مشروع وثيقة المشاورة الخامسة 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 ضرورية 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 والبيانات والبنية التحتية المدنية، بما في ذلك عبر الحدود الدولية. وقد تؤدي أوجه التفاوت في القدرات التكنولوجية والقدرة على الصمود في مجال الأمن السيبراني إلى تفاقم هذه المخاطر، بما يشمل التأثير في قدرة الدول والجهات المعنية الأخرى على منع الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات والتخفيف من حدّتها والاستجابة لها خلال النزاعات المسلحة.

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، من أجل حماية البنية التحتية والشبكات والاتصالات والبيانات المدنية من الأنشطة الضارة بواسطة تكنولوجيا المعلومات والاتصالات.

وعند استخدام الدول لتكنولوجيات المعلومات والاتصالات، عليها الامتثال للقانون الدولي، ولا سيما ميثاق الأمم المتحدة، بما يشمل الالتزام بحلّ المنازعات الدولية بالوسائل السلمية، وحظر التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو على أي وجه آخر لا يتّفق ومقاصد الأمم المتحدة. ولا يجوز أن يُفسّر أي نص ورد في القانون الدولي الإنساني على أنه يجيز أو يضفي الشرعية على أي عمل من أعمال العدوان أو استخدام آخر للقوة يتعارض مع ميثاق الأمم المتحدة. ولا يضفي انطباق القانون الدولي

الإنساني الشرعية على النزاعات أو يشجّع عليها.

وعلاوة على ذلك، حدّد مسار العمل ممارسات جيّدة وأعدّ 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.

وأكّد مسار العمل كذلك على أهمية العناصر الرئيسية التالية في تعزيز الحماية التي يوفرها القانون الدولي الإنساني فيما يتعلّق بأنشطة تكنولوجيا المعلومات والاتصالات:

- 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 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 جميع التدابير اللازمة، 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 ووثيقة النتائج هذه، بهدف مواصلة بناء فهم مشترك يكفل حماية المدنيين من الضرر، وتحسين هذا الفهم.
- 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

الأساسية – وتحديداً الخدمات الحيوية التي تكفل عيش السكان المدنيين، إضافة إلى جميع الأنظمة المترابطة التي يعتمد عليها السكان لتلبية احتياجاتهم الأساسية – مثل الكهرباء أو المياه أو الصرف الصحي أو إنتاج الأغذية وتوزيعها أو الاتصالات أو الرعاية الصحية أو التعليم 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 على سبيل المثال لا الحصر، مبادئ الإنسانية والضرورة العسكرية والتمييز والتناسب والاحتياطات.

وإن عمليات تكنولوجيا المعلومات والاتصالات التي يُتوقّع بدرجة معقولة أن تسبّب وفاة أشخاص أو إصابتهم، أو أن تؤدي إلى إتلاف أعيان أو تدميرها، تشكّل هجمات بموجب القانون الدولي الإنساني. ويشمل ذلك العمليات التي يُتوقع بدرجة معقولة أن تعطّل نُظم تكنولوجيا المعلومات والاتصالات وتتطلّب اتّخاذ إجراء بشأنها 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، وتؤدي دوراً مركزياً 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 المحلية لأضرار جسيمة. ولا يحظر القانون الدولي الإنساني أنشطة جمع المعلومات في حد ذاتها، بما في ذلك عندما تنطوي على الوصول إلى البيانات.

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:

- المبدآن اللذان مفادهما أن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقاً لا تقيّده قيود، وأنه 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 مبادئ التمييز والتناسب والاحتياطات وأوجه الحظر المتصلة بها المفروضة على الهجمات ضد المدنيين والأعيان المدنية والهجمات العشوائية والهجمات غير المتناسبة.
- الالتزام بالحرص الدائم على حماية السكان المدنيين والأفراد المدنيين والأعيان المدنية في سير العمليات العسكرية.
- القواعد التي تحمي الممتلكات من النهب والاستلاء عليها وتدميرها.

وتكتسي التدابير التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في تعزيز حماية السكان المدنيين والبيانات والبنية التحتية المدنية من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة:

أ) وضع إجراءات 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 الأضرار العرضية المباشرة وغير المباشرة المتوقعة بقدر معقول على السكان المدنيين والبيانات والبنية التحتية المدنية، والناتجة عن الفقدان الكلي أو الجزئي لاستخدامها المدني، وما يترتب عل ذلك من آثار على الخدمات المدنية 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 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، لإتاحة 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.

ز) اتّخاذ جميع التدابير المناسبة لتنفيذ أنشطة تكنولوجيا المعلومات والاتصالات التي يدعمها أو يمكّنها الذكاء الاصطناعي أو التكنولوجيات الناشئة الأخرى بما يتوافق مع القانون الدولي الإنساني ومع التدابير المذكورة أعلاه.

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، على أن يقتصر ذلك على الوقت الذي تستوفي فيه المعايير المنصوص عليها في القانون الدولي الإنساني. وتتطلب هذه القرارات عناية خاصة وتقييماً لكل حالة على حدة.

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. ويتعيّن اتّخاذ جميع الاحتياطات الممكنة لتنفيذ الهجمات بطريقة تؤثر فقط على تلك المكونات أو الوظائف الخاصة بالبنية

التحتية لتكنولوجيا المعلومات والاتصالات المستخدمة للأغراض العسكرية، وتجنّب الإضرار بتلك التي تؤدي الوظائف المدنية والتقليل إلى أدنى حدّ من الأضرار التي تلحق بها.

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.

وإضافة إلى التدابير الواردة في النتيجة 1 أعلاه، تكتسي التدابير التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في التقليل إلى أدنى حدّ من مخاطر إلحاق الضرر بالسكان المدنيين الناجمة عن استخدام البنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات لأغراض عسكرية خلال النزاعات المسلحة:

أ) تخصيص الموارد المالية والتقنية المناسبة، واعتماد تدابير التخطيط والتصميم والتهيئة قبل اندلا ع النزاع المسلح وخلاله، بهدف التقليل إلى أدنى حدّ من تعرّض المدنيين والبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات لآثار أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة.

ب) الفصل إلى أقصى حد ممكن بين مكونات البنية التحتية لتكنولوجيا المعلومات والاتصالات المستخدمة للأغراض العسكرية وتلك التي تؤدي الوظائف المدنية، سواء بشكل مادي أو تقني، بما في ذلك من خلال تقسيم الشبكات أو غيرها من تدابير التهيئة المناسبة. ويشمل ذلك الفصل إلى أقصى حد مستطاع بين البيانات المستخدمة للأغراض العسكرية وتلك التي تلبّي الاحتياجات المدنية، مثلاً من خلال 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 والقوانين الأخرى واجبة التطبيق عندما ينفّذون أنشطة تكنولوجيا المعلومات والاتصالات في سياق النزاع المسلح أو المرتبطة به.

وبموجب القانون الدولي الإنساني، تتحمّل الدول وأطراف النزاعات المسلحة مسؤولية انتهاكات القانون الدولي الإنساني التي يرتكبها المدنيون الذين تُنسب إليهم أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، بمن فيهم القراصنة وموظفو شركات التكنولوجيا. ويتعيّن على الدول أن تتّخذ جميع التدابير المناسبة لمنع ارتكاب المدنيين انتهاكات القانون الدولي الإنساني بواسطة أنشطة تكنولوجيا المعلومات والاتصالات أو بتيسير منها، الواقعين في أراضيها أو المشمولين بولايتها أو الخاضعين لسيطرتها، وأن تقمع هذه الانتهاكات في حال وقوعها. وتتعهّد الدول بنشر القانون الدولي الإنساني على أوسع نطاق ممكن من أجل إطلاع المدنيين في بلدانها بالقانون الدولي الإنساني، وعليها ألّا تشجّع المدنيين أو تساعدهم أو تدعمهم على انتهاك القانون الدولي الإنساني، بما في ذلك بواسطة أنشطة تكنولوجيا المعلومات والاتصالات.

ويحظى المدنيون بالحماية من الهجمات، ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور. وفي

بعض الظروف المحدودة، قد تصل مشاركة المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات إلى المشاركة المباشرة في الأعمال العدائية. ولتجنب الاستهداف الخاطئ أو التعسفي للمدنيين، يتعيّن على أطراف النزاع اتّخاذ جميع الاحتياطات الممكنة لتحديد ما إذا كان الشخص مدنياً، وفي هذه الحالة، ما إذا كان يشارك مشاركة مباشرة في العمليات العدائية، بما في ذلك من خلال أنشطة تكنولوجيا المعلومات والاتصالات. وفي حال ثار الشك، ينص القانون الدولي الإنساني على ضرورة افتراض أن الشخص محمي من الهجوم.

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

وتكتسي التدابير التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في التقليل إلى أدنى حدّ من المخاطر المرتبطة بإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة:

أ) اتّخاذ خطوات مناسبة 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

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. وتحظى منتجات وخدمات تكنولوجيا المعلومات والاتصالات هذه، وكذلك الموظفون المدنيون الذين يقدمونها، بالحماية بموجب القانون الدولي الإنساني.

وفي الوقت ذاته، تقدّم شركات التكنولوجيا بشكل متزايد خدمات الأمن السيبراني وغيرها من خدمات أو منتجات تكنولوجيا المعلومات والاتصالات إلى أطراف النزاعات المسلحة، مما قد ينتج عنه فقدان الحماية الممنوحة لها بموجب القانون الدولي الإنساني. وفي هذه الحالات، قد يتعرّض أيضاً المدنيون والأعيان المدنية الذين يعتمدون على هذه المنتجات والخدمات للخطر.

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

أ) النظر على النحو الواجب في 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 ممارسة سلوك يصل إلى حد ارتكاب انتهاكات القانون الدولي الإنساني، أو تيسيره أو الانخراط فيه بطريقة أخرى، بما في ذلك من خلال تقديم منتجات أو خدمات تكنولوجيا المعلومات والاتصالات لأطراف النزاعات المسلحة، واتّخاذ الإجراءات المناسبة في حال وقوع أيّ من هذه الحالات.

5- حماية الخدمات الطبية والأنشطة الإنسانية والأشخاص والأعيان والأنشطة الآخرين الذين يتمتعون 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.

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 نُظم بياناتها ونُظم تكنولوجيا المعلومات والاتصالات الخاصة بها ونُظم 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، وفقاً للقانون الدولي الإنساني وغيره من القوانين الدولية المنطبقة.

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.

وتكتسي التدابير التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في حماية الخدمات الطبية والأنشطة الإنسانية والأشخاص والأعيان والأنشطة الآخرين الذين يتمتعون بحماية خاصة من الأضرار الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال

النزاعات المسلحة:

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 نُظم بيانات هذه الخدمات والأنشطة ونُظم تكنولوجيا المعلومات والاتصالات الخاصة بها ونُظم 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، ومنها تلك المتعلقة بالعنف الجنسي وتجنيد الأطفال أو استخدامهم في النزاعات المسلحة، وضمان التنفيذ والتنسيق الفعالين بين السلطات المختصّة. وتحديداً لمنع تجنيد الأطفال واستخدامهم بصورة غير قانونية، ينبغي بذل جهود حكومية أوسع نطاقاً بهدف توعية الأطفال ومقدمي الرعاية بالمخاطر ذات الصلة.

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، حيثما أمكن، 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 بصورة غير قانونية.

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 وأطراف النزاعات المسلحة الامتناع عن نشر المعلومات في انتهاك للقانون الدولي الإنساني واتّخاذ جميع التدابير الممكنة لمنع انتشارها، بما في ذلك 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. وفي بعض الظروف المحدّدة، يشكل انتشار المعلومات غدراً أو ييسّر ممارسته.

ويجب حماية الخدمات الطبية والأنشطة الإنسانية من المعلومات المضللة التي تتيحها تكنولوجيا المعلومات والاتصالات، والتي تعرقل عملها خلال النزاعات المسلحة. وتتدخّل هذه الأفعال بشكل غير مبرّر في عملها وتتعارض مع الالتزام باحترام وحماية العاملين في المجالين الطبي

والإنساني وأنشطتهم.

وتكتسي التدابير التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في التصدي لانتشار المعلومات في انتهاك للقانون الدولي الإنساني:

أ) اتّخاذ جميع التدابير الممكنة لتقييم مخاطر إلحاق العمليات المعلوماتية، بما في ذلك عندما يدعمها أو يمكّنها الذكاء الاصطناعي أو غيره من التكنولوجيات الناشئة، الضرر بالسكان المدنيين وغيرهم من الأشخاص المحميين، بما يشمل 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 وفق أنشطتهم الطبية أو الإنسانية؛ 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) السعي إلى 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 ما لم تبرّره الضرورة العسكرية الملحّة، نظراً إلى أن هذه التدابير قد تعرّض السكان المدنيين للخطر. وحيثما تكون هذه القيود مفروضة، 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

تكتسي التدابير الشاملة التالية، التي تعكس مزيجاً من القوانين والممارسات الجيّدة القائمة، أهمية خاصة في تعزيز تنفيذ القانون الدولي الإنساني فيما يتعلق بأنشطة تكنولوجيا المعلومات والاتصالات، بما في ذلك 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، ومدونات قواعد السلوك، 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 عند دراستها أو تطويرها أو شرائها أو اعتمادها، من أجل ضمان ألّا يكون استخدامها محظوراً في بعض الظروف أو جميعها بموجب القانون الدولي الإنساني. وينبغي إجراء هذه الاستعراضات عن طريق جملة 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 الجزائية 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 تدابير مناسبة خلال تصميم قدرات تكنولوجيا المعلومات والاتصالات، وتطويرها ونشرها، من أجل الحد من خطر انتشارها غير المقصود أو استخدامها لأغراض أخرى أو إعادة هندستها أو إساءة استخدامها بطرق قد تصل إلى حدّ ارتكاب انتهاكات القانون الدولي الإنساني أو المساهمة في ارتكابها، بما في ذلك من خلال وضع ضمانات مناسبة في مجال الأمن السيبراني، مثل التشفير والتدابير التقنية من قبيل مفاتيح الإيقاف المدمجة، من أجل الحد من انتشارها وإعادة استخدامها على نحو غير مصرح به.

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، بما في ذلك في شكل مواقف وطنية ومشتركة، 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.