Humanity In War

مسار العمل 6

احترام القانون الدولي الإنساني في استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة

معلومات أساسية*

*أعدت هذه الورقة الأساسية في الأصل للمشاورة الأولى مع الدول، وأضيفت إليها تصويبات وتحديثات بسيطة لا أكثر في سبتمبر 2025.

مقدمة 2

أولاً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة والقانون الدولي الإنساني: المناقشات العالمية وأوجه الفهم المشتركة الناشئة 2

ثانياً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة اليوم والتكلفة البشرية 4

ثالثاً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة: تحديد إطار المسائل القانونية والإنسانية بموجب القانون الدولي الإنساني 5

أولاً: حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من المخاطر الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة 6

ثانياً– حماية المدنيين وغيرهم من الأشخاص المحميين من انتشار المعلومات في انتهاك للقانون الدولي الإنساني خلال النزاعات المسلحة 9

ثالثاً– خطر الضرر الناجم عن الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، وإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة 10

مقدمة

يثير الاستخدام المتزايد لتكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة تساؤلات إنسانية وقانونية جوهرية. وفي حين يسود اتفاق عام على أن القانون الدولي الإنساني يفرض قيوداً على استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة، تثير خصائص بيئة تكنولوجيا المعلومات والاتصالات تساؤلات معقدة بشأن تنفيذها. وأقرّت الدول بضرورة مواصلة المناقشات بشأن هذه التساؤلات. ويشكل مسار العمل بشأن تكنولوجيا المعلومات والاتصالات جزءاً من جهد متواصل للتشجيع على تكوين أوجه فهم مشتركة.

أولاً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة والقانون الدولي الإنساني: المناقشات العالمية وأوجه الفهم المشتركة الناشئة

إن تطبيق القانون الدولي، بما في ذلك القانون الدولي الإنساني، على أنشطة تكنولوجيا المعلومات والاتصالات كان موضوع مناقشات متعددة الأطراف لما يقارب عقدين من الزمن. وفي عام 2021، أشار فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (فريق الخبراء الحكوميين)، بتوافق الآراء إلى أن "القانون الدولي الإنساني لا ينطبق إلا في حالات النزاع المسلح. وهو يذكّر بالمبادئ القانونية الدولية الراسخة، بما فيها مبادئ الإنسانية والضرورة والتناسب والتمييز التي أشير إليها في تقرير عام 2015، حيثما انطبقت هذه المبادئ. وأقرّ الفريق بالحاجة إلى إجراء مزيد من الدراسة بشأن كيف ومتى تنطبق هذه المبادئ على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وشدد على أن التذكير بهذه المبادئ لا يضفي الشرعية على النزاع أو يشجعه بأي حال من الأحوال".[1] وقد ردّد الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025 هذا الاستنتاج في تقاريره المرحلية.[2]

وحتى الآن، وعلى حد علمنا، نشرت 35 دولة مواقفها الوطنية الفردية بشأن كيفية انطباق القانون الدولي على العمليات السيبرانية.[3] وإضافة إلى ذلك، نشرت منظمتان إقليميتان – هما الاتحاد الأفريقي والاتحاد الأوروبي – مواقف أو أوجه فهم مشتركة بشأن تطبيق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات، مما يُمثل تقدماً في بناء توافق إقليمي في الآراء، ويرفع عدد الدول التي تُبدي آراءها بشأن هذا الموضوع إلى أكثر من 100 دولة. وتشمل أوجه الفهم المشتركة الناشئة إعادة التأكيد على تطبيق مبادئ القانون الدولي الإنساني وقواعده، بما فيها الإنسانية والضرورة والتناسب والتمييز، على استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة. وأعرب أيضاً عدد

---

[1] *تقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي*، A/76/135، 2021، الفقرة 71(و). انظروا أيضاً الفقرتين 2 و3 من قرار الجمعية العامة للأمم المتحدة 19/76، 2021، المعتمد بتوافق الآراء، والذي يرحب بالتقرير النهائي لفريق الخبراء الحكوميين، ويهيب بالدول الأعضاء أن تسترشد بالتقرير في استخدامها لتكنولوجيات المعلومات والاتصالات.

[2] انظروا الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، *التقرير المرحلي السنوي الأول*، A/77/275، 2022، الفقرة 15(ب)(2)؛ *والتقرير المرحلي السنوي الثاني*، A/78/265، 2023، الفقرة 29(ب)(2)؛ *والتقرير المرحلي السنوي الثالث*، A/79/214، 2024، الفقرة 36(ب)(2). ومسودة التقرير الختامي، A/AC.292/2025/CRP.1، 2025، الفقرة 40 (ب)(2).

[3] يمكن الاطلاع على جميع المواقف الوطنية الفردية والمواقف المشتركة في مجموعة أدوات القانون السيبراني (Cyber Law Toolkit)، تحت عنوان "المواقف المشتركة والوطنية"، على الرابط التالي: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.

متزايد من الدول عن آرائها بشأن الحماية التي يوفرها القانون الدولي الإنساني للمدنيين والبنية التحتية المدنية والبيانات المدنية والطواقم والمرافق الطبية والأنشطة الإنسانية والعاملين في المجال الإنساني، في جملة أشخاص وأعيان آخرين، من الأنشطة المغرضة بواسطة تكنولوجيا المعلومات والاتصالات.

وبناءً على هذا الزخم، اعتمد المؤتمر الدولي الرابع والثلاثون للصليب الأحمر والهلال الأحمر (المؤتمر الدولي الرابع والثلاثون) في تشرين الأول/أكتوبر 2024 – الذي جمع كافة الدول وجميع مكونات الحركة الدولية للصليب الأحمر والهلال الأحمر – القرار المعنون "حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من التكلفة البشرية المحتملة لأنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة" (القرار بشأن تكنولوجيا المعلومات والاتصالات). ويحثّ القرار الدول وأطراف النزاعات المسلحة على حماية السكان المدنيين وغيرهم من الأشخاص والأعيان المحميين في حالات النزاع المسلح، بما في ذلك من المخاطر الناجمة عن الأنشطة المغرضة بواسطة تكنولوجيا المعلومات والاتصالات. ويدعو كذلك الدول وأطراف النزاعات المسلحة إلى الالتزام بالحماية التي يوفرها القانون الدولي الإنساني للمدنيين والبنية التحتية المدنية الحيوية (بما فيها البنية التحتية الرقمية الحيوية، مثل الكابلات البحرية والشبكات المدارية للاتصالات)، والعاملين والأنشطة في المجالين الطبي والإنساني والممتلكات الثقافية، بما في ذلك من المخاطر الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات. ويكرّر القرار التأكيد على حظر التشجيع أو التحريض على ارتكاب انتهاكات القانون الدولي الإنساني، ويتناول المسائل المتعلقة بالمدنيين الذين ينفذون أنشطة تكنولوجيا المعلومات والاتصالات، وشركات التكنولوجيا الخاصة التي توفّر خدمات تكنولوجيا المعلومات والاتصالات في سياق النزاعات المسلحة.

وعلى الرغم من التقدم المشار إليه أعلاه، سُلّم بأن خصائص بيئة تكنولوجيا المعلومات والاتصالات تُثير تساؤلات بشأن كيفية انطباق مبادئ القانون الدولي الإنساني وقواعده على أنشطة تكنولوجيا المعلومات والاتصالات، وبأن هناك حاجة إلى إجراء مزيد من المناقشات.[4]

ويستجيب مسار العمل لهذه الحاجة، ويوفّر مساحة مخصّصة لتبادلٍ مركّز ومتعمّق للآراء. وفي ضوء التكلفة البشرية لاستخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة، يهدف مسار العمل هذا إلى التشجيع على تكوين أوجه فهم مشتركة للقيود التي يفرضها القانون الدولي الإنساني على أنشطة تكنولوجيا المعلومات والاتصالات في النزاعات المسلحة لحماية المدنيين من الضرر.

[4] *تقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي*، A/76/135، 2021، الفقرة 71(و). والمؤتمر الدولي الرابع والثلاثون للصليب الأحمر والهلال الأحمر، جنيف، 2024، الفقرة 19 من ديباجة القرار 2 المعنون "حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من التكلفة البشرية المحتملة لأنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة" (المشار إليه فيما يلي بالقرار بشأن تكنولوجيا المعلومات والاتصالات).

ثانياً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة اليوم والتكلفة البشرية

عادت الرقمنة السريعة للمجتمعات بفوائد كبيرة، إذ عزّزت الفرص في المجالين الاجتماعي والاقتصادي ومجال الاتصالات. وفي المناطق المتضررة من النزاعات، تكتسي تكنولوجيات المعلومات والاتصالات الموثوقة أهمية بالغة بالنسبة إلى المدنيين للحصول على السلع والخدمات الأساسية، وبالنسبة إلى الحكومات لتقديم الخدمات، وفيما يخص دعم الأنشطة الطبية والإنسانية، بما فيها أنشطة الحركة الدولية للصليب الأحمر والهلال الأحمر.

ولكن، تأتي هذه المزايا مصحوبة بمخاطر أيضاً، بما فيها تلك الناجمة عن زيادة استخدام الدول والجهات الفاعلة من غير الدول لتكنولوجيات المعلومات والاتصالات في النزاعات المسلحة. ويطوّر عدد من الدول قدرات تكنولوجيا المعلومات والاتصالات لأغراض عسكرية، مع تزايد نشر تكنولوجيات المعلومات والاتصالات واستخدامها كوسائل أو أساليب حرب. وفي حين أن تطوير قدرات تكنولوجيا المعلومات والاتصالات العسكرية واستخدامها قد يوفّران للأطراف المتحاربة إمكانية تحقيق أهدافها دون التسبّب بالضرورة في ضرر مباشر على المدنيين أو ضرر مادي على البنية التحتية المدنية، يظل الخطر الذي تشكله هذه الأنشطة على السكان المدنيين والبنية التحتية المدنية مصدر قلق حقيقي. وباستخدام قدرات تكنولوجيا المعلومات والاتصالات العسكرية، يمكن تشغيل العمليات التي تتحكم فيها النُظم الحاسوبية، أو تغييرها أو معالجتها بطريقة أخرى تنطوي على إمكانية التسبّب في آثار بالغة الضرر على المدنيين.

ويمكن أن يترتّب على استخدام تكنولوجيات المعلومات والاتصالات التي تستهدف البنية التحتية المدنية الحيوية – مثل المرافق النووية وشبكات الكهرباء وشبكات المياه وشبكات الاتصالات – "عواقب إنسانية مدمرة محتملة".[5] ويمكن لأنشطة تكنولوجيا المعلومات والاتصالات أن تعطل أيضاً الخدمات الحكومية الإلكترونية وعمليات القطاع الخاص، وتتسبّب في تكاليف مجتمعية واقتصادية. وتتفاقم هذه المخاطر بسبب الترابط الذي يميّز الفضاء الإلكتروني. فقد يكون لأنشطة تكنولوجيا المعلومات والاتصالات التي تستهدف نظاماً واحداً تداعيات على مختلف النُظم الأخرى، بغض النظر عن مكان وجود تلك النُظم.

ويتعرّض قطاع الرعاية الصحية، إلى جانب المنظمات الإنسانية، بصورة خاصة لخطر أنشطة تكنولوجيا المعلومات والاتصالات في النزاعات المسلحة، التي يمكن أن تعطل العمليات الطبية المنقذة للحياة، وتعيق عمل المنظمات الإنسانية غير المتحيّزة وموظفيها، وتعرض للخطر خدمات تقديم المساعدة الأساسية إلى المحتاجين. وعلى سبيل المثال، استهدفت أنشطة تكنولوجيا المعلومات والاتصالات اللجنة الدولية للصليب الأحمر (اللجنة الدولية) ومكونات أخرى من الحركة الدولية للصليب الأحمر والهلال الأحمر.[6]

وعلاوة على ذلك، أصبح إشراك المدنيين في الأنشطة العسكرية من خلال استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة أكثر وضوحاً. وقد تسامحت الدول مع القراصنة المدنيين ومجموعات القراصنة، أو يسّرت لهم، أو شجعتهم على المشاركة في أنشطة تكنولوجيا المعلومات والاتصالات التي تستهدف المدنيين والأعيان المدنية المرتبطة بالخصم أو تلحق الضرر بهم. وشُجّع المدنيون أيضاً على

---

[5] الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، *تقرير موضوعي نهائي*، A/AC.290/2021/CRP.2، 2021، الفقرة 18.

[6] يبرز اختراق البيانات الذي وقع في عام 2022 والهجمات المتكررة الموزعة لحجب الخدمة على موقع اللجنة الدولية الحاجة إلى حماية قوية للبيانات من أجل حماية المعلومات الحساسة، وضمان استمرارية العمليات، وحماية الحوار الإنساني السري مع أطراف النزاعات. انظروا اللجنة الدولية، "هجوم سيبراني على اللجنة الدولية: المعلومات التي نعرفها"، على الرابط التالي: https://www.icrc.org/ar/document/هجوم-سيبراني-على-اللجنة-الدولية-المعلومات-التي-نعرفها.

الإبلاغ عن تحركات قوات العدو، بما في ذلك عبر تطبيقات الهواتف الذكية. وتقدّم الشركات الخاصة بشكل متزايد خدمات الأمن السيبراني أو غيرها من الخدمات الرقمية لأطراف النزاعات المسلحة. وإذا اقترب المدنيون أكثر من الأعمال العدائية، فهم يواجهون خطر التعرض للضرر. وإضافة إلى ذلك، غالباً ما يجهلون المخاطر التي يواجهونها، أو الآثار القانونية المترتبة على أنشطتهم، أو قواعد القانون الدولي الإنساني التي يجب عليهم احترامها.

ويوجد بُعد آخر يتمثل في استخدام تكنولوجيات المعلومات والاتصالات لنشر المعلومات الضارة خلال النزاعات المسلحة. ففي حين أن العمليات المعلوماتية كانت منذ فترة طويلة جزءاً من الحرب، وليست غير مشروعة في حد ذاتها، يزيد استخدام تكنولوجيات المعلومات والاتصالات – وخاصة في منصات التواصل الاجتماعي أو عند اقترانه بالذكاء الاصطناعي وغيره من التكنولوجيات الناشئة — من سرعة ونطاق انتشار المعلومات الضارة، بما في ذلك الجهود الرامية إلى التحريض على العنف، أو تعريض المحتجزين لفضول الجماهير، أو تقويض الثقة في المنظمات الإنسانية.

وأقرّت الدول بهذه التطورات والمخاطر. وأشار الفريق العامل المفتوح العضوية 2021 – 2025 إلى أن الدول تطوّر قدرات تكنولوجيا المعلومات والاتصالات لأغراض عسكرية، وأن احتمال استخدام تكنولوجيات المعلومات والاتصالات في النزاعات يتنامى، وأن تكنولوجيا المعلومات والاتصالات استخدمت بالفعل في نزاعات في مناطق مختلفة، مع عواقب إنسانية وخيمة محتملة تحملها المدنيون والأعيان المدنية وكذلك منظمات دولية وإنسانية.[7] وسلّط المؤتمر الدولي الرابع والثلاثون الضوء على الضرر المحتمل الذي يلحق بالمدنيين نتيجة استخدام أطراف النزاعات المسلحة لتكنولوجيات المعلومات والاتصالات، لا سيما عندما تستهدف هذه الوسائل البنية التحتية المدنية الحيوية والخدمات الأساسية أو تؤثّر عليها بصورة عرضية، والضرر المحتمل الذي يلحق بالمنظمات الإنسانية غير المتحيّزة الذي يعيق وصول هذه المنظمات إلى السكان المتضررين.[8]

ثالثاً– استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة: تحديد إطار المسائل القانونية والإنسانية بموجب القانون الدولي الإنساني

توفّر معاهدات القانون الدولي الإنساني والقانون العرفي القائمة حماية للمدنيين والأعيان المدنية من الأخطار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة. وعلى نحو ما كرّر تأكيده القرار بشأن تكنولوجيا المعلومات والاتصالات، فإن "الغرض من قواعد القانون الدولي الإنساني ومبادئه — بما فيها مبدأ التمييز، وحظر الهجمات العشوائية وغير المتناسبة، والالتزامات بحماية السكان المدنيين والمدنيين والأعيان المدنية في سير العمليات العسكرية، واتخاذ جميع الاحتياطات الممكنة لتجنب إلحاق الضرر العرضي بالمدنيين أو تقليله إلى أدنى حدّ في أي حال، وحظر التشجيع أو التحريض على ارتكاب انتهاكات القانون الدولي الإنساني، وحظر أعمال العنف أو التهديد به، الرامية بشكل أساسي إلى بث الذعر بين السكان المدنيين — في حالات النزاعات المسلحة هو حماية السكان المدنيين وغيرهم من الأشخاص

[7] الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، مسودة تقرير ختامي، A/AC.292/2025/CRP.1, 2025 الفقرات 15، 16 و21.

[8] الفقرتان 7 و14 من ديباجة القرار بشأن تكنولوجيا المعلومات والاتصالات.

والأعيان المحميين، بما في ذلك من المخاطر الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات".[9]

واستناداً إلى ما تقدّم، يُقترح إجراء مزيد من المناقشة بشأن المسائل القانونية الرئيسية الواردة أدناه التي تتعلّق بالشواغل الإنسانية الأكثر إلحاحاً.

أولاً: حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من المخاطر الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة

حماية السكان المدنيين من آثار عمليات تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة ومفهوم الهجوم بموجب القانون الدولي الإنساني

لدى عمليات تكنولوجيا المعلومات والاتصالات القدرة على تعطيل المنشآت الصناعية وشبكات الاتصالات وغيرها من عناصر البنية التحتية الحيوية للدولة أو إلحاق ضرر مادي بها. ويمكن أيضاً أن تتسبّب هذه العمليات، بشكل مباشر أو غير مباشر، في إصابة المدنيين أو وفاتهم – بما في ذلك عن طريق تعطيل أداء الخدمات الأساسية. وتتفاقم هذه المخاطر بسبب ترابط الفضاء الرقمي. وبينما حظيت عمليات تكنولوجيا المعلومات والاتصالات التي تسفر عن أضرار مادية باهتمام خاص، أظهرت الاستخدامات الحديثة لتكنولوجيات المعلومات والاتصالات، بما في ذلك في النزاعات المسلحة، أنه حتى في غياب الضرر المادي، يمكن لعمليات تكنولوجيا المعلومات والاتصالات أن تعطّل بشدة البنية التحتية المدنية وتعيق تقديم الخدمات الأساسية. وفي الواقع، يشكل هذا الخطر أحد أهم مخاطر تكنولوجيا المعلومات والاتصالات على المدنيين خلال النزاعات المسلحة.

ويكمن الغرض من قواعد القانون الدولي الإنساني التي تنظم سير الأعمال العدائية في ضمان احترام وحماية السكان المدنيين والأعيان المدنية.[10] ومعظم القواعد النابعة من المبادئ والقواعد التي تنظم سير الأعمال العدائية، ولا سيما التمييز والتناسب والاحتياطات – التي توفر حماية عامة للمدنيين والأعيان المدنية – تنطبق فقط على العمليات أو الأنشطة التي تُصنّف على أنها "هجمات"، على النحو الوارد في القانون الدولي الإنساني، أي "أعمال العنف الهجومية والدفاعية ضد الخصم".[11] ولذلك، فإن كيفية تفسير مفهوم "الهجوم" فيما يتعلق باستخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة، ولا سيما عمليات تكنولوجيا المعلومات والاتصالات التي تعطّل الأعيان المدنية دون التسبب في ضرر مادي، هي مسألة أساسية، إذ يحدّد ذلك ما إذا كانت هذه القواعد تنطبق، وبالتالي ما إذا كان المدنيون وغيرهم من الأشخاص والأعيان المحميين يتمتعون بالحماية من الأخطار الناجمة عن هذه العمليات.

ومن المسلم به أن مفهوم العنف الوارد في تعريف "الهجوم" بموجب القانون الدولي الإنساني يمكن أن يشير إما إلى الوسائل المستخدمة أو إلى العواقب أو الآثار المترتبة عليه. فالعملية التي تسبب آثاراً عنيفة تصنّف على أنها هجوم، حتى ولو لم تكن الوسائل المستخدمة عنيفة في حد ذاتها.[12]

---

[9] الفقرة 4 من القرار بشأن تكنولوجيا المعلومات والاتصالات.

[10] المادة 48 من البروتوكول الإضافي الأول المؤرخ 8 حزيران/يونيو 1977، وعنوان الباب الرابع وعنوان القسم الأول.

[11] المادة 49(1) من البروتوكول الإضافي الأول، وتوجد بعض قواعد القانون الدولي الإنساني التي تنطبق على جميع العمليات العسكرية، بما فيها تلك التي تُنفذ عن طريق أنشطة تكنولوجيا المعلومات والاتصالات. انظروا على سبيل المثال المواد 48، و51(1)، و57(1) من البروتوكول الإضافي الأول.

[12] إيف. ساندوز، وكريستوف سوينارسكي، وبرونو زيمرمان (المحررون)، *التعليق على البروتوكولين الإضافيين المؤرخين في 8 حزيران/يونيو 1977 لاتفاقيات جنيف المؤرخة في 12 آب/أغسطس 1949*، اللجنة الدولية، جنيف/مارتينوس نيهوف، لايدن، 1987 (المشار إليه فيما يلي باللجنة الدولية، التعليق على البروتوكولين الإضافيين)، تنص الفقرة 1881 من المادة 49(1) من البروتوكول الأول على أنه "ثمة هجوم عندما يتعرّض شخص لخطر مباشر بسبب لغم مزروع"، وهو تفسير يتّسق مع النهج القائم على العواقب. ومن الأمثلة المقبولة عامة أيضاً أن استخدام عامل كيميائي أو بيولوجي يشكّل هجوماً نظراً إلى الآثار المترتبة عليه، حتى ولو لم تكن وسائل إطلاق هذه العوامل عنيفة.

ومن المتّفق عليه على نطاق واسع أيضاً أن عملية تكنولوجيا المعلومات والاتصالات التي يُتوقع أن تسبب وفاة شخص أو إصابته، أو إتلاف شيء ما أو تدميره، تشكل هجوماً بموجب القانون الدولي الإنساني.[13] ومن المفهوم عامة أن ذلك يشمل الضرر الناجم عن الآثار المباشرة وغير المباشرة (أو الارتدادية) المتوقعة لعملية ما، على سبيل المثال وفاة المرضى في وحدات العناية المركزة نتيجة لعملية تكنولوجيا المعلومات والاتصالات ضد شبكة الكهرباء مما تسبّب بقطع إمداد المستشفى بالطاقة.[14]

وفضلاً عن ذلك، ثمة حاجة إلى إجراء مزيد من المناقشة بين الدول بشأن قواعد القانون الدولي الإنساني التي تفرض قيوداً على عمليات تكنولوجيا المعلومات والاتصالات التي تؤثر على وظائف نُظم تكنولوجيا المعلومات والاتصالات دون أن تسبّب بالضرورة ضرراً مادياً أو دماراً يلحق بعين من الأعيان أو إصابة شخص أو وفاته، بما في ذلك ما إذا كانت تُصنّف على أنها "هجمات" بموجب القانون الدولي الإنساني.

ومن منظور الحرب المعاصرة، من الأهمية الحاسمة لحماية المدنيين والأعيان المدنية من أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة الإقرار بأن عملية تكنولوجيا المعلومات والاتصالات التي تُعطّل عيناً دون التسبّب في ضرر مادي هي هجوم بموجب القانون الدولي الإنساني. ومن الصعب التوفيق بين التفسير التقييدي لمفهوم الهجوم، الذي يستثني بعض أنشطة تكنولوجيا المعلومات والاتصالات من الحماية التي توفرها القواعد الأساسية للقانون الدولي الإنساني المتعلقة بسير الأعمال العدائية، وهدف القانون الدولي الإنساني والغرض منه، والحاجة إلى ضمان أن يظل إطاره الخاص بالحماية فعالاً في ضوء تطور وسائل الحرب وأساليبها. ومن الضروري في هذا الصدد أن تتوصل الدول إلى فهم مشترك لحماية المدنيين والأعيان المدنية من آثار الاستخدام الضار لتكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة.

البيانات المدنية ومفهوم الأعيان المدنية بموجب القانون الدولي الإنساني

إن البيانات المدنية – مثل البيانات الطبية، أو البيانات البيومترية، أو بيانات الضمان الاجتماعي، أو السجلات الضريبية، أو الحسابات المصرفية، أو البيانات الإنسانية، أو ملفات عملاء الشركات، أو قوائم وسجلات الانتخابات — عنصر أساسي في المجتمعات الرقمية. فهذه البيانات أساسية لسير معظم جوانب الحياة المدنية، سواء على المستوى الفردي أو المجتمعي. ويمكن أن يؤدي حذف البيانات المدنية أو العبث بها إلى شلل الخدمات الحكومية والشركات الخاصة بسرعة كبيرة، وقد يسبّب ضرراً للمدنيين أكبر من دمار بعض الأعيان المادية. وإضافة إلى ذلك، قد تعرّض سرقة البيانات المدنية أو تسريبها الأفراد والمجتمعات لخطر ضرر جسيم.

وفي ما يتعلق بالبيانات التي تخص فئات معيّنة من الأشخاص والأعيان التي تتمتع بحماية خاصة بموجب القانون الدولي الإنساني، فقواعد الحماية هي قواعد شاملة. وعلى سبيل المثال، يمتد الالتزام باحترام وحماية أفراد الطواقم الطبية والوحدات الطبية ووسائل النقل الطبي، والعاملين في المجال الإنساني والأعيان الإنسانية، والأعيان التي لا غنى عنها لبقاء السكان المدنيين، ليشمل بياناتهم.[15] ولكن فضلاً عن ذلك، من المهم تحسين فهم نطاق الحماية التي توفره قواعد القانون الدولي الإنساني الحالية للبيانات المدنية،[16] وخاصة إذا كانت البيانات تشكل أعياناً بالمعنى المفهوم بموجب القانون الدولي الإنساني، وفي هذه الحالة تخضع عمليات تكنولوجيا المعلومات والاتصالات ضد البيانات (مثل إتلافها أو حذفها) أساساً لمبادئ التمييز والتناسب والاحتياطات.

وفي هذا الصدد، تبنت بعض الدول وجهة نظر تفيد بأن حماية الأعيان المدنية تشمل جميع أنواع البيانات المدنية؛ في حين يميّز البعض بين

---

[13] اللجنة الدولية للصليب الأحمر، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2015، الصفحتان 41 و42.

[14] اللجنة الدولية للصليب الأحمر، *ورقة موقف بشأن القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة*، 2019، الصفحة 7. للاطلاع على لمحة عامة عن مواقف الدول، انظروا مجموعة أدوات القانون السيبراني (Cyber Law Toolkit)، "الهجوم (القانون الدولي الإنساني)"، على الرابط التالي: https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).

[15] انظروا القسم التالي من هذه الورقة، "الأشخاص والأعيان الذين يتمتعون بحماية خاصة بموجب القانون الدولي الإنساني".

[16] تشمل هذه القواعد مبادئ القانون الدولي الإنساني وقواعده بشأن سير الأعمال العدائية. وقد تشمل القواعد الأخرى ذات الصلة، على سبيل المثال، حماية الممتلكات الثقافية، وحماية الممتلكات من الاستيلاء عليها وتدميرها، وحظر النهب.

"بيانات المحتوى" والبيانات الأخرى؛ أما دول أخرى، فرأت أنه لا يمكن اعتبار البيانات الرقمية عامة أعياناً بموجب القانون الدولي الإنساني.[17]

وثمة حاجة إلى إجراء مزيد من المناقشة بين الدول لبناء أوجه فهم مشتركة بشأن هذه المسألة الحرجة. ومن منظور إنساني، يبدو أن التأكيد على أن العملية المصمّمة أو التي يُتوقع منها أن تحذف البيانات المدنية أو تعبث بها غير محظورة بموجب القانون الدولي الإنساني في عالم اليوم الذي يعتمد على البيانات، هو أمر يصعب التوفيق بينه وبين هدف القانون الدولي الإنساني والغرض منه. ومن المنطقي ألّا يؤدي استبدال الملفات والوثائق الورقية بالملفات الرقمية في شكل بيانات إلى تقليل الحماية التي يوفرها القانون الدولي الإنساني للمعلومات المخزنة في البيانات.

صنوف الحماية الخاصة للأشخاص والأعيان والأنشطة بموجب القانون الدولي الإنساني

توفّر بعض قواعد القانون الدولي الإنساني حماية خاصة لفئات معينة من الأشخاص والأعيان والأنشطة، تتجاوز حظر الهجمات، بما في ذلك ما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات.

وعلى سبيل المثال، يتعيّن على الأطراف المتحاربة احترام وحماية أفراد الطواقم الطبية والمرافق الطبية في جميع الأوقات،[18] بما في ذلك شرط عدم التدخل غير المبرر في عمل الخدمات الطبية واتخاذ التدابير الممكنة لحمايتهم من الضرر أو أشكال التدخل من أشخاص عاديين لا يُنسبون إلى أطراف النزاعات المسلحة.[19] وبالمثل، يجب احترام وحماية العاملين في المجال الإنساني والأعيان المستخدمة في العمليات الإنسانية؛[20] ويجب على أطراف النزاعات المسلحة السماح بمرور الأنشطة الإنسانية غير المتحيّزة وتسهيل مرورها خلال النزاعات المسلحة، مع احتفاظ الأطراف بحق مراقبتها.[21] وبالنسبة إلى كل من الخدمات الطبية والعاملين في المجال الإنساني والأعيان الإنسانية، تمتد الحماية الخاصة لتشمل الاتصالات والبيانات.[22]

ولتعزيز حماية الخدمات الطبية والأنشطة الإنسانية من المخاطر المرتبطة بتكنولوجيا المعلومات والاتصالات، يمكن إجراء مزيد من المناقشة بالتركيز على كيفية تفعيل هذه الحماية. ويتمثل أحد السبل في الجهود التي تبذلها اللجنة الدولية لاستحداث شارة رقمية، أي وسيلة لتحديد البيانات والبنية التحتية الرقمية لمنظمات وكيانات يحقّ لها عرض الشارات المميزة المعترف بها بمقتضى القانون الدولي الإنساني.[23] ويشجع القرار بشأن تكنولوجيا المعلومات والاتصالات، إذ يحيط علماً بالعمل المستمر الذي تجريه اللجنة الدولية بالتشاور مع الدول ومكونات الحركة الدولية للصليب الأحمر والهلال الأحمر، على مواصلة العمل على إجراء المشاورات، بما في ذلك بحث السبل القانونية والدبلوماسية الممكنة لاستخدام

---

[17] للاطلاع على لمحة عامة عن المواقف التي اتخذتها الدول، انظروا مجموعة أدوات القانون السيبراني (Cyber Law Toolkit)، تحت عنوان "البيانات كهدف عسكري"، على الرابط التالي: https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.

[18] انظروا، على سبيل المثال، المادة 19 من اتفاقية جنيف الأولى المؤرخة في 12 آب/أغسطس 1949؛ والمادة 12 من اتفاقية جنيف الثانية المؤرخة في 12 آب/أغسطس 1949؛ والمادة 18 من اتفاقية جنيف الرابعة المؤرخة في 12 آب/أغسطس 1949، والمادة 12 من البروتوكول الإضافي الأول، والمادة 11 من البروتوكول الإضافي الثاني المؤرخ 8 حزيران/يونيو 1977، واللجنة الدولية للصليب الأحمر، دراسة القانون الدولي الإنساني العرفي، على الرابط التالي: https://ihl-databases.icrc.org/ar/customary-ihl/rules (المشار إليها فيما بعد باللجنة الدولية، دراسة القانون الدولي الإنساني العرفي)، القواعد 25 و28 و29.

[19] اللجنة الدولية للصليب الأحمر، *التعليق على البروتوكولين الإضافيين*، الفقرة 517 بشأن المادة 12 من البروتوكول الأول، واللجنة الدولية للصليب الأحمر، *التعليق على اتفاقية جنيف الأولى: الاتفاقية (الأولى) لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان*، الطبعة الثانية، اللجنة الدولية، جنيف/جامعة كامبريدج، كامبريدج، 2016 (المشار إليها فيما بعد باسم اللجنة الدولية، التعليق على اتفاقية جنيف الأولى، 2016)، الفقرة 1799 بشأن المادة 19.

[20] المادتان 70(4) و71(2) من البروتوكول الإضافي الأول؛ واللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدتان 31 و32.

[21] انظروا المادة 23 من اتفاقية جنيف الرابعة، والمادة 70(2) من البروتوكول الإضافي الأول؛ والمادة 18(2) من البروتوكول الإضافي الثاني؛ واللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدة 55.

[22] اللجنة الدولية، التعليق على اتفاقية جنيف الأولى، 2016، الفقرة 1804 بشأن المادة 19.

[23] مشروع الشارة الرقمية هو مشروع مستقل تقوده اللجنة الدولية بالتشاور والتعاون مع الدول ومكونات الحركة الدولية للصليب الأحمر والهلال الأحمر. ولن تركّز المناقشة في مسار العمل هذا على هذا المشروع.

الشارة الرقمية.[24]

وعلاوة على ذلك، تندرج أنشطة تكنولوجيا المعلومات والاتصالات التي "تدمر أو تنقل أو تعطّل" الأعيان التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، ومثالها مرافق مياه الشرب وأشغال الري، ضمن نطاق الحماية الخاصة التي يوفّرها القانون الدولي الإنساني لهذه الأعيان، بغض النظر عما إذا كانت تُصنّف كهجمات أم لا.[25] وتمتد الحماية الخاصة لتشمل البنية التحتية لتكنولوجيا المعلومات والاتصالات التي لا "لا غنى عنها" بحد ذاتها لتشغيل هذه الأعيان. وثمة حاجة إلى إجراء مزيد من المناقشة بشأن التدابير الرامية إلى تفعيل هذه الحماية.

وأخيراً، تحظر قواعد القانون الدولي الإنساني العنف الجنسي وتوفر حماية خاصة لفئات معينة من الأشخاص، بمن فيهم على سبيل المثال لا الحصر النساء وكبار السن والأشخاص ذوو الإعاقة والأطفال (على سبيل المثال، ضد التجنيد غير القانوني أو الاستغلال في العمليات العدائية).[26] وثمة حاجة إلى إجراء مزيد من المناقشة بشأن التدابير العملية لضمان الامتثال لهذه القواعد بما في ذلك عندما تيسّر تكنولوجيا المعلومات والاتصالات ارتكابه.

ثانياً– حماية المدنيين وغيرهم من الأشخاص المحميين من انتشار المعلومات في انتهاك للقانون الدولي الإنساني خلال النزاعات المسلحة

تنشر الدول والمجموعات المسلحة من غير الدول المعلومات الرقمية لأغراض متنوعة، بما في ذلك عند تنفيذ عمليات معلوماتية أو نفسية. وتهدف بعض العمليات إلى الحد من خطر إلحاق الضرر بالبشر خلال النزاعات المسلحة، على سبيل المثال من خلال توجيه إنذار مسبق وفعال للمدنيين في حالة هجوم أو مساعدتهم على الوصول إلى بر الأمان. وتُصمّم عمليات أخرى للتسبّب في ارتباك أو ضرر، أو خداع الخصم، أو دعم الأهداف العسكرية أو السياسية لأحد أطراف النزاع. وفي النزاعات المسلحة اليوم، تُستخدم أنشطة تكنولوجيا المعلومات والاتصالات لنشر المعلومات في انتهاك للقانون الدولي الإنساني. ويمكن أن يسهم انتشار المعلومات عن طريق أنشطة تكنولوجيا المعلومات والاتصالات في العنف أو يشجع عليه، ويسبّب ضرراً نفسياً دائماً، ويعرقل الوصول إلى الخدمات الأساسية، ويعطل عمليات المنظمات الإنسانية، مما قد يقوّض الثقة في هذه المنظمات.

ويتضمن القانون الدولي الإنساني عدة قواعد محددة تفرض قيوداً على نشر المعلومات، بما في ذلك عن طريق الوسائل الرقمية، ولا سيما ما يلي:

- يجب ألّا يشجّع المسؤولون المدنيون والعسكريون التابعون لطرف في نزاع مسلح على ارتكاب انتهاكات القانون الدولي الإنساني، بما في ذلك من خلال المنصات الرقمية.[27] ويعيد القرار بشأن تكنولوجيا المعلومات والاتصالات التأكيد على حظر التشجيع أو التحريض على ارتكاب انتهاكات القانون الدولي الإنساني من خلال الوسائل الرقمية.[28]
- يجب حماية أسرى الحرب وغيرهم من الأشخاص المحميين بموجب القانون الدولي الإنساني من فضول الجماهير.[29] وإن المشاركة العلنية

---

[24] الفقرة 15 من الديباجية والفقرة 12 من منطوق القرار بشأن تكنولوجيا المعلومات والاتصالات.

[25] تشمل الأمثلة على هذه الأعيان، على سبيل المثال لا الحصر، " المواد الغذائية والمناطق الزراعية التي تنتجها والمحاصيل والماشية ومرافق مياه الشرب وشبكاتها وأشغال الري." المادة 54(2) من البروتوكول الإضافي الأول، والمادة 14 من البروتوكول الإضافي الثاني؛ واللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدة 54. وانظروا أيضاً اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2024، الصفحتان 46–47.

[26] اللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القواعد 134 و135 و138.

[27] المادة المشتركة 1 من اتفاقية جنيف الرابعة؛ واللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدة 139.

[28] الفقرة 4 من القرار بشأن تكنولوجيا المعلومات والاتصالات.

[29] انظروا، على سبيل المثال، المادة 13 من اتفاقية جنيف الثالثة المؤرخة في 12 آب/أغسطس 1949 والمادة 27 من اتفاقية جنيف الرابعة.

من قبل السلطات للبيانات والصور ومقاطع الفيديو الخاصة بأسرى الحرب وغيرهم من المحرومين من حريتهم، مع مراعاة الاستثناءات المحدودة، من شأنه أن ينتهك هذه القاعدة، ويجب على الدول أن تحميها من المشاركة من جانب كيانات خاصة أيضاً.[30]

- يُحظر بموجب القانون الدولي الإنساني التهديد بالعنف الرامي أساساً إلى بث الذعر بين السكان المدنيين.[31]
- إن نشر أطراف النزاع المسلح معلومات خاطئة لعرقلة العمل الطبي أو الإنساني يتعارض مع الاتزامات باحترام وحماية العاملين في المجالين الطبي والإنساني وأنشطتهم.[32]
- إن المعلومات أو الدعاية التي تنشر بغرض تجنيد الأطفال، أو الأشخاص المحميين في الأراضي المحتلة، في القوات المسلحة أمر غير قانوني.[33]

ونظراً إلى مخاطر الضرر المذكورة أعلاه على المدنيين وغيرهم من الأشخاص المحميين بموجب القانون الدولي الإنساني، ثمة حاجة إلى مزيد من المناقشة لتكوين أوجه فهم مشتركة بشأن كيفية انطباق القانون الدولي الإنساني على نشر المعلومات، بما يضمن الحماية الفعالة لجميع الأشخاص والأعيان المحميين بموجب القانون الدولي الإنساني.

ثالثاً- خطر الضرر الناجم عن الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، وإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة

الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات وما يترتب عليه من آثار على الحماية التي تتمتّع بها بموجب القانون الدولي الإنساني.

إن الفضاء السيبراني ذو طبيعة مدنية أساساً باستثناء بعض الشبكات العسكرية المعيّنة. ولكن الترابط القائم بين الشبكات المدنية والعسكرية واستخدام الجيش للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات يطرحان تحديات خاصة أمام حمايته.

وإذا استُخدمت البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات – بما فيها البنية التحتية التي توفّرها شركات التكنولوجيا – لأغراض عسكرية (وفي هذه الحالة، تُوصف هذه البنية التحتية أحياناً بأنها "مزدوجة الاستخدام")، فإنها تتعرض لخطر التحوّل إلى هدف عسكري بموجب القانون الدولي الإنساني، وتفقد حمايتها من الهجوم.[34] وفي هذه الحالات، قد يتعرّض المدنيون والأعيان المدنية التي تكون على مقربة فعلية من هذه البنية التحتية، أو متصلة رقمياً بها، أو تعتمد عليها، لأضرار عرضية.

ولكن لا يحوّل كل استخدام عسكري عيناً مدنية إلى هدف عسكري بموجب القانون الدولي الإنساني؛ إذ لا يحدث ذلك إلّا عندما يستوفي

---

[30] للاطلاع على مزيد من المناقشة بشأن هذه المسألة، انظروا، على سبيل المثال، اللجنة الدولية، *التعليق على اتفاقية جنيف الثالثة: الاتفاقية (الثالثة) بشأن معاملة أسرى الحرب، الطبعة الثانية*، اللجنة الدولية، جنيف، 2020 (المشار إليها فيما بعد باسم اللجنة الدولية، التعليق على اتفاقية جنيف الثالثة، 2020)، الفقرات 1623–1632.

[31] المادة 51(2) من البروتوكول الإضافي الأول؛ المادة 13(2) من البروتوكول الإضافي الثاني؛ والمادة اللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدة 2.

[32] وهو يختلف بالطبع عن النقد أو التعبير عن الغضب من قبل السلطات أو المستفيدين الموجه إلى الخدمات الطبية أو المنظمات الإنسانية، والذي لا يعتبر غير قانوني في ظاهره.

[33] فيما يتعلق بتجنيد الأطفال، انظروا اللجنة الدولية، دراسة القانون الدولي الإنساني العرفي، القاعدة 136 والالتزامات بموجب البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في المنازعات المسلحة المؤرخ 25 أيار/مايو 2000. وفيما يتعلق بالأشخاص المحميين في حالات الاحتلال، انظروا المادة 51 من اتفاقية جنيف الرابعة.

[34] قد تصبح الأعيان ذات الاستخدام المزدوج أهدافاً عسكرية إذا كانت، في ظل الظروف السائدة حينذاك، تستوفي التعريف الوارد في المادة 52(2) من البروتوكول الإضافي الأول: "تنحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها أو بموقعها أو بغايتها أو باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة".

الاستخدام معايير الهدف العسكري كما يعرّفه القانون الدولي الإنساني. وعلاوة على ذلك، حتى لو اعتبر أحد الأطراف المتحاربة أن أحد المدنيين أو إحدى الأعيان المدنية قد فقد الحماية بسبب مشاركته في عمليات تكنولوجيا المعلومات والاتصالات، يظل أي هجوم خاضعاً للحظر المفروض على الهجمات العشوائية وغير المتناسبة والالتزام باتخاذ جميع الاحتياطات الممكنة. وإضافة إلى ذلك، قد لا يجوز مهاجمة بعض الأعيان المشمولة بحماية خاصة على الإطلاق، أو قد تخضع لقيود أكثر صرامة، حتى عندما تستوفي تعريف الهدف العسكري.

ولحماية السكان المدنيين والخدمات المدنية الأساسية التي تعتمد على البنية التحتية لتكنولوجيا المعلومات والاتصالات، من الضروري إجراء مزيد من المناقشة لتحديد متى يحوّل الاستخدام العسكري للبنية التحتية لتكنولوجيا المعلومات والاتصالات، التي تكون ذات طبيعة مدنية أساساً، إلى هدف عسكري، ولتحديد تدابير حماية أخرى ممكنة وتنفيذها. وعلى سبيل المثال، دعت اللجنة الدولية الدول، كلما تسنى لها، أن تفصل البنية التحتية لتكنولوجيا المعلومات والاتصالات (أو أجزاء منها) التي تستخدم لأغراض عسكرية عن البنية التحتية المدنية من الناحية المادية أو التقنية.[35] ومن الضروري أيضاً ضمان احترام أي حماية خاصة تُمنح بموجب القانون الدولي الإنساني.

إشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة

في النزاعات المسلحة اليوم، تشكّل عدة اتجاهات مخاطر على المدنيين: إذ يستهدف القراصنة المدنيون بشكل متزايد الأعيان المدنية في عمليات تكنولوجيا المعلومات والاتصالات؛ وتشجّع أطراف النزاعات المسلحة المدنيين على جمع المعلومات ذات الأهمية العسكرية عبر الوسائل الرقمية، مما يعرّضهم للهجمات؛ وتتعرّض شركات التكنولوجيا المدنية التي تقدّم خدمات وبنية تحتية في مجال تكنولوجيا المعلومات والاتصالات إلى القوات المسلحة لخطر فقدان حمايتها القانونية.

ويستند القانون الدولي الإنساني على مبدأ التمييز الأساسي. ويهدّد تزايد إشراك المدنيين في عمليات تكنولوجيا المعلومات والاتصالات والاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات بتقويض الحماية التي يرمي هذا المبدأ الأساسي إلى توفيرها للمدنيين، بما في ذلك من خطر إساءة تحديدهم كأهداف مشروعة.

ويجب على الأفراد والمجموعات، بمن فيهم القراصنة وموظفو شركات التكنولوجيا، الذين ينفذون أنشطة تكنولوجيا المعلومات والاتصالات في سياق النزاعات المسلحة، الامتثال للقيود التي يفرضها القانون الدولي الإنساني على هذه الأنشطة،[36] والعلم بالمخاطر التي تنطوي عليها. وفي حالات استثنائية، قد تصل مشاركة المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات إلى "المشاركة المباشرة في الأعمال العدائية"، وهذا يعني أن المدني يفقد الحماية من الهجوم طوال الفترة التي يكون فيها هذا هو الحال. ولكن ينص القانون الدولي الإنساني، في حالة الشك، على أنه مدني ومشمول بالحماية بصفته هذه.[37]

---

[35] فعلى سبيل المثال، عند اتخاذ قرار بشأن تخزين بيانات عسكرية على سحابة تجارية غير مجزأة، أو جزء من سحابة تجارية، أو بنية تحتية رقمية عسكرية مخصصة، لا ينبغي للمخططين والمشغلين العسكريين استخدام السحابة التجارية غير المجزأة. انظروا اللجنة الدولية، *القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة*، 2024، الصحفتان 53–54.

[36] فيما يتعلق بالقراصنة المدنيين العاملين في سياق النزاعات المسلحة، يرد ملخص لهذه القيود في تقرير اللجنة الدولية، "8 قواعد للقراصنة المدنيين أثناء الحرب، وأربعة التزامات على عاتق الدول لمنعهم"، على الرابط التالي: https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them. وللاطلاع على أهمية القانون الدولي الإنساني للشركات الخاصة، انظروا عامة تقرير اللجنة الدولية، "*Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*"، 2024.

[37] المادة 50(1) من البروتوكول الإضافي الأول. وفي حال وجود خطر استدراج الأطفال إلى الأعمال العدائية من خلال أنشطة تكنولوجيا المعلومات والاتصالات، واعتبارهم مشاركين فيها بشكل مباشر، يقع على عاتق الأطراف المتحاربة التزام إضافي بمنع مشاركة الأطفال دون سن 15 أو 18 عاماً، وفقاً للإطار القانوني المعمول به.

فيما يتعلق بمشاركة المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، تجدر الإشارة إلى أن الدول قد تعهدت باحترام القانون الدولي الإنساني وكفالة احترامه. وإذا كان قراصنة مدنيون، أو شركات خاصة، أو أفراد أو كيانات خاصة أخرى، تعمل بناء على توجيهات أو تحت إشراف أو سيطرة دولة ما، فإن تلك الدولة مسؤولة قانوناً على الصعيد الدولي عن أي سلوك يصدر عن هؤلاء الأفراد يتعارض مع التزاماتها القانونية الدولية، بما في ذلك القانون الدولي الإنساني.[38]

وحتى لو لم يُنسب سلوك المدنيين إلى طرف في نزاع مسلح، فإن الدول ملزمة مع ذلك بضمان احترام القانون الدولي الإنساني. وعلى الأقل، يجب على أطراف النزاع المسلح ألّا تشجّع أو تساعد أو تدعم المدنيين المشاركين في أنشطة تكنولوجيا المعلومات والاتصالات على انتهاك القانون الدولي الإنساني،[39] مثلاً عن طريق تشجيع المدنيين على شنّ عمليات تكنولوجيا المعلومات والاتصالات ضد الأعيان المدنية. وعلاوة على ذلك، يجب على الدول نشر المعرفة بالقانون الدولي الإنساني، ومنع انتهاكاته وقمعها، والتحقيق في جرائم الحرب ومقاضاة مرتكبيها، بما في ذلك تلك التي يرتكبها السكان المدنيون.[40]

[38] بموجب القانون الدولي العام، تتحمل الدولة مسؤولية سلوك الأفراد أو المجموعات أو الكيانات الخاصة – بمن فيهم القراصنة المدنيون أو مجموعات القراصنة – إذا "فوّض لهم قانون تلك الدولة ممارسة بعض اختصاصات السلطة الحكومية"، أو "يعملون في الواقع بناءً على تعليمات تلك الدولة أو تحت إشرافها أو سيطرتها". انظروا لجنة القانون الدولي، *مسؤولية الدول عن الأفعال غير المشروعة دولياً*، 2001، المادتان 5 و8.

[39] اللجنة الدولية، التعليق على اتفاقية جنيف الثالثة، 2020، الفقرة 191 بشأن المادة 1.

[40] اللجنة الدولية، التعليق على اتفاقية جنيف الثالثة، 2020، الفقرة 183 بشأن المادة 1.