Humanity In War

في إطار المبادرة العالمية لتجديد الالتزام السياسي بالقانون الدولي الإنساني (المبادرة العالمية بشأن القانون الدولي الإنساني)، يسر **غانا ولوكسمبورغ والمكسيك وسويسرا واللجنة الدولية للصليب الأحمر (اللجنة الدولية)** تقديم ما يلي:

مسار العمل 6

المشاورة الثانية مع الدول بشأن ضمان احترام القانون الدولي الإنساني في استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة

للمسؤولين الحكوميين المتخصصين في القانون الدولي الإنساني، أو الأمن السيبراني، أو العمليات السيبرانية العسكرية في العواصم، بالإضافة إلى ممثلي البعثات الدائمة في جنيف

الاثنين، 24 تشرين الثاني/نوفمبر 2025
18:00–9:00 (التوقيت العالمي المنسَّق +1)

النسق: حضورياً (قاعة المؤتمرات "HUMANITARIUM" باللجنة الدولية في جنيف) وعبر الإنترنت (تطبيق زوم)

معلومات أساسية

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 الخصائص المحددة لبيئة تكنولوجيا المعلومات والاتصالات تساؤلات معقدة بشأن تنفيذ القانون الدولي الإنساني. وأقرّت الدول بضرورة مواصلة المناقشات بشأن هذه التساؤلات.

ويبني مسار العمل بشأن تكنولوجيا المعلومات والاتصالات ضمن المبادرة العالمية بشأن القانون الدولي الإنساني على المناقشات العالمية حول استخدام تكنولوجيات المعلومات والاتصالات والتقدّم المحرز حتى الآن، ولا سيما القرار 2 الصادر عن المؤتمر الدولي الرابع والثلاثين للصليب الأحمر والهلال الأحمر، المعنون "حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من التكلفة البشرية المحتملة لأنشطة تكنولوجيا المعلومات

والاتصالات خلال النزاعات المسلحة". ويشكل مسار العمل هذا جزءاً من جهد متواصل لبلورة فهم مشترك للقيود التي يفرضها القانون الدولي الإنساني على أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، بهدف حماية السكان المدنيين من الضرر.

عُقدت المشاورة الأولى بخصوص مسار العمل هذا في 15 أيار/مايو 2025. وركّزت على تحديد المسائل والشواغل القانونية والإنسانية الناشئة عن الخصائص الفريدة لأنشطة تكنولوجيا المعلومات والاتصالات في النزاعات المسلحة، وبحث كيفية معالجتها بهدف الالتزام بالحماية التي يوفرها القانون الدولي الإنساني للمدنيين والأعيان المدنية، فضلاً عن غيرهم من الأشخاص والأعيان المحميين في النزاعات المسلحة. وستسهم هذه المشاورة الثانية في دفع المناقشات قُدُماً. وستعقد، بصيغة مختلطة (تجمع بين الحضور المباشر وعبر الإنترنت)، في 24 تشرين الثاني/نوفمبر 2025 في جنيف.

لمزيد من التفاصيل حول المسائل التي جرى مناقشتها في مسار العمل هذا، ندعو المشاركين إلى مراجعة **ورقة المعلومات الأساسية** المرفقة بمذكرة المفاهيم هذه.

الأهداف

ستُبنى المشاورة الثانية على المناقشات التي أجريت في المشاورة الأولى وعلى النقاط الرئيسية المستخلصة من تلك المشاورة. وستركز على تعميق المناقشات المتصلة بالمسائل القانونية والإنسانية الناشئة عن استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المسلحة. وتهدف المشاورة إلى تعزيز الفهم المشترك وتحديد توصيات قانونية وعملية محتملة من شأنها ضمان مستوى أفضل من الحماية للمدنيين والأعيان المدنية في سياق الحروب الرقمية.

وسترمي المشاورة إلى تحقيق الأهداف التالية:

- **تقديم معلومات محدَّثة بشأن مسار العمل والتقدم المحرز فيه:**
  - إحاطة المشاركين بشأن الاستنتاجات التي خلصت إليها المشاورة الأولى والتي أوردها التقرير المرحلي وبشأن الرؤى المنبثقة من الفعاليات الداعمة اللاحقة للمشاورة.
  - تحديد معالم الخطوات التالية نحو تحديد التوصيات النهائية لمسار العمل.
- **تعميق المناقشة بشأن المسائل القانونية والإنسانية المحددة لتعزيز الفهم المشترك لها:**

- تيسير تبادل الآراء المتعمقة بشأن المسائل المحدّدة خلال المشاورة الأولى لمواصلة النظر فيها، مثل:

  - الآثار القانونية بموجب القانون الدولي الإنساني لعمليات تكنولوجيا المعلومات والاتصالات التي تؤدي إلى آثار غير مادية، مثل تعطيل قدرة النظام المستهدف على العمل
  - الحماية، بموجب القانون الدولي الإنساني، للبيانات المدنية وغيرها من البيانات، على سبيل المثال، من العبث بها أو إتلافها أو حذفها أو استخراجها ونشرها
  - الحماية الخاصة، بموجب القانون الدولي الإنساني، للأشخاص، والأعيان، والأنشطة، من آثار أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، بما في ذلك بياناتهم والبنية التحتية الرقمية.
  - الحدود التي يفرضها القانون الدولي الإنساني على نشر المعلومات عن طريق أنشطة تكنولوجيا المعلومات والاتصالات
  - الآثار القانونية بموجب القانون الدولي الإنساني الناجمة عن الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، وإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة، فضلاً عن التدابير النابعة من القانون الدولي الإنساني الرامية إلى التخفيف من مخاطر الضرر الذي يلحق بالمدنيين والخدمات المدنية الأساسية

- تعزيز التدابير العملية لضمان الامتثال للقانون الدولي الإنساني وتخفيف الأضرار الواقعة على المدنيين.

الخطوات التالية

من المقرّر عقد مشاورة ثالثة مع الدول في مطلع عام 2026 لمواصلة المضي قدماً في المناقشات التي جرت خلال المشاورتين الأولى والثانية والبناء على المفاهيم المشتركة التي أسفرتا عنها. وستشكّل هذه المشاورات أساساً لصياغة توصيات مسار العمل. وسيُطلب من جميع الدول المهتمة تقديم آرائها بشأن توصيات مسار العمل خلال الربع الثاني من عام 2026، على أن تُستعرض هذه التوصيات بمزيد من التفصيل في المشاورات اللاحقة مع الدول.

وستستكمل المشاورات مع الدول بمناقشات إقليمية وفعاليات داعمة أخرى، والتي سيتم الإعلان عنها على الموقع الإلكتروني Humanity in War.

المشاركون

- ستُعقد المشاورة بشكل أساسي حضورياً في جنيف. ويُمكن أيضاً المشاركة عبر الإنترنت.

- باب المشاركة **مفتوح أمام جميع الدول المهتمة**. ويُفضَّل بشدة أن يُشارك المسؤولون الحكوميون المتخصصون في القانون الدولي الإنساني، أو الأمن السيبراني، أو العمليات السيبرانية العسكرية في العواصم، بالإضافة إلى ممثلي البعثات الدائمة في جنيف.
- كما يمكن للممثلين الآخرين الذين يحظون بخبرة فنية محددة في الموضوع محل النقاش (مثلاً أعضاء المنظمات الدولية، والمجتمع المدني، والأوساط الأكاديمية) المشاركة بناء على دعوة.
- يُرجى التسجيل في موعد أقصاه 15 تشرين الثاني/نوفمبر 2025 عبر هذا الرابط:

https://forms.office.com/e/LuDKik93vY.

طرائق العمل

- ستكون اللغات **العربية والصينية والإنكليزية والفرنسية والروسية والإسبانية** هي لغات العمل، وستتوفر الترجمة الفورية في هذه اللغات.
- نرجو من الدول ألّا تتجاوز بياناتها مدة **أربع دقائق** لضمان وقت كافٍ لجميع المشاركين لإلقاء كلمتهم. وفي نهاية كل جلسة، وبعد أن تنتهي جميع الجهات المشاركة من تقديم مداخلاتها، تُعطى الفرصة للدول والمشاركين الآخرين لمناقشة الأفكار التي يقترحها الآخرون.
- نطلب من المشاركين عند إعداد بياناتهم النظر في **الأسئلة التوجيهية** المدرجة في جدول الأعمال أدناه. وتقترن بعض الأسئلة التوجيهية **بسيناريوهات توضيحية** يتعيّن قراءتها جنباً إلى جنب مع تلك الأسئلة. وترفق بمذكرة المفاهيم هذه **ورقة معلومات أساسية** مُحدثة للمساعدة في وضع إطار للمناقشة وتيسيرها.
- نظراً إلى التحديات التقنية التي تواجه الاجتماعات المختلطة، نشجّع الوفود الموجودة في القاعة على الإدلاء ببياناتها حضورياً، وفي جميع الحالات إبداء الانتباه التام للوفود التي تدلي ببياناتها عبر الإنترنت.
- سيُحافظ على طابع المناقشات **الشامل والبنّاء وغير المُسيّس والموجّه نحو إيجاد الحلول** طوال فترة المشاورة. في حين يُشجَّع المشاركون على الإشارة إلى الممارسات الوطنية لدولهم خلال المشاورات، يُرجى منهم الامتناع عن مناقشة سياقات محدَّدة أو ممارسات دول أخرى.
- لتيسير الترجمة الفورية، يُرجى من المشاركين إرسال نسخة من بياناتهم بحلول 21 تشرين الثاني/نوفمبر 2025 إلى البريد الإلكتروني ihlinitiative@icrc.org، مع كتابة العنوان "ICT workstream second consultation" في موضوع الرسالة. كما نشجع المشاركين على إرسال بياناتهم المكتوبة كاملة عبر البريد الإلكتروني بعد الاجتماع. **وستُنشر هذه البيانات على الموقع الإلكتروني للجنة الدولية، ما لم يُطلب الحفاظ على السرية صراحة.**
- ستُسجّل المشاورة، ولكن لن يُتاح هذا التسجيل للاطلاع العام.

جدول الأعمال

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

(مسار العمل بشأن تكنولوجيا المعلومات والاتصالات)

الجولة الثانية من المشاورات

18:00–9:00، 24 تشرين الثاني/نوفمبر 2025

قاعة المؤتمرات "HUMANITARIUM" باللجنة الدولية، 17 avenue de la Paix, 1202 Geneva

* *حسب عدد البيانات التي يُدلى بها، جميع التوقيتات الموضحة أدناة قابلة للتغيير.*

التسجيل واستراحة القهوة / تسجيل الدخول والاتصال عبر الإنترنت	9:00–08:30
افتتاح الاجتماع ومقدمة	9:30–09:00
حلقة نقاش: المسائل القانونية والإنسانية الرئيسية الناشئة عن استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة	10:30–09:30
الجلسة الأولى: تدابير عملية لضمان الامتثال للقانون الدولي الإنساني وحماية المدنيين في استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة	11:30–10:30
الأسئلة التوجيهية 1. ما هي التدابير القانونية والميدانية التي اعتمدتها دولتكم أو تنظر في اعتمادها لضمان الامتثال لأحكام القانون الدولي الإنساني، ولمنع الأضرار التي قد تلحق بالمدنيين نتيجة تنفيذ أنشطة في مجال تكنولوجيا المعلومات والاتصالات في سياق النزاعات المسلحة أو التخفيف منها؟ وفي ضوء الخصائص المميزة لعمليات تكنولوجيا المعلومات والاتصالات، كيف تختلف هذه التدابير عن تلك المطبقة على العمليات الحركية، وما السبل الكفيلة بمعالجة هذه الخصائص؟ 2. ما هي التدابير التي اتخذتها دولتكم، أو فكرت في اتخاذها، لمنع انتهاكات القانون الدولي الإنساني المرتكبة من خلال أنشطة تكنولوجيا المعلومات والاتصالات أو الأنشطة المرتبطة بها، وقمع تلك الانتهاكات؟	

3. ما هي أشكال بناء القدرات أو التعاون الدولي الأجدى في دعم الدول لتعزيز امتثالها لأحكام القانون الدولي الإنساني، وتبادل الممارسات العملية في هذا المجال؟	
استراحة القهوة	12:00–11:30
الجلسة الثانية: حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من المخاطر الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة	13:00–12:00
الأسئلة التوجيهية 1. ما هي التكلفة البشرية أو الآثار المترتبة في إطار القانون الدولي الإنساني على عمليات تكنولوجيا المعلومات والاتصالات التي تسفر عن آثار غير مادية، مثل تعطيل قدرة النظام المستهدف على العمل؟ على سبيل المثال، يمكن النظر في عملية في مجال تكنولوجيا المعلومات والاتصالات نُفِّذت في سياق نزاع مسلح واستهدفت هدفاً مدنياً، مثل خادم أحد مزوّدي خدمات النقل، أو مزوّد خدمة إنترنت، أو مصرف. وفي وقت تنفيذ العملية، لم يكن الخادم يُستخدم بطريقة تُكسبه صفة الهدف العسكري. ونتيجة لهذه العملية، لم يعد الهدف المستهدف يقدم الخدمة التي يقدمها عادة؛ ومع ذلك، لم تلحق به أضرار مادية. كيف تقيّم دولتكم مشروعية تلك العملية؟ هل سيتغير تقييمكم إذا حدث ضرر مادي نتيجة للآثار المباشرة أو غير المباشرة المتوقعة للعملية؟ 2. كيف تتناول دولتكم مسألة الحماية التي يكفلها القانون الدولي الإنساني للبيانات المدنية وغيرها من البيانات، على سبيل المثال، من العبث بها أو إتلافها أو حذفها أو استخراجها أو نشرها دون تصريح؟ وهل تميّز دولتكم بين فئات البيانات المختلفة — مثل البيانات الطبية أو البيومترية أو المالية وغيرها — عند تقييم مستوى الحماية المقررة لها بموجب أحكام القانون الدولي الإنساني؟ على سبيل المثال، يمكن النظر في عملية في مجال تكنولوجيا المعلومات والاتصالات نُفِّذت في سياق نزاع مسلح، واستهدفت حذف بيانات مدنية، (مثل بيانات طبية أو بيانات الضمان الاجتماعي أو حسابات مصرفية أو سجلات ضريبية أو بيانات عملاء شركات مدنية). كيف تقيّم دولتكم مشروعية هذه العملية في مجال تكنولوجيا المعلومات والاتصالات؟ وما هي القواعد ذات الصلة في القانون الدولي الإنساني التي تقيّد العبث بالبيانات المدنية وغيرها من البيانات المحمية، أو إتلافها أو تدميرها خلال النزاعات المسلحة؟ وما هي الحماية التي يوفرها القانون الدولي الإنساني من النسخ غير المصرح به للبيانات المدنية أو غيرها من البيانات المحمية، والاستيلاء عليها والنشر المحتمل لها؟ 3. ما هي قواعد القانون الدولي الإنساني التي توفر الحماية للمدنيين والأعيان المدنية من عمليات تكنولوجيا المعلومات والاتصالات التي لا تُصنف على أنها "هجوم" بموجب القانون الدولي الإنساني؟ على سبيل المثال، ما هي التدابير العملية التي ينبغي اتخاذها عند تنفيذ أنشطة في مجال تكنولوجيا المعلومات	

والاتصالات لضمان الامتثال للالتزام بتوخي الحرص الدائم على تجنّب الإضرار بالسكان المدنيين والأعيان المدنية أثناء سير العمليات العسكرية؟	
استراحة الغداء (لا تقدم وجبة الغداء ضمن الفعالية)	14:00–13:00
الجلسة الثالثة: تفعيل أشكال الحماية الخاصة الممنوحة للأشخاص والأعيان والأنشطة ضد الآثار الناجمة عن استخدام تكنولوجيات المعلومات والاتصالات خلال النزاعات المسلحة	15:00–14:00
الأسئلة التوجيهية 1. ما هي التدابير العملية التي اتخذتها دولتكم، أو تنظر في اتخاذها، لضمان ألا تؤدي أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة إلى الإضرار بعمل الخدمات الطبية أو الأنشطة الإنسانية أو الأعيان التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، بما في ذلك نُظُم تكنولوجيا المعلومات والاتصالات المدنية والبيانات المدنية، أو تعطيل تلك الخدمات؟ وما هي الاحتياطات التي تتخذها دولتكم أو تنظر في اتخاذها لحماية هذه الأعيان المشمولة بحماية خاصة من أي أضرار، بما في ذلك الأضرار التي تنجم عن أنشطة تكنولوجيا المعلومات والاتصالات؟ 2. في ما يتعلق بالحماية الخاصة الممنوحة للمرافق الطبية والعاملين فيها، يمكن النظر في مثال لعملية في مجال تكنولوجيا المعلومات والاتصالات في سياق نزاع مسلح، ينفذها أحد أطراف النزاع بهدف الوصول إلى خوادم منشأة طبية تقع في أراضي الطرف الخصم. وتجمع الجهة المعنية البيانات الطبية الخاصة بأفراد القوات المسلحة الذين يتلقّون العلاج في تلك المنشأة، ثم تُقدِم على تشفير ملفات جميع المرضى، مما يؤدي إلى حرمان الطاقم الطبي من الوصول إليها. إلى أي مدى تمتد الحماية الخاصة المقررة للمرافق الطبية لتشمل سرية البيانات التي تصل إليها تلك المرافق أو تجمعها أو تعالجها أو تخزّنها في عملياتها، وكذلك سلامة هذه البيانات وتوافرها؟ وعلى نحو مماثل، كيف تنطبق هذه الحماية على البيانات التي يصل إليها العاملون في المجال الإنساني أو يجمعونها أو يعالجونها أو يخزّنونها، وكذلك على الأعيان المستخدمة في تنفيذ العمليات الإنسانية؟ 3. ما المخاطر المحددة الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات في ما يتعلق بحظر العنف الجنسي، و/أو تجنيد الأطفال أو استخدامهم بصورة غير قانونية في الأعمال العدائية؟ ما التدابير العملية التي اعتمدتها دولتكم أو تنظر في اعتمادها لمنع تلك الأعمال غير المشروعة والاستجابة لها؟	
الجلسة الرابعة: حماية المدنيين وغيرهم من الأشخاص المحميين بموجب القانون الدولي الإنساني من انتشار المعلومات في انتهاك للقانون الدولي الإنساني خلال النزاعات المسلحة	16:00–15:00

الأسئلة التوجيهية 1. ما الحدود التي يفرضها القانون الدولي الإنساني بشأن انتشار المعلومات عن طريق أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة؟ على سبيل المثال، يمكن النظر في حملة إعلامية يشنّها أحد أطراف النزاع المسلح، تتضمّن: • نشر صور لأسرى الحرب على شبكة الإنترنت وإبراز كيفية معاملتهم، • تزييف رسائل وبثّها عبر منصّات التواصل الاجتماعي بما من شأنه تأجيج التوترات بين المجتمعات المحلية وزيادة مخاطر العنف. ما هي الضمانات أو آليات الرقابة التي وضعتها دولتكم أو تنظر في وضعها، لضمان ألا تؤدي الأنشطة في مجال تكنولوجيا المعلومات والاتصالات إلى تعريض الأشخاص المحرومين من حريتهم لفضول الجماهير؟ وكيف تحدّد دولتكم ما إذا كانت العمليات المعلوماتية التي تتيحها تكنولوجيا المعلومات والاتصالات تشكّل تحريضاً أو تشجيعاً محظوراً على ارتكاب انتهاكات للقانون الدولي الإنساني، أو تهدف إلى بث الذعر بين السكان المدنيين؟ 2. كيف تتعامل دولتكم مع مخاطر انتشار المعلومات المضلّلة التي تتيحها تكنولوجيا المعلومات والاتصالات، والتي قد تعوق الخدمات الطبية أو العمليات الإنسانية أثناء النزاعات المسلحة؟ على سبيل المثال، يمكن النظر في حملة عبر الإنترنت تتداول صوراً ملفّقة ومنشورات مزيفة على وسائل التواصل الاجتماعي تدّعي كذباً أن مستشفى ما يشكل معقلاً للمقاتلين. قد تؤدي هذه المعلومات المضلّلة إلى إثارة حالة من عدم الثقة لدى السكان المحليين وتعطيل وصول الطواقم الطبية إلى المنشأة، فضلاً عن تعريض الكوادر الصحية التي تدخلها لتحريض أو ترهيب متزايد. ما هي قواعد القانون الدولي الإنساني التي توفر الحماية للخدمات الطبية والعمليات الإنسانية من التضليل الرقمي؟ وما هي التدابير القانونية أو الميدانية التي اعتمدتها دولتكم، أو تنظر في اعتمادها، للتصدي لهذه المخاطر؟ 3. ما التدابير الأخرى التي اتخذتها دولتكم أو تفكر في اتخاذها لمنع استخدام تكنولوجيات المعلومات والاتصالات، بما في ذلك من خلال وسائل التواصل الاجتماعي، لنشر المعلومات التي تشكل انتهاكاً للقانون الدولي الإنساني؟	
استراحة القهوة	16:30–16:00
الجلسة الخامسة: التصدي لمخاطر الضرر الناجمة عن الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، وإشراك المدنيين في أنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة	17:30–16:30

الأسئلة التوجيهية

1. ما هي التكلفة البشرية أو الآثار المترتبة في إطار القانون الدولي الإنساني على الاستخدام العسكري للبنية التحتية المدنية لتكنولوجيا المعلومات والاتصالات، وما هي التدابير النابعة من القانون الدولي الإنساني التي يتعين اتخاذها للتخفيف من المخاطر المرتبطة بالضرر الذي يلحق بالمدنيين والخدمات المدنية الأساسية؟

لنفترض أن مركز بيانات تجارياً يقع ضمن أراضي دولة طرف في نزاع مسلح، يستضيف بيانات وتطبيقات عسكرية، فضلاً عن بيانات السكان المدنيين والتطبيقات المستخدمة في توفير الخدمات المدنية الأساسية.

- كيف تطبّق دولتكم مبادئ القانون الدولي الإنساني وقواعده، ولا سيما مبادئ التمييز والتناسب والاحتياطات، عند تقييم تنفيذ عملية في مجال تكنولوجيا المعلومات والاتصالات تستهدف مثل هذه البنية التحتية لتكنولوجيا المعلومات والاتصالات؟ في حال اكتسب أي جزء معين من البنية التحتية لتكنولوجيا المعلومات والاتصالات، مثل خادم سحابي، صفة هدف عسكري، فكيف تقيّمون الآثار المترتبة على استخداماته المدنية عند التخطيط لشنّ عملية في مجال تكنولوجيا المعلومات والاتصالات ضده وتنفيذها؟
- ما التدابير الاحترازية التي يمكن بل وينبغي للدولة المنفِّذة لعملية في مجال تكنولوجيا المعلومات والاتصالات اتخاذها، لضمان حماية السكان المدنيين والخدمات المدنية الأساسية التي تعتمد على البنية التحتية لتكنولوجيا المعلومات والاتصالات المستهدفة؟
- ما الاحتياطات التي يمكن بل وينبغي للدولة التي يقع ضمن إقليمها مركز البيانات اتخاذها لضمان حماية السكان المدنيين والأعيان المدنية الخاضعين لسيطرتها من آثار العمليات في مجال تكنولوجيا المعلومات والاتصالات التي تستهدف مركز البيانات؟
- ما الاحتياطات التي يمكن بل وينبغي للشركة المالكة أو المشغِّلة لمركز البيانات اتخاذها، لضمان عدم تأثّر البيانات المدنية من جراء عمليات تكنولوجيا المعلومات والاتصالات الموجهة ضد البيانات والتطبيقات العسكرية التي تستضيفها المنشأة ذاتها؟

2. كيف يمكن أن يتعرّض المدنيون لمخاطر نتيجة مشاركتهم في أنشطة تكنولوجيا المعلومات والاتصالات أثناء النزاعات المسلحة، وما التدابير النابعة من أحكام القانون الدولي الإنساني التي ينبغي اتخاذها للتخفيف من تلك المخاطر؟

على سبيل المثال، لنفترض أن قراصنة مدنيين يعملون من إقليم أحد الأطراف المتحاربة ينفذون عمليات في مجال تكنولوجيا المعلومات والاتصالات، في سياق نزاع مسلّح، تستهدف تعطيل الاتصالات العسكرية أو

الإضرار بالبنية التحتية الرقمية التابعة لشركات خاصة، وذلك بقصد إضعاف اقتصاد الدولة العدو وخفض الروح المعنوية لدى شعبها. • ما هي الالتزامات القانونية التي يتعين على القراصنة المدنيين الوفاء بها بموجب القانون الدولي الإنساني عند تنفيذ عمليات في مجال تكنولوجيا المعلومات والاتصالات؟ • ما التدابير التي يمكن للدولة المتضرّرة من عمليات في مجال تكنولوجيا المعلومات والاتصالات أن تتخذها؟ 3. ما التدابير العملية التي اتخذتها دولتكم، أو فكرت في اتخاذها، لضمان توعية المدنيين الخاضعين لولايتها القضائية أو لسيطرتها — بما في ذلك القراصنة المدنيون، أو مجموعات القرصنة، أو موظفو شركات التكنولوجيا المشاركون في أنشطة في مجال تكنولوجيا المعلومات والاتصالات في سياق نزاع مسلّح — بأحكام القانون الدولي الإنساني وامتثالهم لها، ولضمان إدراكهم للمخاطر المرتبطة بمثل هذه الأنشطة وتمتعهم بأقصى قدر ممكن من الحماية من تلك المخاطر؟	
ملاحظات ختامية	18:00–17:30