

الهجمات السيبرانية كسلاح جديد في النزاعات المسلحة:

دراسة في شرعية الممارسات الروسية والأوكرانية على ضوء قواعد القانون الدولي

Cyberattacks as a New Weapon in Armed Conflicts:

An Assessment of the Legality of Russian and Ukrainian Practices under International Law

مسينيسا زبوجي^{*1}

Massinissa ZEBOUDJI^{*1}

¹ جامعة محمد الصديق بن يحيى، جيجل (الجزائر)، massinissa.zeboudji@univ-jijel.dz

تاريخ النشر: 2026/06/11

تاريخ القبول: 2026/04/15

تاريخ الإرسال: 2025/08/13

ملخص:

تهدف هذه الدراسة إلى تحليل الطبيعة القانونية للهجمات السيبرانية باعتبارها وسيلة مستحدثة في النزاعات المسلحة، مع دراسة مدى التزام كل من روسيا وأوكرانيا بالقواعد القانونية الدولية ذات الصلة، ولا سيما مبادئ التمييز والتناسب والضرورة العسكرية.

تخلص الدراسة إلى أن الإطار القانوني الدولي الحالي لا يزال قاصراً عن ضبط الهجمات السيبرانية بوصفها أعمالاً عدائية، خاصة في ظل صعوبات التكيف القانوني والإسناد، الأمر الذي يستوجب تطوير آليات قانونية دولية أكثر مرونة، قادرة على ضمان احترام قواعد حماية المدنيين أثناء النزاعات المسلحة.

الكلمات المفتاحية: الهجمات السيبرانية، روسيا، أوكرانيا النزاعات المسلحة، القانون الدولي.

Abstract:

This study aims to analyze the legal nature of cyberattacks as an emerging means in armed conflicts, while assessing the extent to which Russia and Ukraine comply with relevant international legal rules, particularly the principles of distinction, proportionality, and military necessity. It concludes that the current international legal framework remains inadequate to regulate cyberattacks as hostile acts, especially given the difficulties of legal qualification and attribution, which calls for the development of more flexible international legal mechanisms capable of ensuring respect for the rules protecting civilians during armed conflicts.

Keywords: Cyberattacks, Russia, Ukraine, Armed Conflicts, International Law.

1. مقدمة

شهدت العقود الأخيرة تحولاً جذرياً في طبيعة النزاعات المسلحة، إذ أضحت الفضاء السيبراني مسرحاً جديداً للصراع، تزامناً مع استهداف الهجمات الرقمية للبنى التحتية وأنظمة الدفاع، وقد تجسد هذا التحول بشكل واضح في النزاع الروسي-الأوكراني منذ فيفري 2022، الذي اتسم بتناغم العمليات العسكرية التقليدية مع الهجمات السيبرانية المكثفة.

تثير الهجمات السيبرانية إشكاليات قانونية معقدة، إذ لا تزال خارج نطاق التنظيم الصريح في معاهدات القانون الدولي الإنساني، خاصة فيما يتعلق بتكييفها القانوني، وتحديد مسؤولية الدول أو الجهات الفاعلة، ومدى التزامها بمبادئ التمييز والتناسب والضرورة العسكرية.

من خلال ما تقدم، يمكن أن نطرح الإشكالية التالية: ما هي الطبيعة القانونية للهجمات السيبرانية ضمن النزاعات المسلحة وفق قواعد القانون الدولي؟ وكيف يمكن تحديد مدى قانونية الممارسات السيبرانية التي قامت بها روسيا وأوكرانيا في النزاع الحالي؟

يندرج ضمن هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية:

1. ما هو المفهوم القانوني للهجمات السيبرانية وطبيعتها ضمن النزاعات المسلحة؟
2. ما مدى فاعلية الجهود الدولية لتأطير الهجمات السيبرانية ضمن القانون الدولي الإنساني؟
3. كيف يمكن تحديد قانونية العمليات السيبرانية الروسية والأوكرانية خلال النزاع المسلح وفق القانون الدولي العام والقانون الدولي الإنساني؟

تتطلب الدراسة من فرضية مفادها أن الهجمات السيبرانية تمثل وسيلة مستحدثة في النزاعات المسلحة يصعب تأطيرها قانونيا في ظل القواعد الحالية، مما يثير تحديات في دراسة مشروعيتها، ويستدعي تطوير آليات قانونية دولية أكثر وضوحا لحماية المدنيين. تسعى الدراسة إلى:

1. تحليل الطبيعة القانونية للهجمات السيبرانية باعتبارها وسيلة مستحدثة في النزاعات المسلحة.
2. تحليل مدى التزام روسيا وأوكرانيا بالقواعد القانونية الدولية ذات الصلة، لا سيما مبادئ التمييز والتناسب والضرورة العسكرية.
3. بيان كفاية الإطار القانوني الدولي القائم أو الحاجة إلى تطوير آليات قانونية أكثر تخصصا.

تعتمد الدراسة على المنهج التحليلي القانوني، مدعوما بالمنهج المقارن والوصفي، من خلال مراجعة اتفاقيات جنيف وبروتوكولها الإضافي الأول، دليل تالين 2.0، وممارسات الطرفين المتنازعين في النزاع الروسي-الأوكراني، وقد قسمت الدراسة إلى:

- الإطار القانوني للهجمات السيبرانية في النزاعات المسلحة.
- التكيف القانوني للعمليات السيبرانية الروسية والأوكرانية خلال النزاع المسلح.

2. الإطار القانوني للهجمات السيبرانية في النزاعات المسلحة

أصبحت الهجمات السيبرانية أحد أبرز أدوات النزاع المسلح المعاصر، وهو ما يفرض ضرورة ضبطها قانونيا ضمن منظومة القانون الدولي.

1.2 مفهوم الهجمات السيبرانية:

يعد فهم الطبيعة القانونية للهجمات السيبرانية أساسا ضروريا لتحديد مدى خضوعها لأحكام القانون الدولي.

1.1.2 الطبيعة القانونية للهجمات السيبرانية:

وفق اللجنة الدولية للصليب الأحمر، الهجوم السيبراني هو استخدام تقنيات متقدمة للتأثير السلبي على أنظمة الحواسيب أو شبكاتها عبر إفساد البيانات، تضليل المعلومات، إضعاف الأداء، تعطيل البرمجيات، أو حرمان المستخدمين من الخدمات، وقد يصل إلى إتلاف المعدات المرتبطة بها¹.

عرفها عبد القادر محمد فهمي بأنها: " هجمات تستخدم فيها الدول أو الفاعلون من غير الدول الشبكات الحاسوبية وأنظمة المعلومات لتعطيل أو إضعاف أنظمة الخصوم والسيطرة عليها، وقد تصل إلى تدمير جزئي أو كلي للبنية التحتية الرقمية، خاصة المرتبطة بالقدرات العسكرية، مما يشكل تهديدا خطيرا للأمن القومي"².

بناء على ما تقدم، يمكن القول أن الهجمات السيبرانية ترتبط ارتباطا وثيقا باستخدام الحواسيب وشبكة الإنترنت كوسائل لتنفيذ تهديدات وتحقيق أهداف ذات طابع عسكري أو سياسي، كما أنها تستخدم أيضا من قبل جماعات غير حكومية في إطار أنشطة إجرامية أو إرهابية، بهدف تحقيق مكاسب سياسية أو اقتصادية.

2.1.2 تطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية:

على الرغم من أن قواعد الحرب التقليدية المنصوص عليها في اتفاقيات جنيف الأربع لعام 1949 وبروتوكولاتها الإضافية لا تنطبق بصفة مباشرة على هذا النوع، ولا يوجد إلى اليوم تشريع دولي خاص أو معاهدة دولية صريحة تنظم هذه الهجمات، إلا أن ذلك لا يعني أن الفضاء السيبراني يعمل في فراغ قانوني مطلق.

فقد أكد التقريران الصادران عامي 2013 و2015 عن مجموعة الخبراء الحكوميين التابعة للأمم المتحدة المعنية بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، أن قواعد القانون الدولي العام، ولا سيما ميثاق الأمم المتحدة، قابلة للتطبيق على الفضاء السيبراني من حيث المبدأ، وذلك من خلال آليات التكيف والامتداد، وليس عبر إطار قانوني خاص أو موحد ينظم الهجمات السيبرانية أو يعرف العدوان السيبراني وضوابط الرد عليه بشكل صريح³.

هو ما يفضي إلى القول بأن القانون الدولي الإنساني يطبق على الحرب السيبرانية متى ما توافرت حالة نزاع مسلح، وأسفرت الهجمات الإلكترونية عن تدمير للبنى التحتية أو ألحقت أضراراً بالمدنيين، كتعطيل أنظمة المواصلات أو المستشفيات، أو التسبب في خسائر في الأرواح البشرية⁴.

في هذا السياق، أكدت محكمة العدل الدولية، في رأيها الاستشاري بشأن مشروعية التهديد باستخدام الأسلحة النووية أو استخدامها، أن مبادئ وقواعد القانون الدولي الإنساني المنطبقة في النزاعات المسلحة تسري على جميع أشكال الحروب وجميع أنواع الأسلحة، بما في ذلك الأسلحة المستقبلية⁵.

يشير تقرير اللجنة الدولية للصليب الأحمر لعام 2015، المعنون بـ"القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، إلى أن أي لجوء إلى القوة، سواء كان

سيبرانيا أو ماديا ، يبقى خاضعا لميثاق الأمم المتحدة وقواعد القانون الدولي المنظم للجوء إلى القوة، ويؤكد التقرير أن ثمة قيودا قانونية قائمة بموجب القانون الدولي، في حال لجوء الدول أو الجماعات المسلحة إلى شن اعتداءات سيبرانية خلال نزاع مسلح⁶.

لعل الاستجابة الدولية الأبرز لمعالجة الهجمات السيبرانية تجسدت في إصدار ما يعرف بـ دليل تالين الذي يبحث في مدى قابلية تطبيق قواعد القانون الدولي على الفضاء السيبراني، وقد تناول هذا الدليل جملة من المفاهيم ذات الصلة، مثل الحصار السيبراني، والهجمات المصحوبة باستخدام القوة، مشيرا إلى أن هذه المفاهيم تخضع لأحكام القانون الدولي الإنساني، سواء نفذت في البر أو الجو أو البحر، ويقر الدليل بأن الهجمات الإلكترونية قد ترقى، في ظروف معينة، إلى مستوى النزاع المسلح، خاصة عندما تخلف آثارا مدمرة⁷.

بالتالي فإن تطبيق مبدأ الضرورة العسكرية على هذه الهجمات يواجه صعوبات، أبرزها صعوبة التمييز بين الأهداف العسكرية والأعيان المدنية، خاصة في المنشآت مزدوجة الاستخدام، فضلا عن تعقيد تقدير وجود بدائل أقل ضررا، ويقتضي هذا المبدأ أن تكون القوة المستخدمة ضرورية لتحقيق هدف عسكري مشروع، دون أن تتطوي على دوافع انتقامية⁸.

كما أن تطبيق مبدأ التناسب على الهجمات السيبرانية يواجه أيضا تحديات كبيرة، بسبب صعوبة برمجة العمليات لقياس الأضرار المتوقعة بدقة مقارنة بالميزة العسكرية المرجوة، وغياب التقدير اللحظي والتدخل البشري المباشر، ويظل الالتزام قائما بعدم إلحاق أضرار مفرطة بالخصم، ما يتطلب قيادة عسكرية خبيرة لتحقيق التوازن بين النصر العسكري وتقليل الضرر⁹.

أما بالنسبة لمبدأ التمييز بين المقاتلين والمدنيين في سياق الهجمات السيبرانية، فيعد تطبيقه من أكثر المسائل تعقيدا مقارنة بالهجمات التقليدية، فغالبا ما يكون منفذ الهجوم السيبراني بعيدا جغرافيا عن الهدف، أحيانا بمئات الكيلومترات، الأمر الذي يجعل من عملية

التمييز بين الأفراد المقاتلين والمدنيين مسألة شديدة الصعوبة، إن لم تكن مستحيلة في بعض الحالات¹⁰.

يزداد الأمر تعقيدا عند محاولة التمييز بين الأهداف العسكرية والمدنية، إذ إن الأنظمة الحاسوبية العسكرية غالبا ما تكون متصلة، كليا أو جزئيا، بشبكات مدنية وتجارية، فالهجوم على بنية تحتية عسكرية عبر الفضاء السيبراني قد يؤدي، بحكم طبيعة الترابط الشبكي، إلى آثار غير مباشرة على المدنيين والمنشآت المدنية¹¹.

فعلى سبيل المثال، قد يؤدي استهداف الشبكات المعلوماتية التابعة للقوات المسلحة في دولة ما إلى تعطيل خدمات أساسية يعتمد عليها السكان المدنيون، مثل مياه الشرب، أو الكهرباء، أو الرعاية الصحية، نظرا لاشتراك هذه الخدمات في نفس البنية التحتية الرقمية المستهدفة.

2.2 الجهود الدولية لتأطير الهجمات السيبرانية ضمن القانون الدولي الإنساني:

سعت الأمم المتحدة إلى ضمان الاستخدام السلمي والأمن للتكنولوجيا وشبكات المعلومات، وذلك من خلال إشراك عدد من أجهزتها الرئيسية، مثل الجمعية العامة، ومجلس الأمن، ويمكن إبراز تلك الجهود على النحو الآتي:

1.2.2 الجمعية العامة للأمم المتحدة:

اعتمدت الجمعية العامة للأمم المتحدة عام 2006 الاستراتيجية العالمية لمكافحة الإرهاب، وأصدرت عدة توصيات وقرارات لتعزيز الأمن السيبراني ورفع وعي الدول بالتحديات التي تستوجب التعاون الدولي¹²، من أبرزها:

❖ القرار 63/55 والقرار 121/56 اللذان يضعان أسسا قانونية لمكافحة إساءة استخدام تكنولوجيا المعلومات في الأغراض الإجرامية.

❖ القرار 239/57 الذي يدعو إلى بناء ثقافة عالمية للأمن السيبراني.

❖ القرار 199/58 المتعلق بحماية البنى التحتية الحيوية للمعلومات وتعزيز ثقافة أمن المعلومات على الصعيد الدولي.

❖ القرار 187/73 بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية.

❖ القرار 174/74 الذي يشدد على أهمية المساعدة التقنية وبناء القدرات الوطنية من أجل دعم التعاون الدولي في مكافحة الجريمة السيبرانية، خاصة من خلال تبادل المعلومات والخبرات.

❖ القرار 211/64 الصادر عام 2010، والذي يحث الدول على مراجعة وتحديث تشريعاتها وهيئاتها المعنية بمكافحة الجرائم السيبرانية، كما يدعو إلى تعزيز ثقافة أمنية عالمية في الفضاء الرقمي¹³.

تولي الجمعية العامة للأمم المتحدة اهتماما متزايدا بالأمن السيبراني، داعية إلى حوار دولي لإبرام اتفاقية تنظم استخدام الفضاء السيبراني وتحد من الهجمات، رغم الصعوبات الناتجة عن التفاوت في القدرات التكنولوجية بين الدول، ومنذ 2004، أنشأت مجموعة خبراء حكوميين (GGE) لدراسة تأثير تكنولوجيا المعلومات على الأمن القومي والعسكري¹⁴، وفي 2009 أطلقت مبادرة (IMPACT) لتعزيز التعاون الدولي، كما شكلت في 2010 فريق خبراء دوليا لمعالجة مشكلات الهجمات السيبرانية، في تقريرها، حذرت مجموعة الخبراء من غياب التوجيه الدولي وأوصت بتعزيز التعاون بين الدول لتنظيم استخدام تكنولوجيا المعلومات والاتصالات، وتبادل الخبرات والمعلومات لبناء الثقة وتعزيز الأمن السيبراني، بالإضافة إلى دعم بناء القدرات في الدول النامية تقنيا وتشريعيا¹⁵.

أوصت مجموعة الخبراء الحكوميين في 2015، بتطبيق القانون الدولي على الفضاء السيبراني، ورفض استهداف البنى التحتية السيبرانية أو دعم ذلك، مع تحميل الدول مسؤولية الهجمات المنطلقة من أراضيها، وفي 28 ديسمبر 2019، اعتمدت الجمعية العامة قرارا

للشروع في إعداد معاهدة دولية لمكافحة الاستخدام الإجرامي لتكنولوجيا المعلومات والاتصالات عبر لجنة خبراء حكوميين، ورغم تباين المواقف حول الحاجة لاتفاقية جديدة، تعكس المبادرة وعي المجتمع الدولي بخطورة الاستخدام غير الآمن للفضاء السيبراني، على غرار اتفاقية بودابست لعام 2001 بشأن الجريمة السيبرانية¹⁶.

2.2.2 مجلس الأمن:

أولى مجلس الأمن التابع للأمم المتحدة اهتماما متزايدا بتنامي التهديدات المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات في أعمال الإرهاب والهجمات السيبرانية، وذلك من خلال إصداره مجموعة من القرارات ذات الصلة، من أبرزها:

1. القرار 2017/2341، دعا فيه مجلس الأمن الدول الأعضاء إلى إنشاء وتعزيز الشراكات الوطنية والإقليمية والدولية مع مختلف الأطراف المعنية، سواء من القطاع العام أو الخاص، بهدف تبادل المعلومات والخبرات المتعلقة بالتصدي للهجمات الإرهابية التي تستهدف البنى التحتية الحيوية، والحد من آثارها السلبية.
2. القرار رقم 2017/2370، حث فيه المجلس الدول الأعضاء على تعزيز التعاون فيما بينها لمنع الإرهابيين من الحصول على الأسلحة عبر استغلال تكنولوجيا المعلومات والاتصالات، مع التأكيد على ضرورة احترام حقوق الإنسان والحريات الأساسية، والامتثال التام للالتزامات الناشئة عن القانون الدولي¹⁷.

3. التكييف القانوني للعمليات السيبرانية الروسية والأوكرانية خلال النزاع

المسلح

يمثل النزاع الروسي الأوكراني مثالا عمليا بارزا لتوظيف الهجمات السيبرانية كجزء من العمليات الحربية، ويسمح هذا السياق بدراسة مدى التزام الطرفين بقواعد القانون الدولي، وتحديد مشروعية ما نسب إليهما من أعمال سيبرانية هجومية أو دفاعية.

1.3 بحث مشروعية الهجمات السيبرانية الروسية في النزاع المسلح مع أوكرانيا:

تعرضت أوكرانيا منذ اندلاع النزاع لهجمات سيبرانية واسعة النطاق من الجانب الروسي، أثارت جدلاً قانونياً بشأن مشروعيتها، ومن هنا تبرز أهمية تحليل مدى توافق هذه الهجمات مع مبادئ القانون الدولي العام، وقواعد القانون الدولي الإنساني.

1.1.3 انتهاك روسيا لمبادئ القانون الدولي العام من خلال الهجمات السيبرانية:

استخدمت روسيا الهجمات السيبرانية منذ غزو أوكرانيا في فيفري 2022، كأداة استراتيجية استهدفت البنية التحتية المدنية والعسكرية، في انتهاك للقانون الدولي الإنساني، شملت الهجمات مواقع حكومية بهجمات حجب الخدمة والاختراق، ومحطات طاقة ببرمجيات مثل (Industroyer2) ما تسبب بانقطاعات كهربائية شتوية حادة، إضافة إلى شبكات الاتصالات التي أصيبت ببرمجيات خبيثة مثل (VPNFilter)، مما أثر على تدفق المعلومات الحيوية¹⁸.

الأخطر من ذلك هو استهداف القطاع الصحي، بما في ذلك المستشفيات والمنشآت الطبية، بضربات سيبرانية تزامنت مع الهجمات العسكرية التقليدية، وهو ما يشكل انتهاكاً صارخاً للمادة 8 من نظام روما الأساسي، التي تحظر الهجمات العشوائية ضد المدنيين والبنى التحتية المحمية، ويكشف عن استخدام الفضاء السيبراني كساحة موازية للعمليات العسكرية دون مراعاة للقيود الإنسانية والقانونية المفروضة في النزاعات المسلحة¹⁹.

وفقاً لمبدأ عدم استخدام القوة المنصوص عليه في المادة 4/2 من ميثاق الأمم المتحدة، فإن التهديد باستعمال القوة أو استخدامها يعد محظوراً في جميع أشكاله، وعلى الرغم من أن الصياغة الأصلية للمادة كتبت قبل بروز التهديدات السيبرانية، إلا أن الفقه القانوني والآراء الاستشارية الحديثة باتت تجمع على أن الهجمات السيبرانية التي تسبب أضراراً مادية جسيمة أو تعطل بنى تحتية حيوية على نطاق واسع كقطع الكهرباء عن المستشفيات، أو شل

مؤسسات الدولة، يمكن أن ترقى إلى مستوى القوة المسلحة، وبالتالي تشكل انتهاكا صريحا للمادة 4/2 إذا لم تكن مبررة قانونيا بأحد الاستثناءات المعترف بها، وهي الدفاع الشرعي بموجب المادة 51، أو التفويض الصريح من مجلس الأمن الدولي تحت الفصل السابع²⁰.

تطبيقا لذلك، فإن سلسلة الهجمات السيبرانية التي نسبت إلى روسيا واستهدفت مؤسسات الطاقة، والاتصالات، والقطاع الصحي في أوكرانيا، تمثل حالات قد ترقى إلى مستوى القوة أو حتى العدوان بحسب مدى الأثر والضرر الواقع، خصوصا إذا اقترنت بنية سياسية أو عسكرية لتفويض استقرار الدولة المعتدى عليها.

كما يرتبط هذا التوصيف القانوني بمبدأ عدم التدخل في الشؤون الداخلية للدول، وهو مبدأ عرفي أكدت عليه محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة عام 1986، حيث رأت المحكمة أن التدخل غير المشروع يشمل كل تدخل في الأمور التي تندرج في نطاق السيادة الداخلية للدولة، مثل اختيار النظام السياسي، أو العمليات الانتخابية، أو تشكيل الرأي العام²¹.

بناء على ذلك، فإن التدخلات الرقمية الروسية التي استهدفت منصات الإعلام الأوكراني، أو حاولت التأثير على توجهات الرأي العام عبر بث معلومات مضللة أو شن حملات تشويه إلكترونية خلال الانتخابات، تعد خرقا لهذا المبدأ، وتصنف ضمن أشكال التدخل المحظور.

2.1.3 مخالفة الهجمات الروسية لقواعد القانون الدولي الإنساني:

رغم أن القانون الدولي الإنساني يجيز استخدام القوة في النزاعات المسلحة، فإنه يفرض قيودا لحماية المدنيين، بالتالي فإن تقارير اللجنة الدولية للصليب الأحمر ومنظمة هيومن رايتس ووتش تتهم روسيا بانتهاك هذه القيود، عبر هجمات سيبرانية وعسكرية استهدفت البنية التحتية المدنية في أوكرانيا، في خرق واضح للقانون الدولي الإنساني²².

أولاً، تمثل هذه الأفعال انتهاكا لمبدأ التمييز، الذي يفرض على أطراف النزاع ضرورة التفرقة الواضحة بين الأهداف العسكرية المشروعة والأعيان المدنية المحمية²³، فقد استهدفت الهجمات السيبرانية الروسية منشآت لا تحمل طابعا عسكريا، كشبكات الكهرباء التي تعد شريان الحياة للمدنيين، خصوصا في فصول الشتاء القاسية، بالإضافة إلى المستشفيات والمرافق الصحية التي تعرضت للتعطيل بفعل هذه الهجمات، مما حال دون تقديم الخدمات الطبية الطارئة، كما شملت الأهداف المصارف والبنية المالية المدنية، رغم عدم ارتباطها بأي دور قتالي، وهو ما يتعارض مع نصوص البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977 والمادة 18 من اتفاقية جنيف الرابعة لعام 1949²⁴.

ثانياً، يلاحظ خرق واضح لمبدأ التناسب في الهجمات، الذي يمنع تنفيذ عمليات قد تؤدي إلى خسائر مفرطة في صفوف المدنيين إذا ما قورنت بالفائدة العسكرية المرجوة، الهجمات على محطات الطاقة وأنظمة المياه، فضلا عن تعطيل شبكات الاتصالات، تسببت في أضرار مدنية جسيمة طالت ملايين الأوكرانيين، في حين لم تظهر أي مبررات عسكرية حقيقية تبرر تلك الخسائر، ما يجعل هذه الأفعال مخالفة صريحة للمادة 51/ب من البروتوكول الإضافي الأول²⁵.

ثالثاً، تبرز أيضا مخالفة لمبدأ الاحتياط، الذي يفرض على القوات المتحاربة اتخاذ جميع التدابير اللازمة لتجنب إلحاق الأذى بالمدنيين عند تنفيذ الهجمات، وفيما يتعلق بالقضاء السيبراني، لم تظهر الهجمات الروسية أي مؤشرات على محاولة تقليل الآثار الجانبية أو تجنب الضرر غير الضروري، بل استخدمت أدوات إلكترونية عشوائية مثل فيروس (NotPetya) وبرمجيات أخرى شبيهة، ما يعكس غيابا كاملا لاعتبارات الحذر والاحتياط²⁶، خلافا لما نص عليه دليل تالين 2.0 بشأن تطبيق القانون الدولي على العمليات السيبرانية.

عليه، تشكل هذه الانتهاكات، مجتمعة، جرائم حرب وفقا للمادة 8 من نظام روما الأساسي للمحكمة الجنائية الدولية، كما تمثل خروقات جسيمة لقواعد النزاع المسلح في الفضاء السيبراني، وتدعو هذه الوقائع إلى تفعيل آليات المساءلة الدولية، سواء من خلال تدخل مجلس الأمن أو مباشرة اختصاص المحكمة الجنائية الدولية، وذلك لضمان محاسبة المسؤولين، تعويض الضحايا، وتحسين النزاعات المستقبلية ضد استخدام الفضاء السيبراني كساحة مفتوحة للانتهاكات.

2.3 مشروعية الدفاع السيبراني الأوكراني في إطار القانون الدولي:

بادرت أوكرانيا في مواجهة التصعيد السيبراني الروسي، إلى اعتماد آليات دفاع سيبراني مختلفة، ويقتضي ذلك بحث مدى قانونية هذه العمليات في إطار الحق في الدفاع الشرعي، مع بيان مدى احترامها لقواعد النزاع المسلح، خاصة فيما يتعلق بحماية المدنيين والبنى التحتية الحيوية.

1.2.3 مدى قانونية الدفاع السيبراني الأوكراني استنادا إلى مبدأ الدفاع الشرعي:

شرعية الرد الأوكراني على الهجمات السيبرانية الروسية تقوم على مبدأ الدفاع الشرعي وفق المادة 51 من ميثاق الأمم المتحدة، التي تجيز الرد في حال وقوع عدوان مسلح²⁷ ويعتبر الهجوم السيبراني عدوانا مسلحا إذا تسبب بأضرار مادية جسيمة، مثل فقدان الأرواح أو تعطيل البنية التحتية الحيوية، كما أشار دليل تالين 2.0²⁸.

تستند أوكرانيا في هذا السياق، إلى هذه المادة لتبرير ردودها السيبرانية ضد روسيا، خصوصا بعد أن استهدفت الهجمات الروسية محطات توليد الطاقة، وأنظمة الاتصالات، والمستشفيات، مما عرض السكان المدنيين للخطر، لكن يبقى تطبيق المادة 51 على الفضاء السيبراني معقدا قانونيا، ويشترط أن تكون الاستجابة الأوكرانية متناسبة وضرورية وموجهة

لصد الهجوم فقط، دون إلحاق ضرر مفرط بالمدنيين أو المنشآت غير العسكرية، مع مراعاة واجب إخطار مجلس الأمن بالإجراءات الدفاعية المتخذة.

تثير مشاركة المدنيين الأوكرانيين، بل وحتى متطوعين دوليين، في ما يعرف بجيش تكنولوجيا المعلومات (IT Army)²⁹ إشكالا قانونيا، بالنظر إلى تعارض هذا السلوك مع قواعد القانون الدولي الإنساني، فوفقا للمادة 3/51 من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977، يفقد المدنيون الحماية التي يتمتعون بها إذا شاركوا مباشرة في الأعمال العدائية³⁰، بينما لا يتمتع المتطوعون في هذا السياق بوضع المقاتلين الشرعيين كما هو مبين في المادة 43 من نفس البروتوكول، لعدم انتمائهم إلى القوات المسلحة الرسمية أو خضوعهم لنظام عسكري منضبط، وإلى جانب المخاطر الفردية التي قد تطل هؤلاء المدنيين، تطرح مسألة مسؤولية الدولة الأوكرانية عن أفعالها، خاصة إذا ثبت وجود تنسيق أو دعم مباشر لهم، وهو ما قد يؤدي إلى اتهامات بخرق مبدأ سيادة الدول في حال استهدفت منشآت مدنية روسية دون تمييز، من جهة أخرى، تطرح إشكالية التناسب وعدم التمييز في الهجمات السيبرانية المضادة التي يشنها هؤلاء، إذ يجب أن تراعي أوكرانيا المبادئ الأساسية للقانون الإنساني، خصوصا مبدأ التمييز (المادة 48) والتناسب، لضمان ألا تؤدي تلك الهجمات إلى أضرار مفرطة بالمدنيين أو إلى انتهاك القانون الدولي العرفي، لا سيما ما يتعلق بعدم استخدام القوة في العلاقات الدولية.

على الرغم من أن حق الدفاع الشرعي عن النفس إذا ثبت أن الهجمات الروسية ترقى إلى مستوى العدوان المسلح يمكن أن يبرر لجوء أوكرانيا إلى الرد السيبراني، إلا أن إشراك المدنيين وصعوبة ضبط التناسب في بيئة تقنية معقدة مثل الفضاء السيبراني يجعلان من مشروعية هذا الدفاع محل نقاش قانوني دولي.

2.2.3. التزامات أوكرانيا باحترام قواعد النزاع المسلح في الرد السيبراني:

يلتزم أطراف النزاع حتى في حالات الدفاع الشرعي باحترام قواعد القانون الدولي الإنساني بشكل صارم، بما في ذلك في العمليات السيبرانية³¹، التزمت أوكرانيا إلى حد كبير بمبادئ القانون الدولي الإنساني في ردها السيبراني على الهجمات الروسية، حيث اقتصر معظم عملياتها على أهداف عسكرية أو حكومية روسية مشروعة، مع تجنب الهجمات الواسعة ضد المنشآت المدنية³².

غير أن الوضع يزداد تعقيدا مع وجود جيش تكنولوجيا المعلومات (IT Army) الذي يضم متطوعين مدنيين محليين ودوليين، يطرح هذا الأمر إشكالية قانونية حول مدى انضباط هذه المجموعات تحت القيادة المسؤولة، كما ينص عليه البروتوكول الإضافي الأول لاتفاقيات جنيف، وقد يعرض ذلك أوكرانيا للمساءلة الدولية إذا تم ربطها بأعمال غير قانونية تنفذها هذه الجماعات³³.

كما أن مشاركة المدنيين المباشرة في العمليات العدائية السيبرانية قد تفقد لهم الحماية التي يكفلها لهم القانون الدولي الإنساني، وفقا للمادة 3/51 من البروتوكول المذكور، مما يجعلهم أهدافا مشروعة ويخل بمبدأ التمييز بين المقاتلين والمدنيين³⁴.

بالتالي، لا يقتصر التحدي القانوني أمام أوكرانيا على إثبات شرعية ردها، بل يشمل أيضا ضمان امتثال جميع الأطراف المشاركة بما في ذلك المتطوعون المدنيون لقواعد النزاع المسلح، والتحقق من خضوعها للمساءلة القانونية لتفادي أي انتهاكات قد تخل بالموثوق الدولية المنظمة للنزاعات، سواء التقليدية أو السيبرانية.

4. خاتمة

وسعت الهجمات السيبرانية مفهوم النزاع المسلح ليشمل الفضاء الرقمي، حيث يمكن إحداث أضرار جسيمة بالبنى التحتية دون استخدام السلاح التقليدي، كما أظهر النزاع الروسي الأوكراني تعقيد تكييفها قانونيا وتحديد مسؤولية أطرافها وفق القانون الدولي الإنساني، عليه تم التوصل إلى النتائج التالية:

1. قد تتدرج الهجمات السيبرانية تحت مفهوم الهجوم في القانون الدولي الإنساني متى ما خلفت آثارا مادية ملموسة أو أثرت على قدرة الدولة المستهدفة في تسير بنيتها الحيوية، وهو ما يجعلها خاضعة لمبادئ التمييز، والتناسب، والضرورة العسكرية.
2. رغم الجهود الدولية، لا يزال هناك فراغ تشريعي واضح على مستوى تنظيم الهجمات السيبرانية في سياق النزاعات المسلحة، خصوصا مع عدم وجود اتفاقية دولية خاصة تنظم هذا النوع من الحروب.
3. أبرزت الممارسات الروسية في الفضاء السيبراني خلال النزاع مع أوكرانيا انتهاكا واضحا لمبادئ القانون الدولي.
4. في المقابل، فإن الدفاع السيبراني الأوكراني قد يجد له تبريرا في إطار مبدأ الدفاع الشرعي، إلا أنه يظل مشروطا بالتقيد الكامل بقواعد النزاع المسلح، لا سيما حماية المدنيين.

بناء على ما سبق، نقترح:

1. ضرورة تطوير اتفاقية دولية ملزمة تنظم الهجمات السيبرانية في النزاعات المسلحة، وتحدد شروط استخدامها، ومتى تعد جريمة حرب، أو عدوانا مسلحا.
2. إدراج الهجمات السيبرانية ضمن نطاق اختصاصات المحاكم الجنائية الدولية متى ما توافرت أركان الجريمة، لردع استخدامها ضد المدنيين.

3. تحديث مناهج تدريب القوات المسلحة في الدول على احترام قواعد القانون الدولي الإنساني في المجال السيبراني، شأنه شأن ميادين القتال الأخرى.
4. دعم جهود المنظمات الدولية، وعلى رأسها اللجنة الدولية للصليب الأحمر والجمعية العامة للأمم المتحدة، في تطوير فهم قانوني مشترك للهجمات السيبرانية ضمن النزاعات المسلحة.

5. الهوامش والمراجع

- ¹International Committee of the Red Cross.2011 . International humanitarian law and the challenges of contemporary armed conflicts, Report prepared for the 31st International Conference of the Red Cross and Red Crescent, Geneva, p.58, disponible sur <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf>
- ²كاوجة محمد الصغير. 2022. "الهجمات السيبرانية بين الواقع وسبل المواجهة"، مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 03، كلية العلوم الإنسانية والاجتماعية، ص.111.
- ³اللجنة الدولية للصليب الأحمر. أكتوبر 2015. " تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر المنظم في الفترة ما بين 8 إلى 10 كانون الأول / ديسمبر 2015 بجنيف، أكتوبر 2015، ص. ص. 55.54 الوثيقة رقم IC/15/XXX 32
- ⁴إيهاب خليفة. 2017. القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الانترنت. دار العربي للنشر والتوزيع. ص. 165.
- ⁵محكمة العدل الدولية. 8 تموز / يوليو 1996مشروعية التهديد بالأسلحة النووية أو استخدامها، الرأي الاستشاري رقم 95. متوفر على <https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>
- ⁶اللجنة الدولية للصليب الأحمر، " تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، مرجع سابق، ص. 55.
- ⁷بن صابر بلقاسم، حيدرة محمد، "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مرجع سبق ذكره، ص. 202.
- ⁸يحيى ياسين سعود. 2018. " الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، مجلة الدراسات القانونية والسياسية المجلد 4، العدد 04، ص. 96.
- ⁹نسيب نجيم. 2021. "الحرب السيبرانية من منظور القانون الدولي الإنساني"، المجلة النقدية للقانون والعلوم السياسية، المجلد 16، العدد 04، ص. 231.

¹⁰ أحمد عبيس نعمة الفتلاوي. 2016. "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة كلية القانون للعلوم القانونية والسياسية، العدد 4، السنة الثامنة، ص. 636.

¹¹ بلقاسم بن صابر، محمد حيدرة، مرجع سبق ذكره، ص. 202. انظر أيضا: عادل عبد الصادق. 2016. أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، ص. 96.

¹² خالد حسن أحمد لطفي. 2019. الإرهاب الإلكتروني (آفة العصر الحديث والآليات القانونية للمواجهة). دار الفكر الجامعي. ص. 149.

¹³United Nations General Assembly. 2010. Resolution 64/211 on reviewing and updating national legislation and institutions to combat cybercrime and promote a global culture of cybersecurity [A/RES/64/211]. disponible sur: <https://documents.un.org/> consulté le 27/04/2025 à 09h12.

¹⁴ أحمد زكريا الباسوسي. 2023. "الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة"، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 24، العدد 04، ص. 171.

¹⁵ محمد عادل محمد عسكر. 2021. "وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم: دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية 2013-2017"، مجلة البحوث القانونية والإقتصادية، المجلد 33، العدد الأول، ص. 303.

¹⁶ هالة أحمد الرشيد. 2013. "الطابع التشريعي لقرارات مجلس الأمن: دراسة حالة قرارات مكافحة الإرهاب"، المجلة المصرية للقانون الدولي، العدد 19، ص. 159-158.

¹⁷ United Nations Security Council. 2017. Resolution 2370 on enhancing cooperation to prevent terrorists from acquiring weapons and cyber threats [S/RES/2370]. disponible sur: <https://documents.un.org/> consulté le 27/04/2025 à 09h :48.

¹⁸United Nations, Security Council. 2024. Verbatim Record of the 9714th Meeting: Maintaining International Peace and Security (S/PV.9714). disponible sur: <https://docs.un.org/ar/S/PV.9714> consulté le 14/06/2025 à 00h02.

¹⁹GREENBERG Andy. 2023. «Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike ». disponible sur: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/?utm_source=chatgpt.com consulté le 14/06/2025 à 1h14.

²⁰ELACHEACHE Ishak. 2019. « Les cyber-attaques face au jus ad bellum, Etude et commentaires sur le manuel de Tallinn », Revue des Sciences Juridiques et Politiques, V. 10, N° 03, p. 981.

²¹ محكمة العدل الدولية. 1986. القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية). متوفر على:

chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://legal.un.org/icjsummaries/documents/arabic/st_leg_serfl_add6.pdf

²²Human Rights Watch. 2022. "Russia: Unlawful attacks on civilian infrastructure. Retrieved from <https://www.hrw.org>

²³International Committee of the Red Cross.2023. The principles of humanity and military necessity, Geneva: ICRC. Retrieved from ICRC website: chrome-

extension://efaidnbmnnnibpcajpcgglefindmkaj/https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf?utm_source=chatgpt.com

²⁴Human Rights Watch. 2022. Russia: Unlawful attacks on civilian infrastructure, opcit.

²⁵اللجنة الدولية للصليب الأحمر. 2019. القانون الدولي الإنساني والعمليات السيبرانية أثناء النزاعات المسلحة. متوفر على <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>

²⁶اللجنة الدولية المستقلة المعنية بأوكرانيا. 2024. تقرير مقدم إلى الجمعية العامة في دورتها التاسعة والسبعين ، الوثيقة رقم (A/79/549)، <https://docs.un.org/en/A/79/549>

²⁷منظمة الأمم المتحدة. 1945. ميثاق منظمة الأمم المتحدة. 26 جوان 1945، دخل حيز التنفيذ في 24 أكتوبر 1945.

²⁸Michael N. Schmitt, op cit, p. 27.

²⁹بعد وقت قصير من اندلاع الحرب، أطلقت الحكومة الأوكرانية نداء إلى كل خبراء التكنولوجيا في جميع أنحاء العالم لاستخدام مهاراتهم بهدف تطوير قدراتهم في شن حرب معلوماتية ضد روسيا، وسرعان ما استجاب المتطوعون المتحمسون، وفي غضون شهر واحد أصبح هناك نحو 300 ألف مشترك، للمزيد راجع <https://al-ain.com/article/ukraines-it-army-gamble>

³⁰اللجنة الدولية للصليب الأحمر. 1977. البروتوكول الإضافي الأول لاتفاقيات جنيف الأربع لعام 1949، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، 8 جوان 1977

³¹Tallinn Manual 2.0. 2017. On the International Law Applicable to Cyber Operations, Rule 100–102.

³²The Atlantic Council. 2023. Ukraine's Cyber Defense Strategy: Between Compliance and Necessity. https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/?utm_source=chatgpt.com

³³انظر المادة 43 من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977، المرجع السابق.

³⁴انظر المادة 3/51 من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977، المرجع السابق.