ICRC

القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة

ورقة موقف اللجنة الدولية للصليب الأحمر

مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي

تشرين الثاني/ نوفمبر 2019

المحتويات

ملخص تنفيذي

- **أصبحت العمليات السيبرانية حقيقة واقعة في النزاعات المسلحة المعاصرة**. وينتاب اللجنة الدولية للصليب الأحمر (اللجنة الدولية) القلق إزاء **التكلفة البشرية المحتملة** لزيادة استخدام العمليات السيبرانية خلال النزاعات المسلحة.
- **ترى اللجنة الدولية أن القانون الدولي الإنساني يحد من استخدام العمليات السيبرانية خلال النزاعات المسلحة** مثلما يحد من استخدام الأسلحة والوسائل والأساليب الأخرى للقتال في أي نزاع مسلح، جديدة كانت أو قديمة.
- إن التأكيد على انطباق القانون الدولي الإنساني على الحرب السيبرانية لا يضفي الشرعية عليها، تمامًا مثلما لا يضفي الشرعية على أي شكل آخر من أشكال القتال. **ويظل أي لجوء من الدول إلى القوة – ذات الطابع السيبراني أو الحركي - محكومًا بميثاق الأمم المتحدة وقواعد القانون الدولي العرفي ذات الصلة**، لاسيما حظر اللجوء للقوة. ويجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاء السيبراني كما في جميع المجالات الأخرى.
- أصبح من المهم الآن **للمجتمع الدولي أن يؤكد على انطباق القانون الدولي الإنساني** على استخدام العمليات السيبرانية خلال النزاعات المسلحة. وتدعو اللجنة الدولية أيضًا إلى عقد **مناقشات بين الخبراء الحكوميين وغيرهم من الخبراء حول *كيفية* انطباق قواعد القانون الدولي الإنساني الحالية** وما إذا كان القانون الحالي ملائمًا وكافيًا. **وترحب اللجنة الدولية في هذا الصدد بالمناقشات الحكومية الدولية الجارية** حاليًا في إطار عمليتين مكلفتين من قبل الجمعية العامة للأمم المتحدة.
- أظهرت الأحداث التي جرت على مدار السنوات الأخيرة أن العمليات السيبرانية، سواء في نطاق النزاع المسلح أو خارجه، يمكن أن تعطل عمل البنية التحتية المدنية الأساسية وتعيق تقديم الخدمات الأساسية للسكان المدنيين. **وتتمتع البنية التحتية المدنية في سياق النزاع المسلح بالحماية ضد الهجمات السيبرانية من خلال مبادئ وقواعد القانون الدولي الإنساني الحالية**، وخاصة مبادئ التمييز والتناسب والاحتياطات أثناء الهجوم. ويوفر القانون الدولي الإنساني أيضًا حماية خاصة للمستشفيات والأعيان التي لا غنى عنها لبقاء السكان المدنيين، من بين أمور أخرى.
- **يُحظر خلال النزاعات المسلحة استخدام الأدوات السيبرانية التي تنشر الضرر وتتسبب فيه دون تمييز**. ويمكن من الناحية التكنولوجية تصميم بعض الأدوات السيبرانية واستخدامها لاستهداف أعيان محددة فقط وإلحاق الضرر بها مع عدم انتشار الضرر أو التسبب به عشوائيًا. ومع ذلك، فإن الترابط الذي يميز الفضاء السيبراني يعني أن أي شيء مرتبط بالإنترنت يمكن استهدافه من أي مكان في العالم، وأن الهجوم السيبراني على نظام معين قد يكون له عواقب على أنظمة أخرى مختلفة. ونتيجة لذلك، هناك خطر حقيقي من عدم تصميم الأدوات السيبرانية أو استخدامها وفقًا للقانون الدولي الإنساني، سواء عن قصد أو عن طريق الخطأ.
- **يحدد تفسير الدول لقواعد القانون الدولي الإنساني الحالية مدى الحماية التي يوفرها القانون الدولي الإنساني من آثار العمليات السيبرانية.** وينبغي للدول على وجه الخصوص أن تتخذ مواقف واضحة بشأن التزامها بتفسير القانون الدولي الإنساني للحفاظ على البنية التحتية المدنية من أي تعطل كبير وحماية البيانات المدنية. وسيؤثر تحديد مثل هذه المواقف أيضًا على تقييم ما إذا كانت القواعد الحالية كافية أم هناك حاجة لقواعد جديدة. وإذا رأت الدول أن هناك حاجة لاستحداث قواعد جديدة، فعليها **أن تستند إلى الإطار القانوني الحالي وتعززه، بما في ذلك القانون الدولي الإنساني.**

أولًا: مقدمة

إن استخدام العمليات السيبرانية خلال النزاعات المسلحة حقيقة واقعة.[1] فبينما أقر عدد ضئيل من الدول علانية بإجراء مثل هذه العمليات، فمن المرجح أن يزداد استخدامها مستقبلًا مع تزايد عدد الدول التي تطور قدرات سيبرانية لأغراض عسكرية.

علاوة على ذلك، هناك تقدم تكنولوجي كبير في القدرات السيبرانية الهجومية: إذ أظهرت أحداث السنوات الأخيرة أن العمليات السيبرانية يمكن أن تؤثر بشكل خطير على البنية التحتية المدنية وقد تتسبب في إلحاق أضرار بشرية.

وتهتم اللجنة الدولية، وفقًا لمهمتها وولاتيها، في المقام الأول باستخدام العمليات السيبرانية باعتبارها وسائل وأساليب للقتال خلال نزاع مسلح، وبالحماية التي يوفرها القانون الدولي الإنساني ضد آثار استخدامها.

[1] يستخدم مصطلح "العمليات السيبرانية خلال النزاعات المسلحة" في ورقة الموقف هذه لوصف عمليات ضد حاسوب أو شبكة أو نظام حاسوبي أو أي جهاز آخر متصل بالإنترنت، من خلال دفق بيانات، عندما تُستخدم باعتبارها وسائل وأساليب للقتال في سياق نزاع مسلح. وتعتمد العمليات السيبرانية على تكنولوجيا المعلومات والاتصالات.

وترحب اللجنة الدولية بالمناقشات الحكومية الدولية التي تجري حاليًا في إطار العمليتين المكلفتين من قبل الجمعية العامة للأمم المتحدة: فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني الارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، إذ كُلفت المجموعتان بدراسة "كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات".[2] وتقدم اللجنة الدولية ورقة الموقف هذه إلى كلتا المجموعتين لدعم مداولات الدول في هذا الصدد.

وتقتصر ورقة الموقف هذه على المسائل القانونية والإنسانية الناشئة عن استخدام العمليات السيبرانية خلال النزاعات المسلحة. ولا تتناول المسائل المتعلقة بالإطار القانوني المنطبق على العمليات السيبرانية غير المرتبطة بالنزاعات المسلحة.

ثانيًا: التكلفة البشرية المحتملة للعمليات السيبرانية

استخدمت العمليات السيبرانية خلال النزاعات المسلحة لدعم العمليات الحركية أو بجانبها. وقد يوفر استخدام العمليات السيبرانية بدائل لا تتيحها سائر وسائل وأساليب القتال، غير أنه ينطوي على مخاطر أيضًا. فمن ناحية، قد تمكن العمليات السيبرانية أطراف النزاعات المسلحة من تحقيق أهدافها دون إلحاق أضرار بالمدنيين أو التسبب في أضرار مادية بالبنية التحتية المدنية. ومن ناحية أخرى، تُبين العمليات السيبرانية الأخيرة- التي تُنفذ أساسًا خارج سياق النزاعات المسلحة- أن الجهات الفاعلة المتطورة أصبحت الآن قادرة على تعطيل تقديم الخدمات الأساسية للسكان المدنيين.

يمكن للأطراف المتحاربة التسلل إلى نظام ما عن طريق العمليات السيبرانية وجمع البيانات أو تهريبها أو تعديلها أو تشفيرها أو إتلافها. ويمكن أيضًا استخدام نظام حاسوب مخترق لتشغيل العمليات التي يسيطر عليها هذا النظام أو تغييرها أو معالجتها بطريقة أخرى. ويمكن تعطيل مجموعة متنوعة من "الأهداف" في العالم الحقيقي أو تغييرها أو إتلافها - مثل الصناعات والبنية التحتية والاتصالات السلكية واللاسلكية وأنظمة النقل أو الأنظمة الحكومية أو المالية. ونتيجة للمناقشات التي أجرتها اللجنة الدولية مع خبراء من جميع أنحاء العالم إلى جانب بحوثها الخاصة، ينتاب اللجنة الدولية القلق خاصة إزاء التكلفة البشرية المحتملة للعمليات السيبرانية ضد البنية التحتية المدنية الأساسية، بما في ذلك البنية التحتية للخدمات الصحية.[3]

وكشفت الهجمات السيبرانية على مدار السنوات الأخيرة مدى ضعف الخدمات الأساسية. وتفيد التقارير أن هذه الهجمات أصبحت أكثر تواترًا وأن حدتها تزداد بسرعة أكبر مما توقع الخبراء. وعلاوة على ذلك، لا يزال هناك مجالات لا نعرف عنها سوى القليل جدًا: القدرات والأدوات السيبرانية الأكثر تعقيدًا التي طُورت بالفعل أو الجاري تطويرها؛ كيف يمكن أن تتطور التكنولوجيا؛ ومدى اختلاف استخدام العمليات السيبرانية خلال النزاعات المسلحة عن التوجهات التي رُصدت حتى الآن.

بالإضافة إلى ذلك، تثير خصائص الفضاء السيبراني مخاوف بعينها. على سبيل المثال، تنطوي العمليات السيبرانية على خطر التصعيد وإلحاق الأضرار البشرية،إذ يصعب على الطرف المستهدف معرفة ما إذا كان المهاجم يهدف إلى جمع المعلومات الاستخباراتية أو إلحاق ضرر أكبر، مما يؤدي إلى رد فعل من الطرف المستهدف بقوة أكبر من اللازم تحسبًا لوقوع السيناريو الأسوأ.

وتنتشر الأدوات السيبرانية بطريقة فريدة. ويمكن بمجرد استخدامها الاستفادة منها لأغراض أخرى وتوظيفها على نطاق واسع من قبل الجهات الفاعلة بخلاف المطور أو المستخدم الأصلي.

ثالثًا: انطباق القانون الدولي الإنساني على العمليات السيبرانية خلال النزاعات المسلحة

ليس لدى اللجنة الدولية أي شك في أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، وبالتالي يحد من استخدامها، تمامًا مثلما ينظم استخدام الأسلحة والوسائل والأساليب الأخرى للقتال في أي نزاع مسلح، جديدة كانت أو قديمة.[4] وهذا أمر

---

[2] وثيقتا الأمم المتحدة: A/RES/73/27, OP 5; A/RES/73/266, OP 3

[3] انظر اللجنة الدولية، *The Potential Human Cost of Cyber Operations*، 2019، متاح على:
https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

4 اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2011، 31IC/11/5.1.2، ص 36-37: متاح على:
https://www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf؛ *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2015 ،32IC/15/11 ، ص 40، متاح على:

صحيح سواء إذا كان الفضاء السيبراني يعتبر مجالًا جديدًا للحرب يشبه الفضاء الجوي والبري والبحري والفضاء الخارجي، أو إذا كان مجالًا مختلفًا، لأنه مجال من صنع الإنسان في حين أن المجالات السابقة مجالات طبيعة، أم أنه ليس مجالًا في حد ذاته.

وتعتمد الدول معاهدات القانون الدولي الإنساني بهدف تنظيم النزاعات الحالية والمستقبلية. إذ أدرجت الدول - في معاهدات القانون الدولي الإنساني - قواعد تتوقع تطوير وسائل وأساليب جديدة للقتال، على افتراض أن القانون الدولي الإنساني سينطبق عليها. على سبيل المثال، إذا لم ينطبق القانون الدولي الإنساني على وسائل وأساليب القتال في المستقبل، فلن يكون من الضروري استعراض شرعية استخدام هذه الوسائل والأساليب بموجب القانون الدولي الإنساني الحالي، حسبما تقتضيه المادة 36 من البروتوكول الإضافي الأول المؤرخ 8 حزيران /يونيو 1977.

ويحظى هذا الاستنتاج بدعم قوي في فتوى محكمة العدل الدولية بعنوان "*مشروعية التهديد بالأسلحة النووية أو استخدامها*"، حيث أشارت المحكمة إلى أن المبادئ والقواعد الثابتة للقانون الدولي الإنساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع الأسلحة"، بما في ذلك" ما سيكون في المستقبل".[5] وترى اللجنة الدولية أن هذا الاستنتاج ينطبق على استخدام العمليات السيبرانية خلال النزاعات المسلحة.

وترحب اللجنة الدولية بتأكيد عدد متزايد من الدول والمنظمات الدولية على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، وتتطلع إلى إجراء مناقشات حول كيفية انطباق القانون الدولي الإنساني في هذا المجال.

وقد تقرر الدول أيضًا فرض قيود على العمليات السيبرانية بالإضافة إلى القيود الموجودة في القانون الحالي، وقد تضع قواعد تكميلية، لا سيما لتعزيز حماية المدنيين والبنية التحتية المدنية من آثار العمليات السيبرانية. وترى اللجنة الدولية أن أي قواعد جديدة يجري التفكير بشأنها ينبغي أن تستند إلى الإطار القانوني الحالي وتعززه، بما في ذلك القانون الدولي الإنساني.

وفي الحالات التي لا تشملها القواعد الحالية للقانون الدولي الإنساني، يظل المدنيون والمقاتلون محميين بما يسمى "شرط مارتنز"، مما يعني أنهم يظلون تحت حماية وسلطان مبادئ القانون القانون الدولي كما استقر بها العرف، ومبادئ الإنسانية، وما يمليه الضمير العام.[6]

ويجدر التوضيح أن التأكيد على انطباق القانون الدولي الإنساني على العمليات السيبرانية خلال النزاعات المسلحة لا يضفي الشرعية على الحرب السيبرانية أو يشجع على عسكرة الفضاء السيبراني. في الواقع، يفرض القانون الدولي الإنساني بعض القيود على عسكرة الفضاء السيبراني من خلال حظر تطوير القدرات السيبرانية العسكرية التي تنتهك القانون الدولي الإنساني[7]. وعلاوة على ذلك، يظل أي لجوء من الدول إلى القوة – ذات الطابع السيبراني أو الحركي - محكومًا بميثاق الأمم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، لا سيما حظر اللجوء للقوة. ويجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاء السيبراني كما في جميع المجالات الأخرى.

رابعًا: الحماية التي توفرها قواعد القانون الدولي الإنساني الحالية

تنظم العديد من أحكام معاهدات القانون الدولي الإنساني الحالية والقانون العرفي النزاعات المسلحة. وفيما يتعلق بالفضاء السيبراني، تحظى القواعد التي تحكم سير العمليات العدائية بأهمية خاصة، إذ تهدف هذه القواعد إلى حماية السكان المدنيين من آثار العمليات العدائية. وهي

اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2019، 33IC/19/9.7، ص 18: متاح على: https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf؛ https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.

[5] محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى ، 8 تموز/ يوليو 1996، الفقرة 86.

[6] انظر المادة 1 (2)، البروتوكول الإضافي الأول لاتفاقيات جنيف المؤرخ 8 حزيران / يونيو 1977؛ الفقرة 9 من ديباجة اتفاقية لاهاي الثانية لعام 1899؛ والفقرة 8 من ديباجة اتفاقية لاهاي الرابعة لعام 1907.

[7] انظر هنكرتس ودوزوالد- بك، *القانون الدولي الإنساني العرفي، المجلد الأول، القواعد*، اللجنة الدولية، مطبعة جامعة كامبريدج، كامبريدج، 2005 (المشار إليه فيما يلي بدراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية)، القاعدتان 70 و 71؛ انظر أيضًا المادة 36، البروتوكول الإضافي الأول.

تستند إلى مبدأ أساسي وهو مبدأ التمييز، الذي يفرض على أطراف النزاع التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية في جميع الأوقات، ومن ثم توجيه عملياتها ضد الأهداف العسكرية دون غيرها.[8]

وعلى الرغم من الترابط الذي يميز الفضاء السيبراني، يبين الفحص الدقيق لطريقة عمل الأدوات السيبرانية أنها ليست عشوائية بالضرورة. ويبدو من الناحية التقنية أن العديد من الهجمات السيبرانية التي أُبلغ عنها علانية كانت محددة الهدف إلى حد ما: إذ صممت واستخدمت بغرض استهداف أعيان محددة وإلحاق الضرر بها دون غيرها، ولم تنشر أضرارًا عشوائية أو تتسبب في حدوثها. ومع ذلك، يشكل ضمان تأثر الأعيان المستهدفة دون غيرها تحديًا تقنيًا ويتطلب تخطيطًا دقيقًا في تصميم العمليات السيبرانية واستخدامها. وتجدر الإشارة أيضًا إلى أن أي عملية سيبرانية محددة الهدف من الناحية التقنية لا تكون بالضرورة مشروعة من الناحية القانونية، إذا جرت خلال نزاع مسلح أو خارج سياقه.

وعلى الرغم من ذلك، فإن بعض الأدوات السيبرانية التي نعرفها صُممت لكي تنتشر ذاتيًا وتؤثر عشوائيًا على النظم الحاسوبية المستخدمة على نطاق واسع، وهي لا تقوم بهذه المهام عن طريق الصدفة: بل يجب أن تُدرج القدرة على الانتشار الذاتي عادةً تحديدًا في تصميم هذه الأدوات. ومع ذلك، فإن الترابط الذي يميز الفضاء السيبراني يعني أن أي شيء مرتبط بالإنترنت يمكن استهدافه من أي مكان في العالم، وأن الهجوم السيبراني على نظام معين قد يكون له عواقب على أنظمة أخرى مختلفة. ونتيجة لذلك، هناك خطر حقيقي من عدم تصميم الأدوات السيبرانية أو استخدامها وفقًا للقانون الدولي الإنساني، سواء عن قصد أو عن طريق الخطأ.

إن التأكيد على أن القانون الدولي الإنساني - بما في ذلك مبادئ التمييز والتناسب والاحتياط - ينطبق على العمليات السيبرانية خلال النزاعات المسلحة يعني أن بموجب أحكام القانون الحالي، من بين العديد من الأحكام الأخرى:

- يُحظر استخدام القدرات السيبرانية العشوائية الطابع التي تصنف على أنها أسلحة.[9]
- يُحظر توجيه الهجمات المباشرة ضد المدنيين والأعيان المدنية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.[10]
- تُحظر أعمال العنف أو التهديد به الرامية أساسًا إلى بث الرعب بين السكان المدنيين، بما في ذلك عند ارتكابها عبر وسائل أو أساليب الحرب السيبرانية.[11]
- تُحظر الهجمات العشوائية، أي الهجمات التي من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.[12]
- تُحظر الهجمات غير المتناسبة، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية. الهجمات غير المتناسبة هي تلك التي يُتوقع منها أن تسبب خسائر عرضية في أرواح المدنيين أو إصابة بهم أو أضرارًا بالأعيان المدنية أو أن تحدث خلطًا من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن تسفر عنه تلك الهجمات من ميزة عسكرية ملموسة ومباشرة.[13]
- تُبذل رعاية متواصلة في إدارة العمليات العسكرية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية، من أجل تفادي السكان المدنيين والأعيان المدنية؛ وتُتخذ جميع الاحتياطات المستطاعة عند تنفيذ الهجمات من أجل تجنب إلحاق الضرر بالمدنيين، وذلك بصفةعرضية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.[14]

---

[8] المادة 48، البروتوكول الإضافي الأول؛ القاعدتان 1 و 7، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية؛ محكمة العدل الدولية، *مشروعية التهديد بالأسلحة النووية أو استخدامها*، فتوى، 8 تموز/يوليو 1996، الفقرة 78.

[9] القاعدة 71، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[10] المواد 48 و 51 و 52، البروتوكول الإضافي الأول؛ القاعدتان 1 و 7، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[11] المادة 51 (2)، البروتوكول الإضافي الأول؛ القاعدة 2، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[12] المادة 51 (4)، البروتوكول الإضافي الأول؛ القاعدتان 11 و 12، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية. تعتبر هجمات عشوائية: أ) تلك التي لا توجه إلى هدف عسكري محدد، ب)أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد، ج) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا القانون الدولي الإنساني، ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز.

[13] المادتان 51 (5) (ب) و 57، البروتوكول الإضافي الأول؛ القاعدة 14، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[14] المادة 57، البروتوكول الإضافي الأول؛ القواعد من 15 إلى 21، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

- يُحظر مهاجمة أو تدمير أو نقل أو تعطيل الأعيان التي لا غنى عنها لبقاء السكان المدنيين، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.[15]
- يجب حماية الوحدات الطبية واحترامها، بما في ذلك عند تنفيذ العمليات السيبرانية خلال النزاعات المسلحة.[16]

بالإضافة إلى ذلك، تُتخذ جميع الاحتياطات المستطاعة لحماية المدنيين والأعيان المدنية من آثار الهجمات التي تُشن باستخدام وسائل وأساليب الحرب السيبرانية، ويجب تنفيذ هذا الالتزام أصلًا في وقت السلم.[17] وتشمل التدابير التي يمكن أخذها في الاعتبار: فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية؛ وفصل النظم الحاسوبية التي تعتمد عليها البنية التحتية الأساسية المدنية عن الإنترنت؛ والعمل على تحديد هوية البنية التحتية والشبكات السيبرانية التي تخدم بشكل خاص الأعيان المشمولة بالحماية مثل المستشفيات.[18]

خامسًا: ضرورة مناقشة *كيفية* انطباق القانون الدولي الإنساني

إن التأكيد على انطباق القانون الدولي الإنساني على العمليات السيبرانية خلال النزاعات المسلحة خطوة أولى أساسية لتجنب المعاناة الإنسانية التي يمكن أن تسببها العمليات السيبرانية أو تقليصها إلى أدنى حد ممكن. ومع ذلك، تحث اللجنة الدولية الدول أيضًا على العمل من أجل فهم مشترك *لكيفية* انطباق مبادئ القانون الدولي الإنساني وقواعده على العمليات السيبرانية، وهو أمر ضروري إذ تفرض الطبيعة المترابطة للفضاء السيبراني وطابعه الرقمي إلى حد كبير تحديات على تفسير مبادئ ومفاهيم القانون الدولي الإنساني الرئيسية بشأن سير العمليات العدائية.

وتركز اللجنة الدولية في ورقة الموقف هذه على ثلاثة من القضايا المختلفة ذات الصلة.

الاستخدام العسكري للفضاء السيبراني وتأثيره على الطابع المدني للفضاء السيبراني

يُستخدم الفضاء السيبراني بشكل أساسي للأغراض المدنية باستثناء بعض الشبكات العسكرية المحددة. ومع ذلك، قد تكون الشبكات المدنية والعسكرية مترابطة؛ وقد تعتمد الشبكات العسكرية على البنية التحتية السيبرانية المدنية: كابلات الألياف البصرية البحرية أو الأقمار الاصطناعية أو أجهزة التوجيه أو العُقد. وفي المقابل، تعتمد المركبات ووسائط النقل البحري وأجهزة مراقبة حركة الطيران المدنية بشكل متزايد على أنظمة الملاحة بالأقمار الاصطناعية التي تُستخدم أيضًا من قبل العسكريين. وتستخدم سلاسل الإمدادات اللوجستية المدنية والخدمات المدنية الأساسية شبكات الإنترنت والاتصالات ذاتها التي تمر من خلالها بعض الاتصالات العسكرية.

إن استخدام عين مدنية لأغراض عسكرية لا يحول هذه العين إلى هدف عسكري تلقائيًا بموجب القانون الدولي الإنساني.[19] ومع ذلك، إذا استخدمت العين لأغراض عسكرية، تفقد حمايتها المفروضة بموجب حظر الهجمات المباشرة على الأعيان المدنية. وسيكون من المثير للقلق الشديد أن يؤدي الاستخدام العسكري للفضاء السيبراني إلى استنتاج مفاده أن العديد من الأعيان التي تشكل جزءًا منه لم تعد محمية بصفتها أعيان مدنية. وقد يؤدي ذلك إلى تعطل واسع النطاق للاستخدام المدني للفضاء السيبراني الذي تزداد أهميته أكثر فأكثر.

وبذلك، إذا لم تعد أجزاء معينة من البنية التحتية للفضاء السيبراني محمية بصفتها أعيان مدنية خلال النزاعات المسلحة، سيظل أي هجوم عليها محكومًا بالحظر المفروض على الهجمات العشوائية وقواعد التناسب والاحتياطات أثناء الهجوم. وتحديدًا لأن الشبكات المدنية

---

[15] المادة 54، البروتوكول الإضافي الأول؛ المادة 14، البروتوكول الإضافي الثاني لاتفاقيات جنيف المؤرخ 8 حزيران/ يونيو 1977؛ القاعدة 54، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[16] انظر، على سبيل المثال، المادة 19، اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان؛ المادة 12، اتفاقية جنيف الثانية لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار، المادة 18، اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب؛ المادة 12، البروتوكول الإضافي الأول؛ المادة 11، البروتوكول الثاني الإضافي؛ القواعد 25 و28 و29، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية.

[17] المادة 58، البروتوكول الإضافي الأول؛ القواعد من 22 إلى 24، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة *الدولية*.

[18] اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2015، ص 43.

[19] انظر المادة 52 (2)، البروتوكول الإضافي الأول؛ القاعدة 8، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية: " فيما يتعلق بالأعيان، تُقصَر الأهداف العسكرية على الأعيان التي تسهم إسهامًا فعّالًا في العمل العسكري سواء بطبيعتها أو موقعها أو غايتها أو استخدامها، والتي يحقق تدميرها كليًا أو جزئيًا، أو الاستيلاء عليها، أو تعطيلها في الأحوال السائدة في حينه ميزة عسكرية مؤكدة." ولمزيد من التفاصيل حول حدود تصنيف البنية التحتية السيبرانية على أنها أهداف عسكرية بموجب القانون الدولي الإنساني، انظر اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2015، ص 42.

والعسكرية مترابطة بشكل وثيق، فإن تقييم الضرر المدني العرضي المتوقع أن تسفر عنه أي عملية سيبرانية هو أمر بالغ الأهمية لضمان حماية السكان المدنيين من آثار هذه العمليات.[20]

مفهوم "الهجوم" بموجب القانون الدولي الإنساني والعمليات السيبرانية

تعتمد بشكل متزايد البنية التحتية المدنية الأساسية التي تتيح توفير الخدمات الأساسية على الأنظمة الرقمية. ويلزم حماية هذه البنية التحتية والخدمات ضد الهجمات السيبرانية أو الأضرار العرضية من أجل حماية السكان المدنيين.

ويوفر القانون الدولي الإنساني حماية خاصة لبنية تحتية معينة، مثل الخدمات الطبية والأعيان التي لا غنى عنها لبقاء السكان المدنيين، بغض النظر عن نوع العملية التي تلحق بها الضرر.[21] ومع ذلك، فإن معظم القواعد الناشئة عن مبادئ التمييز والتناسب والاحتياط - التي توفر حماية عامة للمدنيين والأعيان المدنية - تنطبق فقط على العمليات العسكرية التي تشكّل "هجمات" على النحو المحدد في القانون الدولي الإنساني.[22] وتعرّف المادة 49 من البروتوكول الإضافي الأول الهجمات بأنها "أعمال العنف الهجومية والدفاعية ضد الخصم".[23] وبالتالي ، فإن مدى تفسير مفهوم "الهجوم" على نطاق واسع أو ضيق فيما يتعلق بالعمليات السيبرانية أمر ضروري لانطباق هذه القواعد والحماية التي توفرها للمدنيين والبنية التحتية المدنية.

ومن المتفق عليه على نطاق واسع أن العمليات السيبرانية التي يُتوقع منها أن تسبب وفاة أو إصابة أو ضررًا ماديًا تشكّل هجمات بموجب القانون الدولي الإنساني. ويشمل ذلك، من وجهة نظر اللجنة الدولية، العمليات السيبرانية التي تلحق ضررًا نتيجة الآثار المباشرة أو غير المباشرة (أو الارتدادية) المتوقعة للهجوم، على سبيل المثال وفاة المرضى في وحدات العناية المركّزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء مما تسبب بقطع إمداد المستشفى بالتيار الكهربائي.

وعلاوة على ذلك، تشكل الهجمات التي تعطل الخدمات الأساسية بشكل كبير دون أن تتسبب بالضرورة في إلحاق أضرار مادية أحد أهم المخاطر على المدنيين. ومع ذلك، هناك اختلاف في الرأي حول ما إذا كانت العملية السيبرانية التي تؤدي إلى تعطل الخدمات دون التسبب في ضرر مادي تصنف على أنها هجوم على النحو الوارد في القانون الدولي الإنساني. وتعتبر اللجنة الدولية أيضًا أن العملية التي تهدف إلى تعطيل حاسوب أو شبكة حاسوبية خلال النزاع المسلح تشكل هجومًا بموجب القانون الدولي الإنساني، سواء عن طريق وسائل حركية أو سيبرانية.[24] وإذا فُسر مفهوم الهجوم على أنه يشير فقط إلى العمليات التي تسبب الوفاة أو الإصابة أو الضرر المادي، فإن أي عملية سيبرانية تهدف إلى تعطيل شبكة مدنية (مثل الكهرباء أو الخدمات المصرفية أو الاتصالات)، أو من المتوقع أن تتسبب في حدوث هذا التأثير بصورة عرضية، قد لا تكون مشمولة بقواعد القانون الدولي الإنساني الأساسية التي تحمي السكان المدنيين والأعيان المدنية. وسيكون من الصعب التوفيق ما بين مثل هذا الفهم التقييدي المفرط لفكرة الهجوم وبين هدف قواعد القانون الدولي الإنساني بشأن سير العمليات العدائية والغرض منها. ومن الضروري أن تتوصل الدول إلى فهم مشترك لمفهوم الهجوم لضمان الحماية الكافية للسكان المدنيين من آثار العمليات السيبرانية.

البيانات المدنية ومفهوم "الأعيان المدنية"

تعد البيانات المدنية الأساسية - مثل البيانات الطبية والبيانات البيومترية وبيانات الضمان الاجتماعي والسجلات الضريبية والحسابات المصرفية وملفات عملاء الشركات أو قوائم وسجلات الانتخابات - عنصرًا مهمًا في المجتمعات الرقمية، إذ أن هذه البيانات أساسية لسير معظم جوانب الحياة المدنية، سواء على المستوى الفردي أو المجتمعي. وأصبحت حماية هذه البيانات المدنية الأساسية أمرًا مثيرًا للقلق المتزايد.

---

[20] انظر اللجنة الدولية، *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*، 2018: متاح على: https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf، ص 37-40.

[21] انظر النص المتعلق بالحاشيتين 16 و 15 أعلاه. يُحظر مهاجمة أو تدمير أو نقل أو تعطيل "الأعيان التي لا غنى عنها لبقاء السكان المدنيين".

[22] يختلف مفهوم "الهجوم" بموجب القانون الدولي الإنساني، المحدد في المادة 49 من البروتوكول الإضافي الأول، عن مفهوم "الهجوم المسلح" بموجب المادة 51 من ميثاق الأمم المتحدة الذي يندرج في نطاق قانون اللجوء للحرب، ويجب عدم الخلط بينهما. والتأكيد على أن أي عملية سيبرانية معينة، أو نوع من العمليات السيبرانية، ترق إلى حد الهجوم بموجب القانون الدولي الإنساني لا يعني بالضرورة أنها تصنف على أنها هجوم مسلح بموجب ميثاق الأمم المتحدة.

[23] انظر النص المتعلق بالحواشي من 10 إلى 14 أعلاه للاطلاع على القواعد التي تنطبق بشكل خاص على الهجمات.

[24] انظر اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2011، ص 37؛ اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة* 2015، ص 41-42.

وتشمل بعض الحماية المحددة التي يوفرها القانون الدولي الإنساني البيانات الأساسية، مثل البيانات الخاصة بالوحدات الطبية ، لأنها مشمولة بالالتزام باحترام وحماية هذه الوحدات.[25]

وتحمي المبادئ والقواعد الرئيسية للقانون الدولي الإنساني التي تحكم سير العمليات العدائية المدنيين والأعيان المدنية بوجه عام.[26] لذلك من المهم أن توافق الدول على أن البيانات المدنية محمية بموجب هذه القواعد.

ويمكن أن يؤدي حذف البيانات المدنية الأساسية أو العبث بها إلى شلل الخدمات الحكومية والشركات الخاصة بسرعة كبيرة. ويمكن أن تتسبب مثل هذه العمليات في أضرار للمدنيين أكبر من تدمير الأعيان المادية. وتظل عالقة مسألة ما إذا كانت البيانات المدنية تشكل أعيانًا مدنية وإلى أي مدى تكون كذلك. وترى اللجنة الدولية أن التأكيد على أن حذف هذه البيانات المدنية الأساسية أو العبث بها غير محظور بموجب القانون الدولي الإنساني في عالم اليوم الذي يعتمد على البيانات هو أمر يصعب التوفيق بينه وبين هدف القانون الدولي الإنساني والغرض منه. ولا ينبغي أن يؤدي استبدال الملفات والوثائق الورقية بالملفات الرقمية في شكل بيانات إلى تقليل الحماية التي يوفرها القانون الدولي الإنساني لها.[27] إن استثناء البيانات المدنية الأساسية من الحماية التي يوفرها القانون الدولي الإنساني للأعيان المدنية من شأنه أن يؤدي إلى ثغرة كبيرة في هذه الحماية.

سادسًا: إسناد التصرف في الفضاء السيبراني لأغراض مسؤولية الدولة

يتيح الفضاء السيبراني للجهات الفاعلة إمكانيات تقنية متنوعة لإخفاء هويتهم أو تزويرها، مما يزيد من تعقيد إسناد التصرف ويخلق صعوبات كبيرة. فعلى سبيل المثال، ينطبق القانون الدولي الإنساني، حتى أثناء النزاع المسلح، على العمليات المرتبطة بالنزاع فحسب. وإذا تعذر تحديد منفذ العملية السيبرانية - وبالتالي تعذر تحديد الصلة بين العملية والنزاع المسلح المعني - فقد يكون من الصعب تحديد ما إذا كان القانون الدولي الإنساني ينطبق حتى على العملية أم لا. ويُعد إسناد التصرف في العمليات السبرانية مهمًا أيضًا لضمان مساءلة الجهات الفاعلة التي تنتهك القانون الدولي، بما في ذلك القانون الدولي الإنساني. وقد يؤدي التصور بأنه من الأسهل إنكار المسؤولية عن هذه الهجمات أيضًا إلى إضعاف الحظر المفروض على استخدامها- وقد يجعل الجهات الفاعلة أقل تدقيقًا بشأن مخالفة القانون الدولي باستخدامها.[28]

وبذلك، لا يُسبب إسناد التصرف أي مشكلة للجهات الفاعلة التي تنفذ العمليات السيبرانية أو تديرها أو تتحكم فيها: فهي تملك كل الوقائع المتاحة لتحديد الإطار القانوني الدولي الذي تعمل فيه والالتزامات التي يجب أن تحترمها.

الدولة مسؤولة بموجب القانون الدولي عن التصرفات المسندة إليها بما في ذلك انتهاكات القانون الدولي الإنساني، والتي تشمل:

- تصرف من قبل أجهزة الدولة، بما في ذلك قواتها المسلحة أو أجهزتها الاستخباراتية؛
- تصرف من قبل أشخاص أو كيانات فوّضتها الدولة للقيام بقدر من السلطة الحكومية، مثل الشركات الخاصة ؛
- تصرف من قبل أشخاص أو مجموعات تعمل في الواقع بناء على تعليمات الدولة أو تحت إشرافها أو سيطرتها، مثل الميليشيات أو مجموعات من المتسللين؛ و
- تصرف من قبل أشخاص أو مجموعات خاصة، والتي تعترف بها الدولة وتتبناها كتصرفات صادرة عنها.[29]

تنطبق هذه المبادئ سواء نُفذ التصرف سيبرانيًا أو بأي وسيلة أخرى.

---

[25] انظر الحاشية 16.

[26] انظر النص المتعلق بالحواشي من 10 إلى 15 أعلاه.

[27] اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2015، ص 43؛ اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة* 2019، ص 21.

[28] اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2011، ص 37؛ اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة* 2019، ص 20.

[29] القاعدة 149، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية. انظر ايضًا لجنة القانون الدولي، *مسؤولية الدول عن الأفعال غير المشروعة دوليًا*، 2001، لاسيما المواد من 4 إلى 11.

سابعًا: الخاتمة

إن استخدام العمليات السيبرانية باعتبارها وسائل أو أساليب للقتال في نزاع مسلح يشكل خطرًا حقيقيًا بإلحاق الضرر بالمدنيين. ومن الضروري التأكد من أن هذه العمليات لا تحدث في ظل فراغ قانوني وذلك من أجل ضمان حماية السكان المدنيين والبنية التحتية المدنية. وتحث اللجنة الدولية جميع الدول على التأكيد على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، على أساس أن هذا التأكيد لا يشجع على عسكرة الفضاء السيبراني ولا يضفي الشرعية على الحرب السيبرانية.

وتعتقد اللجنة الدولية في الوقت نفسه أن هناك حاجة إلى مزيد من المناقشات - خاصة بين الدول - حول كيفية تفسير القانون الدولي الإنساني وانطباقه على الفضاء السيبراني. وهناك حاجة ملحة لإجراء مثل هذه المناقشات لأن الدول التي تقرر تطوير القدرات السيبرانية التي تصنف على أنها أسلحة ووسائل وأساليب للقتال أو الحصول عليها - سواء لأغراض هجومية أو دفاعية - يجب أن تضمن إمكانية استخدام هذه القدرات وفقًا لالتزاماتها بموجب القانون الدولي الإنساني.[30] ويجب أن تستند هذه المناقشات إلى فهم متعمق لتطوير القدرات العسكرية السيبرانية، وتكلفتها البشرية المحتملة، والحماية التي يوفرها القانون الحالي. ويجب على الدول تحديد ما إذا كان القانون الحالي ملائمًا وكافيًا لمواجهة التحديات التي يفرضها الطابع المترابط والرقمي إلى حد كبير للفضاء السيبراني، أو ما إذا كان يتعين موائمة القانون الحالي مع الخصائص المحددة للفضاء السيبراني. وإذا وُضعت قواعد جديدة لحماية المدنيين من آثار العمليات السيبرانية أو لأسباب أخرى، فعليها أن تستند إلى الإطار القانوني الحالي وتعززه - بما في ذلك القانون الدولي الإنساني.

وترحب اللجنة الدولية بالمناقشات الحكومية الدولية التي تجري حاليًا في إطار العمليتين المكلفتين من قبل الجمعية العامة للأمم المتحدة، وهي ممتنة لإتاحة الفرصة لتبادل آرائها مع الدول المشاركة. وتقف اللجنة الدولية على أهبة الاستعداد لإتاحة خبرتها في مثل هذه المناقشات، حسبما تراه الدول مناسبًا.

---

[30] انظر اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة* 2019، ص 28-29؛ اللجنة الدولية، *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*، 2006؛ المادة 36، البروتوكول الإضافي الأول.