مشروع وثيقة للمشاورة الرابعة مع الدول

مسار العمل 6 – ضمان احترام القانون الدولي الإنساني في استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة

تشارك في رئاسة المشاورة غانا ولوكسمبورغ والمكسيك وسويسرا واللجنة الدولية للصليب الأحمر

لمحة عامة

أصبحت تكنولوجيات المعلومات والاتصالات وسائل لا غنى عنها في حياة الأشخاص في جميع أنحاء العالم. ففي عالمنا الذي يستخدم التكنولوجيات الرقمية وتكنولوجيات الاتصال بالإنترنت، تعتمد الخدمات الأساسية للسكان المدنيين، فضلاً عن قدرة الناس على التواصل مع أحبائهم والسعي إلى تحقيق التنمية الاقتصادية، على سلامة تكنولوجيات المعلومات والاتصالات وتوفّرها. وفي المناطق المتضررة من النزاعات، تكتسي تكنولوجيات المعلومات والاتصالات الموثوقة أهمية بالغة بالنسبة إلى المدنيين للحصول على السّلع والخدمات الأساسية، وبالنسبة إلى الحكومات لتقديم الخدمات، وفيما يخص دعم الأنشطة الطبية والإنسانية، بما فيها أنشطة الحركة الدولية للصليب الأحمر والهلال الأحمر. وفي حين قد تمكّن قدرات تكنولوجيا المعلومات والاتصالات الأطراف المتحاربة من تحقيق أهداف عسكرية دون التسبّب بالضرورة في ضرر على المدنيين أو الأعيان المدنية، أو تقليل الضرر اللاحق بهم، مقارنة بالعمليات الحركية، فإن استخدامها في النزاعات المعاصرة قد أدى أيضاً إلى ظهور أنشطة ضارة بواسطة تكنولوجيا المعلومات والاتصالات تؤثر على السكان المدنيين والبنية التحتية المدنية، بما في ذلك عبر الحدود الدولية.

وأكّد مسار العمل على وجوب حماية السكان المدنيين وصون كرامة الإنسان في النزاعات المعاصرة والمستقبلية. وتحقيقاً لهذه الغاية، من الضروري ضمان احترام القانون الدولي الإنساني وتعزيز احترامه في استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة، لكفالة عدم تعطيل بنيتنا التحتية وشبكاتنا، وعدم تقويض قدرتنا على التواصل، وعدم حذف بياناتنا، وعدم شلّ مجتمعاتنا.

وعلاوة على ذلك، أعدّ مسار العمل توصيات عملية مبيّنة أدناه، تهدف بالأخص إلى ما يلي:

- حماية السكان المدنيين والبيانات والبنية التحتية المدنية من الأنشطة الضارة بواسطة تكنولوجيا المعلومات والاتصالات.
- حماية الخدمات الطبية والأنشطة الإنسانية من التهديدات الرقمية، والالتزام بالحظر المفروض على العنف الجنسي وتجنيد الأطفال واستخدامهم في الأعمال العدائية، بما في ذلك عبر الوسائل الإلكترونية.
- التصدي لانتشار المعلومات في انتهاك للقانون الدولي الإنساني.
- التقليل إلى أدنى حد من مخاطر إلحاق الضرر بالسكان المدنيين الناجمة عن استخدام البنية التحتية المدنية لتكنولوجيا المعلومات

والاتصالات لأغراض عسكرية، ومنع المدنيين – بدءاً من القراصنة ووصولاً إلى موظفي شركات التكنولوجيا – المشاركين في أنشطة تكنولوجيا المعلومات والاتصالات من انتهاك القانون الدولي الإنساني أو تعريض أنفسهم للخطر دون قصد.

ومن أجل تعزيز الامتثال للقانون الدولي الإنساني فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات، أكّد مسار العمل على أهمية ما يلي:

- الإقرار بأن تكنولوجيات المعلومات والاتصالات الموثوقة تكتسي أهمية بالغة بالنسبة إلى المدنيين والحكومات والجهات الفاعلة الإنسانية في المناطق المتضررة من النزاعات، وأن أنشطة تكنولوجيا المعلومات والاتصالات قد تتسبّب في خسائر بشرية، بما في ذلك المعاناة أو الإصابات أو الدمار، حتى دون إحداث أضرار مادية، مما يؤكد على ضرورة احترام مبدأ الإنسانية وصون كرامة الإنسان في الحرب.
- الالتزام بتعزيز وتوضيح انطباق القانون الدولي الإنساني على أنشطة تكنولوجيا المعلومات والاتصالات، واتّخاذ تدابير عملية، بشكل فردي وجماعي، للتخفيف من المخاطر التي يتعرّض لها السكان المدنيون، وضمان أن تظل أنشطة تكنولوجيا المعلومات والاتصالات متّسقة مع أوجه الحماية التي يوفّرها القانون الدولي الإنساني.
- مواصلة دراسة ومناقشة كيفية انطباق القانون الدولي الإنساني على أنشطة تكنولوجيا المعلومات والاتصالات، استناداً إلى المناقشات التي جرت في إطار مسار العمل، بهدف تعزيز فهم مشترك يكفل حماية المدنيين من الضرر.
- تعزيز الشفافية من خلال مشاركة وجهات النظر الوطنية علناً بشأن كيفية انطباق القانون الدولي، بما في ذلك القانون الدولي الإنساني، على أنشطة تكنولوجيا المعلومات والاتصالات، فضلاً عن تبادل الدروس المستخلصة والممارسات الجيّدة بشأن التخفيف من الضرر الذي يلحق بالمدنيين.
- دعم بناء القدرات على المستويات الثنائية والإقليمية والعالمية لتعزيز قدرة الدول على تنفيذ القانون الدولي الإنساني وتطبيقه فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات.

النتائج

1- حماية السكان المدنيين والبيانات والبنية التحتية المدنية من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة

تبيّن النزاعات المسلحة المعاصرة أن أنشطة تكنولوجيا المعلومات والاتصالات قد تشكّل مخاطر على السكان المدنيين والبيانات والبنية التحتية المدنية. ويمكن أن تؤثر هذه الأنشطة تأثيراً خطيراً على المدنيين وغيرهم من الأشخاص والأعيان المحميين، بما في ذلك في حال تعطّيل الخدمات المدنية الأساسية، مثل الكهرباء أو المياه أو الصرف الصحي أو الاتصالات أو الرعاية الصحية أو الخدمات الإنسانية وخدمات الطوارئ أو الخدمات المالية، حتى في غياب الأضرار المادية.

وعند تنفيذ أنشطة تكنولوجيا المعلومات والاتصالات في سياق النزاع المسلح أو المرتبطة به، يتعيّن الالتزام بالقانون الدولي الإنساني في جميع الأوقات، بما في ذلك مبادئ الإنسانية والضرورة العسكرية والتمييز والتناسب والاحتياطات.

وإن عمليات تكنولوجيا المعلومات والاتصالات التي يُتوقّع أن تسبّب وفاة أشخاص أو إصابتهم، أو أن تؤدي إلى إتلاف أعيان أو تدميرها، تشكّل هجمات بموجب القانون الدولي الإنساني. ويشمل ذلك العمليات التي قد تعطّل المعدات أو الأنظمة وتتطلّب اتّخاذ إجراء بشأنها (مثل الاستبدال أو إعادة التركيب أو الإصلاح) لاستعادة تشغيلها. ويجب تنفيذ عمليات تكنولوجيا المعلومات والاتصالات هذه وفقاً لجميع قواعد القانون الدولي الإنساني ومبادئه المتعلقة بسير الأعمال العدائية، بما فيها الحظر المفروض على الهجمات ضد المدنيين والأعيان المدنية والهجمات العشوائية والهجمات غير المتناسبة، ومبدأ الاحتياطات.

وتقع البيانات في صلب عالم آخذ في التوسّع الرقمي، وهي عنصر أساسي في عمل الخدمات المدنية الحيوية والأنشطة الإنسانية. وقد تؤثر طريقة معالجة البيانات خلال النزاعات المسلحة على حياة الناس وكرامتهم. فالبيانات الطبية والبيومترية والمالية والإنسانية، وغيرها من البيانات، جزء لا يتجزأ من تقديم الخدمات العامة والاجتماعية. وقد يؤدي حذف هذه البيانات أو التلاعب بها أو منع الوصول إليها أو الإفصاح عنها دون تصريح إلى تعطيل الخدمات الأساسية وتعريض الأفراد والمجتمعات لأضرار جسيمة.

وتوفّر العديد من مبادئ القانون الدولي الإنساني وقواعده الحماية للسكان المدنيين والبيانات والبنية التحتية المدنية من الأخطار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، ومنها:

- المبدأ القاضي بأنه لا يجوز لطرف في نزاع مسلح اللجوء إلّا إلى وسائل الحرب وأساليبها الضرورية لإضعاف القوات العسكرية للعدو.
- المبادئ والقواعد التي تحكم سير الأعمال العدائية، بما فيها الحظر المفروض على الهجمات ضد المدنيين والأعيان المدنية والهجمات العشوائية والهجمات غير المتناسبة، ومبدأ الاحتياطات.
- الالتزام بالحرص الدائم على حماية السكان المدنيين والأفراد المدنيين والأعيان المدنية في سير العمليات العسكرية.
- القواعد التي تحمي الممتلكات من النهب والاستلاء عليها وتدميرها.

ولا يحظر القانون الدولي الإنساني أنشطة جمع المعلومات في حد ذاتها، بما في ذلك عندما تنطوي على الوصول إلى البيانات.

ومن أجل تعزيز حماية السكان المدنيين والبيانات والبنية التحتية المدنية من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، من الضروري أن تقوم الدول وأطراف النزاعات المسلحة بما يلي:

أ) وضع إجراءات استهداف صارمة وتطبيقها فيما يتعلّق بعمليات تكنولوجيا المعلومات والاتصالات لضمان الامتثال للقانون الدولي الإنساني، بما يشمل التحقّق من أن الأهداف تُصنّف كأهداف عسكرية وليست مشمولة بحماية خاصة، وتقييم مخاطر إلحاق أضرار عرضية بالمدنيين وتجنبها أو على الأقل تقليلها إلى أدنى حد.

ب) بناء عمليات تكنولوجيا المعلومات والاتصالات التي تشمل إجراءات الاستهداف على أساس جميع المعلومات المتاحة بشكل معقول والتي التُمست بجدية من المصادر ذات الصلة، بما في ذلك البيانات والمعلومات الاستخباراتية الموثوقة، والمدعومة بمشورة قانونية، وفقاً لما يقتضيه القانون الدولي الإنساني؛ والسعي قدر المستطاع، إلى الاستعانة بخبرات متخصّصين في الأمن السيبراني وغيرهم من الخبراء التقنيين المعنيين بهيكلية البنية التحتية لتكنولوجيا المعلومات والاتصالات وترابطها ومدى اعتماد المدنيين عليها.

ج) في الحالات التي تُصنّف فيها البنية التحتية لتكنولوجيا المعلومات والاتصالات كهدف عسكري بموجب القانون الدولي الإنساني، ولكنها لا تزال تؤدي وظائف مدنية، الأخذ في الاعتبار جميع الآثار العرضية المباشرة وغير المباشرة المتوقعة بقدر معقول على السكان المدنيين والبيانات والبنية التحتية المدنية، والناتجة عن الفقدان الكلي أو الجزئي لاستخدامها المدني، بما في ذلك الآثار على الخدمات المدنية الأساسية التي توفّرها أو تمكّنها، وذلك وفقاً لمبادئ وقواعد التناسب والاحتياطات في التخطيط للهجمات وتنفيذها.

د) عند تنفيذ واجب اتّخاذ جميع الاحتياطات الممكنة عند اختيار وسائل وأساليب الحرب، اختيار الوسائل والأساليب التي يُتوقع أن تسبّب أقلّ قدر من الضرر العرضي على المدنيين، بما في ذلك من خلال إجراء تقييم دقيق لما إذا كانت الوسائل والأساليب التي تتيحها تكنولوجيا المعلومات والاتصالات أو غيرها من الوسائل والأساليب غير الحركية من شأنها أن تقلّل من مخاطر إلحاق الضرر بالمدنيين مقارنة بالبدائل الحركية المتاحة.

هـ) تطبيق قيود مناسبة جغرافياً وزمنياً وعلى مستوى الأنظمة ("التسييج") عند تنفيذ عمليات تكنولوجيا المعلومات والاتصالات،

وذلك لتجنب خطر إلحاق ضرر عرضي بالمدنيين أو التقليل منه على الأقل.

و) الرصد المستمر لعمليات تكنولوجيا المعلومات والاتصالات، وضمان وجود القدرة على تعديلها أو إيقافها لمنع إلحاق ضرر غير مقصود أو مفرط بالمدنيين. وحيثما كان ممكناً، إدراج ضمانات تقنية (مثل "مفاتيح الإيقاف في حالة الطوارئ") تمكّن من وقف عمليات تكنولوجيا المعلومات والاتصالات أو تقييدها أو عزلها إذا كان من المحتمل أن تمتد خارج نطاق هدفها المقصود، بما في ذلك إلى الشبكات أو البنية التحتية المدنية أو تلك التابعة لدول أخرى.

2- التقليل إلى أدنى حد من مخاطر إلحاق الضرر بالسكان المدنيين الناجمة عن استخدام البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات لأغراض عسكرية خلال النزاعات المسلحة

إن بيئة تكنولوجيا المعلومات والاتصالات ذات طبيعة مدنية أساساً باستثناء بعض الشبكات العسكرية المعيّنة. ولكن الترابط القائم بين الشبكات المدنية والعسكرية والاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات يطرحان تحديات خاصة أمام حمايتها.

وعندما تُستخدم البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، بما فيها البنية التحتية التي توفّرها شركات التكنولوجيا، لأغراض عسكرية، فإن كل استخدام من هذا القبيل لا يجعلها، أو حتى أجزاء منها، هدفاً عسكرياً بموجب القانون الدولي الإنساني. ومع ذلك، قد يزيد الاستخدام العسكري من خطر تعرّض هذه البنية التحتية للهجوم، مما يعرّض المدنيين والأعيان المدنية التي تكون على مقربة فعلية منها أو متّصلة رقمياً بها أو تعتمد عليها، لأضرار عرضية.

ويحظر القانون الدولي الإنساني مهاجمة الأعيان المدنية، بما فيها البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات. ومع ذلك، قد يحوّل الاستخدام العسكري هذه البنية التحتية، أو أجزاء منها، إلى أهداف عسكرية.

وعند مهاجمة هذه الأهداف العسكرية، يتعيّن على الدول وأطراف النزاعات المسلحة احترام الحظر المفروض على الهجمات العشوائية وغير المتناسبة ومبدأ الاحتياطات، بما في ذلك عندما يعتمد السكان المدنيون على هذه البنية التحتية لتكنولوجيا المعلومات والاتصالات لتوفير الخدمات الأساسية. وحيثما أمكن، يتعيّن عليها السعي إلى تنفيذ الهجمات بطريقة تؤثر فقط على تلك المكونات أو الوظائف الخاصة بالبنية التحتية لتكنولوجيا المعلومات والاتصالات المستخدمة للأغراض العسكرية وليس تلك التي تؤدي الوظائف المدنية.

ولحماية السكان المدنيين من آثار الهجمات، يتعيّن على الدول وأطراف النزاعات المسلحة، بأقصى قدر مستطاع، اتّخاذ جميع الاحتياطات اللازمة لحماية المدنيين والأعيان المدنية الخاضعة لسيطرتها من الأخطار الناجمة عن العمليات العسكرية.

ومن أجل التقليل إلى أدنى حدّ من مخاطر إلحاق الضرر بالسكان المدنيين الناجمة عن استخدام البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات لأغراض عسكرية خلال النزاعات المسلحة، وإضافة إلى التدابير الواردة في النتيجة 1 أعلاه، من الضروري أن تقوم الدول وأطراف النزاعات المسلحة التي تقع هذه البنية التحتية تحت سيطرتها بما يلي:

أ) تخصيص الموارد المالية والتقنية المناسبة، واعتماد تدابير التخطيط والتصميم والتهيئة قبل اندلا ع النزاع المسلح وخلاله.

ب) حيثما أمكن، فصل مكونات البنية التحتية لتكنولوجيا المعلومات والاتصالات المستخدمة للأغراض العسكرية عن تلك التي تؤدي الوظائف المدنية، سواء بشكل مادي أو تقني، بما في ذلك من خلال تقسيم الشبكات أو غيرها من تدابير التهيئة المناسبة. ويشمل ذلك، حيثما أمكن، فصل البيانات المستخدمة للأغراض العسكرية عن تلك التي تلبّي الاحتياجات المدنية، مثلاً عبر وضع ترتيبات منفصلة بشأن التخزين والإدارة ومراقبة الدخول.

ج) تعزيز قدرة البنية التحتية والخدمات المدنية الأساسية لتكنولوجيا المعلومات والاتصالات على الصمود، بما في ذلك من خلال الدعم الاحتياطي والتخطيط لحالات الطوارئ وغيرها من التدابير الرامية إلى الحد من مخاطر إلحاق الضرر العرضي بالمدنيين.

3- التقليل إلى أدنى حدّ من المخاطر المرتبطة بإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة الواقعين في أراضي الدولة أو المشمولين بولايتها أو الخاضعين لسيطرتها

في النزاعات المسلحة اليوم، أصبح إشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة أكثر وضوحاً. وفي بعض الحالات، تسامحت الدول مع المدنيين، أو يسّرت لهم، أو شجعتهم على تنفيذ أنشطة تكنولوجيا المعلومات والاتصالات ضد الخصم، بما فيها الأنشطة التي قد تؤثر على المدنيين والأعيان المدنية.

ومع اقتراب المدنيين أكثر من الأعمال العدائية، فهم يواجهون خطر التعرّض للضرر. وقد يجهل الكثيرون المخاطر المترتبة على ذلك، أو العواقب القانونية المحتملة لسلوكهم، أو قواعد القانون الدولي الإنساني التي يتعيّن عليهم اتباعها.

ويجب على المدنيين — بدءاً من القراصنة ووصولاً إلى موظفي شركات التكنولوجيا – الامتثال للقانون الدولي الإنساني عندما ينفّذون أنشطة تكنولوجيا المعلومات والاتصالات في سياق النزاع المسلح أو المرتبطة به.

وتتحمّل الدول وأطراف النزاعات المسلحة مسؤولية انتهاكات القانون الدولي الإنساني التي يرتكبها المدنيون، بمن فيهم القراصنة وموظفو شركات التكنولوجيا، الذين تُنسب إليهم أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة. ويتعيّن على الدول أن تبذل العناية الواجبة لمنع ارتكاب المدنيين انتهاكات القانون الدولي الإنساني بواسطة أنشطة تكنولوجيا المعلومات والاتصالات أو بتيسير منها، الواقعين في أراضيها أو المشمولين بولايتها أو الخاضعين لسيطرتها، وعليها أن تقمع هذه الانتهاكات في حال وقوعها، وفقاً لالتزاماتها بموجب القانون الدولي الإنساني. وتتعهّد الدول بإطلاع المدنيين في بلدانها بالقانون الدولي الإنساني، ولا يجوز لها أن تشجّع المدنيين أو تساعدهم أو تدعمهم على انتهاك القانون الدولي الإنساني، بما في ذلك بواسطة أنشطة تكنولوجيا المعلومات والاتصالات.

وفي بعض الظروف المحدودة، قد تصل مشاركة المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات إلى المشاركة المباشرة في الأعمال العدائية، وهذا يعني أن المدنيين يفقدون الحماية من الهجوم، ولكن فقط في الفترة التي تكون فيها مشاركتهم مباشرة. وفي حال ثار الشك، ينص القانون الدولي الإنساني على ضرورة اعتبار الشخص محمياً من الهجمات.

ولا يُسمح للأطفال بالمشاركة في الأعمال العدائية خلال النزاعات المسلحة، بما في ذلك بواسطة أنشطة تكنولوجيا المعلومات والاتصالات.

ومن أجل التقليل إلى أدنى حدّ من المخاطر المرتبطة بإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، من الضروري أن تقوم الدول وأطراف النزاعات المسلحة بما يلي:

أ) اتّخاذ خطوات ملموسة لإبلاغ المدنيين الذين قد يشاركون في أنشطة تكنولوجيا المعلومات والاتصالات في سياق النزاع المسلح أو المرتبطة به، بالمخاطر القانونية والعملية المترتبة على ذلك. ويمكن أن تشمل هذه الخطوات نشر معلومات عن قواعد القانون الدولي الإنساني عبر وسائل التواصل الاجتماعي، أو التطبيقات المخصّصة، أو الإذاعة، أو غيرها من وسائل الاتصال الجماهيري، أو وضع نماذج بشأن مدونات قواعد سلوك متوافقة مع القانون الدولي الإنساني، يُطلب من المدنيين الذين ينفّذون أنشطة تكنولوجيا المعلومات والاتصالات الالتزام بها.

ب) تجنّب إشراك المدنيين، قدر المستطاع، في عمليات تكنولوجيا المعلومات والاتصالات التي تصل إلى مستوى المشاركة المباشرة في الأعمال العدائية، وذلك لحمايتهم من الأخطار الناجمة عن العمليات العسكرية. وفي حال حدوث هذه المشاركة مع ذلك، إدراج هؤلاء المدنيين في القوات المسلحة قدر المستطاع.

ج) اتّخاذ جميع التدابير الممكنة لمنع مشاركة الأطفال في الأعمال العدائية بواسطة أنشطة تكنولوجيا المعلومات والاتصالات، على سبيل المثال من خلال برامج التوعية والتثقيف الموجّهة إلى الأطفال ومقدّمي الرعاية؛ ومواءمة التشريعات والسياسات الوطنية التي تحظر تجنيد الأطفال واستخدامهم لتشمل التعامل مع الوسائل الإلكترونية، وإنفاذها؛ والنظر، عند الاقتضاء، في فرض قيود عمرية

على الوصول إلى الأدوات الرقمية الذي قد يصل إلى مستوى المشاركة المباشرة في الأعمال العدائية.

4- حماية منتجات وخدمات تكنولوجيا المعلومات والاتصالات المدنية التي تقدمها شركات التكنولوجيا خلال النزاعات المسلحة

تقدّم شركات التكنولوجيا بشكل متزايد خدمات الأمن السيبراني وغيرها من خدمات أو منتجات تكنولوجيا المعلومات والاتصالات إلى أطراف النزاعات المسلحة. وفي هذه الحالات، قد يتعرّض المدنيون والأعيان المدنية التي تعتمد على هذه المنتجات والخدمات أو ترتبط بها للخطر.

وفي الوقت نفسه، تُستخدم منتجات وخدمات تكنولوجيا المعلومات والاتصالات التي تقدمها شركات التكنولوجيا على نطاق واسع من قبل السكان المدنيين والحكومات والمنظمات الإنسانية غير المتحيّزة، بما في ذلك خلال النزاعات المسلحة. ولذلك، فإن تعطيلها أو تدهورها أو إساءة استخدامها قد يؤدي إلى عواقب إنسانية وخيمة. وتخضع هذه المنتجات والخدمات المدنية لتكنولوجيا المعلومات والاتصالات، وكذلك الموظفون المدنيون الذين يقدمونها، للحماية بموجب القانون الدولي الإنساني.

ومن أجل تعزيز حماية المنتجات والخدمات المدنية لتكنولوجيا المعلومات والاتصالات التي تقدمها شركات التكنولوجيا خلال النزاعات المسلحة، ينبغي لشركات التكنولوجيا القيام بما يلي:

أ) إدراك أن تقديم منتجات وخدمات تكنولوجيا المعلومات والاتصالات لأطراف النزاعات المسلحة ينطوي على مخاطر قانونية وعملية على حد سواء.

ب) فهم هذه المخاطر وتقييمها واتّخاذ التدابير اللازمة للتقليل إلى أدنى حدّ من مخاطر إلحاق الضرر بالمدنيين والأعيان المدنية، سواء كانوا موظفين في هذه الشركات أو ممتلكات لها، أو بسبب قربهم المادي أو اتصالهم الرقمي بالبنية التحتية أو الخدمات ذات الصلة أو اعتمادهم عليها. ويشمل ذلك، قدر المستطاع، الفصل المادي أو التقني لبنيتها التحتية وخدماتها ومنتجاتها المستخدمة لدعم العمليات العسكرية عن تلك المستخدمة للأغراض المدنية.

ج) اتّخاذ تدابير لمنع موظفيها من المشاركة في ارتكاب انتهاكات القانون الدولي الإنساني أو تيسيرها أو التورّط فيها، بما في ذلك من خلال تقديم منتجات أو خدمات تكنولوجيا المعلومات والاتصالات لأطراف النزاعات المسلحة، واتّخاذ الإجراءات المناسبة في حال وقوع أيّ من هذه الأفعال.

5- حماية الخدمات الطبية والأنشطة الإنسانية وسائر الأشخاص والأعيان والأنشطة المشمولين بحماية خاصة من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة

يتعرّض قطاع الرعاية الصحية والمنظمات الإنسانية غير المتحيّزة بصورة خاصة لخطر أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة. ويعني الاعتماد المتزايد للخدمات الطبية والإنسانية على الأنظمة المترابطة والبيانات الرقمية أن أيّ تعطيل في البنية التحتية أو الخدمات الخاصة بتكنولوجيا المعلومات والاتصالات قد يؤثر بشكل مباشر على العمليات الطبية المنقذة للحياة، ويعرّض البيانات الحساسة للخطر، ويعيق عمل المنظمات الإنسانية غير المتحيّزة وموظفيها، ويقوّض تقديم المساعدات الأساسية.

ويجب احترام وحماية أفراد الخدمات الطبية والوحدات الطبية ووسائط النقل الطبي، فضلاً عن العاملين في المجال الإنساني والأعيان الإنسانية، في جميع الأوقات بموجب القانون الدولي الإنساني، بما في ذلك حمايتهم من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات. ويجب ألّا تعطّل أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة عمل الخدمات الطبية والأنشطة الإنسانية دون مبرّر، بما في ذلك أنظمة بياناتها وأنظمة تكنولوجيا المعلومات والاتصالات الخاصة بها وأنظمة اتصالاتها.

ويجب احترام سرية البيانات الطبية والإنسانية وفقاً للقانون الدولي الإنساني. وهذه الحماية ضرورية للحفاظ على الثقة في عمل الخدمات الطبية

والمنظمات الإنسانية غير المتحيّزة.

ويتعيّن أيضاً على أطراف النزاعات المسلحة اتّخاذ جميع التدابير الممكنة، في ظل الظروف السائدة والموارد المتاحة لها، لمنع إلحاق الضرر بالخدمات الطبية والأنشطة الإنسانية، بما في ذلك بواسطة أنشطة تكنولوجيا المعلومات والاتصالات التي تنفّذها أطراف ثالثة مثل مرتكبي الجرائم السيبرانية وغيرهم من الجهات الفاعلة من غير الدول التي لا تُنسب إلى أيّ طرف في نزاع مسلح.

وقد تواجه بعض الأعيان والأنشطة الأخرى التي تتمتّع بحماية خاصة بموجب القانون الدولي الإنساني، بما فيها الأعيان التي لا غنى عنها لبقاء السكان المدنيين والأشغال والمنشآت التي تحتوي على قوى خطرة والممتلكات الثقافية والدفاع المدني، مخاطر جسيمة ناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات. ويجب احترام الحماية الخاصة الممنوحة لها، بما في ذلك عند تنفيذ أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة. وتشمل هذه الحماية بياناتها والبنية التحتية لتكنولوجيا المعلومات والاتصالات التي لا غنى عنها لتشغيلها.

ويمكن أن تُستخدم أنشطة تكنولوجيا المعلومات والاتصالات لارتكاب أفعال العنف الجنسي أو تيسيرها، أو تجنيد الأطفال أو استخدامهم في الأعمال العدائية. ويحظر القانون الدولي الإنساني العنف الجنسي وتجنيد الأطفال واستخدامهم في الأعمال العدائية، بما في ذلك عندما تُرتكب هذه الأفعال بواسطة أنشطة تكنولوجيا المعلومات والاتصالات أو تُشجّع أو تُيسّر من خلالها.

ومن أجل حماية الخدمات الطبية والأنشطة الإنسانية وسائر الأشخاص والأعيان والأنشطة المشمولين بحماية خاصة من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، من الضروري أن تقوم الدول وأطراف النزاعات المسلحة بما يلي:

أ) دعم المناقشات والجهود الرامية إلى جعل الحماية الخاصة التي يكفلها القانون الدولي الإنساني للخدمات الطبية والأنشطة الإنسانية واضحة ومرئية في بيئة تكنولوجيا المعلومات والاتصالات، بما في ذلك من خلال إعداد "شارة رقمية"، ومواصلة التعاون مع اللجنة الدولية بشأن السُبل القانونية والتقنية والدبلوماسية لتنفيذها.

ب) التأكيد مجدداً وصراحة على التزامها باحترام الخدمات الطبية والأنشطة الإنسانية وحمايتها، بما يشمل أنظمة بيانات هذه الخدمات والأنشطة وأنظمة تكنولوجيا المعلومات والاتصالات الخاصة بها وأنظمة اتصالاتها، وتيسير عملياتها في بيئة تكنولوجيا المعلومات والاتصالات، فضلاً عن احترام الحماية الخاصة الممنوحة للأعيان التي لا غنى عنها لبقاء السكان المدنيين، بما في ذلك بياناتها والبنية التحتية لتكنولوجيا المعلومات والاتصالات التي لا غنى عنها لتشغيلها. وينبغي أن تنعكس هذه الالتزامات في القوانين والسياسات والعقيدة العسكرية والممارسات الوطنية.

ج) حيثما أمكن، دعم وضع تدابير مناسبة للأمن السيبراني وحماية البيانات وتيسيرها لمقدمي الخدمات الطبية والمنظمات الإنسانية غير المتحيّزة، والمساعدة في تعزيز قدرتهم على الصمود في وجه تهديدات تكنولوجيا المعلومات والاتصالات التي تؤثر على أنظمتهم وعملياتهم.

د) تعزيز الأطر القانونية والسياساتية الوطنية ذات الصلة التي تتناول مسألة السلوك على الإنترنت التي قد تشكل أو تيسّر انتهاكات القانون الدولي الإنساني المتعلقة بالعنف الجنسي وتجنيد الأطفال أو استخدامهم في النزاعات المسلحة، وضمان التنفيذ والتنسيق الفعالين بين السلطات المختصّة.

هـ) إدراج ضمانات محدّدة في العقيدة العسكرية وإجراءات العمل الموحدة وقواعد الاشتباك لمنع الانتهاكات التي تُرتكب بواسطة أنشطة تكنولوجيا المعلومات والاتصالات أو التي تيسّرها هذه الأنشطة، والتصدي لها، بما فيها العنف الجنسي وتجنيد الأطفال أو استخدامهم في الأعمال العدائية. وتشمل التدابير الممكنة تنظيم استخدام أجهزة تكنولوجيا المعلومات والاتصالات الشخصية في البيئات العملياتية، وتقييد مشاركة الصور أو المعلومات الحساسة، وحظر استخدام تكنولوجيات المعلومات والاتصالات لتجنيد الأطفال أو إشراكهم في الأعمال العدائية، وتوعية الأطفال ومقدّمي الرعاية بالمخاطر المرتبطة بذلك.

6- التصدي لانتشار المعلومات في انتهاك للقانون الدولي الإنساني

في النزاعات المسلحة المعاصرة، يتزايد استخدام أنشطة تكنولوجيا المعلومات والاتصالات لنشر المعلومات التي قد تنتهك القانون الدولي الإنساني. وفي حين أن العمليات المعلوماتية كانت منذ فترة طولية جزءاً لا يتجزّأ من الحرب، وليست غير مشروعة في حد ذاتها، قد يزيد استخدام تكنولوجيات المعلومات والاتصالات، وخاصة في منصات التواصل الاجتماعي أو تطبيقات المراسلة أو عند اقترانه بالذكاء الاصطناعي وغيره من التكنولوجيات الناشئة، من سرعة المعلومات الضارة ونطاقها ومدى انتشارها بدرجة كبيرة.

ويتعيّن على الدول الامتناع عن نشر المعلومات في انتهاك للقانون الدولي الإنساني واتّخاذ جميع التدابير الممكنة لمنع ذلك، بما فيها بواسطة استخدام تكنولوجيات المعلومات والاتصالات. ويشمل ذلك نشر المعلومات التي تحرّض أو تشجّع على ارتكاب انتهاكات القانون الدولي الإنساني، أو تعرّض الأشخاص المحرومين من حريتهم للشّتائم أو فضول الجماهير، أو التي يكون هدفها الأساسي بثّ الذّعر بين السكان المدنيين.

ويجب حماية الخدمات الطبية والأنشطة الإنسانية من المعلومات المضللة التي تتيحها تكنولوجيا المعلومات والاتصالات بهدف عرقلة عملها خلال النزاعات المسلحة، إذ إن هذه الأفعال تتدخّل بشكل غير مبرّر وتتعارض مع الالتزام باحترام وحماية العاملين في المجالين الطبي والإنساني وأنشطتهم.

ومن أجل معالجة انتشار المعلومات في انتهاك للقانون الدولي الإنساني، من الضروري أن تقوم الدول وأطراف النزاعات المسلحة بما يلي:

أ) اتّخاذ جميع التدابير الممكنة لتقييم مخاطر إلحاق العمليات المعلوماتية الضرر بالسكان المدنيين وغيرهم من الأشخاص المحميين، بما في ذلك من خلال تقويض سلامتهم أو كرامتهم أو قدرتهم على الحصول على الخدمات الأساسية، ومنع وقوع هذه المخاطر والتخفيف منها.

ب) الامتناع عن نشر المعلومات التي تجرّد الخصم من إنسانيته أو تنشر الكراهية ضد السكان المدنيين، بما في ذلك بواسطة تكنولوجيات المعلومات والاتصالات، واتّخاذ التدابير المناسبة لضمان عدم مشاركة قواتها المسلحة أو سلطاتها العامة الأخرى أو الأشخاص الذين يعملون نيابة عنها في انتهاج هذا السلوك.

ج) تقديم الدعم، حيثما أمكن، إلى مقدمي الخدمات الطبية والمنظمات الإنسانية غير المتحيّزة في بناء القدرات على تعزيز الصمود في وجه المعلومات المضللة وغيرها من الأنشطة المعلوماتية الضارة، بما في ذلك تيسير قدرتهم على جمع المعلومات الدقيقة والتحقّق منها ونشرها؛ وتعزيز جاهزيتهم وخططهم للطوارئ لمواجهة التعرّض للمعلومات الضارة؛ وتشجيع تطوير استجابات مناسبة للسياق من أجل التصدي للمعلومات الضارة التي تؤثر على المدنيين في مناطق عملياتهم.

د) التعاون مع الجهات الفاعلة ذات الصلة، بما فيها قطاع التكنولوجيا، للحد من مخاطر استخدام المنصات الإلكترونية أو غيرها من خدمات تكنولوجيا المعلومات والاتصالات للتحريض على انتهاكات القانون الدولي الإنساني أو تشجيعها أو تيسيرها، أو لإلحاق الضرر بالمدنيين والأعيان المدنية على نحو آخر. وقد يشمل ذلك وضع أُطر قانونية وسياساتية مناسبة، وتشجيع شركات التكنولوجيا على اعتماد ضمانات وممارسات مصمّمة للكشف عن المعلومات الضارة وتقييمها ومعالجتها في حالات النزاع المسلح.

هـ) تعزيز قدرة المجتمعات على الصمود في وجه الأنشطة المعلوماتية الضارة، بما في ذلك دعم إتاحة المعلومات الموثوقة، وحماية الصحفيين ووسائل الإعلام حيثما يقتضي ذلك القانون الدولي الإنساني وغيره من القوانين المنطبقة، وتعزيز تدابير التأهب التي تحسّن قدرة السكان المدنيين على الوصول إلى المعلومات الجديرة بالثقة خلال النزاعات المسلحة.

و) الامتناع عن إغلاق سُبل وصول المدنيين إلى الإنترنت أو خدمات تكنولوجيا المعلومات والاتصالات الأخرى، نظراً إلى أن هذه التدابير قد تعرّض السكان المدنيين للخطر. وحيثما تكون القيود مبرّرة بالضرورة العسكرية الملحة، اتّخاذ تدابير تخفيفية للتقليل إلى

أدنى حدّ ممكن من الآثار السلبية على المدنيين.

7- تدابير شاملة لتعزيز تنفيذ القانون الدولي الإنساني فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات

من الضروري أن تقوم الدول بما يلي عند تنفيذ التزاماتها بموجب القانون الدولي الإنساني فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات، وبما يشمل تدابير التنفيذ المتّخذة في وقت السلم:

أ) نشر المعرفة بالقانون الدولي الإنساني داخل القوات المسلحة وفي أوساط السكان على نطاق أوسع، ولا سيما أولئك الذين قد يشاركون في أنشطة تكنولوجيا المعلومات والاتصالات، وإدراج مبادئ القانون الدولي الإنساني وقواعده وتطبيقها على أنشطة تكنولوجيا المعلومات والاتصالات في التشريعات الوطنية، والعقيدة العسكرية، والإجراءات العملياتية الموحدة، وقواعد الاشتباك وبرامج التدريب، حسب الاقتضاء.

ب) توفير مستشارين قانونيين مؤهلين للوحدات والقيادات العسكرية المسؤولة عن أنشطة تكنولوجيا المعلومات والاتصالات، ولا سيما في التخطيط لهذه العمليات وتنفيذها.

ج) إجراء استعراضات قانونية لقدرات تكنولوجيا المعلومات والاتصالات التي تعمل كأسلحة أو وسائل أو أساليب حرب جديدة، عن طريق أمور منها إجراء عمليات اختبار وتقييم وتحقّق وتصديق صارمة لقدرات تكنولوجيا المعلومات والاتصالات، من أجل التوصّل إلى فهم أفضل لكيفية عملها وانتشارها وآثارها المحتملة على الأنظمة المدنية.

د) اتّخاذ جميع التدابير التشريعية والتنظيمية وغيرها من التدابير اللازمة، بما في ذلك العقوبات الجنائية عند الاقتضاء، لمنع وقمع انتهاكات القانون الدولي الإنساني التي تُرتكب بواسطة أنشطة تكنولوجيا المعلومات والاتصالات أو بتيسّير منها، سواء من قِبل أشخاص مشمولين بولايتها أو خاضعين لسيطرتها أو على إقليم خاضع لولايتها أو لسيطرتها.

هـ) اتّخاذ جميع التدابير الممكنة لمنع أو الحد من انتشار أدوات وقدرات تكنولوجيا المعلومات والاتصالات أو استخدامها لأغراض أخرى أو إساءة استخدامها، حيثما يوجد خطر واضح من أنها ستساهم في انتهاكات القانون الدولي الإنساني.

و) تشجيع التبادل الطوعي للمعلومات وتدابير بناء الثقة الرامية إلى الحد من المخاطر التي تهدّد البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، بما في ذلك تبادل أفضل الممارسات بين الدول، وإنشاء قنوات اتصال وغيرها من الترتيبات العملية للحد من المخاطر، وعند الاقتضاء، الإبلاغ الطوعي عن حوادث تكنولوجيا المعلومات والاتصالات الجسيمة التي تسبّبت في أضرار مدنية غير مقصودة، وذلك لتعزيز الفهم الجماعي والتخفيف من المخاطر.

ز) تعزيز الشفافية والفهم المشترك من خلال صياغة وجهات النظر الوطنية ومشاركتها علناً بشأن كيفية انطباق القانون الدولي، بما في ذلك القانون الدولي الإنساني، على أنشطة تكنولوجيا المعلومات والاتصالات، ومن خلال تبادل الدروس المستخلصة والممارسات الجيّدة للتقليل إلى أدنى حدّ من الأضرار التي تلحق بالمدنيين.

ح) دعم بناء القدرات على المستويات الثنائية والإقليمية والعالمية لتعزيز قدرة الدول على تنفيذ القانون الدولي الإنساني وتطبيقه فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات.

ط) تعزيز التعاون بين الدول وشركات التكنولوجيا والمنظمات الإنسانية غير المتحيّزة والمجتمع المدني لاستخدام تكنولوجيات المعلومات والاتصالات بما يعزّز حماية المدنيين، وبسبل منها وضع توجيهات أو ترتيبات عملية محدّدة حسب السياق.

ي) تشجيع التعاون بين شركات التكنولوجيا والمنظمات الإنسانية غير المتحيّزة لتحسين التأهب والاستجابة لتهديدات تكنولوجيا المعلومات والاتصالات التي تؤثر على الأشخاص والأعيان المحميين، بما في ذلك من خلال تبادل المعلومات ودعم الأمن السيبراني،

مع احترام المبادئ الإنسانية المتمثلة في الحياد وعدم التحيّز والاستقلال.

ك) إدراج النُهج المراعية للنوع الاجتماعي والعمر والشاملة لمسألة الإعاقة، في الأطر الوطنية والممارسات الميدانية لتعزيز تنفيذ القانون الدولي الإنساني، بما في ذلك تحديد المخاطر المتعلقة بتكنولوجيا المعلومات والاتصالات ومعالجتها.