of International Humanitarian Law and Human Rights and International Committee of the Red Cross, *International Humanitarian Law and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities during Armed Conflict*, Geneva, 2025.

Volume 11 issue 4
N:65 August 2026
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

الذي يمس خدمة مدنية أو بيانات لازمة لعمل مرفق مدني أو ينتج أثرًا إنسانيًا على المدنيين، ولو لم يظهر في صورة تهدم أو احتراق أو تلف عيني مباشر.

كما خلصت الدراسة إلى أن البيانات المدنية لا ينبغي أن تعامل بمنطق مطلق. فهي ليست دائمًا عينًا مدنية مستقلة بالمعنى التقليدي، لكنها ليست خارج الحماية لمجرد عدم ماديتها. المعيار الأدق هو وظيفتها وأثر المساس بها. فإذا كانت البيانات شرطًا لعلاج أو إغاثة أو إنذار أو مياه أو كهرباء أو حماية مدنية، فإن إتلافها أو تغييرها أو حجبها قد يدخل في الضرر المحمي متى بلغ أثره حدًا جوهريًا.

وانتهت الدراسة كذلك إلى أن البنية التحتية المدنية في العصر الرقمي لا تفهم من خلال عناصرها المادية وحدها. فالمستشفى، ومحطة الكهرباء، وشبكة المياه، وأنظمة النقل والاتصال، تقوم على طبقات رقمية تجعلها قادرة على أداء وظيفتها. ولذلك فإن استهداف هذه الطبقات قد يكون، من حيث الأثر الإنساني، استهدافًا للوظيفة المدنية نفسها. ومن هنا جاءت أهمية إدخال الوظيفة المدنية ودرجة التعطيل وقابلية الامتداد في حساب التناسب والاحتياطات.

وتتمثل المساهمة العلمية للدراسة في اقتراح معيار مركب للضرر السيبراني المحمي يقوم على خمسة عناصر: طبيعة المصلحة المدنية المتأثرة، ووظيفة النظام أو البيانات المستهدفة، ودرجة التعطيل، وقابلية الأثر للامتداد، وموقع العملية من النزاع المسلح. وليس المقصود بهذا المعيار إنشاء قاعدة جديدة مستقلة، بل تقديم طريقة منضبطة لتشغيل القواعد القائمة في وقائع لا تستجيب دائمًا للصور التقليدية للضرر.

وبناء على ذلك، تنتهي الدراسة إلى أن الطريق الأجدى لا يتمثل في الاكتفاء بالدعوة العامة إلى اتفاقية جديدة، ولا في ترديد أن القواعد القائمة كافية بذاتها، بل في تطوير تفسيري منضبط يستند إلى القانون الدولي الإنساني القائم، ويستفيد من مواقف اللجنة الدولية للصليب الأحمر ودليل تالين وممارسات الدول، مع إيلاء عناية خاصة لحماية البيانات المدنية والبنية التحتية الرقمية والأنظمة مزدوجة الاستخدام. فالقانون الدولي الإنساني لا يفقد قيمته لأن الحرب تغير أدواتها؛ وإنما يضعف أثره حين تعجز القراءة القانونية عن إدراك الأثر الإنساني للتعطيل الرقمي في الأنظمة والبيانات والوظائف المدنية المحمية.

قائمة المصادر والمراجع

اتفاقية بودابست بشأن الجريمة المعلوماتية، مجلس أوروبا، 2001.

البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977.

بونة، ياسين محمد أحمد، "الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية"، مجلة شمال إفريقيا للنشر العلمي، مج 1، ع 4، 2023، ص 154-168، DOI: 10.65414/najsp.v1i4.88.

رابح، منزر، ودرويش، سعيد، "الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول"، مجلة صوت القانون، مج 8، ع 1 ، 2021، ص 538-557.

سعود، يحيى ياسين، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، مج 4، ع 4، 2018، ص 80-108، DOI: 10.21608/JLAW.2018.45192.

المقريف، نورية الساعدي، "الحرب السيبرانية في ضوء أحكام القانون الدولي العام"، مجلة أبحاث قانونية، جامعة سرت، ع 14 ، ديسمبر 2022، ص 1-30.

المملكة العربية السعودية، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم م/19 بتاريخ 9/2/1443هـ، والمعدل بالمرسوم الملكي رقم م/148 بتاريخ 5/9/1444هـ.

النظام الأساسي لمحكمة العدل الدولية، 1945.

الهيئة الوطنية للأمن السيبراني، "الضوابط الأساسية للأمن السيبراني ECC-2:2024"، الرياض، 2024.

الهيئة الوطنية للأمن السيبراني، "ضوابط الأمن السيبراني للأنظمة الحساسة CSCC-1:2019"، الرياض، 2019.

اللجنة الدولية للصليب الأحمر، "الحرب السيبرانية والقانون الدولي الإنساني"، أسئلة وأجوبة، جنيف، 2013.

اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، جنيف، تشرين الثاني/نوفمبر 2019.

اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، جنيف، 2011.

Council of the European Union, "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union", Press Release, 10 May 2022.

Cybersecurity and Infrastructure Security Agency (CISA), "Cyber-Attack Against Ukrainian Critical Infrastructure", ICS Alert IR-ALERT-H-16-056-01, 2016, last revised 20 July 2021.

Dinniss, Heather Harrison, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012.

Geneva Academy of International Humanitarian Law and Human Rights and International Committee of the Red Cross, *International Humanitarian Law and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities during Armed Conflict*, Geneva, 2025.

Gisel, Laurent, Rodenhäuser, Tilman, and Dörmann, Knut, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", International Review of the Red Cross, Vol. 102, Issue 913, 2020, pp. 287–334, DOI: 10.1017/S1816383120000387.

Henckaerts, Jean-Marie, and Doswald-Beck, Louise, *Customary International Humanitarian Law*, Vol. I: Rules, Cambridge University Press, Cambridge, 2005.

International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996.

National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*, HC 414, London, 2017.

NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual 3.0 Project", Tallinn, launched 2021.

Sandoz, Yves, Swinarski, Christophe, and Zimmermann, Bruno (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC/Martinus Nijhoff, Geneva, 1987.

Schmitt, Michael N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, pp. 885-937.

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