الأمم المتحدة A/AC.291/4

الجمعية العامة

Distr.: General
17 November 2021
Arabic
Original: Arabic/Chinese/English/
Spanish

**اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية**

# تجميع للآراء المقدَّمة من الدول الأعضاء فيما يتعلق بنطاق اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأهدافها وهيكلها (عناصرها)

**مذكرة من الأمانة**

*ملخص*

تحضيراً للدورة الأولى للجنة المخصَّصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، أعدَّت الأمانة هذه المذكرة عملاً بتعليمات رئيسة اللجنة. وتعرض المذكرة الآراء الواردة من الدول الأعضاء بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها).

291221 291221 V.21-08418 (A)

# المحتويات

# أولاً- مقدمة

1- تحضيراً للدورة الأولى للجنة المخصَّصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، دعت رئيسة اللجنة، السيدة فوزية بومعيزة مباركي (الجزائر)، في 11 آب/أغسطس 2021، الدول الأعضاء إلى تقديم آرائها بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها). وكان الموعد النهائي المحدَّد لتقديم تلك الآراء هو 29 تشرين الأول/أكتوبر 2021، ثم مُدِّد إلى غاية 5 تشرين الثاني/نوفمبر 2021.

2- كما أصدرت الرئيسة تعليمات إلى الأمانة بتجميع الآراء كما وردت وترجمتها إلى اللغات الرسمية الست للأمم المتحدة لكي تتاح للدورة الأولى للجنة المخصَّصة.

3- وأعدَّت الأمانة هذه المذكرة بناء على تعليمات الرئيسة، وهي تتضمن الآراء الواردة من الدول الأعضاء بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها).

# ثانياً- الآراء الواردة من الدول الأعضاء

## أستراليا

[الأصل: بالإنكليزية]
[29 تشرين الأول/أكتوبر 2021]

ترحِّب أستراليا بفرصة تقديم آرائها بشأن نطاق وهيكل وأهداف اتفاقية دولية جديدة بشأن الجريمة السيبرانية. وتتيح الاتفاقية الجديدة فرصة فريدة لضمان توافق واسع النطاق في الآراء بشأن التعاون الدولي على مكافحة الجريمة السيبرانية، مما يمكِّن الدول من التصدي لهذا التهديد المتفشي والمتطور باستمرار على نحو أفضل.

ولن تكون أي اتفاقية جديدة ذاتَ قيمة إلا إذا حظيت بتأييد واسع النطاق من غالبية الدول الأعضاء، استناداً إلى اتفاق توافقي ينبثق عن مناقشات تجرى بحسن نية تحت رعاية اللجنة المخصَّصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، التي أنشئت عملاً بقراري الجمعية العامة 247/74 و282/75. وتحقيقاً لهذه الغاية، تلتزم أستراليا بالانخراط في عملية مفتوحة وشاملة وشفافة ومتعددة الأطراف تتيح أفضل فرصة لضمان تمكُّن الدول من التوصل إلى نتيجة تحظى بقبول أكبر عدد ممكن من الدول. ويتماشى ذلك مع المبادئ الواردة في الورقات السابقة التي قدَّمتها أستراليا إلى اللجنة المخصَّصة، وكذلك مع الورقات المشتركة التي شاركت فيها أستراليا. وتغتنم أستراليا هذه الفرصة لتؤكِّد من جديد النقاط الواردة في تلك الورقات.

تمثِّل الجريمة السيبرانية تهديداً لجميع الدول، بيْد أنها تشكِّل تحديات خاصة للدول الصغيرة. ويكتسي التعاون الدولي الفعال بشأن الجريمة السيبرانية أهمية خاصة للدول الجزرية الصغيرة النامية، للمساعدة في تعزيز قدرتها المحلية على مكافحة عمليات الجريمة السيبرانية عبر الوطنية. ومن الضروري أن تتمكن الدول الجزرية الصغيرة النامية من المشاركة بصورة بنّاءة في أعمال اللجنة المخصَّصة. وأستراليا ملتزمة بضمان إتاحة فرص وافية للبلدان الجزرية في المحيط الهادئ للمشاركة في أعمال اللجنة المخصَّصة. وترحِّب أستراليا بقرار دعم المشاركة المختلطة (بالحضور الشخصي وعبر الإنترنت) في دورات اللجنة المخصَّصة، وتشدِّد على أهمية منح الوفود الصغيرة وقتاً كافياً للتحضير والمشاركة.

وتؤدّي كيانات القطاع الخاص دوراً فريداً وقيّماً في التصدي للجريمة السيبرانية. ولتحقيق النجاح، يجب أن يستفيد عمل اللجنة المخصَّصة من الخبرة القيِّمة التي يوفِّرها أصحاب المصلحة. وينبغي للدول أيضاً

أن تنفتح على الرؤية والخبرة الواسعتين اللتين يمكن أن تسهم بهما جهات فاعلة أخرى من غير الدول، مثل منظمات المجتمع المدني والأوساط الأكاديمية والهيئات الحكومية الدولية، في مناقشة أفضل السبل لمكافحة الجريمة السيبرانية. ولضمان إجراء مناقشات مستنيرة وتحقيق نتائج فعالة، ينبغي للجنة المخصَّصة أن تتيح لهذه المجموعات أكبر قدر ممكن من الفرص للمساهمة.

**النطاق**

نظراً لضيق الإطار الزمني للمفاوضات، فإنَّ لدى الدول وقتاً محدوداً للتوصل إلى اتفاق بشأن المسائل العديدة التي تنطوي عليها اتفاقية جديدة. ويجب تحديد نطاق الاتفاقية بوضوحٍ، وينبغي له أن يركِّز بصورة وثيقة على تدابير العدالة الجنائية الرامية إلى التصدي للجريمة السيبرانية، وألا يعالج مسائل الأمن السيبراني الأوسع نطاقاً التي تتناولها محافل أخرى.

وبغية التعجيل بعملنا في هذا الشأن، ينبغي للدول أن تركِّز اهتمامها على المجالات التي يلزم فيها اتباع نُهج مشتركة إزاء الجريمة السيبرانية. وينبغي أن يعتمد عمل اللجنة المخصَّصة مفاهيم ومصطلحات تتعلق بالجريمة السيبرانية والتعاون الدولي في مجال العدالة الجنائية، وهي مفاهيم يفهمها المجتمع الدولي حقَّ الفهم بالفعل. فلا حاجة لنا إلى العودة إلى نقطة الصفر، كما أننا لا نود أن نخلق غموضاً.

ولذلك ينبغي أن تستند الاتفاقية الجديدة بصورة كبيرة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، واتفاقية الأمم المتحدة لمكافحة الفساد، وكذلك إلى المفاهيم الأخرى التي تم الاتفاق عليها بتوافق الآراء في مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية وفي سائر محافل الأمم المتحدة، حسب الاقتضاء. وينبغي لها أن تسترشد بالصكوك الدولية الفعلية القائمة التي اعتمدتها الدول على الصعيدين الدولي والإقليمي، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وأن تتجنب تقويض القواعد القائمة التي أرستها تلك الاتفاقات. ويتماشى ذلك مع الولاية الواردة في قرار الجمعية العامة 247/74، الذي دعت فيه الجمعية العامة إلى أن يراعي عمل اللجنة المخصَّصة مراعاةً كاملة الصكوك الدولية القائمة والجهود المبذولة حالياً على كل من الصعيد الوطني والإقليمي والدولي.

وينبغي للاتفاقية، على وجه الخصوص، أن تستمر في استخدام مصطلح "الجريمة السيبرانية"، ذلك أنَّ هذا المصطلح يجسِّد مفهوماً متداولاً على نطاق واسع، وقد استُخدم في عدد كبير من وثائق الأمم المتحدة، بما في ذلك الوثائق الختامية لمؤتمرات الأمم المتحدة الثاني عشر والثالث عشر والرابع عشر لمنع الجريمة والعدالة الجنائية، وكذلك في قرارات الجمعية العامة (وأبرزها القرار 230/65) والعديد من القرارات والتقارير الأخرى الصادرة عن لجنة منع الجريمة والعدالة الجنائية والمجلس الاقتصادي والاجتماعي.

**عناصر المعاهدة (الهيكل والأهداف)**

*التجريم*

تتيح الاتفاقية الجديدة فرصة لتحسين التعاون الدولي بدرجة كبيرة فيما يتعلق بالجريمة السيبرانية. فوجود معايير منسَّقة لمجموعة أساسية من الجرائم السيبرانية سيزيد من قدرة الدول على التصدي للجريمة السيبرانية على الصعيد العالمي والإقليمي والمحلي.

وتحقيقاً لهذه الغاية، ترى أستراليا أنَّ الاتفاقية ينبغي أن تتَّبع نهجاً مركَّزاً إزاء أنواع السلوك الإجرامي التي شهدت تغيراً كبيراً من جراء الجريمة السيبرانية. وعادةً ما تكون القوانين الجنائية المحلية للدول أكثر من كافية لتعريف

الجرائم المألوفة مثل التعدي على ممتلكات الغير والتخريب والسرقة والجرائم المتصلة بالمخدرات وجرائم العنف. ولا تحتاج الاتفاقية إلى إعادة تعريف هذه الجرائم لمجرد أنَّ حاسوباً أو نظام معلومات استُخدم في ارتكابها.

ويجب أن تتضمن الاتفاقية الجديدة معايير جديدة لتجريم الأفعال الإجرامية التي لا يمكن ارتكابها إلا باستخدام نُظم المعلومات والاتصالات، والمعروفة بمسميات مختلفة مثل "الجريمة السيبرانية البحتة" أو "الجريمة المرتكبة في الفضاء السيبراني". فلم تكن هذه الجرائم موجودة قبل ظهور شبكات المعلومات والاتصالات، وكثيراً ما تكون القوانين الجنائية المحلية للدول غير كافية أو غير متسقة في انطباقها على هذه الجرائم. وسوف تحقِّق معايير تجريم منسَّقة في هذا المجال فوائد جمة للدول، سواء من حيث جهودها المحلية لمكافحة الجريمة السيبرانية أو من حيث تيسير المزيد من التعاون الدولي.

وترى أستراليا أيضاً أنَّ هناك بعض الجرائم "التقليدية" التي زاد نطاقها وحجمها وسهولة ارتكابها زيادة كبيرة من جراء ما توفره شبكات المعلومات والاتصالات من سرعة وإمكانية إخفاء الهوية وانتشار واسع النطاق. وهذه الجرائم توصف أحياناً بأنها جرائم "ييسِّر الفضاء السيبراني ارتكابها". وينبغي للاتفاقية أن تعالج هذه الجرائم بحكمة من خلال وضع إطار واضح لتحديد سبب تغيُّر بعض الجرائم تغيراً كبيراً من جراء تضمنها عنصراً "سيبرانياً" بحيث صارت تتطلب معياراً دولياً منسَّقاً جديداً يجعل هذا السلوك يتجاوز نطاق الجرائم "التقليدية". وليس لزاماً أن تنشئ الاتفاقية فئات جديدة من الأفعال الإجرامية لكل جريمة قائمة قد تتضمن عنصراً "سيبرانياً"، لا سيما عندما لا يؤثِّر هذا العنصر تأثيراً كبيراً في شدة السلوك المجرَّم أو نطاقه.

وترى أستراليا أنَّ هناك جريمتين واضحتيْن ينبغي إدراجهما في الاتفاقية ضمن فئة الجرائم التي ييسِّر الفضاء السيبراني ارتكابها وهما: التهديد الشديد الذي يشكِّله الاستغلال الجنسي للأطفال والتعدي عليهم جنسياً عبر الإنترنت، وجريمتا الاحتيال والسرقة اللتان يتيح الفضاء السيبراني اقترافهما على نطاق واسع وبزيادة كبيرة، بما في ذلك الابتزاز المتصل ببرمجيات انتزاع الفدية. وأستراليا مستعدة لسماع حجج تؤيِّد إدراج جرائم أخرى ييسِّر الفضاء السيبراني ارتكابها، ولكن ينبغي للاتفاقية، للأسباب المبيَّنة آنفاً، أن تعتمد نهجاً مقيداً في إدراج أي فئة جديدة من فئات الجرائم.

وينبغي للاتفاقية أيضاً أن تولي الاعتبار الواجب للجرائم الأصلية والمسؤولية الإضافية عن الجرائم المرتكبة في الفضاء السيبراني والجرائم التي ييسِّرها الفضاء السيبراني. وينبغي أن يشمل ذلك توسيع نطاق المسؤولية الجنائية المنصوص عليها في صكوك مثل اتفاقية الجريمة المنظمة واتفاقية مكافحة الفساد. واعتباراً لدور التكنولوجيا في تيسير الجرائم السيبرانية، ينبغي للاتفاقية أيضاً أن تنظر في وضع معيار جنائي متسق للجرائم التي تنطوي على إنتاج أو اشتراء أو توفير التكنولوجيا والبرامج الحاسوبية المكيَّفة حصراً أو أساساً لارتكاب جرائم سيبرانية.

والجريمة السيبرانية مجال سريع التطور، ويسعى مجرمو الفضاء السيبراني باستمرار إلى نشر تكنولوجيات ومنهجيات جديدة لتوسيع أنشطتهم والإفلات من إنفاذ القانون. وللتصدي لذلك، يجب أن تكفل الاتفاقية صياغة معايير التجريم بطريقة محايدة من الناحيتين التكنولوجية والمنهجية، لضمان أن تظل المعاهدة ذات صلة وفعالة في المستقبل.

*التدابير الإجرائية لمكافحة الجريمة السيبرانية*

يشكِّل القانون الإجرائي عنصراً حاسماً في التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها قضائياً. وينبغي للاتفاقية أن توفِّر إطاراً واضحاً للتدابير الإجرائية لضمان حصول سلطات إنفاذ القانون على الأدلة اللازمة لمكافحة الجريمة السيبرانية. وينبغي أن يدعم نطاق أي إطار للتدابير الإجرائية قوانين محلية واضحة وشديدة بما يكفي لتمكين

سلطات إنفاذ القانون أو غيرها من السلطات ذات الصلة من التصدي للتحديات التي تطرحها الجريمة السيبرانية، بسبل منها الكشف عن هذا النوع من الجريمة وتعطيله ومنعه والتحقيق فيه وملاحقة مرتكبيه قضائياً.

وينبغي أن تأخذ التدابير الإجرائية في الاعتبار أيضاً طبيعة البيانات الإلكترونية، بحيث يتسنى لسلطات إنفاذ القانون وغيرها من السلطات ذات الصلة الحصول على تلك البيانات بسرعة وفعالية لضمان ألا تعطِّل المنهجيات والممارسات الإجرامية في الفضاء السيبراني جهود السلطات في مجال جمع البيانات. ويمكن أن تشمل أنواع التدابير الإجرائية المعتمدة صلاحيات التفتيش والمصادرة، والصلاحيات المتصلة بإنتاج البيانات (مثل الوصول إلى الاتصالات المخزَّنة وأنشطة الاعتراض)، والطلبات أو الأوامر الطارئة أو العاجلة للكشف عن هذه البيانات. ويجب أن تستند التدابير الإجرائية إلى ضمانات وقيود قوية توفِّر حماية كافية لحقوق الإنسان وسيادة القانون.

وسيتعين على الدول على الأرجح أن تنظر في كيفية تجسيد ممارسات الدول فيما يتصل بجمع البيانات الإلكترونية على نطاق الولايات القضائية في اتفاقية جديدة.

*التعاون الدولي والمساعدة التقنية*

الجريمة السيبرانية بطبيعتها عابرة للحدود الوطنية في الغالب. والتعاون الدولي، مسنوداً بتدابير تجريم منسَّقة، أمر حاسم لقدرة الدول على التحقيق بفعالية في الأفعال التي يرتكبها مجرمو الفضاء السيبراني وملاحقتهم قضائياً.

وقد أحرز المجتمع الدولي تقدماً كبيراً في التعاون الدولي في مجال العدالة الجنائية في العقود الماضية، إذ وضع أدوات فعالة في طائفة من المعاهدات الدولية القائمة التي تنظِّم تبادل المساعدة القانونية وتسليم المطلوبين وغير ذلك من أشكال التعاون الدولي. فأحكام اتفاقية الجريمة المنظَّمة واتفاقية مكافحة الفساد، على سبيل المثال، توفِّر أساساً ممتازاً لهذا التعاون، وقد اعتُمدت على الصعيد العالمي تقريباً.

وينبغي أن تستند أحكام الاتفاقية الجديدة قدر الإمكان إلى أحكام مماثلة لها في اتفاقية الجريمة المنظَّمة واتفاقية مكافحة الفساد فيما يتعلق بالمساعدة القانونية المتبادلة وتسليم المطلوبين ونقل السجناء واسترداد عائدات الجريمة، فهذه الأحكام أثبتت فعاليتها، وتحظى بتأييد دولي واسع النطاق. وتماشياً مع الولاية الواردة في قرار الجمعية العامة 247/74، ينبغي أيضاً ضمان أن تكمِّل الاتفاقية الجديدة آليات التعاون الدولي الأخرى القائمة في مجال العدالة الجنائية وألا تقوِّضها.

وتوفِّر نظم دولية وإقليمية أخرى أطراً فعالة للتعاون الدولي في مجال التصدي للجريمة السيبرانية، مسنودة بضمانات وقيود قوية. وينبغي أن تستفيد الاتفاقية الجديدة من هذه النُّظم قدر الإمكان. ومن أهم هذه النظم اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي لا تزال توفِّر أساساً فعالاً للتعاون الدولي بين عدد كبير من الدول في جميع مناطق العالم.

وبالإضافة إلى التعاون الدولي، ينبغي للاتفاقية الجديدة أن تعزز بفعالية الجهود الرامية إلى تحسين القدرات الدولية على مكافحة الجريمة السيبرانية. وينبغي أن تصاغ على نحو يؤكِّد من جديدٍ الدور الرئيسي الذي يضطلع به مكتب الأمم المتحدة المعني بالمخدرات والجريمة في تقديم المساعدة التقنية وفي بناء القدرات، بما في ذلك بوصفه منظِّم البرنامج العالمي المعني بالجريمة السيبرانية.

*ضمانات حماية حقوق الإنسان وتعزيزها*

إنَّ لوصول الدول إلى البيانات الإلكترونية وبيانات الاتصالات السلكية واللاسلكية للأفراد، بحكم طبيعته، تأثيراً على حقوق الأفراد. ويجب أن تؤكِّد الاتفاقية من جديدٍ مسؤولية الدول عن تعزيز وحماية حقوق الإنسان للأفراد أثناء سعيها إلى مكافحة الجريمة السيبرانية، بما يتفق مع القانون الدولي لحقوق الإنسان.

ويجب أن تظل حقوق الأفراد في الخصوصية وحرية الرأي والتعبير وتكوين الجمعيات محمية على نحو كاف، وفقاً للمعايير الدولية القائمة. وتشمل الحقوق الأخرى التي يجب حمايتها أيضاً الحق في محاكمة عادلة، بما في ذلك المساواة أمام القانون، فضلاً عن الحق في عدم التعرض للتعذيب والمعاملة أو العقوبة اللاإنسانية أو المهينة، والاحتجاز التعسفي والتمييز. وقد أكد المجتمع الدولي مراراً أنَّ هذه الحقوق تنطبق على شبكة الإنترنت بقدر ما تنطبق خارجها، وينبغي للاتفاقية أن تكرِّر التأكيد على مسؤوليات الدول في التمسك بهذه الحقوق في سياق عملياتها الرامية إلى مكافحة الجريمة السيبرانية.

**الهيكل وأسلوب العمل**

بمجرد أن تتاح للدول فرصة إبداء آرائها فيما يتعلق بنطاق الاتفاقية في أولى جلسات التفاوض، المقرر عقدها في كانون الثاني/يناير 2022، تتوقع أستراليا أن ينبثق بسرعةٍ توافق في الآراء بشأن هيكل الاتفاقية.

وبعد أن تكون الدول قد أعربت عن آرائها بشأن نطاق الاتفاقية الجديدة وهيكلها وأهدافها في كانون الثاني/يناير 2022، تقترح أستراليا دعوة الدول إلى تقديم مقترحات بشأن البنود التي يتعين أن تُدرج في كل عنصر من عناصر هيكل الاتفاقية الجديدة (مثل مقترحات تتعلق بالتجريم والتعاون الدولي). وينبغي للرئيسة، بالتشاور مع أعضاء المكتب حسب الاقتضاء، أن تعمل على تجميع مختلف هذه المقترحات في مشروع اتفاقية يمكن للدول التفاوض بشأنه بعد ذلك، على أن يُنظَر في كل مجموعة من البنود بدورها وفقاً لخطة عمل تضعها اللجنة المخصَّصة في اجتماعها الأول.

وبعد مفاوضات أولية بشأن كل عنصر من عناصر هيكل الاتفاقية، يمكن التفاوض على الاتفاقية برمتها، مرة أخرى وفقاً لخطة عمل تضعها اللجنة المخصَّصة في اجتماعها الأول وتتولى الرئيسة إدارتها بعد ذلك.

## البرازيل

[الأصل: بالإنكليزية]
[29 تشرين الأول/أكتوبر 2021]

كما هو الحال في بلدان كثيرة، ما فتئت البرازيل تواجه الجريمة السيبرانية، وهي ظاهرة تتزايد وتيرتها وتطورها. ويقتضي انتقال ارتكاب جرائم جنائية مختلفة إلى المنصات الرقمية بذل جهود حاسمة من أجل تحديث التدابير المعيارية وتدابير إنفاذ القانون المناسبة للتصدي لهذه التهديدات، بما في ذلك على الصعيد الدولي. ويطرح النطاق الجغرافي لهذه الجرائم وسرعتها التشغيلية تحدياً للآليات التقليدية لإنفاذ القانون والتعاون القانوني على الصعيد العالمي.

والتحديات القائمة في هذا الصدد هائلة. وكثيراً ما يكون لمقدِّمي خدمات الإنترنت، الذين يملكون معلومات هامة يستلزمها التحقيق في الجريمة السيبرانية وجمع الأدلة الإلكترونية، مقار مادية في بلد واحد، ويقدِّمون الخدمات في قارات مختلفة، ويخزِّنون معلوماتهم على خوادم في أي مكان آخر من العالم. وفي ظل هذا السيناريو، تسعى سلطات إنفاذ القانون إلى أن تحدِّد وتخاطب على النحو الواجب كل من له الولاية القضائية على البيانات ويتسنى له الوصول إليها مباشرة.

ويُعَدُّ التنسيق الدولي المتماسك بين الولايات القضائية خطوة ضرورية إلى الأمام في ملاحقة مرتكبي الجريمة السيبرانية. وهناك حاجة إلى مزيد من التعاون وإلى تحسين التعاون القائم. ويتطلب تعطيل الجرائم بفعالية وسائل تعاون سريعة ومباشرة تمكِّن وكالات إنفاذ القانون من تبادل الأدلة المستمدة من مختلف القضايا التي تشمل نفس المجموعة الإجرامية في الوقت المناسب.

وتلتزم البرازيل بالمشاركة مشاركةً كاملة في التفاوض على اتفاقية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وهي فرصة فريدة لوضع معايير مشتركة للتعاون على التصدي لهذه المسألة التي تتميز بكونها عابرة للحدود الوطنية، بالبناء على أفضل التقاليد والممارسات القائمة في هذا الصدد.

وترى البرازيل أنه يجب أن تتناول اتفاقية توضع مستقبلاً العناصر التالية من حيث الأهداف والنطاق والهيكل لكي يتسنى لها التصدي للتحديات المذكورة آنفاً.

**الأهداف**

ينبغي أن يكون الهدف الرئيسي للاتفاقية توفير أدوات محدَّدة للتعاون الدولي حتى يتسنى للدول الأطراف الوصول في الوقت المناسب إلى الأدلة وغيرها من المعلومات التي تسهم في التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها قضائياً. وبالرغم من أهمية هذا الهدف الأساسي في حد ذاته، ينبغي أن يتوخى الصك أيضاً، في أمثل الأحوال، هدفين آخرين: (أ) وضع حد أدنى من الالتزامات المتعلقة بالتجريم (القانون الجنائي الموضوعي) في كل ولاية قضائية من ولايات الدول الأطراف؛ و(ب) وضع حد أدنى من الالتزامات لتهيئة أسباب الاستجابة والتحقيق والملاحقة القضائية في الوقت المناسب (القانون الجنائي الإجرائي) في كل ولاية قضائية من ولايات الدول الأطراف.

والبرازيل ملتزمة التزاماً كاملاً بفكرة صوغ اتفاقية عالمية. ونحن ندرك التحديات التي تواجه التفاوض على صك يتضمن معايير دنيا للتجريم، لا سيما بالنظر إلى هذه الظاهرة الحديثة والمتقلبة الاتجاهات. بيْد أنَّ هناك سوابق ناجحة في هذا الصدد. ففي مجالات أخرى من مجالات الجرائم، مثل الاتفاقيات العالمية القائمة لمكافحة الجريمة، أتاحت المفاوضات الفعالة لمعظم دول العالم الالتزام بمعايير موضوعية دنيا. وينبغي ألا تبدأ المناقشة من تعارض مفترض مسبقاً بين النطاق الجغرافي ونطاق التجريم، بل من استحضار أنَّ المفاوضات نفسها ستكون الطريقة الأكثر أماناً للتوصل إلى أفضل حد أدنى ممكن من توافق الآراء بشأن القانون الجنائي الموضوعي المتعلق بالجريمة السيبرانية. ومهما يكن مقيَّداً، يمكن للحد الأدنى من توافق الآراء بشأن التجريم – القائم برسوخ على مفاهيم محايدة وعامة – أن يحُدَّ من اختيار مرتكبي الجرائم السيبرانية للولاية القضائية، ويسهِّل تبادل الخبرات، ويقلِّص من الخلاف بشأن المعايير بين البلدان التي تطالب بتطبيق مبدأ ازدواجية التجريم شرطاً للتعاون.

وسيتوقف حسن توقيت التعاون الدولي في جميع الأحوال على الصكوك الإجرائية المتاحة للمحقِّقين والمدَّعين العامين والقضاة في أكثر الولايات القضائية تنوعاً. فلا توجد في أي مكان أدوات تقليدية للتعاون القانوني، مثل الإنابات القضائية والاعتراف بالأحكام الأجنبية، قادرة لوحدها على ضمان تدابير كافية للتصدي للجريمة السيبرانية. ويتطلب الانتشار عبر الأوطان والتقلب الشديد المتأصلان في هذه الظاهرة تنفيذ عملية توحيد للإجراءات، حتى وإن كان بالقدر اللازم من المرونة والعمومية لمراعاة جميع خصائص النُّظم القانونية المحلية المعنية. بيْد أنَّ من اللازم أن يعالج جوهر هذا التوحيد الإجرائي بعض المعايير الدنيا من أجل إتاحة السرعة في حفظ الأدلة الإلكترونية عن طريق قناة دولية سريعة ومباشرة، وإلا فلن يمكِّن من تحديد هوية المجرمين، ولا سيما في حالات الجريمة المنظَّمة.

**النطاق**

ينبغي أن توفّر الاتفاقية أساساً لتبادل الأدلة والبيانات المتعلقة بما يلي: (أ) الجرائم التي تستهدف النُّظم الحاسوبية؛ و(ب) أي جرائم تُرتكب باستخدام وسائل إلكترونية. وينبغي، في أمثل الأحوال، تناول البيانات الإلكترونية المتعلقة بالاتصالات والمحتوى والمشتركين.

وينبغي للاتفاقية أيضاً أن تمكّن الأطراف من تقديم طلبات للتعاون الدولي (من أجل التعجيل بحفظ البيانات الإلكترونية والمساعدة القانونية المتبادلة) وتزويد ولايات قضائية أخرى بالمعلومات تلقائياً. ويتعين تكريس فصل لبناء شبكة دولية من الممارسين يتولون مسؤولية الاستجابة للحالات العاجلة. وتعزّز هذه الآلية التنفيذية فهماً مفاده أنَّ هذه الاتفاقية تقتضي إنشاء هيئة لصنع القرار من أجل رصد تنفيذها واستعراضه.

ويمكن للمعاهدة، بوصفها صكاً إطارياً، أن تنص على إمكانية التفاوض على بروتوكولات باعتبارها أدوات إضافية، وهو ما من شأنه أن يعمّق التعاون بشأن أنواع محدَّدة من الجريمة السيبرانية.

ولذلك ينبغي أن تشكِّل الاتفاقية أداة للتطبيق العملي للقانون الجنائي، دون الخوض في السياسة المتعلقة بالسلم والأمن الدوليين، أو الدفاع السيبراني، أو المسائل المتصلة بهيكل الإنترنت أو إدارته على المستوى المحلي أو الإقليمي أو العالمي.

**الهيكل**

في ضوء الاعتبارات التي تقدَّم بيانها، ترى البرازيل أنَّ هيكل الاتفاقية ينبغي أن يكون على النحو التالي:

الفصل الأول– التجريم

الفصل الثاني– قانون الإجراءات الجنائية الذي يتيح التحقيق والملاحقة القضائية في الوقت المناسب

الفصل الثالث– التعاون الدولي

ألف– التعجيل بحفظ البيانات الإلكترونية

باء– المساعدة القضائية المتبادلة

جيم– تقديم المعلومات تلقائياً

الفصل الرابع– شبكة التعاون

الفصل الخامس– آلية متابعة رصد التنفيذ واستعراضه

**كندا**

[الأصل: بالإنكليزية]
[1 تشرين الثاني/نوفمبر 2021]

تقدِّم كندا هذه الورقة استجابة للدعوة التي وجَّهتها أمانة اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية في 11 آب/أغسطس تطلب فيها إلى الدول الأعضاء تقديم آراء بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها.

واسترشدت كندا، لدى إعداد هذه التعليقات، بالعمل الهام الذي أُنجز داخل الأمم المتحدة بشأن الجريمة السيبرانية على مدى أكثر من 20 عاماً تحت رعاية لجنة منع الجريمة والعدالة الجنائية، ولا سيما من جانب فريق الخبراء الحكومي الدولي المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، ومكتب الأمم المتحدة المعني

بالمخدرات والجريمة، من خلال برنامجه العالمي المعني بالجريمة السيبرانية، ومؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية. وقد مهَّدت هذه المبادرات الطريق لوضع اتفاقية للأمم المتحدة ينبغي أن تركِّز حصراً على مكافحة الجريمة السيبرانية، وألا تتناول الأمن السيبراني وتنظيم الفضاء السيبراني وغيرهما من المسائل ذات الصلة التي تعالَج على نحو أفضل في محافل أخرى من محافل الأمم المتحدة.

وتود كندا أن تؤكِّد مجدَّداً، وفقاً لقرار الجمعية العامة 282/75 والورقات السابقة التي قدَّمتها إلى اللجنة المخصَّصة، أنَّ التفاوض على الاتفاقية الجديدة يجب أن يكون عملية شفافة وشاملة، مما يتيح لهيئات المجتمع المدني وغيرها من الجهات المعنية صاحبة المصلحة فرصة حقيقية للمشاركة.

**النطاق**

ينبغي أن توفِّر الاتفاقية الجديدة إطاراً لمكافحة الجريمة السيبرانية والأفعال الإجرامية الخطيرة التي كثيراً ما تُرتكب باستخدام نظم حاسوبية، يتضمن العناصر التالية:

(أ) أحكاماً بشأن جرائم الفضاء السيبراني المستقلة والتحقيق في الجريمة السيبرانية والأفعال الإجرامية الخطيرة التي كثيراً ما تُرتكب باستخدام نظم حاسوبية وملاحقة مرتكبيها قضائياً؛

(ب) أحكاماً عن التعاون الدولي فيما يتعلق بما تقدَّم بيانه، وكذا عن استقاء أدلة إلكترونية خاصة بجرائم جنائية أخرى؛

(ج) أحكاماً تتضمن تدابير ترمي إلى منع الجريمة السيبرانية؛

(د) أحكاماً تتضمن تدابير تشجِّع الدول الأعضاء وغيرها من الجهات صاحبة المصلحة على تقديم مساعدة تقنية بصفة مستدامة واتخاذ مبادرات لبناء القدرات.

ويجب أن تكون عناصر الاتفاقية الجديدة متسقة مع الالتزامات الدولية في مجال حقوق الإنسان، ولا سيما فيما يتعلق بحرية التعبير والرأي وتكوين الجمعيات، فضلاً عن حق الفرد في عدم تعرضه لتدخل غير قانوني أو تعسفي في حياته الخاصة.

**الأهداف**

ينبغي أن تنشد الاتفاقية الجديدة تحقيق الأهداف التالية:

(أ) وضع خط أساس للأفعال الإجرامية المستقلة والصلاحيات الإجرائية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، استناداً إلى تفاهم مشترك؛

(ب) ضمان صياغة أحكامها صياغة محايدة تكنولوجياً حتى لا تصبح الأحكام متجاوَزة أو غير قابلة للتنفيذ مع تطور التكنولوجيات؛

(ج) تعزيز وتيسير التعاون الدولي في الجهود المشتركة الرامية إلى مكافحة الجريمة السيبرانية؛

(د) النص على صلاحية جمع الأدلة الإلكترونية بشأن جرائم أخرى والحصول عليها وتبادلها؛

(هـ) القضاء على الملاذات الآمنة لمرتكبي الجرائم السيبرانية؛

(و) ضمان امتثالها للالتزامات الدولية في مجال حقوق الإنسان، ولا سيما فيما يتعلق بحرية التعبير والرأي وتكوين الجمعيات، وحق الفرد في عدم تعرضه لتدخل غير قانوني أو تعسفي في حياته الخاصة؛

(ز) ضمان اتساقها مع معاهدات الأمم المتحدة القائمة في مجال منع الجريمة والعدالة الجنائية، ولا سيما اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد، ومراعاتها للصكوك المتعددة الأطراف التي أثبتت بالفعل جدواها في مكافحة الجريمة السيبرانية، ولا سيما الاتفاقية المتعلقة بالجريمة الإلكترونية؛

(ح) دعم الدول الأعضاء لتعزيز قدرتها على التصدي للجريمة السيبرانية من خلال المساعدة التقنية وبناء القدرات.

**الهيكل**

فيما يتعلق بهيكل الاتفاقية الجديدة، ترى كندا أنَّ من المهم، بالإضافة إلى إدراج تعاريف واضحة وأحكام نهائية فيها، أن تشكِّل العناصر الخمسة التالية جزءاً من هيكلها:

(أ) أحكام عن الجرائم المستقلة تقتضي من الدول الأعضاء اعتماد ما قد يلزم من تدابير تشريعية وتدابير أخرى:

'1' لتجريم الإجراءات التي تمسُّ بسرية النُّظم والبيانات الحاسوبية والشبكات وسلامتها وتوافرها، وتجريم إساءة استخدام النُّظم والبيانات الحاسوبية والشبكات؛

'2' لضمان أن تغطي قوانينها الجنائية على نحو كافٍ جرائم تقليدية محدَّدة كثيراً ما تُرتكب عن طريق استخدام النُّظم الحاسوبية، مثل نشر مواد إباحية عن الأطفال؛

(ب) أحكام إجرائية تُلزم الدول الأعضاء باعتماد ما قد يلزم من تدابير تشريعية وغيرها لتقرير صلاحية حفظ واستقاء الأدلة الإلكترونية على الجرائم الجنائية، المخزَّنة على النُّظم الحاسوبية في ولايات قضائية أجنبية أو متعددة أو غير معروفة. وينبغي أن تُدرج في الاتفاقية الجديدة صلاحيات تحقيق أكثر عمومية، مثل أوامر التفتيش والمصادرة وتقديم المستندات، ولكن ينبغي أيضاً النص على أدوات تحقيق أكثر تخصصاً لمواكبة السرعة التي يمكن بها ارتكاب الجرائم والطابع العابر للأدلة الإلكترونية وتقلبها. وينبغي أن تخضع هذه الأحكام لضمانات تكفل امتثال أنشطة إنفاذ القانون للالتزامات الدولية في مجال حقوق الإنسان؛

(ج) التعاون الدولي مهم في مكافحة الجريمة السيبرانية. وينبغي أن تنص الاتفاقية الجديدة على آليات لتيسير التعاون الدولي الرسمي وغير الرسمي على حد سواء من أجل كشف الجريمة السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائياً، وأيضاً بهدف الحصول على أدلة إلكترونية على أفعال إجرامية أخرى؛

(د) يجب أن تنص الاتفاقية الجديدة على تدابير وقائية مماثلة للتدابير المنصوص عليها في اتفاقية الجريمة المنظَّمة واتفاقية مكافحة الفساد، مثل أحكام بشأن التوعية والمبادرات التثقيفية. ويمكن للمجتمع المدني والشراكات فيما بين أصحاب المصلحة المتعددين أن يؤدّيا دوراً حيوياً في هذا الشأن، وهو ما ينبغي لأحكام الاتفاقية أن تجسده؛

(هـ) ينبغي للاتفاقية الجديدة أن تشجّع الدول الأعضاء على تعزيز قدرتها على التصدي للجريمة السيبرانية من خلال المساعدة التقنية وبناء القدرات. ويمكن أن يشمل ذلك أحكاماً تنص على ما يلي:

'1' دعم انخراط أصحاب مصلحة متعددين؛

'2' تشجيع التعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة وبرنامجه العالمي المعني بالجريمة السيبرانية لتعزيز مهارات الممارسين والسلطات المركزية في استخدام التكنولوجيا بغية تيسير التعاون الدولي في مجال مكافحة الجريمة السيبرانية؛

'3' وضع برامج تدريبية للمحقِّقين والمدَّعين العامين ودعم تبادل المعلومات والخبرات مع أصحاب المصلحة المعنيين.

## شيلي

[الأصل: بالإنكليزية]
[5 تشرين الثاني/نوفمبر 2021]

يطيب لحكومة شيلي أن تستجيب للدعوة الموجَّهة إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها) تنفيذاً لقراري الجمعية العامة 247/74 و282/75.

وترى شيلي أنَّ الاتفاقية الجديدة ينبغي ألا تتعارض مع معاهدات أو اتفاقات أخرى قائمة بشأن الجريمة السيبرانية، وأن تستند إلى التعاون الدولي والمساعدة التقنية باعتبارهما أساساً للنهج المتعدد الأطراف في مكافحة الجريمة السيبرانية. ويجب إيلاء نفس القدر من الأهمية لآراء جميع البلدان من أجل الحفاظ على عملية مفتوحة وشاملة وشفافة وقائمة على تعدد أصحاب المصلحة.

### 1- جوانب عامة

(أ) *الولاية القضائية*: الاتفاقية الجديدة فرصة ممتازة لمناقشة هذه المسألة، التي تشكِّل الأساس للعديد من الأدوات الإجرائية التي يمكن تناولها؛

(ب) ضمان صياغة التعاريف صياغة شاملة لضمان أن تكون ذات صلة وقابلة للتطبيق في سياق التحول التكنولوجي السريع. وإدراج تعاريف مثل تعريف مختلف أنواع البيانات.

### 2- القانون الجنائي الموضوعي

(أ) *إدراج جريمة تلقّي البيانات الحاسوبية*. رغم أنَّ لدى بعض البلدان مفهوماً مقيَّداً لهذا النوع من الجريمة، يبدو من المناسب إدراج فعل غير قانوني يُعنى بهذا النوع من السلوك عندما تكون "البضائع" المسروقة بيانات حاسوبية وكلُّ من يخزِّنها يعلم أو يُفترض فيه أن يعلم مصدرها غير المشروع؛

(ب) من حيث ارتكاب الفعل والمشاركة فيه، يبدو من المناسب أن تتناول الاتفاقية على وجه التحديد تعاون متلقي الأموال أو الأوراق المالية التي يتم الاستيلاء عليها بصورة غير قانونية عن طريق الاحتيال الحاسوبي، لأنَّ من المناسب، أخذاً في الحسبان خصائص هذه الفئة من الجرائم والتحديات الحقيقية التي يواجهها التحقيق فيها في الغالبية العظمى من الحالات، إيلاء اهتمام خاص لمحاكمة الأشخاص الذين يشكِّلون، بوجه عام، الحلقة الأولى التي يتعين تتبُّعها في السلسلة الإجرامية، ومن ثم فإنَّ من المناسب أن يُنسب إليهم قدر أكبر من المسؤولية عن ارتكاب فعل الاحتيال بحكم مشاركتهم، دون المساس بإمكانية تخفيض العقوبات في حالة إبدائهم تعاوناً فعالاً في القبض على مرتكبي الجرائم السيبرانية المتبقين.

**3- قواعد القانون الإجرائي**

(أ) من المناسب مناقشة أفكارٍ وأدوات عمل جديدة محتملة يمكن أن تستخدمها السلطات في الكشف عن الجرائم التي يجري الإعداد لها أو يزمع تنفيذها على شبكة الإنترنت، وأنجع طريقة للتصدي لهذا النوع من الجريمة؛

(ب) يبدو من المناسب مناقشة التوازن الذي يجب إقامته بين متطلبات الحماية اللازمة والواجبة للمواطنين والبيانات الشخصية ومتطلبات التحقيق الجنائي، لأنَّ الإفراط في حماية هذا النوع من المعلومات قد يؤثر على عملية بلورة إجراءات التحقيق التي تمكِّن من الملاحقة الجنائية بصورة صحيحة وفي الوقت المناسب لمرتكبي هذا النوع من الجريمة الذي يستفيد من إخفاء الهوية ومن عبوره للحدود الوطنية وتعذر اقتفاء أثره، وهي خصائص ملازمة لهذا النوع من السلوك.

**4- فصل متعلق بالتعاون الدولي**

(أ) من المهم إرساء مبادئ بشأن المساعدة القانونية المتبادلة في المسائل الجنائية؛

(ب) ينبغي للبلدان أن تستكشف سبل المساعدة على ضمان تبادل المعلومات في الوقت المناسب وبطريقة آمنة بين المحقِّقين والمدَّعين العامين الذين يعالجون قضايا الجريمة السيبرانية؛

(ج) ينبغي للبلدان أن تتعاون فيما بينها تعاوناً وثيقاً، بما يتوافق مع نُظمها القانونية والإدارية الداخلية في سبيل تعزيز فعالية إجراءات إنفاذ القانون الرامية إلى مكافحة الجريمة السيبرانية. وينبغي لكل بلد أن يعتمد تدابير فعالة لإنشاء قنوات اتصال بين سلطاته وأجهزته ودوائره المختصة بغية تيسير تبادل المعلومات المتعلقة بجميع جوانب الجريمة السيبرانية بطريقة آمنة وسريعة؛

(د) النظر في تبادل المساعدة القانونية إلكترونياً باعتباره شكلاً صحيحاً ودائماً وليس فقط في حالات الطوارئ؛

(هـ) حفظ البيانات وتقديمها؛

(و) تحليل المساهمة الإيجابية للشبكات التي تعمل على مدار الساعة وطيلة أيام الأسبوع باعتبارها مساهمة مبتكرة في التعاون الدولي؛

(ز) تنظيم حالات الطوارئ؛

(ح) ينبغي للبلدان أن تحدِّد بصورة مشتركة "الفجوة الرقمية" بين البلدان، لأنَّ بعض البلدان تفتقر إلى القدرة على منع الجريمة السيبرانية وكشفها ومكافحتها، وهي أكثر ضعفاً في مواجهة التحديات التي تطرحها الجريمة السيبرانية.

**5- أدوات خاصة للتعاون الدولي**

(أ) تقديم البيانات من قِبَل مقدِّمي خدمات الإنترنت وعلاقتهم بالدول؛

(ب) الوصول إلى البيانات عبر الحدود؛

(ج) أساليب التحري الخاصة: عملاء سريون على الإنترنت، وأفرقة تحقيق مشتركة، وتحقيقات مشتركة، في جملة أساليب أخرى.

### 6- المنع

(أ) يستلزم منع الجريمة السيبرانية مشاركة مختلف أصحاب المصلحة، بما في ذلك الحكومات وسلطات إنفاذ القانون والقطاع الخاص والمنظمات الدولية والمنظمات غير الحكومية والأوساط الأكاديمية؛

(ب) تعزيز استراتيجيات المنع المركّزة على الضحايا التي تتناول الجرائم السيبرانية بين الأفراد؛

(ج) ينبغي للبلدان أن تنظر في تنفيذ آليات للتعاون مع الجهات المعنية، بما في ذلك الإحالة إلى السلطات الوطنية المختصة وإتلاف المواد الإجرامية الضارة مثل مواد الاستغلال الجنسي للأطفال وغيرها من المواد العنيفة البغيضة.

### 7- المنظور الجنساني في سياق اتفاقية بشأن الجرائم السيبرانية

(أ) إدراج المنظور الجنساني في تنفيذ وتقييم أثر أحكام الاتفاقية، والنص على إجراء تحليل يراعي نوع الجنس فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات، ولا سيما عند الإشارة إلى القضايا الجنسانية المتصلة بالجريمة السيبرانية، بغية تعزيز المساواة بين الجنسين وتمكين المرأة على شبكة الإنترنت وخارجها؛

(ب) التصدي للجريمة السيبرانية ومنع ومكافحة العنف ضد النساء والأطفال.

## الصين

[الأصل: بالصينية]
[5 تشرين الثاني/نوفمبر 2021]

ترحِّب الصين بالدعوة التي وجَّهتها رئيسة لجنة الأمم المتحدة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية وأهدافها وهيكلها (عناصرها). وعملاً بقرار الجمعية العامة 282/75، يتعين أن تقدِّم اللجنة المخصَّصة مشروع اتفاقية إلى الجمعية العامة في دورتها الثامنة والسبعين. وتتطلع الصين إلى إجراء مناقشات بنّاءة بقيادة الرئيسة للتوصل وفقاً للجدول الزمني المقرَّر إلى اتفاقية جديدة عالمية ومرجعية ومقبولة لجميع الأطراف، من أجل إرساء إطار قانوني لتعزيز التعاون في مجال مكافحة الجريمة السيبرانية في جميع أنحاء العالم.

وقد استندت الدول الأعضاء حتى الآن إلى آليات الأمم المتحدة ذات الصلة لإجراء مناقشات متعمقة بشأن مكافحة الجريمة السيبرانية، وتوصلت إلى بعض الاستنتاجات والتوصيات المتَّفق عليها. كما قدَّمت إحدى الدول الأعضاء مشروع اتفاقية شاملة يوفِّر مرجعاً هاماً للتفاوض على الاتفاقية. وترحِّب الصين بجهود الرئيسة لتشجيع الدول الأعضاء على تقديم آرائها ومشاريع مقترحاتها بنشاط، وتدعم تحضيرات الرئيسة لإعداد مشروع أولي للاتفاقية استناداً إلى آراء الدول الأعضاء للبدء في التفاوض على نص الاتفاقية في أقرب وقت ممكن.

ودعماً لعمل الرئيسة واللجنة المخصَّصة، صاغت الصين الآراء التالية بشأن نطاق الاتفاقية وأهدافها وهيكلها (عناصرها)، وهي على استعداد للدخول في مفاوضات بنّاءة مع جميع الأطراف.

### أولاً- الأهداف

(أ) تشجيع وتعزيز التدابير الرامية إلى مكافحة ومنع استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية على نحو أكثر كفاءة وفعالية، إسهاماً في تفعيل رؤية مستقبل مشترك في مجتمع الفضاء السيبراني؛

(ب) تشجيع وتيسير ودعم التعاون الدولي في مجال منع ومكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، مع مراعاة خصائص تكنولوجيا المعلومات والاتصالات وضرورة مكافحة الأنشطة الإجرامية ذات الصلة. ويمكن أن يشمل هذا التعاون الدولي تنسيق معايير التجريم فيما بين الدول الأعضاء، وتوفير إرشادات بشأن تسوية المنازعات المتعلقة بالاختصاص القضائي، ووضع ترتيبات مؤسسية أدقَّ في إطار التعاون في مجال إنفاذ القانون، والمساعدة القانونية، وتسليم المطلوبين، واسترداد الموجودات؛

(ج) تعزيز التعاون في مجال بناء القدرات والمساعدة التقنية وتشجيع تبادل المعلومات في هذا المجال بما يتماشى مع احتياجات التعاون الدولي الأوسع نطاقاً ومصالح البلدان النامية.

## ثانياً- نطاق الانطباق

ينبغي أن تنطبق الاتفاقية على منع استخدام الأفراد أو الجماعات الإجرامية لتكنولوجيا المعلومات والاتصالات للأغراض الإجرامية والتحقيق فيه وملاحقة مرتكبيه قضائياً، فضلاً عن ضبط عائدات الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات وتجميدها وحجزها ومصادرتها وإرجاعها.

وينبغي أن ينطبق استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، في الحد الأدنى، على الجرائم المرتكبة ضد مرافق ونُظم وبيانات تكنولوجيا المعلومات والاتصالات، والجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات.

## ثالثاً- الهيكل (العناصر)

يمكن تقسيم الاتفاقية إلى سبعة فصول: أحكام عامة؛ والمنع؛ والتجريم وإنفاذ القانون؛ والتعاون الدولي؛ والمساعدة التقنية وتبادل المعلومات؛ وآلية التنفيذ؛ وأحكام ختامية.

وتقدَّم الاقتراحات الأولية التالية فيما يتعلق بعناصر الفصول المذكورة.

### 1- أحكام عامة

بالإضافة إلى الأهداف ونطاق التطبيق، ينبغي إدراج المحتوى التالي أيضاً:

(أ) *صون السيادة*. مبدأ المساواة في السيادة المكرَّس في ميثاق الأمم المتحدة هو القاعدة الأساسية للعلاقات الدولية المعاصرة، كما أنَّ الدول الأعضاء تؤيد على نطاق واسع تطبيق مبدأ السيادة على الفضاء السيبراني. وينبغي أن تنص الاتفاقية على أنَّ الدول الأطراف ملزمة بالوفاء بالتزاماتها بموجب الاتفاقية وفقاً لمبادئ المساواة في السيادة والسلامة الإقليمية وعدم التدخل في الشؤون الداخلية للدول الأخرى؛

(ب) *المصطلحات المستخدمة*. ينبغي إدراج تعاريف للمصطلحات الرئيسية الواردة في الاتفاقية، مثل الأدلة الإلكترونية، والمعلومات الشخصية، والبنية التحتية الحيوية للمعلومات، والتخزين السحابي، ومزوِّد خدمات الشبكات، والبرامجيات الضارة، وشبكات السيطرة على الأجهزة الإلكترونية (البوتنيت)، والمعلومات الضارة، والهجمات السيبرانية.

### 2- المنع

ينبغي إبراز أهمية منع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية. وينبغي أن يكون المبدأ الأساسي هو "وضع المنع في المقام الأول، مع مكافحة الجريمة في الوقت نفسه". وينبغي توضيح

مسؤوليات الحكومات والقطاع الخاص في منع الجريمة، وينبغي للحكومات أن تضع تدابير محدَّدة الأهداف لمنع الجريمة، مع تشجيع مشاركة المجتمع والتعاون بين القطاعين العام والخاص. وينبغي إدراج النقاط التالية:

(أ) ينبغي تشجيع الدول الأعضاء على تعيين وكالات متخصصة لوضع سياسات بشأن منع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية وإجراء تقييمات منتظمة. وينبغي للدول الأعضاء أن توفِّر حماية أمنية للبنية التحتية الحيوية للمعلومات، فضلاً عن استحداث نُظم للحماية الأمنية استناداً إلى مختلف مستويات الشبكات. وينبغي اعتماد تكنولوجيات مختلفة لأمن المعلومات وتدابير إدارية لمختلف مرافق الشبكات من أجل حماية البنية التحتية الحيوية للمعلومات من التعرض للهجوم من جانب المجرمين أو الجماعات الإجرامية. وينبغي تعزيز قدرة الإدارات الحكومية المعنية على منع الجريمة؛

(ب) ينبغي للدول الأعضاء أن تسنَّ تشريعات وطنية أو تحسِّن التشريعات القائمة لتوضيح مسؤوليات القطاع الخاص، بمن في ذلك مقدِّمو خدمات الشبكات، في منع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية. وينبغي أن تشمل تلك المسؤوليات، في جملة ما تشمل، الاحتياطات الأمنية (على سبيل المثال، وضع خطط طوارئ لحوادث أمن الشبكات، ومعالجة أوجه القصور في النُّظم والمعدات، والتصدي للفيروسات الحاسوبية أو الهجمات التي تستهدف الشبكات أو اقتحام الشبكات، في الوقت المناسب، واتخاذ تدابير بصورة آنية كلما تبيَّن أنَّ خدمات مقدِّمي الخدمات قد تُستخدم في الأنشطة الإجرامية) والاحتفاظ بمعلومات السجلات (ينبغي للحكومات أن تحدِّد معيار المحتوى ومدة الاحتفاظ بمعلومات السجلات). وعند تحديد مسؤوليات مقدِّمي خدمات الشبكات، ينبغي وضع ترتيبات مصمَّمة خصِّيصاً لكل مستوى ومتوافقة مع مبدأ التناسب، مع مراعاة الاختلافات في قدرات مقدِّمي خدمات الشبكات من مختلف الأحجام مراعاة تامة؛

(ج) ينبغي تشجيع الحكومات والقطاع الخاص والمجتمعات المحلية على الانخراط في مختلف أشكال التعاون بين القطاعين العام والخاص. وينبغي على وجه الخصوص بذل المزيد من الجهود لتعزيز وعي الجمهور بمنع الجريمة.

### 3- التجريم وإنفاذ القانون

تتزايد إساءة استخدام المجرمين والجماعات الإجرامية لتكنولوجيا المعلومات والاتصالات في ارتكاب الجرائم، مما يؤدي إلى ظهور "سلسلة إنتاج" خفية متخصصة في استخدام تكنولوجيا المعلومات والاتصالات لأغراض ومعاملات إجرامية تستخدم هذه التكنولوجيات والبيانات ذات الصلة. وينبغي أن توفِّر الاتفاقية إطاراً أكثر مرونة واستشرافاً للمستقبل لتنسيق التجريم، بما يلبي الاحتياجات في مجال تطوير تكنولوجيا المعلومات والاتصالات حاضراً ومستقبلاً، ويستجيب لضرورة مكافحة الجريمة. وينبغي أن تنص الاتفاقية أيضاً على الآليات ذات الصلة فيما يتعلق بالاختصاص القضائي وإنفاذ القانون والأدلة الإلكترونية:

(أ) ينبغي أن يُطلب إلى الدول الأعضاء تجريم اقتحام وتدمير مرافق تكنولوجيا المعلومات والاتصالات أو نُظمها أو بياناتها أو البنية التحتية الحيوية للمعلومات. ويمكن أن تشمل هذه الأفعال الوصول بصورة غير قانونية إلى نُظم المعلومات الحاسوبية، والتلاعب بصورة غير قانونية بنُظم المعلومات الحاسوبية، والحصول بصورة غير قانونية على البيانات الحاسوبية، والتدخل بصورة غير قانونية في البيانات الحاسوبية، والاعتداء على البنية التحتية الحيوية للمعلومات، من بين أمور أخرى؛

(ب) يمكن أن تورد الاتفاقية، حسب الاقتضاء، الأنشطة الإجرامية التي تُرتكب باستخدام تكنولوجيا المعلومات والاتصالات ويعترف بها المجتمع الدولي على نطاق واسع، مثل الابتزاز الإلكتروني، والاحتيال الإلكتروني، والمواد الإباحية على الإنترنت (ولا سيما استغلال الأطفال في المواد الإباحية)، واستخدام

تكنولوجيا المعلومات والاتصالات لانتهاك حقوق المؤلف والحقوق ذات الصلة، واستخدام الإنترنت للتحريض على ارتكاب أعمال إرهابية أو لارتكابها أو نشر معلومات ضارة، من بين أمور أخرى؛

(ج) فيما يتعلق بالجرائم الأخرى التي تُرتكب باستخدام تكنولوجيا المعلومات والاتصالات، ينبغي التشديد على أنه يجوز للدول الأعضاء أن تكافح وتمنع الجرائم ذات الصلة غير المدرجة في الاتفاقية، وأن تنخرط في التعاون الدولي وفقاً للاتفاقية والاتفاقيات الدولية الأخرى والتشريعات الوطنية السارية في الدول الأعضاء؛

(د) نظراً لتزايد "تصنيع" الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات، ينبغي إدراج "سلسلة الإنتاج" الخفية ضمن نطاق التجريم، إلى جانب تدابير أشدَّ لقمع التحريض على ارتكاب هذه الأفعال الإجرامية أو الإعداد لها، بما في ذلك تطوير أو بيع أو نشر تكنولوجيا المعلومات والاتصالات أو البيانات للأغراض الإجرامية؛

(هـ) فيما يخص عبارة "الأدلة الإلكترونية"، ينبغي النص على القواعد التي تحدد الأدلة الإلكترونية في الإجراءات القضائية الجنائية، بما في ذلك كيفية التحقق من صحة الأدلة الإلكترونية وسلامتها وشرعيتها وأهميتها؛

(و) يمكن أن يُطلب إلى الدول الأعضاء صوغ تشريعات وطنية أو تحسين التشريعات القائمة بغية توضيح التزامات القطاع الخاص، مثل التزام مقدِّمي خدمات الشبكات بالتعاون مع سلطات إنفاذ القانون في رصد الجرائم والتحقيق فيها ومكافحتها. وينبغي أن تشمل هذه الالتزامات، في جملة التزامات أخرى، الاحتفاظ بمعلومات السجلات، والحفاظ على البيانات والأدلة وفقاً لمعايير ومُدد المحتوى الموحَّدة، والتعاون مع سلطات إنفاذ القانون. وعند تقرير التزامات مقدِّمي خدمات الشبكات، ينبغي وضع ترتيبات مصمَّمة خصِّيصاً لكل مستوى ومتوافقة مع مبدأ التناسب، مع مراعاة الاختلافات في قدرات مقدِّمي خدمات الشبكات من مختلف الأحجام مراعاة تامة. وإذا لم يَفِ مقدِّم خدمات الشبكات بالتزاماته ذات الصلة، ينبغي للدول الأعضاء أن تفرض عليه عقوبات إدارية وجنائية فعالة وفقاً لتشريعاتها الوطنية؛

(ز) ينبغي توفير إرشادات بشأن تسوية المنازعات المتعلقة بالاختصاص القضائي. فبالنظر إلى خصوصيات الفضاء السيبراني وتكنولوجيا المعلومات والاتصالات، ينبغي النص على معايير بشأن كيفية تحديد الاختصاص القضائي وتجنب المنازعات المتعلقة به. وينبغي أن يستند الاختصاص القضائي إلى وجود صلة "حقيقية وكافية" بالنشاط الإجرامي المعني، مع إعطاء الأولوية للمكان الذي تقع فيه عواقب النشاط الإجرامي، والمكان الذي ارتُكبت فيه الجريمة، والمكان الذي يوجد فيه الشخص أو المجموعة التي ارتكبت الجريمة. فإن كان من الصعب صوغ هذه المعايير، ينبغي عندئذ صوغ معايير استثناء؛ فعلى سبيل المثال، لا ينبغي تمكين دولة ما من المطالبة بالاختصاص القضائي على قضية تتعلق بتكنولوجيا المعلومات والاتصالات لمجرد أنَّ البيانات تمر عبر تلك الدولة. وفي حالات النزاع بشأن الاختصاص القضائي، ينبغي تقرير الولاية القضائية من خلال التشاور وفقاً لمبادئ أنسب محكمة للنظر في القضية وتيسير استرداد الموجودات؛

(ح) ينبغي أيضاً وضع أحكام بشأن المساعدة على ارتكاب جريمة أو التشجيع على ارتكابها، والإعداد لارتكاب جريمة، والشروع في ارتكاب جريمة، والجريمة التي يرتكبها كيان، وغير ذلك.

### 4- التعاون الدولي

يتسم استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية بطابع عابر للحدود الوطنية إلى حد بعيد ويمثِّل تحدياً مشتركاً يواجه المجتمع الدولي. وبالإضافة إلى ذلك، فإنَّ عدم الكشف عن الهوية والذكاءَ البالغ الذي تتسم به الأنشطة الإجرامية وعدم استقرار الأدلة الإلكترونية وقابليتها للتلف كلها عوامل تشكِّل تحديات هائلة تواجه آليات التعاون الدولي مثل المساعدة القانونية المتبادلة بمقتضى الإطار القانوني الدولي القائم. وينبغي للدول الأعضاء أن تتعاون فيما بينها إلى أقصى حد ممكن على مكافحة ومنع استخدام تكنولوجيا

المعلومات والاتصالات للأغراض الإجرامية، وذلك بالتمسك بمبدأ المعاملة بالمثل، واستكشاف سبل الابتكار المؤسسي بنشاط، واقتراح آليات جديدة لتعاون دولي أكثر تركيزاً:

(أ) جمع الأدلة الإلكترونية عبر الحدود ضروري لمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، ولكن ينبغي للدول الأعضاء أن تحترم سيادة الدولة التي توجد فيها الأدلة. وينبغي للدول الأعضاء أيضاً أن تتقيد بالمحاكمة وفق الأصول القانونية، وأن تحترم الحقوق المشروعة للأفراد والكيانات، وألا تستخدم أي وسائل تحقيق تقنية تقتحم الخصوصيات أو مدمِّرة في جمع الأدلة الإلكترونية عبر الحدود. وينبغي للدول ألا تجمع مباشرةً بيانات في حوزة مؤسسات أو أفراد في دول أجنبية أو باستخدام وسائل تقنية تتجاوز تدابير حماية أمن الشبكات إذا كانت هذه الوسائل تنتهك قوانين تلك الدولة الأجنبية. وينبغي للدول الأعضاء أن تستكشف ترتيبات مؤسسية جديدة لجمع الأدلة الإلكترونية من دول أخرى، مثل توثيق الأدلة الإلكترونية وجمع الأدلة بالفيديو (أو الأدلة الصوتية) على أساس الثقة المتبادلة. وينبغي بذل جهود في إطار هذه الترتيبات لتوفير إرشادات موحَّدة ومعتمدة لجمع الأدلة الإلكترونية عبر الحدود مع الموازنة بين مختلف أهداف احترام السيادة الوطنية ومكافحة الجريمة؛

(ب) ينبغي للدول الأعضاء أن تضع آليات لتسريع التعاون في مجال إنفاذ القانون. ويمكن للدول الأعضاء أن تعيِّن وكالات محدَّدة لأغراض الاتصال، مما يتيح تبادل أدلة الجريمة بسرعة، وإسداء المشورة التقنية وغير ذلك من أشكال التعاون في مجال إنفاذ القانون في حالة الاحتياجات الخاصة؛

(ج) من أجل تحسين كفاءة المساعدة القانونية المتبادلة في المسائل الجنائية، يمكن للدول الأعضاء أن تنشئ آلية للاتصال والاستجابة السريعين بين السلطات المختصة لضمان التواصل بصورة آنية عند الاقتضاء. ويمكن نقل الوثائق القانونية والأدلة الإلكترونية في إطار جمع الأدلة عبر الحدود على الإنترنت عن طريق الوسائل التقنية (مثل التوقيعات الإلكترونية) في إطار النظم الوطنية العابرة للحدود لإدارة أمن إرسال البيانات. ويمكن أيضاً إدراج حكم بشأن المساعدة القانونية المتبادلة في حالات الطوارئ، مثل التعجيل بحفظ الأدلة الإلكترونية، والتعجيل بالإفصاح عن البيانات بعد حفظها، وغير ذلك؛

(د) بالنظر إلى التزامات القطاع الخاص – التي يتعين النص عليها في التشريعات الوطنية –، بمن في ذلك مقدِّمو خدمات الشبكات، بالتعاون مع سلطات إنفاذ القانون في رصد الأنشطة الإجرامية وكشفها ومكافحتها، ينبغي للدول الأعضاء، ولا سيما الدول الأعضاء التي لديها موارد شبكية متقدمة، أن تعزِّز التعاون الدولي أكثر. فإذا استُخدمت مرافق تكنولوجيا المعلومات والاتصالات أو نُظمها أو شبكاتها المملوكة لمزوِّد خدمات شبكات في الدولة ألف من قِبل شخص مشتبه به في دولة أخرى من أجل ارتكاب جريمة، ينبغي للدولة ألف، ما دامت تجرِّم بدورها الفعل المعني، أن تطلب، بمبادرة منها أو بناء على طلب الدولة الأخرى، إلى مقدِّم خدمات الشبكات المعني أن يستفيد من التدابير التقنية وأي تدابير أخرى ضرورية للتصدي بفعالية لذلك النشاط الإجرامي؛

(هـ) ينبغي تعزيز التدابير ذات الصلة لمنع وإعاقة النقل الدولي لعائدات الجريمة وتعزيز التعاون الدولي في مجال استرداد الموجودات. وينبغي للدول الأعضاء أن تتقيد بمبدأ استرداد الموجودات بسرعة وفعالية وألا تضع أي شروط مسبقة لاسترداد الموجودات غير الإجراءات القضائية.

### 5- المساعدة التقنية وتبادل المعلومات

من الضروري تقديم المساعدة التقنية إلى البلدان النامية وتعزيز تبادل المعلومات معها من أجل تحقيق الفعالية في مكافحة ومنع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية:

(أ) ينبغي أن تشمل المساعدة التقنية المقدَّمة إلى البلدان النامية ما يلي:

'1' تدريب موظفي القضاء وإنفاذ القانون؛

'2' تدريب الفِرَق المهنية التي تمتلك الخبرة القانونية والتقنية على حد سواء؛

'3' بناء القدرات في مجال جمع الأدلة الإلكترونية؛

'4' توفير المعدات والتكنولوجيا ذات الصلة، حسب الاقتضاء، لمساعدة البلدان النامية على تعزيز قدرتها على مكافحة الجريمة؛

'5' تشجيع المنظمات الدولية مثل مكتب الأمم المتحدة المعني بالمخدرات والجريمة والقطاع الخاص والخبراء والأكاديميين على المشاركة في جهود المساعدة التقنية وبناء القدرات؛

(ب) ينبغي تشجيع الدول الأعضاء على تقاسم خبراتها في مجال صياغة القوانين والسياسات وتنفيذها، وعلى تبادل البيانات المتعلقة بمكافحة الجريمة واتجاهات الجريمة ومنعها.

### 6- آلية التنفيذ

لتعزيز تنفيذ الاتفاقية، ينبغي إنشاء مؤتمر للدول الأطراف وأفرقة خبراء أو أفرقة عاملة ذات صلة، مثل فريق عامل معني بالمساعدة التقنية، وفريق عامل معني بالتعاون الدولي. ويمكن أن توفِّر اجتماعات هذه الأفرقة أيضاً منبراً للدول الأطراف لتبادل الخبرات وتعزيز التعاون.

### 7- أحكام ختامية

لا تعليقات في هذه المرحلة.

## كولومبيا

[الأصل: بالإسبانية]
[5 تشرين الثاني/نوفمبر 2021]

بالنظر إلى اعتماد الجمعية العامة للقرار 247/74، الذي أنشئت من خلاله لجنة خبراء حكومية دولية مخصَّصة مفتوحة العضوية لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، واستجابةً لدعوة رئيسة اللجنة المخصَّصة الموجَّهة إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية التي ستوضع مستقبلاً بشأن الجريمة السيبرانية، وأهدافها وهيكلها، نود أن نقدِّم تعليقات كولومبيا الأولية التالية.

### النطاق

ينبغي أن تركِّز الاتفاقية الجديدة على هدف إرساء أداة للتعاون القانوني الدولي لكي يتسنى للسلطات الوطنية منع الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائياً ومعاقبتهم، ومعالجة المسائل المتعلقة بالأدلة الإلكترونية. ولذلك ينبغي تجنب المناقشات التي لا تركِّز على المشكلة القانونية المتمثلة في الجريمة السيبرانية وإدارة الأدلة الإلكترونية.

وينبغي أيضاً تفادي المناقشات بشأن المسائل التي قد تكون حساسة من الناحية السياسية ولا تتصل مباشرة بجوهر الاتفاقية المراد التفاوض بشأنها.

ومن الضـــروري أن تراعي الاتفاقية الجديدة الأطر والصـــكوك القانونية الدولية القائمة، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفســـاد والاتفاقية المتعلقة بالجريمة الإلكترونية، لأنَّ التشـريعات والممارسـات الوطنية لمعظم الدول تتماشـى مع الاتفاقات القائمة أو تسـتند إليها؛ ومن ثم، يجب أن تكون المعايير التي توضـع مسـتقبلاً متوافقة مع تلك الاتفاقات. وعلاوة على ذلك، ينبغي الحرص على ألا تؤدي القواعد التي ســـيتم إعدادها إلى عدم التوافق مع الالتزامات الدولية الأخرى التي تعهدت بها الدول أو إلى تعارضها معها.

وفي هذا الصدد، ينبغي أن تتَّبع الاتفاقية نهجاً تكميلياً، بمعنى أن تأخذ المفاوضات في الاعتبار، من حيث المبدأ، العمل الذي يضطلع به المجتمع الدولي منذ عدة سنوات في مجال مكافحة الجريمة السيبرانية وألا تتعارض مع الالتزامات الدولية ذات الصلة التي تضطلع بها الدول. ولذلك ينبغي اغتنام الإمكانات التي أتاحتها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والتقدم الذي أحرزته في إرســـاء مبادئ راســـخة وأدوات للتعاون القضائي.

وينبغي أن تؤخذ في الاعتبار الأطر القائمة المتعددة الأطراف والإقليمية والثنائية التي تنظِّم المسـاعدة القانونية المتبادلة من أجل تجنب التضارب المحتمل في القوانين والأنظمة، ومن أجل استكمال الصكوك الدولية القائمة وتطبيقها، وتجنب عرقلة تنفيذها الفعال. ولذلك، ينبغي التوصـــية بإيلاء اعتبار شـــامل ليس للاتفاقيات المتعددة الأطراف السـابقة فحسـب، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والاتفاقية المتعلقة بالجريمة الإلكترونية، بل أيضـــاً للاتفاقات الثنائية والإقليمية، مثل اتفاقية البلدان الأمريكية للمســـاعدة المتبادلة في المسائل الجنائية.

وينبغي أن تؤخذ في الاعتبار على وجه التحديد الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست، 2001)، لأنها تغطي المفاهيم التي نوقشت باستفاضة وتجسد 20 عاماً من الخبرة الدولية العملية. ومن شأن عدم القيام بذلك أن ينطوي على احتمال اتباع مسار قد يقوِّض التقدم المحرز بالفعل في مكافحة الجريمة السيبرانية.

وينبغي أن تأخذ العملية في الاعتبار أيضـــاً نتائج عمل فريق الخبراء المعني بإجراء دراســـة شـــاملة لمشكلة الجريمة السيبرانية في إطار الأمم المتحدة، وأن تستند إلى قائمة الاستنتاجات والتوصيات الأولية التي اقترحتها الدول الأعضاء خلال اجتماعات ذلك الفريق.

ونشـدِّد على أهمية صـياغة الاتفاقية الجديدة بطريقة شـاملة وشـفافة وعلى أسـاس توافق الآراء، قدر الإمكان، كما كان الشـــأن في عمليات الأمم المتحدة الســـابقة لإبرام اتفاقية الجريمة المنظَّمة واتفاقية مكافحة الفساد، من أجل المساعدة على منع نشوب نزاعات في المستقبل.

**الهدف**

ينبغي أن يكون الهدف العام للاتفاقية اعتمادَ إطار للتعاون القضـــائي الدولي ينص على نحو شـــامل على الوقاية والتحقيق والملاحقة القضـــائية في مجال مكافحة اســـتخدام تكنولوجيات المعلومات والاتصـــالات للأغراض الإجرامية – الجريمة السيبرانية – ويتناولُ المسائل المتعلقة بالأدلة الإلكترونية.

**الهيكل**

- تعاريف رئيسية ومفاهيم تكنولوجية موحَّدة تظل صالحة مع مرور الوقت.
- أحكام موضوعية (الأفعال الإجرامية التي يتعين أن تنص عليها التشريعات الوطنية).

وفي هذا الصدد، ينبغي للاتفاقية أن تجرِّم طائفة من الأفعال التي تمسُّ بالنُّظم والمعلومات الحاسوبية.

وسيكون من المنطقي، من حيث المبادئ والمنهجية على السواء، التركيز حصراً على الجرائم "الأساسية" المتعلقة بالجرائم السيبرانية: الجرائم المتصلة بالوصول الرقمي غير المأذون به إلى شبكات أو نُظم حاسوبية عن طريق ارتكاب جرم الوصول بصورة غير قانونية إلى نظام حاسوبي؛ والتجسس السيبراني، الذي يشمل جميع الأفعال التي تنتهك خصوصية الأشخاص الطبيعيين والاعتباريين من خلال اعتراض البيانات أو الاتصالات أو الملفات أو قواعد البيانات المخزَّنة في النُّظم الحاسوبية أو المرسلة عبر شبكات الاتصالات، أو الحصول عليها، كما يشمل جرائم اعتراض البيانات الحاسوبية، وخرق البيانات الشخصية وإنشاء مواقع للتصيد الإلكتروني بهدف الاستيلاء على البيانات الشخصية؛ وتخريب الحواسيب بهدف تعطيل النُّظم الحاسوبية أو قواعد البيانات أو عمليات معالجتها ونقلها وإرسالها، أو بهدف إتلافها أو جعلها غير صالحة للاستعمال أو تعطيل نشاطها أو العبث بها، ويشمل ذلك جرائم تعطيل نظام حاسوبي أو شبكة اتصالات بصورة غير مشروعة.

وبالإضافة إلى ذلك، يمكن أن يعرِض الصك عدداً من الأفعال التي تنطوي على أثر خطير وبعيد المدى ويصعب التحقيق فيها لأنها تُرتكب بوسائل رقمية؛ ومن شأن هذا الأمر أن يجعل الاتفاقية مرنة بما يكفي لتكون أداة لمكافحة الأنشطة غير القانونية المتصلة بجرائم أخرى:

- شرط ازدواجية التجريم: هذه الآلية مهمة في تيسير تبادل المساعدة القانونية بصرف النظر عما إذا كان الفعل الذي يؤدِّي إلى تقديم هذه المساعدة خاضعاً للعقاب بموجب قانون الدولة متلقية الطلب، مما يكفل، في جملة أمور، الحيلولة دون وجود ملاذات آمنة لمرتكبي الجرائم السيبرانية في بعض البلدان في غياب تشريعات نموذجية موحَّدة.

- الأحكام الإجرائية التي تتيح التعاون القانوني الفعال: من اللازم، في هذا الصدد، تعزيز التعاون الدولي في مجال التحقيق في الجرائم السيبرانية، ولا سيما فيما يتعلق بإدارة الأدلة الرقمية، وسلسلة المسؤوليات، والاحتفاظ بالبيانات، وتحليل الأدلة الجنائية. وتتطلب مسألة إرسال البيانات وتخزينها اهتماماً عاجلاً، فضلاً عن إرساء آليات تمكِّن من الاتصال والاستجابة السريعين بين السلطات النظيرة في مختلف الدول، من خلال قنوات رقمية مناسبة وآمنة.

- الظروف المشدِّدة المنطبقة على الأفعال التي تمس بالحق القانوني في حماية المعلومات والبيانات، مثل الأفعال المتعلقة بالاستيلاء على البيانات الشخصية على نطاق واسع، أو انتهاك حقوق الإنسان، أو الأفعال التي تستهدف البنية التحتية الحيوية والخدمات الأساسية.

- التعاون القضائي الدولي: تيسير وتوسيع وتسريع طلبات المساعدة القانونية المتبادلة من خلال القنوات الرقمية، مع توفير الضمانات المناسبة، ومن خلال نماذج موحَّدة.

- إرساء آليات تحقيق خاصة لجمع الأدلة الرقمية، خاصة فيما يتعلق بالأدلة المخزَّنة في ولايات قضائية مختلفة.

- من المهم أن تتَّفق الدول الأعضاء على آليات تكفل مستوى ملائماً من الحماية للبيانات الشخصية في سياق تبادل المعلومات من خلال هذا الصك الدولي، لا بحكم أهمية حماية البيانات الشخصية في البيئة الرقمية فحسب، بل أيضاً لتجنب احتمال أن تعيق القواعد الخاصة بكل بلد تبادل المعلومات بين الدول بفعالية.

- تعزيز المساعدة التقنية وتعميم المعارف والممارسات الجيدة المتعلقة بالتحقيق والملاحقة القضائية والعقاب. وبالإضافة إلى ذلك، من الضروري، لسد الفجوة الرقمية، أن تتناول الاتفاقية بناء قدرات مؤسسات إنفاذ القانون وغيرها من السلطات القضائية الوطنية، ولا سيما فيما يتعلق ببرامج التعليم والتدريب باعتبارها شكلاً من أشكال الوقاية.

- تعزيز التعاون التقني من خلال مدارس التدريب الإقليمية. فبالنظر إلى تعقُّد وخصوصية التحقيق في الجرائم التي تُرتكب عن طريق الوسائل الرقمية وتعوق التحقيق الفعال، من الضروري توفير تدريب متخصِّص للمدَّعين العامين والمحقِّقين على نحو منظَّم ومستمر واستناداً إلى خطط عمل محدَّدة سلفاً تعرض النتائج المتوقعة.
- تشجيع تعاون قوي قائم على الثقة بين القطاعين العام والخاص في مجال الجريمة السيبرانية أمر بالغ الأهمية، ومن هذا المنطلق يلزم صوغ موقف مشترك بشأن هذه المسألة وتيسير جمع الأدلة الرقمية من جانب الجهات الفاعلة في المجال الرقمي، بمن في ذلك مقدِّمو خدمات الإنترنت وشركات الاتصالات.
- تعزيز وتيسير وصول السلطات إلى المنابر التعاونية لبناء القدرات وتبادل المعلومات والأدوات التحليلية والسياقية للتحقيق في الجرائم السيبرانية.
- صوغ أحكام تسهِّل الوصول إلى المعلومات في الوقت المناسب في حالات الطوارئ.
- وآخر المقترحات أن تنص الاتفاقية على إنشاء شبكة من جهات تنسيق تعمل على مدار الساعة وطيلة أيام الأسبوع، للاستجابة لطلبات التعاون القانوني الدولي فيما يتعلق بالجريمة السيبرانية. وبالإضافة إلى ذلك، يمكن استكمال الشبكة بشبكة جهات اتصال من أجل: (أ) تعزيز تبادل المعارف والخبرات فيما يتعلق بالجريمة السيبرانية والجرائم ذات الصلة؛ و(ب) إرساء الممارسات الجيدة وتعميمها؛ و(ج) تحسين التعاون القضائي الدولي وتبسيطه.

## الجمهورية الدومينيكية

[الأصل: بالإسبانية]
[5 تشرين الثاني/نوفمبر 2021]

ترحب الجمهورية الدومينيكية بفرصة المساهمة في هذه العملية الجماعية مع جميع الدول الأعضاء بهدف تقديم تعليقات حول نطاق صك دولي جديد بشأن الجريمة السيبرانية وأهدافه وهيكله، وفقا لقراري الجمعية العامة 247/74 و282/75، المؤرخين 27 كانون الأول/ديسمبر 2019 و26 أيار/مايو 2021 على التوالي.

والجريمة السيبرانية شكل مستجد من أشكال الجريمة عبر الوطنية، وواحدة من أسرع أشكال الجريمة نموا في العالم. ويرتبط تزايدها بصورة وثيقة بتطور تكنولوجيات المعلومات والاتصالات ونموها الهائل، وهو ما يؤثر على ملايين المواطنين والشركات كل عام.

وقد تأثرت منطقتنا، منطقة أمريكا اللاتينية والبحر الكاريبي، بشكل خاص بهذه الظاهرة. فالبلدان النامية تفتقر إلى حد كبير إلى القدرة اللازمة لمكافحة الجريمة السيبرانية، وهو وضع له تأثير مباشر من حيث العدد الكبير من الأشخاص المسجلين باعتبارهم ضحايا لهذه الجريمة.

وعلاوة على ذلك، فإن جائحة مرض فيروس كورونا (كوفيد-19) الحالية سلطت الضوء على ازدياد تعرض المجتمع الدولي للجريمة السيبرانية، وهو الوضع الذي يؤكد على أهمية وجود تدابير للتصدي على الصعيد العالمي قائمة على التعاون والتنسيق، لا بين الدول الأعضاء فحسب، وإنما أيضا بين الحكومات والمنظمات غير الحكومية والمجتمع المدني والأوساط الأكاديمية والقطاع الخاص، إذ إن تعقد الجريمة السيبرانية واتساع نطاقها يقتضيان أن تستند أية تدابير إلى نهج متعدد التخصصات لكي تكون فعالة.

وتدعم الجمهورية الدومينيكية هذا المسعى من جانب المجتمع الدولي دعما كاملا، وتكرر تأكيد استعدادها للعمل مع جميع الدول الأعضاء من أجل إبرام معاهدة دولية تمثل كل الدول وتسترشد في جميع الأوقات بمبادئ الشفافية والنزاهة والشمول.

**النطاق**

ترى الجمهورية الدومينيكية أن الغرض الأساسي من صك دولي جديد بشأن الجريمة السيبرانية هو توفير أداة فعالة لمنع الجريمة السيبرانية وكشفها والتحقيق فيها وملاحقة مرتكبيها جنائيا، مع الاحترام الكامل للخصوصية وحماية البيانات والحريات المدنية وحقوق الإنسان.

وينبغي أن ييسر الصك، على وجه الخصوص، عمليات التحقيق الجنائي للتمكين من جمع الأدلة الرقمية في الوقت المناسب واستخدامها فيما بعد، وهو ما يحد من الإفلات من العقاب على هذا النوع من الجرائم، حيث يشكل هذا الإفلات أحد العوائق الرئيسية التي يواجهها موظفو إنفاذ القانون في الميدان.

وينبغي له أيضا أن يشجع وييسر التعاون الدولي فيما بين الدول الأعضاء وتقديم المساعدة التقنية وبناء قدرات الدول الأطراف التي تحتاج إلى هذا الدعم فيما يتعلق بالجريمة السيبرانية.

وترى الجمهورية الدومينيكية أيضا أنه ينبغي النص بوضوح على أن يقتصر الصك الجديد على مجال الجريمة السيبرانية؛ ولا ينبغي أن يتناول المسائل المتعلقة بموضوعي الأمن السيبراني وإدارة الإنترنت اللذين تجري مناقشتهما في محافل أخرى.

ومع ذلك، فإنه من المفهوم ضرورة مراعاة أحكام الصكوك الدولية والإقليمية القائمة من أجل تجنب عدم التوافق غير الضروري مع النظم القانونية للدول الأعضاء التي استخدمت تلك الصكوك كأساس لتشريعاتها الوطنية، أو مع تطبيق تلك الصكوك. ومن ثم، فمن المهم الاستفادة من الخبرة المكتسبة في تنفيذ الصكوك المعنية، وتحديد مواطن القوة والضعف التي يمكن للاتفاقية الجديدة تناولها. وينبغي أيضا أن تؤخذ جهود الأفرقة المتخصصة، مثل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، في الاعتبار.

**الأهداف**

ينبغي للصك الدولي الجديد بشأن منع الجريمة السيبرانية ومكافحتها، في جملة أمور، أن:

- يشجع وييسر التعاون الدولي السريع والعملي والفعال بين الدول الأطراف.
- يغطي منع الجرائم السيبرانية التي ينطبق عليها الصك وكشفها والتحقيق فيها وملاحقة مرتكبيها جنائيا، وجمع ومعالجة الأدلة الرقمية المتعلقة بجرائم أخرى، مما يزود الدول الأطراف بالأدوات اللازمة لمكافحة هذا النوع من الجرائم عبر الوطنية.
- يحدد بوضوح أنواع الجرائم التي تنطبق عليها أحكام الاتفاقية الجديدة والتي ينبغي اعتبارها أفعالا غير مشروعة في النظم القانونية لجميع الدول الأطراف.
- يعزز وييسر بناء القدرات في الدول الأطراف التي تحتاج إلى بناء هذه القدرات بغرض منع إنشاء "ملاذات آمنة لمرتكبي الجرائم السيبرانية".
- يشجع تبادل الممارسات الجيدة والدروس المستفادة.

- يحدد قواعد واضحة لسريان الولاية القضائية بغرض طلب أدلة رقمية من مقدمي خدمات الإنترنت "على الصعيد العالمي"، وهو ما يعد حاليا أحد أكبر التحديات التي تعوق الحد من الإفلات من العقاب ودعم ضحايا الجريمة السيبرانية.
- وضع ضمانات واضحة ونظام للعقوبات على عدم الامتثال لتلك الضمانات.
- وضع صلاحيات كافية للتحقيق في الجرائم الجنائية المشمولة، مع مراعاة احترام الخصوصية وحماية البيانات والحريات المدنية وحقوق الإنسان في جميع الأوقات.
- نظرا للتطور السريع للتكنولوجيا، ينبغي أن تكون للاتفاقية رؤية واسعة بعيدة المدى؛ وينبغي من ثم استخدام لغة محايدة تكنولوجيا لضمان عدم تأثر انطباق الاتفاقية بالتطورات التكنولوجية مع مرور الوقت.
- وضع نهج متعدد التخصصات يمكِّن من التعاون الفعال بين القطاعين العام والخاص.

**الهيكل**

- التعاريف.
- الجرائم الجنائية.
- الأدوات الإجرائية في مجال التحقيق.
- الضمانات.
- التعاون الدولي.
- الوصول إلى الأدلة الرقمية.
- المساعدة التقنية وبناء القدرات في مجال التحقيق.
- إجراءات العمل الموحدة.
- تدابير المنع.
- آلية التنفيذ.

**مصر**

[الأصل: بالعربية]
[28 تشرين الأول/أكتوبر 2021]

انطلاقاً من حرص جمهورية مصر العربية على المساهمة إيجابياً في المساعي الدولية المبذولة لبلورة اتفاقية أممية شاملة في مجال مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، والتزاماً بتعهداتها في المواثيق والتشريعات الوطنية والإقليمية والدولية ذات الصلة بحقوق الإنسان ومكافحة الجرائم العابرة للحدود الوطنية، تم إعداد ورقة تتضمن عناصر مبدئية يُقترح إدراجها في متن الاتفاقية المشار إليها، وذلك أملاً في تحقيق الأهداف المنشودة منها من خلال تعزيز التعاون الدولي وصياغة سياسة جنائية مشتركة تهدف إلى مكافحة كافة أشكال الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، بغية درء أخطار هذه الجرائم على أمن الدول ومصالحها وسلامة مجتمعاتها وأفرادها.

## أولاً- الهدف من الاتفاقية

تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول الأعضاء في الأمم المتحدة في مجال مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، بغية منع أية إجراءات من شأنها تهديد سلامة وسرية تكنولوجيا المعلومات والاتصالات، وتجريم إساءة استخدام هذه التكنولوجيا لأغراض غير قانونية، وتيسير سبل التحقيق فيها، وملاحقة مرتكبيها، وتنفيذ التدابير الرامية إلى إزالة تداعيات هذه الجرائم، بما في ذلك تعليق المعاملات المتعلقة بالأصول التي تم الحصول عليها نتيجة ارتكاب أي فعل غير قانوني منصوص عليه بموجب هذه الاتفاقية، ومصادرة عائدات هذه الجرائم وإعادتها، وذلك من خلال توفير صلاحيات كافية لمكافحة هذه الجرائم بشكل فعال عن طريق وضع ترتيبات للتعاون الدولي من أجل تسهيل اكتشاف هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها ومقاضاتهم وتسليم المجرمين.

## ثانياً- نطاق انطباق الاتفاقية

1- تطبق هذه الاتفاقية، باستثناء ما تنص عليه خلافا لذلك، على منع الجرائم المنصوص عليها بموجب هذه الاتفاقية.

2- تتخذ كل دولة طرف جميع التدابير اللازمة لإقامة الولاية القضائية على الجرائم الجنائية وغيرها من الأعمال غير المشروعة المنشأة وفقا لهذه الاتفاقية، عندما ترتكب:

(أ) في إقليم تلك الدولة الطرف؛ أو

(ب) على متن سفينة ترفع علم تلك الدولة الطرف عندما ارتكبت الجريمة، أو على متن طائرة مسجلة بموجب قانون تلك الدولة الطرف في ذلك الوقت؛

(ج) حيثما يكون الجرم ذا طابع عبر وطني وتكون جماعة إجرامية منظمة ضالعة في ارتكابه، ويعد الجرم ذا طابع عبر وطني في الأحوال التالية: '1' ارتُكب في أكثر من دولة واحدة؛ '2' ارتُكب في دولة واحدة ولكن جرى جانب من الإعداد أو التخطيط له أو توجيهه أو الإشراف عليه في دولة أخرى؛ '3' ارتُكب في دولة واحدة، ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة؛ '4' ارتُكب في دولة واحدة، ولكن له آثارا جسيمة في دولة أخرى.

3- لأغراض تنفيذ هذه الاتفاقية، لا يلزم أن تؤدي الجرائم وغيرها من الأعمال غير القانونية التي تنشأ فيها إلى إلحاق أضرار بالممتلكات، إلا على النحو المنصوص عليه في هذه الاتفاقية.

4- على كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة بعاليه.

## ثالثاً- صون السيادة

1- تلتزم كل دولة طرف وفقاً لقوانينها الداخلية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

**رابعاً- الجرائم المقترح أن تشملها الاتفاقية**

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لمنع ارتكاب الجرائم المنصوص عليها في هذه الاتفاقية أو أية جرائم أخرى ترتكب بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك حجب وإزالة المحتوى المرتبط بهذه الجرائم، واكتشافها وملاحقة مرتكبيها ومقاضاتهم وتسليم المجرمين وتسهيل إجراءات التعاون الدولي وجمع الأدلة فيها.

2- تعتمد أيضا كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية:

**المادة الأولى: الانتفاع بدون وجه حق بخدمات الاتصال والمعلومات وتقنياتها:**

كل من انتفع أو سهل للغير بغير وجه حق الانتفاع بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية، وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات واتصالات.

**المادة الثانية: الدخول غير المشروع و/أو تجاوز حدود الحق في الدخول:**

1- كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.

2- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

3- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

'1' محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين؛

'2' الحصول على معلومات حكومية سرية.

**المادة الثالثة: الاعتداء على تصميم موقع:**

كل من أتلف أو عطل أو أبطأ أو شوَّه أو أخفى أو غيَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

**المادة الرابعة: الاعتراض غير المشروع:**

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

**المادة الخامسة: الاعتداء على سلامة البيانات:**

تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

**المادة السادسة: إساءة استخدام وسائل تقنية المعلومات:**

إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أو حيازة أية أدوات أو برامج مصممة أو مكيفة أو كلمة سر أو معلومات مشابهة يتم بواسطتها دخول نظام المعلومات بقصد استخدامها لارتكاب إحدى الجرائم المنصوص عليها بموجب تلك الاتفاقية، أو إنشاء البرمجيات الخبيثة التي يقصد بها التدمير أو الحجب أو التعديل أو النسخ أو نشر المعلومات الرقمية أو تحييد سماتها الأمنية، باستثناء البحوث المشروعة.

**المادة السابعة: التزوير :**

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنيّة استعمالها كبيانات صحيحة.

**المادة الثامنة: الاحتيال:**

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين – عن قصد وبدون وجه حق – بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، بما في ذلك من خلال جرائم احتيالية إلكترونية متعلقة بالعملات الافتراضية (الرقمية او المشفرة).

**المادة التاسعة: التهديد والابتزاز :**

استخدام تكنولوجيا المعلومات والاتصالات أو أية وسيلة تقنية أخرى في التهديد أو الابتزاز لحمل شخص على ارتكاب فعل أو الامتناع عنه.

**المادة العاشرة: الإباحية:**

1- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية بغرض الدعارة من خلال تقنيات الاتصالات والمعلومات.

2- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية للأطفال والقُصر، بما في ذلك حيازة مواد إباحية للأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية الاتصالات والمعلومات أو وسيط تخزين تلك التقنيات.

**المادة الحادية عشر: الجرائم الأخرى المرتبطة بالإباحية:**

الاستغلال الجنسي أو التحرش، لاسيما بالنساء والأطفال والقصر.

**المادة الثانية عشر: التشجيع على الانتحار أو الإكراه عليه:**

تشجيع الانتحار أو الإكراه عليه، بما في ذلك انتحار الأطفال، عن طريق الضغط النفسي أو غيره من الضغوط على شبكات المعلومات والاتصالات، بما فيها شبكة الإنترنت، سواء كان ذلك عن طريق التعامل المباشر أو عن طريق التقنيات الحديثة والألعاب الالكترونية.

**المادة الثالثة عشر: تورط الأطفال في ارتكاب أعمال غير مشروعة:**

تورط القصر عن طريق تكنولوجيا المعلومات والاتصالات في ارتكاب أفعال غير مشروعة تعرض حياتهم أو صحتهم الجسمانية والنفسية للخطر.

**المادة الرابعة عشر – الاعتداء على حرمة الحياة الخاصة بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك تجريم كل من اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري.**

**المادة الخامسة عشر – الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:**

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها أو تبريرها.

2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، وتوفير الدعم اللوجيستي لمرتكبيها.

3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4- نشر النعرات والفتن والكراهية والعنصرية.

5- تتخذ الدول التدابير اللازمة لمنع نشر هذا المحتوى على وسائل تكنولوجيا المعلومات والاتصالات، بما في ذلك حجب وإزالة المحتوى المرتبط بهذه الجرائم.

**المادة السادسة عشر – الجرائم المالية بما في ذلك المتعلقة بغسل الأموال:**

1- استخدام تكنولوجيا المعلومات والاتصالات لارتكاب أية جرائم مالية وإساءة استخدام العملات الافتراضية (الرقمية والمشفرة)

2- القيام بعمليات غسل أموال، أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

**المادة السابعة عشر: الاستخدام غير المشروع لأدوات الدفع الالكترونية:**

1- كل من زوّر أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.

3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

**المادة الثامنة عشر – الجرائم المتعلقة بالجرائم المنظمة أو ذات طابع عبر وطني والمرتكبة بواسطة تقنية المعلومات:**

1- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.

2- التوزيع غير المشروع للأدوية والمنتجات الطبية المقلدة.

3- تهريب المهاجرين.

4- الاتجار بالأشخاص.

5- الاتجار بالأعضاء البشرية.

6- الاتجار غير المشروع بالأسلحة.

7- الاتجار غير المشروع بالممتلكات الثقافية.

**المادة التاسعة عشر – الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة:**

انتهاك حق المؤلف والحقوق المجاورة ذات الصلة كما هي مُعرفة في قانون الدولة الطرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد.

**المادة العشرون– الدخول غير المصرح به في البنية التحتية للمعلومات الحيوية:**

1– لإنشاء وتوزيع واستخدام برامج أو معلومات رقمية أخرى مصممة للدخول غير المشروع في البنية التحتية للمعلومات الحيوية، بما في ذلك تدمير أو حظر أو تعديل أو نسخ المعلومات الواردة فيه أو تحييد ميزات الأمان.

2– انتهاك قواعد تشغيل الوسائط المصممة لتخزين ومعالجة ونقل البيانات الرقمية المحمية في البنية التحتية للمعلومات أو نظم المعلومات الهامة، بموجب القانون الداخلي للدولة الطرف، وشبكات المعلومات والاتصالات التي تنتمي إلى البنية التحتية الحيوية للمعلومات، أو وسائل الوصول إليها طالما أنها تضر بالبنية التحتية الحيوية للمعلومات.

**المادة الحادية والعشرون– التحريض على الأنشطة التخريبية أو المسلحة أو الجرائم الجنائية الأخرى:**

تجريم الدعوات الصادرة عن طريق تكنولوجيا المعلومات والاتصالات من أجل الدعوة للأنشطة التخريبية أو المسلحة الموجهة ضد نظام دولة أخرى مما من شأنه زعزعة الأمن العام والاستقرار، أو ارتكاب الجرائم الجنائية المعاقب عليها بالحبس مدة لا تقل عن سنة.

**المادة الثانية والعشرون– الجرائم المتعلقة بالتطرف:**

تجريم توزيع المواد التي تدعو إلى ارتكاب أفعال غير مشروعة بدافع سياسي أو إيديولوجي أو اجتماعي أو عرقي، عن طريق تكنولوجيا المعلومات والاتصالات، أو أي فعل غير قانوني آخر يدعو لكراهية عرقية أو دينية أو العداء بصفة عامة، وتجريم الدعوة وتبرير مثل هذه الأعمال أو توفير النفاذ إليها.

**المادة الثالثة والعشرون– الشروع في ارتكاب جريمة:**

الشروع في ارتكاب أحد الأفعال المجرمة المنصوص عليها في الاتفاقية، و/أو المساهمة كشريك في أحد الأفعال المجرمة المنصوص عليها في الاتفاقية، و/أو تنظيم أو توجيه أشخاص آخرين لارتكاب أحد الأفعال المجرمة المنصوص عليها في الاتفاقية.

**المادة الرابعة والعشرون– الأفعال الأخرى غير القانونية:**

لا تمنع هذه الاتفاقية الدولة الطرف من تجريم أي فعل غير قانوني آخر يُرتكب عمدا عن طريق تكنولوجيا المعلومات والاتصالات ويسبب ضررا جسيما.

**خامساً– المسئولية القانونية والإجراءات الجنائية وإنفاذ القانون والمساعدة القانونية الدولية:**

**المادة الأولى– مسئولية الأشخاص الاعتباريين:**

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسئولية الجنائية للأشخاص الاعتباريين عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها، دون الإخلال بفرض العقوبة على الشخص الطبيعي – بما في ذلك مدير الموقع – الذي يرتكب الجريمة.

**المادة الثانية– مسئولية مقدمي الخدمات/مديري المواقع:**

مع عدم الإخلال بالأحكام الواردة بهذه الاتفاقية، يلتزم مقدمو الخدمات/ مديرو المواقع والتابعون لهم بما يلي، مع تجريمه في حالة مخالفة أي من تلك الالتزامات:

1– حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة (يتم تحديدها). وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

(أ) البيانات التي تمكن من التعرف على مستخدم الخدمة؛

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل متى كانت تحت سيطرة مقدم الخدمة؛

(ج) البيانات المتعلقة بحركة الاتصال؛

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال؛

(هـ) أي بيانات أخرى تحددها الدولة لأغراض تنفيذ هذه الاتفاقية.

2- المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها

3- تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

4- يجب على مقدم الخدمة/مدير الموقع أن يوفر لمستخدمي خدماته ولأي جهة مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:

(أ) اسم مقدم الخدمة وعنوانه؛

(ب) معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني؛

(ج) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.

5- يوفر مقدم الخدمة/مدير الموقع –حال طلب السلطات المختصة التي تم تحديدها من قبل الدولة– كافة الإمكانيات الفنية التي تتيح لتلك السلطات ممارسة اختصاصاتها.

**المادة الثالثة– الإجراءات الجنائية:**

1- تتخذ كل دولة طرف ما يلزم من تدابير تشريعية وتدابير أخرى لتحديد السلطات والإجراءات لأغراض منع وتحديد وكشف الجرائم وغيرها من الأعمال غير المشروعة والتحقيق فيها، واتخاذ الإجراءات القضائية المتعلقة بهذه الجرائم.

2- تطبق كل دولة طرف الصلاحيات والإجراءات المشار إليها على:

(أ) الأفعال الإجرامية وغيرها من الأفعال غير المشروعة المقررة في هذه الاتفاقية؛

(ب) الجرائم الجنائية الأخرى وغيرها من الأعمال غير المشروعة المرتكبة بواسطة تكنولوجيا المعلومات والاتصالات؛

(ج) جمع الأدلة عن الجرائم بشكل الكتروني.

3- تتضمن الإجراءات الجنائية ما يلي:

(أ) التحفظ العاجل على البيانات المخزنة في تقنية المعلومات والاتصالات بما في ذلك معلومات تتبع المستخدمين والتي خُزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل، وذلك من خلال إصدار أمر إلى شخص من أجل إلزامه بحفظ سلامة هذه المعلومات الموجودة بحيازته أو تحت سيطرته من أجل تمكين السلطات المختصة من البحث والتقصي، مع الحفاظ على سرية أية إجراءات تتخذ في هذا الشأن؛

(ب) التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات، وضمان قيام السلطات المختصة بالكشف العاجل لمقدار عادل من المعلومات لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات؛

(ج) أمر تسليم المعلومات في حوزة شخص في إقليم دولة طرف والمخزنة على تقنية معلومات أو وسيط تخزين، أو في حوزة مزود خدمة يقدم خدماته في إقليم الدولة الطرف أو تحت سيطرته؛

(د) تفتيش المعلومات المخزنة أو الوصول إلى المعلومات المخزنة في تقنية المعلومات أو وسيط تخزين؛

(ه) ضبط المعلومات المخزنة وعمل نسخة منها والاحتفاظ بها من أجل إتمام إجراءات تفتيش والوصول إلى المعلومات المخزنة؛

(و) الجمع الفوري لمعلومات تتبع المستخدمين وإلزام مزود الخدمة ضمن اختصاصه بجمع وتسجيل المعلومات والاحتفاظ بسرية أية معلومات؛

(ز) اعتراض معلومات المحتوى من خلال تمكين السلطات المختصة بالجمع والتسجيل من خلال الوسائل الفنية بشكل فوري للمعلومات التي تبث بواسطة تكنولوجيا المعلومات والاتصالات؛

(ح) تتخذ كل دولة طرف ما يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من وقف بث وإذاعة أي محتوي يشكل الجرائم المنصوص عليها في هذه الاتفاقية.

4- قبول الأدلة الرقمية:

يكون للأدلة الرقمية المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الالكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات والاتصالات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية وفقاً لقوانين الدول الأطراف.

**المادة الرابعة- التعاون القانوني والقضائي الدولي:**

1- تعمل الدول الأطراف على تيسير التعاون فيما بينها وفقاً لهذه الاتفاقية أو تطبيق مبدأ المعاملة بالمثل، من أجل تبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها.

2- تتعاون الدول الأطراف إلى أقصى حد ممكن وفقا لأحكام هذه المادة وعملا بالصكوك الدولية الأخرى المتعلقة بالتعاون الدولي في المسائل الجنائية ومبدأ المعاملة بالمثل، وكذلك القوانين الداخلية ذات الصلة بهدف منع وقمع وكشف والتحقيق في الجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات.

3- لأغراض تسليم المجرمين والمساعدة القانونية المتبادلة في المسائل الجنائية، لا تعتبر أي من الجرائم المنصوص عليها في هذا الاتفاقية جريمة سياسية. وبناء عليه، لا يجوز رفض طلب التسليم أو المساعدة القانونية في المسائل الجنائية المتصلة بهذه الجرائم، بدعوى ان الطلب يتعلق بجريمة سياسية أو جريمة مرتبطة بجريمة سياسية أو بجريمة ذات دوافع سياسية.

4- الاختصاص: تلتزم كل دولة بتبني الإجراءات الضرورية لمد اختصاصها على الجرائم المنصوص عليها سلفاً إذا ما ارتُكبت الجريمة كلياً أو جزئيا أو تحققت:

(أ) في إقليم الدولة الطرف؛

(ب) على متن سفينة تحمل علم الدولة الطرف؛

(ج) على متن طائرة مسجلة تحت قوانين الدولة الطرف؛

(د) من جانب أحد مواطني الدولة الطرف إذا كانت الجريمة يُعاقب عليها حسب القانون المحلي في مكان ارتكابها، أو إذا كان ارتُكبت خارج منطقة الاختصاص القضائي لأية دولة؛

(هـ) إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

5- تسليم المجرمين:

(أ) يتم تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها بعاليه، بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية، ويجوز للدولة الطرف – التي يسمح قانونها بذلك – أن توافق على طلب تسليم شخص ما بسبب أي من الجرائم المشمولة بهذه الاتفاقية والتي لا يعاقب عليها بموجب قانونها الداخلي؛

(ب) إن الجرائم المنصوص عليها بعاليه تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف؛

(ج) إذا قامت دولة طرف بجعل تسليم المجرمين مشروطاً بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم، فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين؛

(د) يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة، بما في ذلك الأسس التي يمكن للدول الطرف الاستناد إليها لرفض طلب التسليم؛

(هـ) يجوز لكل دولة طرف أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية، وذلك إذا ما وجهت إليها الدول الطرف الأخرى طلباً بالملاحقة مصحوباً بالملفات والوثائق والمعلومات والدلائل التي تكون في حيازتها، وتحاط الدولة الطرف الطالبة علماً بما تم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم؛

(و) تسعى الدول الأطراف، رهنا بقوانينها الداخلية، إلى التعجيل بإجراءات التسليم وتبسيط ما يتصل بها من متطلبات إثباتية فيما يخص أي جُرم تنطبق عليه هذه المادة؛

(ز) يجوز للدولة الطرف متلقية الطلب، رهنا بأحكام قانونها الداخلي ومعاهداتها المتعلقة بالتسليم، وبناء على طلب من الدولة الطرف الطالبة، أن تحتجز الشخص المطلوب تسليمه والموجود في إقليمها، أو أن تتخذ تدابير مناسبة أخرى لضمان حضوره إجراءات التسليم، متى اقتنعت بأن الظروف تستدعي ذلك وبأنها ظروف ملحّة؛

(ح) إذا رُفض طلب تسليم مقدَّم لغرض تنفيذ حكم قضائي بحجة أن الشخص المطلوب تسليمه هو من مواطني الدولة الطرف متلقية الطلب، وجب على الدولة الطرف متلقية الطلب، إذا كان قانونها الداخلي يسمح بذلك ووفقا لمقتضيات ذلك القانون، أن تنظر، بناء على طلب من الدولة الطرف الطالبة، في إنفاذ العقوبة المفروضة بمقتضى القانون الداخلي للدولة الطرف الطالبة أو ما تبقى منها؛

(ط) تُكفل لأي شخص تُتخذ بشأنه إجراءات فيما يتعلق بأي من الجرائم التي تنطبق عليها هذه المادة معاملة منصفة في كل مراحل الإجراءات، بما في ذلك التمتع بجميع الحقوق والضمانات التي ينص عليها القانون الداخلي للدولة الطرف التي يوجد ذلك الشخص في إقليمها؛

(ي) لا يجوز تفسير أي حكم في هذه الاتفاقية على أنه يفرض التزاما بالتسليم إذا كان لدى الدولة

الطرف متلقية الطلب أسباب وجيهة لاعتقاد أن الطلب قدّم لغرض ملاحقة أو معاقبة شخص بسبب جنسه أو عرقه أو ديانته أو جنسيته، أو أن الامتثال للطلب سيلحق ضررا بوضعية ذلك الشخص لأي سبب من هذه الأسباب؛

(ك) لا يجوز للدول الأطراف أن ترفض طلب تسليم لمجرد أن الجرم يعتبر جرما يتعلق بأمور مالية؛

(ل) قبل رفض التسليم، تتشاور الدولة الطرف متلقية الطلب، حيثما اقتضى الأمر، مع الدولة الطرف الطالبة لكي تتيح لها فرصة وافية لعرض آرائها وتقديم معلومات داعمة لادعائها؛

(م) تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإبلاغ بيانات السلطة المسئولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي إلى (جهاز متخصص يتم الاتفاق عليه) وتحديثها بشكل دوري.

6- المساعدة المتبادلة:

(أ) على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم؛

(ب) يتم تقديم طلب المساعدة الثنائية والاتصالات المتعقلة بها كتابةً، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف؛

(ج) باستثناء ما يرد فيه نص في هذه الاتفاقية، فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون؛

(د) حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة.

7- المعلومات العرضية المُتلقاة:

يجوز لأي دولة طرف – ضمن حدود قانونها الداخلي – وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف.

8- الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة:

(أ) تطبق مواد هذه الفقرة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة أو المطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي؛

(ب) على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها، مع تحديث بيانات هذه السلطة بشكل دوري؛

(ج) يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة؛

(د) يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها؛

(هـ) قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة، بعد استشارة الدولة الطرف الطالبة لها، أن تقرر فيما إذا سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية؛

(و) تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب، وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير؛

(ز) يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية أي طلب ما عدا القدر الكافي لتنفيذ الطلب، وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب؛

(ح) في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها؛

(ط) يجوز عمل الاتصالات وتقديم الطلبات حسب الفقرة السابقة بواسطة الإنتربول.

9- رفض المساعدة:

(أ) يجوز للدولة الطرف المطلوب منها المساعدة - بالإضافة إلى أسس الرفض المنصوص عليها في المواد السابقة أعلاه- أن ترفض المساعدة إذا اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادتها أو أمنها أو نظامها أو مصالحها الأساسية؛

(ب) لا يجوز رفض المساعدة القضائية في الجرائم المنصوص عليها في هذه الاتفاقية تأسيسا على كون تلك الجرائم من الجرائم السياسية أو ما في حكمها.

10- السرية وحدود الاستخدام:

عندما لا يكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع النافذ بين الدول الأطراف الطالبة والمطلوب منها فيجب تطبيق هذه المادة، ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق هذه المادة جزئيا أو كلها.

11- الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات:

(أ) لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات التي تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات؛

(ب) يمكن للدولة الطرف المطلوب منها المساعدة أن ترفض تنفيذ طلب الحفظ إذا اعتبرته قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

12- الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة:

(أ) حيثما تكتشف الدولة الطرف المطلوب منها – في سياق تنفيذ الطلب الخاص بحفظ معلومات تتبع المستخدمين الخاصة باتصالات معينة – بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات؛

13- التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة:

(أ) يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها؛

(ب) تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية؛

(ج) تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل.

14- الوصول إلى معلومات تقنية المعلومات عبر الحدود:

يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات.

15- التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:

(أ) على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينه في أقاليمها والتي تبث بواسطة تقنية المعلومات؛

(ب) على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية.

16- التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينه تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية.

17- جهاز متخصص:

(أ) تكفل كل دولة طرف، وفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة طوال الأسبوع لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ:

'1' توفير المشورة الفنية؛

'2' حفظ المعلومات استناداً للمواد ذات الصلة؛

'3' جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين؛

(ب) يجب أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة؛

(ج) إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءاً من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة؛

(د) على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه.

**سادساً- المساعدة التقنية والتدريب:**

1- المبادئ العامة للمساعدة التقنية:

(أ) تنظر الدول الأطراف في منح بعضها بعضا أكبر قدر من المساعدة التقنية، وخصوصا لصالح البلدان النامية من أجل دعم خططها وبرامجها الرامية إلى مكافحة الجرائم في مجال تكنولوجيا المعلومات والاتصالات، بما في ذلك الدعم المادي والتدريب في المجالات المشار إليها في هذه الاتفاقية، إضافة إلى التدريب والمساعدة ونقل التكنولوجيا والمعرفة وتبادل أفضل التجارب والخبرات المكتسبة ذات الصلة، مما ييسر التعاون الدولي بين الدول الأطراف فيما يتعلق بتسليم المجرمين والمساعدة القانونية المتبادلة؛

(ب) تعزز الدول الأطراف جهودها الرامية إلى زيادة فعالية الأنشطة التنفيذية والتدريبية إلى أقصى حد في المنظمات الدولية والإقليمية وفي إطار الاتفاقات أو الترتيبات الثنائية والمتعددة الأطراف ذات الصلة؛

(ج) تنظر الدول الأطراف في مساعدة بعضها بعضا، عند الطلب، لإجراء تقييمات ودراسات وبحوث بشأن أنواع الجرائم المرتكبة في مجال تكنولوجيا المعلومات والاتصالات في بلدانها والأسباب الكامنة وراءها والآثار الناجمة عنها، لكي تضع بمشاركة السلطات المختصة والفاعلين الرئيسيين استراتيجيات وخطط عمل لمكافحة هذه الأنواع من الجرائم؛

(د) تنظر الدول الأطراف في إنشاء آليات تمويل بهدف توفير المساعدة للجهود التي تبذلها البلدان النامية من خلال برامج ومشروعات المساعدة الفنية؛

(هـ) تنظر الدول الأطراف في تبادل المعلومات بشأن التطورات القانونية، السياسية أو التكنولوجية ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في شكل إلكتروني؛

2- التدريب وبناء القدرات:

(أ) تتولى كل دولة طرف، حسب الاقتضاء، وضع أو تنفيذ أو تحسين برامج تدريب خاصة لأعضاء السلطات المسؤولين عن منع الجرائم في مجال تكنولوجيا المعلومات والاتصالات ومكافحتها. ويمكن أن تشمل برامج التدريب هذه عدة مجالات، منها ما يلي:

'1' التدابير الفعالة لمنع الجرائم في مجال تكنولوجيا المعلومات والاتصالات والكشف عنها والتحقيق فيها والمعاقبة عليها ومكافحتها، بما في ذلك استخدام الوسائل الإلكترونية لجمع الأدلة وأساليب التحقيق؛

'2' منع تحويل عائدات الجرائم المحددة بموجب هذه الاتفاقية واسترداد تلك العائدات؛

'3' الكشف عن المعاملات المتصلة بتحويل عائدات الجرائم المحددة وفقا لهذه الاتفاقية واعتراضها؛ ومراقبة حركة عائدات الجرائم المحددة وفقا لهذه الاتفاقية والأساليب المستخدمة في تحويل تلك العائدات أو

إخفائها أو تمويهها؛

'4' إنشاء آليات وأساليب قانونية وإدارية ملائمة وذات كفاءة؛ تسهل ضبط والتحفظ ومصادرة واسترداد عائدات الجرائم المنشأة وفقا لهذه الاتفاقية؛

'5' الأساليب المستخدمة في حماية الضحايا والشهود والمبلغين الذين يتعاونون مع السلطات القضائية؛

'6' إعداد وتخطيط سياسة استراتيجية لمكافحة الجرائم في مجال تكنولوجيا المعلومات والاتصالات، كما ينبغي للبلدان أن تستثمر في بناء وتعزيز قدرات التحليل الجنائي الرقمي، بما في ذلك توفير التدريب والتأهيل الأمني، فضلاً عن نظم إدارة أمن المعلومات لدعم الملاحقات القضائية الناجحة في الجرائم السيبرانية عن طريق فحص الأجهزة الإلكترونية من أجل جمع الأدلة بطريقة موثوقة؛

'7' إعداد طلبات للمساعدة القانونية المتبادلة تستوفي الشروط التي تنص عليها هذه الاتفاقية؛

'8' التحقيق في الجريمة السيبرانية والتعامل مع الأدلة الإلكترونية وتسلسل العهدة والتحليل الجنائي؛

'9' توفير التدريب اللغوي والمهني بكافة الأنشطة المتعلقة بمكافحة استخدام تكنولوجيا المعلومات والاتصالات وحماية وسرعة التواصل مع الأجهزة المتخصصة لضبط وكشف الجرائم ذات الصلة؛

(ب) ينبغي للدول الأعضاء التي لديها قدرات وهياكل أساسية أكثر تقدما في مجال الجريمة السيبرانية أن تتحمل مسؤوليات تتناسب مع تلك القدرات عند تقديم المساعدة القانونية إلى الدول الأخرى وخاصة النامية وتقديم الدعم والمشورة ونقل المعرفة لهم في مجالات مكافحة الجريمة السيبرانية.

## الاتحاد الأوروبي والدول الأعضاء فيه

[الأصل: بالإنكليزية]
[2 تشرين الثاني/نوفمبر 2021]

تجسد هذه الوثيقة آراء ومواقف الاتحاد الأوروبي والدول الأعضاء فيه[1] بشأن ما يتعين مراعاته من نطاق وأهداف وهيكل (عناصر) عند وضع الاتفاقية الجديدة للأمم المتحدة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ومساهمة الاتحاد الأوروبي والدول الأعضاء فيه في الأعمال التحضيرية للدورة الأولى للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، التي أُنشئت لهذا الغرض عملا بقرار الجمعية العامة 247/74.

ولا تتعارض هذه المساهمة مع أي مواقف مستقبلية قد يتخذها الاتحاد الأوروبي والدول الأعضاء فيه خلال المفاوضات المقبلة بشأن نطاق أي اتفاقية مقبلة للأمم المتحدة وأهدافها وهيكلها.

### أولا- الأهداف

يشدد الاتحاد الأوروبي والدول الأعضاء فيه على أن الاتفاقية المقبلة للأمم المتحدة في هذا المجال ينبغي أن تكون أداة عملية تستخدمها سلطات إنفاذ القانون الجنائي والسلطات القضائية في مكافحة الجريمة السيبرانية على الصعيد العالمي، بغية إضافة قيمة إلى التعاون الدولي. وكذلك ينبغي لهذه الاتفاقية المقبلة أن تراعي على نحو كامل الإطار الحالي للصكوك الدولية والإقليمية المجربة والمختبرة في مجال الجريمة المنظمة

(1) إسبانيا، إستونيا، ألمانيا، أيرلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، بولندا، تشيكيا، الدنمارك، رومانيا، سلوفاكيا، سلوفينيا، السويد، فرنسا، فنلندا، قبرص، كرواتيا، لاتفيا، لكسمبرغ، ليتوانيا، مالطة، النمسا، هنغاريا، هولندا، اليونان.

والجريمة السيبرانية، على النحو المبين في قراري الجمعية العامة 247/74 و282/75. ومن ثمَّ، ينبغي للاتفاقية الجديدة أن تكمِّل الصكوك القائمة وأن تتجنب إعاقة تطبيقها أو انضمام المزيد من البلدان إليها بأي شكل من الأشكال، وأن تتجنب الازدواجية قدر الإمكان.

وينبغي للاتفاقية المقبلة أن تنص على حماية حقوق الإنسان والحريات الأساسية، التي تنطبق على الإنترنت وخارجها، وأن تكون متوافقة مع الصكوك المعنية في هذا المجال.

وكذلك ينبغي لهذه الاتفاقية المقبلة، عملا بما اتفقت عليه الجمعية العامة في قرارها 282/75، أن تراعي مراعاة كاملة ما قام به فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية من أعمال[2] وما توصل إليه من نتائج.[3]

## ثانيا- النطاق

يرى الاتحاد الأوروبي والدول الأعضاء فيه أن تحقيق هذه الغاية يستلزم أن تركز الاتفاقية المقبلة للأمم المتحدة في المقام الأول على القانون الجنائي الموضوعي وقانون الإجراءات الجنائية وكذلك آليات التعاون ذات الصلة. وينبغي أيضا أن تكون ممتثلة للمعايير الدولية لحقوق الإنسان، وأن تسعى إلى مكافحة الجريمة السيبرانية بالطريقة الأكثر فعالية، بما من شأنه أن يوفر الحماية للضحايا.

ويرى الاتحاد الأوروبي والدول الأعضاء فيه أن هذا الصك الجديد ينبغي أن يعرِّف بدقة المصطلحات المستخدمة فيه، وأن يعطي الأفضلية للمفاهيم المتفق عليها بالفعل في النصوص الدولية القائمة.

ويوصي الاتحاد الأوروبي والدول الأعضاء فيه بأن يكون مضمون هذه الاتفاقية موجزا، وأن يركز على العناصر الأساسية للعدالة الجنائية، ومن ثمَّ ينبغي أن يستبعد قدر الإمكان أي عناصر فرعية.

وبالاستناد إلى المبادئ المبينة أعلاه، يرى الاتحاد الأوروبي والدول الأعضاء فيه أنه ينبغي إدراج العناصر التالية في الاتفاقية المقبلة للأمم المتحدة:

### 1- أحكام القانون الجنائي الموضوعية المرتبطة بالجرائم السيبرانية التي يجب أن تجرِّمها جميع الدول الأطراف في الاتفاقية المقبلة. وبوجه عام، ينبغي أن تقتصر هذه الأحكام على جرائم التكنولوجيا العالية والجرائم التي تُرتكَب بواسطة الفضاء السيبراني، مثل الوصول إلى البيانات والنظم الحاسوبية أو اعتراضها أو التدخل فيها بصورة غير قانونية.[4]

ويجب أن تكون أحكام القانون الجنائي الموضوعية محددة بوضوح ودقَّة ومتوافقة توافقا تاما مع المعايير الدولية لحقوق الإنسان ومتطلبات الحفاظ على الطابع العالمي والمفتوح والحر والمستقر والآمن الذي يتسم به الفضاء السيبراني. ومن شأن الأحكام الغامضة التي تجرِّم أنواعا من السلوك ليست محددة بوضوح في الاتفاقية المقبلة للأمم المتحدة أو في الصكوك القانونية العالمية الأخرى أن تؤدي إلى إعاقة إعمال حقوق الإنسان والحريات الأساسية، بما في ذلك الحق في حرية الكلام والتعبير، بلا مبرر وعلى نحو غير متناسب، وأن تفضي أيضا إلى عدم اليقين القانوني.

---

(2) انظر www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.

(3) انظر UNODC/CCPCJ/EG.4/2021/2.

(4) يتماشى ذلك مع التوصية 5 بشأن التجريم، التي اعتمدها فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية في اجتماعه المعقود في فيينا في الفترة من 6 إلى 8 نيسان/أبريل 2021 (انظر UNODC/CCPCJ/EG.4/2021/2، المرفق، التوصية 5).

وينبغي أن تُصـــاغ أحكام القانون الجنائي الموضـــوعية، بالقدر الممكن، بلغة محايدة تكنولوجيا لكي تشـمل التطورات التقنية في المسـتقبل.[5] وفي الوقت نفسـه، ينبغي تشـجيع تبادل الآراء والمعلومات بشـأن التحديات الجديدة التي تفرضها التطورات التقنية اللاحقة.

ويجب تجنُّب عدم التوافق مع الاتفاقيات الدولية الأخرى، وبخاصة في حالة جرائم معينة، مثل الاتجار بالأسلحة أو توزيع العقاقير المخدرة على نحو غير مشروع، تتناولها بالفعل على نحو مستفيض أحكامٌ قائمة في الاتفاقيات الدولية، لدرجة تجعل إدراج هذه الأنواع من السـلوك في اتفاقية بشـأن الجريمة السـيبرانية أمرا لا يضيف أي قيمة.

وبوجه عام، ينبغي ألا تضـــع الاتفاقية المقبلة للأمم المتحدة معايير (دنيا) للجزاءات أو العقوبات المفروضـــة على جرائم محددة على بما يتجاوز النماذج القائمة، ومنها مثلا الفقرة 1 من المادة 11 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

وفيما يتعلق بقواعد الاختصاص القضائي، ينبغي أن تُصاغ الاتفاقية المقبلة للأمم المتحدة على غرار النهج المبيَّن في الصكوك القانونية القائمة، كما هو الحال في المادة 15 من اتفاقية الجريمة المنظمة.

2- **الشروط والضمانات الموضوعية والإجرائية المناسبة** لضمان التوافق مع حقوق الإنسان والحريات الأساسية، بما في ذلك مبادئ الشرعية والضرورة والتناسب في إجراءات إنفاذ القانون، والضمانات الموضـــوعية والإجرائية المحددة التي تكفل على وجه الخصـــوص الحق في الخصـــوصـــية وحماية البيانات الشخصية، والحق في حرية التعبير والمعلومات، والحق في محاكمة عادلة. وينبغي أن تستند هذه الضمانات إلى نظيراتها المدرجة في الصكوك القانونية الدولية المعنية الأخرى، وأن تكون على الأقل في نفس المستوى.

3- **التدابير الإجرائية وأحكام الإجراءات الجنائية المتعلقة بآليات التعاون بين الأطراف في الاتفاقية المقبلة للأمم المتحدة**، بما يشـمل التعاون في عمليات التحقيق وسـائر الإجراءات القضـائية، وفي الحصول على الأدلة الإلكترونية، حيثما يكون ذلك مناسبا وملائما، مع ضمان إمكانية جمعها وحفظها والتوثق من صـحتها واسـتخدامها في الإجراءات الجنائية. وينبغي أن تكون هذه التدابير[6] والأحكام متسـقة مع النماذج التي توفرها سائر الصكوك القانونية الدولية المعنية، وأن تستند إليها، وأن تُكمَّل بضمانات مناسبة، بما في ذلك التعاون في حالات الطوارئ.

4- العناصـر المتوافقة مع حقوق الإنسـان والمتعلقة **ببناء القدرات، وتبادل الممارسـات الفضـلى والدروس المسـتفادة، وتقديم المسـاعدة التقنية**، بما في ذلك الدور الهام لمكتب الأمم المتحدة المعني بالمخدرات والجريمة في هذه المجالات.

ويرى الاتحاد الأوروبي والدول الأعضـاء فيه أنه يجب اسـتبعاد ما يلي من نطاق الاتفاقية المقبلة للأمم المتحدة:

- المسائل المتعلقة بالأمن القومي أو سلوك الدول أو تنظيمهما
- المسـائل المتعلقة بإدارة الإنترنت أو تنظيم قواعد إدارتها، التي يجري تناولها بالفعل في إطار سـياسـات ومنتديات مخصَّصة لأصحاب المصلحة المتعددين

(5) انظر UNODC/CCPCJ/EG.4/2021/2، المرفق، التوصية 1 بشأن التشريعات والأطر.

(6) المرجع نفسه، التوصية 16 بشأن الأدلة الإلكترونية والعدالة الجنائية.

وأخيرا، ينبغي للاتفاقية المقبلة، بوصفها صكا حكوميا دوليا، ألا تفرض التزامات مباشرة على الكيانات غير الحكومية، بما في ذلك كيانات القطاع الخاص مثل مقدمي خدمات الإنترنت.

**ثالثا- الهيكل**

استنادا إلى ما سبق، يمكن أن تشمل الاتفاقية المقبلة للأمم المتحدة الفصول المختلفة التالية:

الديباجة (نطاق الاتفاقية المقبلة للأمم المتحدة وأهدافها)

أولا- أنواع الجرائم وتعاريفها الدقيقة

ثانيا- القواعد الإجرائية المحلية والمبادئ الأساسية التي ينبغي التقيد بها في هذا الشأن، ومنها مثلا احترام حقوق الإنسان، بما في ذلك الحق في الخصوصية وحماية البيانات الشخصية، ومبدأي الضرورة والتناسب

ثالثا- التعاون الدولي

رابعا- المساعدة التقنية، والتدريب وبناء القدرات، ودور مكتب الأمم المتحدة المعني بالمخدرات والجريمة في هذا الشأن

## إندونيسيا

[الأصل: بالإنكليزية]
[28 تشرين الأول/أكتوبر 2021]

**المعلومات الأساسية العامة والأهداف**

تسلم إندونيسيا، بوصفها واحدة من أكبر مستخدمي الإنترنت في العالم، بأهمية تكنولوجيا المعلومات والاتصالات للمجتمع. غير أن أوجه التقدم في تكنولوجيا المعلومات والاتصالات قد استُغلَّت في سلوكيات غير مسؤولة، وأبرزها الجريمة السيبرانية والإرهاب السيبراني، مما يقوض استخدام تكنولوجيا المعلومات والاتصالات لأغراض التنمية السياسية والاقتصادية والاجتماعية.

وقد أثرت الجريمة السيبرانية، مثلها مثل الجرائم عبر الوطنية الأخرى، على المجتمع الدولي نظرا للطابع الفريد العابر للحدود الذي تتسم به التكنولوجيا والفضاء السيبراني. ولذلك فإن التعاون الدولي في هذا الشأن أمر ذو أهمية حاسمة. وتشيد إندونيسيا باعتماد قرار الجمعية العامة 247/74 الذي قررت فيه الجمعية إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

وتعتقد إندونيسيا أن مناقشة اتفاقية محددة بشأن الجريمة السيبرانية في إطار اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية أمرٌ حاسم الأهمية وملائم تماما من حيث التوقيت، وتأمل أن تستفيد الدول من هذا الزخم من أجل مناقشة صك دولي قادر على التصدي للتحديات المتعلقة بالجريمة السيبرانية والتفاوض بشأنه بطريقة شفافة وشاملة للجميع.

وقد أُحرز تقدم كبير على مدى العقد الماضي في مناقشة وإعداد صكوك دولية تهدف إلى استبانة أنجع الطرائق لمنع الجريمة السيبرانية. ونتيجة لذلك، ينبغي للدول لدى النظر في صك مقبل بشأن الجريمة السيبرانية أن تأخذ في الحسبان جميع المنابر والأطر القائمة، بما في ذلك ما قام به فريق الخبراء الحكومي

الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية من أعمال، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

وفي المقام الأول، ينبغي أن تهدف المناقشة بشأن اتفاقية مكافحة الجريمة السيبرانية إلى تعزيز التعاون الدولي وتشجيعه بغية دعم الجهود الوطنية والإقليمية والدولية لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما في ذلك عن طريق تقديم المساعدة التقنية من أجل تحسين التشريعات والأطر الوطنية للدول الأعضاء، وبناء قدرات سلطاتها الوطنية على التصدي لهذه الجرائم.

وبالإضافة إلى ذلك، ينبغي أن تنص الاتفاقية على تدابير مناسبة وفعالة تُتَّخذ فيما بين الدول وكذلك بالتعاون مع المنظمات الدولية والإقليمية المعنية، حسب الاقتضاء.

**المبادئ**

كما هو الحال في العديد من الاتفاقيات الدولية، ينبغي أن يجسد نظرنا في هذه الاتفاقية التزامات الدول الأعضاء، وفقا لمبدأي تساوي الدول في السيادة وسلامة أراضي الدول، وكذلك مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى. وبالإضافة إلى ذلك، ينبغي للدول أن تحترم الحقوق السيادية للدول الأخرى عند وضع السياسات والتشريعات المتصلة بمكافحة الجريمة الحاسوبية، وفقا لظروفها واحتياجاتها الوطنية.

ويجب أن يتضمن هذا الصك المقبل اعترافا بما لاستخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية من أثر على الأمن وتبعات اجتماعية واقتصادية وإنسانية. وفي الوقت نفسه، يجب أن تكفل الاتفاقية تركيز تدابير مكافحة الجريمة السيبرانية على السلوك الإجرامي، وكفالة ألا تؤدي إلى عرقلة تطوير تكنولوجيات المعلومات والاتصالات، بما في ذلك أنشطة البحث والتطوير ونقل التكنولوجيا.

ومن مصلحة الجميع، وكذلك من الأمور الحاسمة الأهمية للصالح العام، تشجيع استخدام تكنولوجيات المعلومات والاتصالات للأغراض السلمية. ويظل احترام السيادة وحقوق الإنسان والحريات الأساسية، وكذلك تحقيق التنمية المستدامة والرقمية، من الأمور المحورية في هذه الجهود.

وتدرك إندونيسيا أيضا المزية التي يحققها ضمان وضع إجراءات جنائية وتنفيذها وتطبيقها وفقا للقانون الداخلي لكل دولة، وتسلِّم أيضا بالحاجة إلى معالجة التحديات التي تطرحها أوجه الاختلاف في الإجراءات الجنائية المعمول بها في الدول، وكذلك التزامات كل دولة بموجب الصكوك الدولية المعنية، مثل اتفاقية الجريمة المنظمة، والمعاهدات الدولية لحقوق الإنسان، وحقوق الملكية الفكرية، والترتيبات الثنائية لتسليم المطلوبين وتقديم المساعدة القانونية المتبادلة.

وبالإضافة إلى ذلك، يجب على الدول الأعضاء أن تشدد على ضرورة أن تكون هذه العملية مفتوحة وشفافة وشاملة لأصحاب المصلحة المتعددين، وأن تتيح لجميع الدول الأعضاء فرصة التفاوض بحسن نية من أجل التوصل إلى حلول مستنيرة وواقعية وقائمة على توافق الآراء.

**النطاق**

يجب أن يكون نطاق الاتفاقية قادرا على التصدي للتحديات الحالية والمستقبلية التي يطرحها استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وحماية مستخدمي تلك التكنولوجيات، والتخفيف من الأضرار التي تلحق بالناس والبيانات والنظم والخدمات والبنى التحتية ومنعها.

وينبغي أيضا أن تكون الاتفاقية قادرة على ضمان تمكين الدول الأعضاء من اعتماد تدابير تشريعية وغيرها من التدابير التي قد تكون ضرورية لتجريم الاضطلاع بأنشطة تحظرها الاتفاقية، وخصوصا الجرائم الحاسوبية والجرائم المتصلة بالحواسيب وكذلك الأنشطة غير المشروعة الأخرى.

وتعتقد إندونيسيا أن الاتفاقية المقبلة ينبغي أن تشمل مجموعة كاملة من الجرائم السيبرانية الأساسية. وتشمل هذه الجرائم، على سبيل المثال لا الحصر، ما يلي:

(أ) الدخول إلى النظم الحاسوبية بصورة غير قانونية أو باستخدام القرصنة الحاسوبية؛

(ب) اعتراض البيانات الحاسوبية وبيانات النظم بصورة غير قانونية؛

(ج) الاحتيال؛

(د) إساءة استخدام البيانات والنظم الحاسوبية للأغراض الإجرامية؛

(هـ) انتهاك حقوق التأليف والنشر والحقوق ذات الصلة؛

(و) التلاعب في البيانات والنظم الحاسوبية؛

(ز) توزيع ونقل أشكال المحتوى والمواد غير المشروعة، مثل المواد الإباحية، والمواد الإباحية التي تصور الأطفال، والمعلومات المضللة، ونظريات المؤامرة، والخدع، والمواد التي تنشر مشاعر الكراهية القائمة على أسس عنصرية أو قومية أو دينية أو سياسية.

وينبغي للدول الأعضاء أن تنظر في اعتماد التدابير اللازمة لتنفيذ الإجراءات الجنائية المبينة في الاتفاقية، بما في ذلك، على سبيل المثال لا الحصر، ما يلي:

(أ) حفظ البيانات والنظم، وحفظ بيانات حركة المرور التي يخزنها مقدم خدمات واحد أو عدة مقدمي خدمات، مع ملاحظة أن المهلة الزمنية لحفظ البيانات وتصنيف البيانات المخزَّنة في البلدان التي يعملون فيها تُحدَّد وفقا للقوانين الوطنية والمحلية؛

(ب) تقديم البيانات الحاسوبية المخزَّنة أو نقلها من جانب الأفراد أو الكيانات القانونية، ووضع التدابير الكافية لإلزام مقدمي خدمات النظم عبر الإنترنت بتقديم البيانات الحاسوبية المخزَّنة أو نقلها، بما في ذلك البيانات المتعلقة بنوع الخدمات المقدَّمة؛

(ج) البحث عن البيانات والنظم الحاسوبية ومصادرتها، وإنشاء نسخ من البيانات الحاسوبية وحفظها، وتعديل البيانات المخزَّنة ونقلها؛

(د) جمع البيانات الآنية بشأن حركة المرور وتسجيلها، وكذلك الحصول على بيانات حركة المرور من مقدمي الخدمات و/أو مقدمي خدمات النظم عبر الإنترنت.

وإضافة إلى ذلك، ينبغي للدول الأعضاء أن تكفل إجراء التحقيقات في الجرائم السيبرانية وفقا لمبادئ حماية الخصوصية والسرية، ومتطلبات استدامة الخدمات العامة والحفاظ على استمراريتها وإعلاء المصلحة العامة، فضلا عن تكامل البيانات.

**التعاون**

ينبغي التحقيق بفعالية في الجرائم السيبرانية والجرائم التي ييسرها استخدام تكنولوجيات المعلومات والاتصالات، على الصعيدين الوطني وعبر الوطني على السواء. ولذلك ينبغي أن يكون هذا الصك بمثابة آلية فعالة للتعاون الدولي على مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

وينبغي تنفيذ هذا التعاون على أساس المنفعة المتبادلة والمعاملة بالمثل وفقا للتشريعات الوطنية، مع مراعاة الصكوك القائمة والآليات والأطر الدائمة.

ونظرا لأهمية نهج العمل المشترك بين أصحاب المصلحة المتعددين في كشف الجريمة السيبرانية ومنعها والقضاء عليها، ينبغي أن تركز المناقشة أيضا على تعزيز التعاون الوثيق مع الكيانات المعنية بالجريمة السيبرانية، بما في ذلك التعاون بين سلطات إنفاذ القانون ومقدمي خدمات تكنولوجيات المعلومات والاتصالات. وفي هذا السياق، يكتسي التعاون مع المؤسسات الخاصة، الذي تعززه الشراكات بين القطاعين العام والخاص متى أمكن ذلك، أهمية حاسمة لتحسين الإلمام بالجريمة السيبرانية وتعزيز فعالية تدابير التصدي لها. وينبغي أيضا للدول الأعضاء أن تستثمر في التوعية بالجريمة السيبرانية في القطاعين العام والخاص.

وكذلك ينبغي أن تسلط مداولاتنا الضوء على التدابير التي تسمح للسلطات بإجراء تحقيقات تُجمع فيها البيانات وتُصادَر من خلال آليات المساعدة القانونية المتبادلة، ولعل الدول الأعضاء تود النظر في استخدام أطرها القانونية القائمة في هذا الغرض.

وفيما يتعلق بالمساعدة القانونية المتبادلة، ينبغي أن نراعي في مداولاتنا، إلى أقصى حد ممكن، القوانين والمعاهدات والاتفاقات ذات الصلة المتعلقة بالتحقيقات وعمليات الملاحقة القضائية والإجراءات القضائية. وتُشجَّع الدول الأعضاء، في جملة أمور، على مناقشة الترتيبات اللازمة للتعجيل بجمع الأدلة الإلكترونية أو المتعلقة بآليات تبادل المعلومات بين السلطات المعنية.

ويجب أن توفر الأحكام الواردة في الاتفاقية بشأن التعاون الدولي إطارا قانونيا أساسيا للتصدي للتحديات الإجرائية وسد الثغرات ومعالجة عدم كفاية آليات التعاون الدولي، وخصوصا فيما يتعلق بالتحقيقات وتبادل المعلومات وجمع البيانات والأدلة الإلكترونية وعمليات الملاحقة القضائية، وكذلك تيسير تسليم المطلوبين فيما بين الدول. وتُشجَّع الدول الأعضاء أيضا على تعيين جهات اتصال أو سلطات مختصة للتعجيل بتنفيذ أحكام الاتفاقية بشأن التعاون الدولي.

وبالإضافة إلى ذلك، لعل الدول الأعضاء تود النظر في تعزيز قدرتها الوطنية على كشف حالات استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية والتحقيق في تلك الحالات والتصدي لها، وذلك من خلال جهود بناء القدرات والمساعدة التقنية التي تسهم في زيادة قدرة الدول الأعضاء على الصمود. وينبغي أن تستند تدابير بناء القدرات المذكورة إلى الثقة المتبادلة، وأن تكون مدفوعة بمستوى طلب متوافق مع الاحتياجات المحددة وطنيا، في ظل الاعتراف الكامل بالملكية الوطنية.

وبالنظر إلى أن التعاون على منع الجريمة السيبرانية والقضاء عليها يظل أولوية في مناقشاتنا، ينبغي أن يتضمن الصك المقبل، على أقل تقدير، قائمة بالأنشطة الرامية إلى تحسين التعاون من خلال اتخاذ التدابير التالية:

(أ) تبادل المعلومات بشأن التهديدات التي تطرحها الجريمة السيبرانية؛

(ب) تشجيع التعاون والتنسيق المعزَّزين بين أجهزة إنفاذ القانون والمدعين العامين والسلطات القضائية؛

(ج) تبادل أفضل الممارسات والخبرات المتصلة بالتحقيق في الجرائم السيبرانية عبر الحدود؛

(د) العمل مع مقدمي الخدمات من خلال الشراكات بين القطاعين العام والخاص من أجل تحديد طرائق التعاون في مجال إنفاذ القانون والتحقيق في الجرائم السيبرانية وجمع الأدلة عليها؛

(هـ) وضع مبادئ توجيهية لمقدمي الخدمات لمساعدة أجهزة إنفاذ القانون في التحقيقات في الجرائم السيبرانية، بما في ذلك فيما يتعلق بصيغة الأدلة والمعلومات الرقمية ومدة حفظها؛

(و) تنمية المهارات والموارد البشرية من خلال سياسات تكفل تمكين الدول الأعضاء من زيادة قدرتها على التكيف مع التكنولوجيات الرقمية؛

(ز) تعزيز القدرات التقنية والقانونية لأجهزة إنفاذ القانون والقضاة والمدعين العامين من خلال برامج بناء القدرات وتنمية المهارات.

ومن خلال هذه الآلية، ينبغي أيضا للدول الأعضاء أن تواصل تحسين فعالية التنسيق وأوجه التآزر فيما بين الوكالات، بأساليب منها تبادل المعلومات والعمل مع المنظمات الإقليمية والقطاع الخاص وفرق التصدي للطوارئ الحاسوبية وفرق التصدي لحوادث الأمن الحاسوبي ومنظمات المجتمع المدني وسائر أصحاب المصلحة، بغية تيسير التعاون الدولي الفعال.

وينبغي أن تشمل المناقشة أيضا آلية لاستعراض تطبيق أو تنفيذ جميع الالتزامات والتعهدات الواقعة بموجب الصك المقبل.

## جامايكا

[الأصل: بالإنكليزية]
[29 تشرين الأول/أكتوبر 2021]

عملا بطلب اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية بأن تقدم الدول تعليقاتها بشأن نطاق اتفاقية دولية لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية وأهداف تلك الاتفاقية وهيكلها، تُقدم جامايكا الآراء الواردة أدناه.

وتتطلع جامايكا إلى التعاون مع الدول الأعضاء الأخرى من أجل الإسهام في الأعمال المضطلع بها لصياغة اتفاقية بشأن الجريمة السيبرانية. وتتوقع أن تخدم هذه الاتفاقية المجتمع العالمي من خلال السعي إلى حماية المواطنين من التهديدات السيبرانية وغيرها من الهجمات الإجرامية، وأن تحظى بالقبول والتصديق على نطاق عالمي. وترحب جامايكا بمشاركة خبراء المجتمع المدني في هذا المجال بغية إثراء المداولات.

وترى جامايكا أن صياغة اتفاقية لمكافحة الاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات تشكل خطوة هامة في التصدي العالمي للمشاكل التي تواجهها الدول بسبب هذا التهديد. وقد حُدِّد هدف هذه الاتفاقية باقتدار في التقرير الصادر بتوافق الآراء عن فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي لعام 2015، الذي ينص، في الفقرة الفرعية (د) من الفقرة 13 منه، على أنه ينبغي للدول أن تنظر في أفضل سبل التعاون على تبادل المعلومات، ومساعدة بعضها البعض، ومحاكمة المسؤولين عن الاستخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، وتنفيذ تدابير تعاونية أخرى للتصدي لهذه التهديدات.[7]

وينبغي أن يكون الهدف العام لهذه الاتفاقية هو التعاون من أجل تبادل المعلومات لمساعدة الدول في مكافحة الاستخدام الإجرامي لتكنولوجيا المعلومات والاتصالات وملاحقة المسؤولين عنه قضائيا. وينبثق عن ذلك الهدف العام هدف آخر يتمثل في زيادة التفاهم بين الدول فيما يتعلق بوجهات النظر المتباينة بشأن الجريمة السيبرانية. ويؤمل أن يؤدي ذلك إلى مواءمة النهج المتبعة ووضع إطار دولي يعود بالفائدة على الجميع. غير أن نجاح هذا الهدف يتوقف على أن تراعي هذه العملية مواقف جميع الدول، بما فيها الدول الجزرية الصغيرة النامية، بطريقة متوازنة وعادلة وشفافة وشاملة.

(7) A/70/174.

وينبغي أن تؤخذ في الاعتبار العمليات الأخرى التي يمكن أن تسهم في إحراز تقدم نحو إبرام الاتفاقية، دون أن تؤخره بلا مبرر. وكذلك ينبغي التقيد بالأطر الزمنية المتفق عليها للتفاوض على مشروع الاتفاقية وإتمامه، كدليل على مدى جديتنا في مكافحة الجريمة السيبرانية.

ومن المفهوم أن تعريف المصطلحات هو نقطة بدء المفاوضات. فالمصطلحات هي ما يحدد نطاق الاتفاقية، وهي مهمة أيضا لتحقيق الأهداف المشتركة للمشاركين. ولذلك ينبغي أن تكون التعاريف واضحة ومحدَّدة، وأن تُصاغ بعناية لضمان ألا تكون تقييدية أو واسعة النطاق بصورة غير مبرَّرة، بل مناسبة لسياق الاتفاقية وأغراضها.

وبالنظر إلى أن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية هي ولاية واسعة النطاق، فإن تعاريف الجرائم من ثم يجب أن تكون "متجاوبة مع التطورات المقبلة". وينبغي أن تُصاغ هذه التعاريف على نحو لا يحصر معناها في نطاق التكنولوجيات القائمة، بل ينبغي كفالة إمكانية تفسيرها على نحو يواكب التكنولوجيات المستقبلية وما تتسم به بيئة تكنولوجيا المعلومات والاتصالات من طابع دائب التغيُّر.

وينبغي أن تبرز الاتفاقية تعاريف الجرائم التي تعزز مجموعات الأدوات المتاحة للبلدان في إطار مساعيها لاستهداف الجريمة السيبرانية، ولا تنتهك حقوق الأشخاص وحرياتهم الأساسية بل تسعى إلى تعزيز إعمال هذه الحقوق واحترامها. ولذلك ينبغي أن تؤخذ المعاهدات الدولية المتعلقة بحقوق الإنسان في الاعتبار.

وكذلك يتعين أن تولي أحكام الاتفاقية الجديدة الاعتبار الواجب لمبدأ سيادة الدول وكذلك المبادئ الأخرى المبينة في ميثاق الأمم المتحدة والقانون الدولي بشأن المسائل المتصلة بالإجراءات الجنائية والإنفاذ والتعاون الدولي.

وترى جامايكا أن التعاون الدولي يجب أن يُعالج على نحو واف في الاتفاقية، بالنظر إلى أن من شأن ذلك أن يشجع زيادة التعاون في مجال مكافحة الجريمة السيبرانية على الصعيد العالمي. وحيثما لا توجد معاهدة للمساعدة القانونية المتبادلة بين الدول، ينبغي للاتفاقية أن تقدم الإرشاد للدول بشأن عملية تقديم طلبات المساعدة القانونية المتبادلة والرد عليها، بما يشمل مسائل مثل المسؤولية عن التكاليف.

ويجب أن تتضمن الاتفاقية اعترافا بتباين قدرات الدول، وهو ما يؤثر بدوره في قدراتها على التعاون بالقدر اللازم لتحقيق أفضل النتائج. ولذلك، من الأهمية بمكان أن تُقدَّم المساعدة التقنية من أجل بناء قدرات الدول على المساهمة بقدر أكبر في الإطار العالمي لمكافحة الجريمة السيبرانية. وفي هذا الصدد، ينبغي أن تكون جهود بناء القدرات مستدامة، وأن يكون لها هدف واضح، وأن تلبي الاحتياجات المحلية، وأن تحقق أهداف تنمية الموارد البشرية في هذا المجال المتخصص. وكذلك ينبغي النظر في إنشاء آلية تمويل لدعم جهود بناء القدرات من أجل تنفيذ اتفاقية الجريمة السيبرانية.

## اليابان

[الأصل: بالإنكليزية]
[29 تشرين الأول/أكتوبر 2021]

يسر اليابان، بوصفها دولة عضوا تعلق أهمية على تحقيق عملية شاملة وشفافة وعادلة لصياغة الاتفاقية المقبلة للأمم المتحدة بشأن الجريمة الحاسوبية، أن تقدم مدخلاتها في الاتفاقية الجديدة قبل بدء عملية الصياغة الرسمية، وتعرب عن تقديرها لمبادرة الرئيسة بإتاحة هذه الفرصة.

وعلى الرغم من أن الجريمة السيبرانية تطرح تحديات متنوعة تواجهها دول مختلفة، فإن اليابان تدرك أن الجريمة السيبرانية تتسم بطابع دائب التغيُّر وتشكل تهديدا خطيرا ومشتركا لجميع الدول الأعضاء. ومن أجل مكافحة الجريمة السيبرانية، التي تتجاوز الحدود الوطنية بسهولة، من الضروري ضمان أن تتعاون جميع الدول الأعضاء فيما

بينها. ولذلك فإن اليابان تعتقد أنه ينبغي لنا أن نسعى إلى كفالة الحفاظ على الطابع الحر والعادل والآمن الذي يتسم به الفضاء السيبراني وتعزيز قدرتنا على منع الجريمة السيبرانية ومكافحتها في جميع أنحاء العالم، وذلك من خلال جعل مضمون الاتفاقية الدولية الجديدة عالمي النطاق ومقبولا لجميع الدول الأعضاء.

وتبين هذه المدخلات آراء اليابان بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها، والغرض منها تعزيز النقاش داخل اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، التي أُنشئت عملا بقرار الجمعية العامة 247/74.

**النطاق**

من أجل تعزيز التدابير العالمية لمكافحة الجريمة السيبرانية وإرساء إطار دولي عالمي، ينبغي للمجتمع الدولي، في المقام الأول، أن يضع إطارا متينا يركز على الأحكام الأساسية والضرورية بشأن الجرائم الجنائية والإجراءات الجنائية، وكذلك المساعدة القانونية المتبادلة وغير ذلك من أشكال التعاون الدولي في هذا المجال.

وينبغي أن تقتصر الاتفاقية الجديدة على تجريم الأفعال التي تدخل في نطاق الجريمة السيبرانية؛ وينبغي أن تشمل الأفعال المجرَّمة وفقا للاتفاقية الجديدة الجرائم التي تُرتكب بواسطة الفضاء السيبراني، وألا تتناول الجرائم التي تُيسَّر بواسطة الفضاء السيبراني إلا عند الضرورة وبالاستناد إلى توافق واسع في الآراء بهذا الشأن.

وينبغي أن تستند الاتفاقية الجديدة استنادا راسخا إلى المناقشات السابقة والحالية التي أجريت ضمن الأطر القائمة لمكافحة الجريمة السيبرانية، مع مراعاة أي مناقشات وأعمال جارية في محافل أخرى بشأن الجريمة السيبرانية، بغية تجنُّب ازدواجية الجهود أو تقويض العمل.

وبغية وضع إطار دولي عالمي ينطبق بوجه عام على جميع أشكال استخدام تكنولوجيات المعلومات والاتصالات، بصرف النظر عن الاختلافات بين الدول، ومواكبة التطورات التقنية في المستقبل، ينبغي أن تُصاغ الأحكام المدرجة في الاتفاقية الجديدة بلغة محايدة تكنولوجيا.

ورغم ما تكتسيه مكافحة الجريمة السيبرانية من أهمية، يجب ألا تؤدي التدابير المتخذة لمكافحتها إلى الإضرار بمبدأ مراعاة الأصول القانونية أو فرض قيود لا مبرر لها على حقوق الإنسان. وتمثل هذه الضمانات شروطا مسبقة لنجاح التعاون الدولي، ولذلك ينبغي أن تتضمن الاتفاقية الجديدة أحكاما محددة لضمان مراعاة الأصول القانونية واحترام حقوق الإنسان.

**الهدف**

ينبغي أن يكون الهدف الرئيسي للاتفاقية الجديدة هو الإسهام في أمان وأمن جميع من تلزم حمايتهم من المشاركين في مجال تكنولوجيات المعلومات والاتصالات، وكذلك حماية مصالحهم. ويمكن تحقيق ذلك من خلال تعزيز التدابير المتخذة على الصعيد العالمي لمكافحة الجريمة السيبرانية، وذلك بإرساء إطار دولي عالمي ينطبق بأوسع نطاق ممكن على الجريمة السيبرانية بمختلف أشكالها عبر الوطنية ويدعم التعاون الفعال على المستوى الثنائي أو المتعدد الأطراف في عمليات التحقيق والملاحقة القضائية.

ومن أجل تحقيق هذا الهدف، ينبغي أن تنص الاتفاقية الجديدة على أحكام أساسية وضرورية يمكن أن يمتثل لها وينفذها أكبر عدد ممكن من الدول الأعضاء، وهو ما من شأنه أن ينهض بمستوى التدابير المتخذة على الصعيد العالمي لمكافحة الجريمة السيبرانية، وأن يعزز الأطر القائمة.

**الهيكل**

تعتقد اليابان أن الهيكل الأســاســي التالي ســيكون فعالا في تنظيم الاتفاقية الجديدة، ولكنها تؤيد في الوقت نفسه التحلي بالمرونة عند وضع هيكل أكثر تفصيلا في المفاوضات المقبلة:

(أ) تعريف المصطلحات؛

(ب) قائمة بالتدابير المحلية التي ينبغي للدول الأعضاء أن تعتمدها:

'1' تجريم ما يلي:

'أ' الأفعال الإجرامية المصنفة على أنها جرائم تُرتكَب بواسطة الفضاء السيبراني؛

'ب' الأفعال الإجرامية التي ينبغي تجريمها بوصــفها من الجرائم التي تُيسَّــر بواســطة الفضاء السيبراني؛

'2' الأحكام الإجرائية المتعلقة بحفظ البيانات والكشف عنها وإعدادها؛

'3' الضمانات اللازمة لكفالة حقوق الإنسان والمصالح الأخرى؛

(ج) التعاون الدولي في مجال تسليم المطلوبين والمساعدة المتبادلة وغير ذلك من أشكال التعاون؛

(د) الأحكام الختامية.

## الأردن

[الأصل: بالعربية]
[28 تشرين الأول/أكتوبر 2021]

**نطاق الاتفاقية:**

الجرائم المتعلقة بسرية وبسلامة وتوافر البيانات والخدمات الإلكترونية.

- الجرائم المتعلقة بالدخول غير المصرح إلى الشبكة المعلوماتية أو نظام معلومات أو أي جزء منهما.
- الجرائم المتعلقة بتعطيل البنى التحتية الحرجة.
- الجرائم المتعلقة بقصد تخريب شبكة المعلومات أو نظام معلومات.
- الجرائم المتعلقة بالتجسس على سير البيانات على شبكة المعلومات أو نظام معلومات.
- الجرائم المتعلقة بالاحتيال والتزوير وانتحال الشخصية.
- الجرائم المتعلقة باعتراض بيانات أو معلومات الأنظمة المالية.
- الجرائم المتعلقة بانتهاك الخصوصية والملكية الفكرية.
- الجرائم المتعلقة بأجهزة وبرامج فك التشفير ورموز الدخول.
- الجرائم المتعلقة بالتحايل على عناوين الإنترنت.
- الجرائم المتعلقة بالمواد الإباحية.
- الجرائم المتعلقة باستغلال الأطفال والإساءة لهم.

- الجرائم المتعلقة بنشر الأخبار الكاذبة.
- الجرائم المتعلقة بالتمييز العنصري.
- الجرائم المتعلقة باستغلال المرأة والإساءة لها.
- الجرائم المتعلقة بإثارة الفتنة أو التحريض أو نشر خطاب الكراهية.
- الجرائم المتعلقة بالإتجار المخالف للقوانين من خلال الشبكة المعلوماتية أو الموقع الإلكتروني.
- الجرائم المتعلقة بنشر الفكر الإرهابي أو دعمه أو الترويج له.
- الجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات للأغراض الإرهابية.
- الجرائم المتعلقة بالإساءة للأديان والدول والرموز.
- الجرائم المتعلقة بسلاسل الإمداد.
- الجرائم المتعلقة ببرمجيات الفدية.
- الجرائم المتعلقة بالتصيد الإلكتروني.
- الجرائم المتعلقة بقرصنة البرمجيات.
- الجرائم المتعلقة بالاستخدام غير المصرح للبيانات لدى مزودي الخدمات.

**أهداف الاتفاقية:**

تعزيز التعاون والتنسيق الدولي لمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

- تطوير التشريعات الدولية لمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.
- إبراز أهمية حماية البنى التحتية الحرجة من خلال مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.
- تعزيز أهمية بناء ورفع القدرات الوطنية والدولية ورفع مســتوى الوعي للأفراد والمجتمعات في مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

**هيكل (عناصر) الاتفاقية:**

- مقدمة.
- التعريفات.
- الأهداف.
- النطاق.
- الواجبات والمسؤوليات.
- التعاون الدولي.
- بناء القدرات ونشر الوعي.
- آلية تطبيق الاتفاقية.

- التحديث المستمر للاتفاقية حسب التطورات.

يجب أن تكون الاتفاقية واسعة النطاق، بحيث تشمل أكبر عدد ممكن من دول العالم مع التركيز على الدول العظمى الحاضنة للتكنولوجيا.

أن تكون الاتفاقية شاملة للمفاهيم الدولية المتفق عليها في مجال جرائم تكنولوجيا المعلومات، سواء كانت الجرائم الواقعة على الأشخاص أو الأموال.

التركيز على إيجاد سبل التعاون بمشاركة المعلومات بين الدول الأعضاء على مستوى سلطات إنفاذ القانون، لتمكين آليات تتبع الأموال الناتجة عن جرائم الاحتيال الإلكتروني، وكذلك تحديد الهوية الرقمية لمرتكبي تلك الجرائم في ظل مراعاة القوانين النافذة في تلك الدول وخصوصية المجتمعات فيها.

تمكين نقاط اتصال دائمة بين الدول الأعضاء للاستجابة الفورية في قضايا الإرهاب والاستغلال الجنسي للأطفال وغيرها، وإيجاد آليات لتفعيل التعاون مع شركات مواقع التواصل الاجتماعي العالمية لتوفير المعلومات الفنية اللازمة لمكافحة هذا النوع من الجرائم.

تفعيل التعاون الدولي لبناء القدرات للعاملين في وحدات مكافحة الجرائم الإلكترونية للدول الأعضاء من خلال الدورات والورش التدريبية وتبادل الخبرات.

## الكويت

[الأصل: بالعربية]
[17 أيلول/سبتمبر 2021]

1- وضع غطاء رئيسي وشامل لمشروع الاتفاقية يؤكد على أن يكون تطبيقها بهدف تعزيز التعاون وتدعيمه في مجال مكافحة جرائم تقنية المعلومات وتقليل مخاطرها ضمن مرتكزات أهمها المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية بما يشمل الإجراءات المتعلقة بممارسة الولاية القضائية، واحترام سيادة القانون وحفظ النظام العام والأمن ومراعاة القيم المجتمعية.

2- صياغة مجالات تطبيق الاتفاقية مع الأخذ بالاعتبار الصكوك الدولية المتعلقة بمكافحة الأفعال الإرهابية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها بحيث تشمل الجرائم التي ارتكبت في أكثر من دولة أو تم الإعداد أو التخطيط أو توجيهها أو الإشراف عليها في دول أخرى أو ارتكبت في دولة وكان لها آثار عابرة للحدود.

3- تحديد نطاقات التجريم الأفعال المؤثمة بالمواكبة مع الصور المستحدثة لها وذلك ضمن محددات تعتمدها الدول في تشريعاتها الوطنية كجرائم أصلية مع الاهتمام الخاص بالجرائم ذات الصلة بالمحتوى وخطابات الكراهية والعنف.

4- تحديد أطر التعاون القانوني والقضائي وتسليم المجرمين وتبادل المعلومات مع جواز تقديم المعلومات بدون طلب مسبق إذا اعتبرت الدولة أن كشف مثل هذه المعلومات يمكن أن يساعد في البدء بتحقيقات في الجرائم، هذا مع التعاون بشأن الكشف والتحفظ العاجل للمعلومات المخزنة في وسائل تقنية المعلومات والوصول إلى تقنية المعلومات عبر الحدود هذا مع التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين والبيانات المتزامنة والحالية وتحديد عناصر السرية وحدود استخدام البيانات محل المساعدة المتبادلة.

5- تحديد أطر تقييم تطبيق الاتفاقية وفق آليات تضطلع بها الحكومات وكذلك تحديد المؤسسات ونقاط الاتصال للدول الأطراف والاستفادة من شبكات المعلومات القائمة ضمن مكتب الأمم المتحدة لمكافحة المخدرات والجريمة.

## ليختنشتاين

[الأصل: بالإنكليزية]
[28 تشرين الأول/أكتوبر 2021]

تود ليختنشتاين أن تتوجه بالشكر لأمانة اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ورئيستها، سعادة فوزية بومعيزة، على طلب رأي الدول الأعضاء حول نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها). وفيما يلي الموقف العام لليختنشتاين.

يتمثل أحد الأهداف الرئيسية لليختنشتاين في ضمان أن تكون الاتفاقية الجديدة لمكافحة الجرائم السيبرانية متوافقة مع الصكوك الدولية والإقليمية القائمة، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وأن ترتكز على القانون الدولي، بما في ذلك قانون حقوق الإنسان.

ولذا، تسعى ليختنشتاين إلى صياغة اتفاقية موجزة وعملية تُركز على الجرائم الخاصة بالفضاء السيبراني، مثل الوصول غير المشروع إلى البيانات واعتراضها والتدخل فيها بصورة غير مشروعة، والتدخل غير المشروع في النظم، وإساءة استخدام الأجهزة، وأعمال التزوير والاحتيال المتصلة بالحاسوب، والجرائم المتصلة بانتهاك حقوق النسخ واستغلال الأطفال في المواد الإباحية. وترى ليختنشتاين أن التجريم واسع النطاق لأنواع الجرائم الأخرى البعيدة عن نطاق الجرائم المحددة المتعلقة بالفضاء السيبراني ينبغي تناوله في اتفاقيات ومحافل أخرى، ومن ثم يجب رفضه. وعلاوة على ذلك، تعارض ليختنشتاين تكرار تناول الاتفاقية للجرائم المتناولة في معاهدات محددة أخرى.

ونظراً للسرعة الحثيثة التي تتغير بها بيئة الفضاء السيبراني، تسعى ليختنشتاين جاهدة لوضع اتفاقية تستخدم لغة محايدة تكنولوجياً بحيث يمكن تطبيق الجرائم الجنائية الأساسية على كل من التكنولوجيات الحالية والمستقبلية المعنية. ومن المرجح أن تصبح التعريفات التكنولوجية الواسعة النطاق لأنواع معينة من الجرائم السيبرانية متقادمة في المستقبل، وينبغي من ثم تجنب استخدامها في الاتفاقية.

ومن الجوانب المحورية الأخرى من وجهة نظر ليختنشتاين أحكام حماية البيانات وحقوق الإنسان، إذ ترى ضرورة التشديد عليها في الاتفاقية. فمن الأهمية بمكان احترام حماية البيانات ومعايير حقوق الإنسان احتراماً كاملاً.

وسوف يُستعرض موقف ليختنشتاين بمزيد من التفصيل أثناء المفاوضات بشأن الاتفاقية الجديدة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

## المكسيك

[الأصل: بالإسبانية]
[21 تشرين الأول/أكتوبر 2021]

ترى حكومة المكسيك أن تكنولوجيات المعلومات والاتصالات والمنصات الرقمية والبيئة السيبرانية توفر فرصاً عظيمة لتعزيز مسيرة التنمية، وسد فجوات عدم المساواة، وتعزيز الإدماج والرفاه والعدالة والحقوق.

بيد أن المكسيك تُدرك أن ارتكاب الجرائم ونمو سوق غير مشروع من خلال هذه التكنولوجيات يُمثلان مبعث قلق متزايد للحكومات والشركات ومنظمات المجتمع المدني والأفراد كافة.

ولذا، أصبحت الحاجة إلى التعاون الدولي وآليات المساعدة القانونية وتبادل المعلومات أكثر من أي وقت مضى. والمكسيك ملتزمة بتعددية الأطراف، لاسيما دور الأمم المتحدة في إيجاد استجابات شاملة ومثمرة لهذا التحدي العالمي.

وترى المكسيك أن الولاية التي منحتها الجمعية العامة لوضع اتفاقية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات للأغراض الإجرامية تُمثل فرصة مثالية لتنفيذ عملية موضوعية وملتزمة وتعددية وشاملة وشفافة تستند إلى الدروس المستفادة من عمليات الأمم المتحدة الأخرى ذات الصلة بهذا الموضوع ومن التجارب الإقليمية الأخرى ذات الصلة.

وتأمل حكومة المكسيك أن تسهم النقاط التالية في توجيه عملية وضع الاتفاقية المستقبلية وتحديد محتواها.

**نهج الاتفاقية ونطاقها ونوعها**

ينبغي أن تُصاغ الاتفاقية في صورة صك قانوني شامل وملزم يتناول كلاً من المسائل الموضوعية والإجرائية، ويهدف إلى إرساء إطار عمل للتعاون الدولي وتبادل المعلومات والتجارب والخبرات وأفضل الممارسات.

ومن المأمول أن تساعد الاتفاقية على تعزيز المعايير اللازمة من أجل تحسين عمليات التحقيق في الجرائم السيبرانية والحد من الآثار المترتبة عليها وملاحقة مرتكبيها. ورغم أن الاتفاقية لا تحول دون إبرام صكوك دولية أخرى تتناول نفس الموضوع، فإنها ستكون بمثابة معيار مرجعي لإطار عمل منسق يُزيد من فعالية ملاحقة مرتكبي الجرائم السيبرانية.

وينبغي أن تتضمن الاتفاقية الجوانب التالية:

- التعاريف العامة والأنماط الأساسية للجرائم والجهات الفاعلة المختصة.
- التدابير الإجرائية الأساسية التي يجدر بالدول اتخاذها من أجل التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها على النحو الملائم.
- الجرائم الجنائية العامة التي ينبغي أن ينظر فيها المشرعون الوطنيون.
- آليات الوصول إلى المعلومات وتعزيز التعاون الفعال.

كما ينبغي أن تنص الاتفاقية المستقبلية على إجراءات لصوغ التحفظات والإعلانات التفسيرية وعلى إجراء مرن لتعديل نصوص الاتفاقية من أجل تيسير تحديثها، ووضع آليات لتسوية المنازعات. ومن المستصوب جعل بدء نفاذ الاتفاقية مشروطاً بإيداع 50 صك تصديق.

وبمجرد تحديد محتوى الاتفاقية، سيكون من المستصوب الاتفاق على آلية فعالة وشاملة لاستعراض التنفيذ تقوم على استعراض الأقران ولا تُثقل كاهل الدول.

**أهمية الصكوك الدولية الأخرى**

ترى حكومة المكسيك أهمية أن تستند الاتفاقية إلى التأكيد على أن القانون الدولي ينطبق على الفضاء السيبراني وأن تؤخذ في الاعتبار، تبعاً لذلك، الصكوك القانونية الدولية القائمة، مثل:

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الثلاثة الملحقة بها
- النظام الأساسي لمحكمة العدل الدولية
- اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

- المعاهدات المعنية بحماية البيانات الشخصية ونقلها عبر الحدود
- المعاهدات الدولية المعنية بحقوق الإنسان، والمعاهدات التي تحمي حقوق الأشخاص المشاركين في الإجراءات القضائية
- المعاهدات المنطبقة على الملكية الفكرية
- المعاهدات الثنائية بشأن تسليم المطلوبين والمساعدة القانونية المتبادلة في المسائل الجنائية وغيرها من أشكال التعاون القانوني الدولي

وعلاوةً على ذلك، يمكن أن تسترشد عملية التفاوض بشكل مفيد بالوثائق المعتمدة في الأمم المتحدة وغيرها من المحافل الدولية ذات الصلة، وعلى رأسها ما يلي:

- جميع الاستنتاجات والتوصيات المُنبثقة عن اجتماعات فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المعقودة في أعوام 2018 و2019 و2020
- التقرير النهائي الصادر عن فريق الخبراء الحكوميين للفترة 2019-2021 والمعني بالارتقاء بسلوك الدول المسؤول في الفضاء السيبراني، والتقريران السابقان الصادران في عامي 2013 و2015
- التقرير النهائي الصادر عن الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي
- مشروع المبادئ التوجيهية لاستخدام البرنامج العالمي للأمن السيبراني الذي وضعه الاتحاد الدولي للاتصالات
- قرارات الجمعية العامة بشأن الحق في الخصوصية في العصر الرقمي
- قرارات مجلس حقوق الإنسان بشأن تعزيز حقوق الإنسان على الإنترنت وحمايتها والتمتع بها

**الجرائم السيبرانية/السلوكيات الإجرامية التي ينبغي تناولها في الاتفاقية**

ترى حكومة المكسيك أن الاتفاقية ينبغي أن تسلط الضوء على الأفعال المعترف بعدم مشروعيتها في القانون الدولي (وفقاً للأحكام المنصوص عليها في المعاهدات الأخرى المعتمدة في إطار الأمم المتحدة) والتي تُرتكب باستخدام وسائل إلكترونية.

وفي حين أنه من غير المتوقع أن تتضمن الاتفاقية قائمة كاملة بالجرائم السيبرانية، أو أن تكون جميع أنماطها متوافقة مع النظم القانونية المختلفة، فمن المستصوب أن تؤدي عملية صياغة الاتفاقية إلى حوار يكون نقطة مرجعية عامة للجوانب التالية:

- تعريف انتحال الشخصية والتصيد الاحتيالي.
- الاحتيال والابتزاز.
- استخدام فيروسات الفدية.
- البرمجيات الخبيثة والسلوك الإجرامي المرتبط بإنتاج الشفرات الخبيثة وتخزينها وتوزيعها وبيعها واستخدامها.
- الكشف عن المعلومات الشخصية أو المؤسسية بما يضر بأصحابها.
- الجرائم المرتبطة بالاتجار بالبشر واستغلال الأطفال في المواد الإباحية وانتهاكات الخصوصية الجنسية.

- استمالة الأطفال والتنمر السيبراني.
- العنف الرقمي، بما في ذلك العنف الجنساني والعنف القائم على الكراهية أو العرق أو الجنسية أو الدين أو العداء السياسي.
- طرائق الهجوم (التصيد الاحتيالي، والتصيد الإلكتروني الصوتي، وسرقة الهوية من خلال إرسال الروابط الإلكترونية الخبيثة، وتزوير العناوين الإلكترونية).
- الجرائم ضد السيادة الوطنية مثل الإرهاب والتخريب والتجسس واقتحام النظم التي تحتوي على معلومات سرية لأسباب تتعلق بالأمن القومي.
- الأعمال الإجرامية التي تستهدف البنية التحتية للمعلومات الحيوية وسرية المعلومات وسلامتها وتوفرها.
- الجرائم ضد الأطفال والمراهقين.
- انتهاك حرية التعبير.
- الجرائم ضد حقوق الملكية الفكرية.
- الجرائم ضد النظام المالي.
- البيع غير القانوني للأسلحة والحيوانات والأدوية الخاضعة للمراقبة والأدوية غير المُصنفة على أنها منتجات صحية مسجلة.
- تزييف العملات والوثائق الرسمية.
- استخدام العملات المشفرة والأصول ذات الاستخدام المزدوج للأغراض الإجرامية.
- التعديل غير القانوني للبوابات الإلكترونية (تغيير المظهر).
- مسؤولية الشخصيات الاعتبارية.

وسيكون من المناسب أيضاً، عند صياغة الاتفاقية، مناقشة إمكانية النص على عقوبات للشروع في الجريمة وتحديد الظروف المشددة المُفضية إلى إيقاع عقوبات أشد.

**الجوانب المتعلقة بالسيادة والولاية القضائية**

- إعادة تأكيد احترام السيادة الوطنية ومبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.
- وضع قواعد عامة لتحديد الولاية القضائية بالاستفادة من الأحكام المماثلة الواردة في الصكوك والعمليات القانونية الأخرى.
- صياغة تدابير مشتركة للحصول على بيانات حركة المرور والمحتوى مع منع الحظر أو الاعتراض غير القانوني للبيانات.
- تطوير آليات توفر التيقن فيما يخص الحصول على الأدلة الرقمية والاحتفاظ بها وحفظها وتقديمها.
- توضيح خطوات التحقيق المُتخذة مثل مذكرات الاستدعاء أو الاعتقال.
- صياغة أحكام تُنظم تقديم البيانات الفنية وبيانات المحتوى في التحقيقات الجنائية والكشف الفوري عن البيانات الحاسوبية.

- تناول الالتزام القانوني على مشـغلي التكنولوجيات ومقدمي الخدمات ومقدمي محتوى الإنترنت، بغض النظر عن موقعهم الفعلي، فيما يخص تقديم المعلومات إلى السلطات المختصة أثناء التحقيقات.

**الجوانب المتعلقة بتبادل المعلومات والتعاون الدولي**

ترى حكومة المكسـيك أن توفير التيقن فيما يخص تبادل المعلومات والتعاون الدولي ووضـع عمليات تضـمن التنفيذ الفعال للاتفاقية ينبغي أن يكون من بين الأهداف الرئيسـية للاتفاقية. ومن المأمول أن تتناول الاتفاقية، من بين جملة جوانب أخرى، ما يلي:

- المساعدة القانونية المتبادلة.
- تسليم المطلوبين.
- الآليات المشتركة لطلب المعلومات والرد عليها وتلقيها وتبادلها لأغراض التحقيق والاستخبارات.
- إجراءات الرقابة القضائية التي تُيسر التعاون السريع والفعال أثناء التحقيقات.
- التعاون في إجراء التحقيقات الشرطية والحصول على إفادات الشهود لاستخدامها في الإجراءات القضائية، مع مراعاة استخدام تكنولوجيات المعلومات والاتصالات.
- وضع مبادئ توجيهية ومعايير ومنهجيات وأفضل الممارسات لمنع الجرائم السيبرانية والتحقيق فيها.
- تعزيز التعاون بين فرق الاستجابة للطوارئ الحاسوبية أو فرق الاستجابة لحوادث الأمن الحاسوبي من أجل منع الجرائم السيبرانية.
- التحقيقات المنسقة.
- التوصـية بإطار عمل مشـترك أدنى يضـمن الشـفافية وحماية المعلومات بحيث يمكن تبادل البيانات المُستقاة من التحقيقات والإجراءات القضائية بغض النظر عن السياسات الوطنية المختلفة لكل دولة.
- وضع حدود زمنية دنيا للاحتفاظ بالبيانات والحفاظ على الأدلة الرقمية.
- التوصـية بقواعد وشـروط يجب أن يخضـع لها اعتراض الاتصـالات الخاصـة، وتحديد الموقع الجغرافي في الوقت الحقيقي.
- وضع معايير عامة لتنظيم سياسات الخصوصية والامتثال لها.
- تعزيز تنسيق الإحصاءات المحلية والإقليمية والعالمية.

**الجوانب المتعلقة بحماية حقوق الإنسان وممارستها**

ينبغي أن تكون جميع التدابير المقرر تنفيذها بموجب الاتفاقية المسـتقبلية متسـقة مع الالتزامات المنصوص عليها في الصكوك الدولية لحقوق الإنسان. ومن المتوقع أيضاً أن تكون أحكام الاتفاقية متوافقة مع المعايير المتعلقة بحرية التعبير.

وتأمل حكومة المكسيك تناول الجوانب التالية أثناء وضع الاتفاقية:

- المفاهيم والتطورات المتعلقة بالأعمال التجارية وحقوق الإنسان.
- التأكيد على التحقيق في أعمال العنف القائم على النوع الجنساني والجرائم المُرتكبة ضد الأطفال والمراهقين عبر الإنترنت وملاحقة مرتكبيها ومعاقبتهم.

- الحث على التحقيق في السلوك العنصري الذي يُحرض على العنف أو الهادف إلى الإقصاء أو التفرقة وملاحقة مرتكبيه ومعاقبتهم.
- العناصر المشتركة الدنيا لحيادية الشبكة.
- التوصية بآليات حماية المعلومات التي يجب أن تعتمدها الشركات المقدمة لخدمات الإنترنت.

**العناصر المتعلقة ببناء القدرات والمساعدة التقنية**

ترى حكومة المكسيك أن التنفيذ الفعال للاتفاقية المستقبلية يستلزم وضع أحكام تعزز بناء القدرات فيما يخص منع الجريمة السيبرانية وملاحقة مرتكبيها. وسيكون من المستصوب:

- تشجيع الجهود المتعلقة بالتدريب والمساعدة التقنية وأفضل الممارسات، فضلاً عن الإجراءات الموحدة لتنفيذ التحقيقات الجنائية الحاسوبية والحصول على أدلة رقمية صحيحة.
- تعزيز مبادرات التثقيف الموجهة نحو الوقاية وحملات التوعية العامة القابلة للتكرار.
- تشجيع تشكيل أو تعزيز فرق الاستجابة للطوارئ الحاسوبية في مختلف القطاعات مثل الشؤون المالية والتعليم والتجارة والطاقة.
- إعداد أدلة ومبادئ توجيهية وتوصيات تُسهل اعتماد أفضل الممارسات.
- توسيع نطاق الأنشطة التدريبية التي تستهدف مختلف أصحاب المصلحة: المحققون والمدعون العامون والقضاة والدبلوماسيون والمشرعون والجهات الفاعلة من غير الدول.

**الجوانب المتعلقة بمشاركة الجهات الفاعلة المعنية من غير الدول (المجتمع المدني، والقطاع الخاص، والأوساط الأكاديمية)**

ترى حكومة المكسيك أنه من المستصوب أن تستكشف من خلال عملية الصياغة آليات من أجل تيسير مشاركة منظمات المجتمع المدني ومؤسسات القطاع الخاص ومقدمي الخدمات والأوساط الأكاديمية والمراكز البحثية وتقديمها للمدخلات. ومن المستصوب النظر فيما يلي:

- المشاركة المحتملة لتلك الجهات الفاعلة في العمليات الرامية لمنع الجريمة السيبرانية ومكافحتها.
- تعزيز بيئات التعاون مع فرق الاستجابة للطوارئ الحاسوبية الخاصة وشركات النقل وشركات الاتصالات السلكية واللاسلكية المختلفة.
- إقامة حوار مع المؤسسات الخاصة المكلَّفة بتشغيل البنية التحتية المعلوماتية الحيوية، أو العاملة في قطاعات استراتيجية، ومع الشركات المقدمة لخدمات الإنترنت المجانية مثل البريد الإلكتروني والرسائل الفورية والمدونات المصغرة وخدمات النقل عبر الإنترنت.
- دعم التنظيم الذاتي والوعي الاجتماعي، وتعزيز مفهوم الأعمال التجارية وحقوق الإنسان.

## نيوزيلندا

[الأصل: بالإنكليزية]
[29 تشرين الأول/أكتوبر 2021]

يسر نيوزيلندا أن تستجيب لدعوة رئيسة اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها فيما يخص تنفيذ قراري الجمعية العامة 74/247 و75/282. وترحب نيوزيلندا بالفرصة التي أُتيحت لها لمشاركة آرائها، وتتطلع إلى مساهمات الدول الأعضاء الأخرى ومناقشة مسار المضي قدماً في إطار العمل معاً بطريقة شفافة وشاملة لوضع الاتفاقية الجديدة.

تشكل الجريمة السيبرانية تحدياً عابراً للحدود، مما يعني أن التعاون العالمي المتجذر في اعتماد نهج شامل ومتعدد أصحاب المصلحة هو الطريق الوحيد لضمان قدرة المجتمع الدولي على التصدي بفعالية لهذا التهديد المتزايد. ويستلزم التعاون الدولي بشأن القضايا المتصلة بالجرائم السيبرانية وجود قوانين متسقة وفعالة لمكافحة الجريمة السيبرانية تتيح التحقيق في الجرائم السيبرانية عبر الحدود وملاحقة مرتكبيها، ولا شك أن تيسير هذا التعاون بات أكثر أهمية من أي وقت مضى. وفي ظل تحول العمل والبحث والتفاعلات الاجتماعية إلى فضاء الإنترنت، بما في ذلك أثناء تفشي جائحة مرض فيروس كورونا (كوفيد-19)، اتسعت مجالات الفرص السانحة للمجرمين السيبرانيين، وشهدنا تزايداً في تواتر حوادث الجرائم السيبرانية واشتداد وطأتها.

وللتعاون الدولي بشأن الجريمة السيبرانية أهمية خاصة للدول الجزرية الصغيرة النامية، ومن الضروري أن تكون هذه الدول قادرة على المشاركة المثمرة في عمل اللجنة المخصصة. ونيوزيلندا ملتزمة بضمان قدرة دول جزر المحيط الهادئ على المشاركة المثمرة في أعمال اللجنة المخصصة. ونؤيد المشاركة المختلطة (بالحضور الشخصي وعبر الإنترنت) في دورات اللجنة المخصصة، ونؤكد على أهمية إتاحة الوقت الكافي للوفود الأصغر حجماً للتجهيز والمشاركة.

### نطاق الاتفاقية

يجب أن تُكمل الاتفاقية الجديدة بشأن مكافحة الجريمة السيبرانية الصكوك القائمة لا أن تتعارض معها. وقد اتفقت جميع الدول الأعضاء على أن القانون الدولي ينطبق على الفضاء السيبراني، مما يعني أن هذه الاتفاقية الجديدة لن تكون بمعزل عن الصكوك والقوانين الدولية الأخرى. وستكون أكثر فاعلية إذا كانت تُكمل وتعزز الصكوك القائمة والنظام القانوني القائم، والذي يتضمن أدوات للتصدي للجرائم السيبرانية مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. ويتماشى ذلك مع الولاية المنصوص عليها في قرار الجمعية العامة 74/247، الذي دعت فيه الجمعية العامة اللجنة المخصصة إلى أن تأخذ في حسبانها بشكل كامل الصكوك والجهود الدولية القائمة على الأصعدة الوطنية والإقليمية والدولية.

وترى نيوزيلندا أنه من الضروري أن يحمي أي صك مُعدٍ حقوق الإنسان وأن يدعم فضاءً سيبرانياً حراً ومنفتحاً وخاضعاً لتنظيم مجموعة متنوعة من أصحاب المصلحة. ولذا، يجب أن تكون اتفاقية مكافحة الجريمة السيبرانية متسقة مع التزامات الدول بحماية حقوق الإنسان واحترامها على الإنترنت، بما في ذلك الحق في حرية التعبير وحق الفرد في عدم تعرضه لتدخل تعسفي وغير قانوني في حياته الخاصة. كما يجب أن تكون تدابير مكافحة الجريمة السيبرانية متسقة مع القانون الدولي لحقوق الإنسان.

وينبغي أن تركز الاتفاقية تركيزاً شديداً على قضايا الجريمة السيبرانية الأساسية من أجل تعزيز التعاون بشكل فعال لمواجهة التهديد الذي تُشكله هذه الجرائم على الأفراد والصناعات والحكومات. ونرى أن الاتفاقية ينبغي أن تتناول الجرائم التي ترتكب من خلال الفضاء السيبراني، إلى جانب الجرائم التي تُيسر من خلال الفضاء السيبراني فقط متى أدى استخدام تكنولوجيات المعلومات والاتصالات إلى اتساع نطاق تلك الجرائم وزيادة سرعتها ومداها. ونرى أن هناك جريمتين واضحتين مرشحتين لهذه الفئة من الجرائم، وهما: الاستغلال الجنسي للأطفال والتحرش بهم عبر الإنترنت، والاحتيال والسرقة باستخدام نظم سيبرانية، بما في ذلك فيروسات الفدية.

ولا ترى نيوزيلندا أن هناك حاجة إلى تكرار الجرائم التي تشملها صكوك قانونية أخرى، مثل الفساد أو الاتجار أو الإرهاب، لمجرد ارتكابها باستخدام تكنولوجيات المعلومات والاتصالات، إذ من المحتمل أن يؤدي هذا النهج إلى وجود تناقض وارتباك، ولن ينتج عنه صكاً عملياً محدد الأهداف من شأنه تعزيز قدرتنا الجماعية على مكافحة الجريمة السيبرانية.

وتُحدد الولاية الخاصة بهذه العملية تحديداً واضحاً أن علينا التركيز على وضع صك معني بالعدالة الجنائية لتحسين تدابير التصدي الدولية للجرائم السيبرانية، من خلال الإجراءات التي تتخذها أجهزة إنفاذ القانون الوطنية، وهو ما يستلزم تعريف السلوك الإجرامي في الفضاء السيبراني ومعاقبة مرتكبيه، وتنفيذ الدول للعمليات والأدوات التشريعية المناسبة التي تُمكن أجهزة إنفاذ القانون من الوصول إلى الأدلة الرقمية وتبادلها لمكافحة السلوك الإجرامي في الفضاء السيبراني ومعاقبة مرتكبيه. ولا يستلزم هذا وضع قواعد ومعايير للسلوك غير الإجرامي عبر الإنترنت. ونرى أهمية التعلم من معاهدات العدالة الجنائية الأخرى التي نجحت نتيجة لتركيزها على القضايا الجنائية الأساسية، إلى جانب أحكام التعاون الدولي الواسعة النطاق ودعم بناء القدرات في جميع الدول الأعضاء.

ويجب أن تكون لغة الاتفاقية النهائية عملية ومحايدة من الناحية التكنولوجية ومواكبة للمستقبل إلى أقصى قدر ممكن من أجل ضمان صمودها أمام تحدي الزمن وعدم الحاجة إلى مراجعتها بين الحين والآخر. وهذا يعني أننا سنحتاج إلى التركيز على النشاط وليس على الشكل أو الطريقة المعينة المستخدمة لتنفيذ هذا النشاط.

وسيكون من السابق لأوانه في هذه المرحلة تحديد العناصر المطلوبة فيما يخص آلية تنفيذ الاتفاقية. وهناك مجموعة واسعة من النماذج التي يمكن النظر فيها، ولكن يمكن تنحية هذا الجانب من الاتفاقية جانباً لحين تحديد نطاقها وأهدافها بشكل أوضح.

**أهداف الاتفاقية**

ينبغي أن يكون الغرض الأساسي من الاتفاقية الجديدة هو إيجاد إطار عمل عالمي منسق وحديث وفعال للتعاون والتنسيق بين الدول للتصدي للتهديد المتزايد الذي تُشكله الجريمة السيبرانية على الأفراد والشركات والبنية التحتية الحيوية والحكومات. وينبغي أن تشمل تقديم الدعم والمساعدة التقنية لتمكين جميع الدول من تطوير قدراتها وإمكاناتها في التصدي لهذه التحديات، مما سوف يُثمر عن تعزيز قدرة الدول على التصدي بفعالية للجرائم السيبرانية وطنياً وإقليمياً ودولياً.

وهذا يعني أن الاتفاقية تحتاج إلى دعم التعاون بين أجهزة إنفاذ القانون والنيابة العامة والقضاء الوطنية على المستوى الثنائي أو المتعدد الأطراف في منع الجرائم المنصوص عليها في الاتفاقية والتحقيق فيها وملاحقة مرتكبيها. وهذا أمر بالغ الأهمية في مكافحة الجرائم السيبرانية التي غالباً ما تنطوي على جناة وضحايا في العديد من الولايات القضائية نظراً لطبيعتها العابرة للحدود. وسيساعد الفهم المشترك للفعل الذي يُشكل جريمة جنائية في سياق الفضاء السيبراني وتحديد الجرائم التي ينبغي معاقبة مرتكبيها في الولايات القضائية المحلية على تسهيل ذلك، ولا سيما متى استُكمل ذلك بأطر عمل متسقة للوصول إلى الأدلة الرقمية وتبادلها مع الشركاء الدوليين مع توفير الضمانات المناسبة.

ويجب أن يخضع استخدام سلطات التحقيق في الجرائم المنصوص عليها في الاتفاقية وملاحقة مرتكبيها لضمانات فعالة فيما يتعلق بحقوق الإنسان والحريات الأساسية، على النحو المنصوص عليه في المعاهدات الدولية القائمة. ويتعين أيضاً وجود ضمانات لكفالة استخدام صلاحيات التعاون المتبادل بصفة عادلة ومناسبة، وتمكين الدول من رفض التعاون في حال عدم الوفاء بمعايير معينة. وبالإضافة إلى ذلك، ترى نيوزيلندا أن الاتفاقية يجب أن تعترف باستقلالية أجهزة إنفاذ القانون والإدعاء الوطنية، وأن قرار التدخل واتخاذ أية إجراءات يقع على عاتق تلك الأجهزة وحدها في الدول الأعضاء المعنية.

وأفضل طريقة لتحقيق التعاون الدولي الفعال هي إبرام اتفاقية تحظى بتأييد واسع النطاق. وترى نيوزيلندا أن هذا يستلزم أن تكون المفاوضات الخاصة بالاتفاقية شاملة وشفافة، مع بذل أقصى الجهود للتوصل إلى توافق في الآراء من أجل ضمان أن للاتفاقية أقوى ولاية ممكنة. وينبغي أن تكون جميع الدول الأعضاء قادرة على تبادل آرائها والمشاركة بشكل مثمر في المفاوضات مدعومة بخبرات ووجهات نظر المجتمع المدني والصناعات وأصحاب المصلحة الآخرين. وينبغي تضمين وجهات نظر الشعوب الأصلية، بما في ذلك الماوري في أوتياروا (نيوزيلندا)، فضلاً عن جماعات الأقليات الأخرى، إلى جانب التأثير المحتمل للجرائم السيبرانية على هذه الجماعات والجهود المبذولة لمكافحتها.

والتعاون الدولي في مجال مكافحة الجريمة السيبرانية ليس فعالاً بالقدر الذي يُمكن أن يكون عليه. ولا يُعزى ذلك إلى ضعف الإرادة لدى الدول الأعضاء، بل إلى نقص القدرات أو الخبرات. وتُعد المساعدة التقنية وبناء القدرات لمؤسسات إنفاذ القانون مطلب بالغ الأهمية، وتحتاج الاتفاقية إلى دعم تنمية القدرات والإمكانات على الصعيد العالمي.

**هيكل الاتفاقية**

نتطلع إلى الاستماع إلى آراء الدول الأخرى فيما يتعلق بنطاق الاتفاقية وأهدافها من خلال هذه العملية وفي دورة التفاوض الأولى المقرر عقدها في كانون الثاني/يناير 2022. وبعد ذلك، نتوقع أن يظهر سريعاً مسار واضح للمضي قدماً فيما يخص هيكل الاتفاقية.

## نيجيريا

[الأصل: بالإنكليزية]
[5 تشرين الثاني/نوفمبر 2021]

تعتقد نيجيريا أنه من أجل الاستجابة بفعالية للتهديدات سريعة التطور للجريمة السيبرانية، ثمة حاجة ملحة لتعريف السلوك الإجرامي في الفضاء السيبراني ومعاقبة مرتكبيه، وتعزيز التآزر في القدرات الشرطية عبر الوطنية، وتحسين الأدوات الإجرائية، وإصلاح و/أو تعزيز التعاون الدولي، مع احترام حقوق الإنسان. وبالتالي، يجب أن تُركز عملية وضع اتفاقية للأمم المتحدة بشأن هذا الموضوع في هذا الوقت على مكافحة الجريمة السيبرانية وألا تحاول تناول الأمن السيبراني والمسائل الأخرى ذات الصلة بالفضاء السيبراني المتقلبة سياسياً والتي يجري تناولها على نحو أفضل في محافل الأمم المتحدة الأخرى. ومن الضروري أن تكون عملية المفاوضات بشأن الاتفاقية الجديدة شفافة وشاملة للجميع وقائمة على توافق الآراء، بحيث تفضي إلى قبول و/أو اعتماد أوسع نطاقاً للاتفاقية.

**نطاق الاتفاقية**

ينبغي أن تضع الاتفاقية الجديدة إطار عمل قانوني ومؤسسي لمكافحة الجريمة السيبرانية ينطوي على العناصر التالية:

(أ) تجريم الجرائم السيبرانية الأساسية: تعريف وتحديد عقوبات للجرائم التي تُرتكب من خلال الفضاء السيبراني، وهي الجرائم التي تكون فيها الحواسيب أو البيانات أهدافاً للنشاط الإجرامي، وبعض الجرائم التي تُيسر من خلال الفضاء السيبراني، فضلاً عن غسل العائدات المُتأتية من الجرائم السيبرانية؛

(ب) منح السلطات الإجرائية للتحقيق في الجرائم السيبرانية المعترف بها وملاحقة مرتكبيها، وكذلك للحصول على الأدلة الإلكترونية للجرائم الجنائية الأخرى وتبادلها؛

(ج) أحكام أو تدابير لبناء القدرات المستدامة والمساعدة التقنية؛

(د) أحكام أو تدابير لاسترداد العائدات المُتأتية من الجريمة السيبرانية وردها؛

(هـ) أحكام أو تدابير لتحسين التعاون والتنسيق بين أجهزة إنفاذ القانون والقطاع الخاص؛

(و) أحكام أو تدابير لتعزيز التعاون الدولي في شأن المسائل المذكورة أعلاه، بما في ذلك التعاون المباشر مع مقدمي خدمات الإنترنت؛

(ز) أحكام أو تدابير لمنع الجريمة السيبرانية والتوعية بها، بما في ذلك العمل مع منظمات المجتمع المدني والقطاع الخاص ومقدمي الخدمات والأوساط الأكاديمية والمراكز البحثية.

**أهداف الاتفاقية**

ينبغي أن تسعى الاتفاقية الجديدة إلى تحقيق الأهداف التالية:

(أ) إيجاد فهم مشترك لخطوط الأساس الثابتة للجرائم السيبرانية الأساسية، والصلاحيات الإجرائية والتعاون الدولي لمكافحة الجريمة السيبرانية؛

(ب) الحث على تجريم الجرائم السيبرانية بطريقة محايدة من الناحية التكنولوجية للتأكد من أن الأحكام الجنائية الأساسية لا تتناول التكنولوجيات والتقنيات الإجرامية الحالية فحسب، بل والتكنولوجيات والتقنيات المستقبلية أيضاً؛

(ج) إرساء صلاحيات وقدرات جمع الأدلة الإلكترونية على الجرائم السيبرانية والجرائم الأخرى والحصول عليها وتبادلها، بما يتفق مع الأصول القانونية وحماية حقوق الإنسان والحريات الأساسية؛

(د) تشجيع وتسهيل التعاون الدولي في شأن مكافحة الجريمة السيبرانية والقضاء على الملاذات الآمنة لمرتكبي الجرائم السيبرانية؛

(هـ) تدعيم بناء القدرات والمساعدة التقنية لتعزيز قدرة أجهزة إنفاذ القانون على التصدي للجرائم السيبرانية، فضلاً عن الاستعانة بالقدرات المؤسسية المتوفرة مثل قواعد بيانات الإنتربول؛

(و) تشجيع الدول الأعضاء على استخدام الصكوك المتعددة الأطراف التي أثبتت بالفعل جدواها في مكافحة الجرائم السيبرانية، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، والوثيقة الصلة بمعاهدات الأمم المتحدة القائمة في مجال منع الجريمة والعدالة الجنائية، لاسيما اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد؛

(ز) تدعيم العمليات الحكومية الدولية والمتعددة أصحاب المصلحة على مستوى الممارسين من أجل التبادل الموثوق للمعلومات لتحديد الاتجاهات المستقبلية للجريمة السيبرانية وتهديداتها وتدابير التخفيف من وطأتها؛

(ح) وضع آلية لرصد و/أو تيسير الاستخدام والتنفيذ الفعالين للاتفاقية وتبادل المعلومات والنظر في إجراء أي مراجعات و/ أو تعديلات مستقبلية عليها.

**هيكل الاتفاقية**

بالإضافة إلى الديباجة والتعاريف الواضحة والأحكام النهائية المناسبة، من المهم أن تُشكل العناصر التالية جزءاً من هيكل الاتفاقية الجديدة:

(أ) الأحكام و/أو الأهداف العامة وآليات تنفيذها؛

(ب) تدابير لمنع الجريمة السيبرانية تكون مماثلة للتدابير الواردة في اتفاقية مكافحة الجريمة المنظمة عبر الوطنية واتفاقية مكافحة الفساد، ومن ذلك على سبيل المثال الأحكام المتصلة بالتوعية العامة والمبادرات التثقيفية؛

(ج) الجرائم السيبرانية الأساسية والعقوبات المترتبة عليها؛

(د) أحكام القانون الإجرائي وصلاحيات التحقيق العامة؛

(هـ) ضمانات للتأكد من امتثال أنشطة إنفاذ القانون لحقوق الإنسان الدولية؛

(و) التعاون الدولي في مكافحة الجريمة السيبرانية، بما في ذلك التعاون الدولي الرسمي وغير الرسمي على حد سواء للكشف عن الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها، وكذلك للحصول على أدلة إلكترونية على جرائم جنائية أخرى؛

(ز) أحكام لبناء القدرات والمساعدة التقنية لتعزيز مهارات الممارسين، وتدعيم قدرات التصدي للجرائم السيبرانية؛

(ح) أحكام للتعاون بين أصحاب المصلحة المتعددين على مستوى الممارسين من أجل التبادل الموثوق للمعلومات والخبرات مع أصحاب المصلحة؛

(ط) أحكام لوضع آلية لرصد و/أو تيسير الاستخدام والتنفيذ الفعالين للاتفاقية وتبادل المعلومات والنظر في إجراء أي مراجعات و/أو تعديلات مستقبلية عليها.

## النرويج

[الأصل: بالإنكليزية]
[3 تشرين الثاني/نوفمبر 2021]

يسر حكومة مملكة النرويج أن تستجيب للدعوة الموجهة إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية الجديدة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية وأهدافها وهيكلها، فيما يخص تنفيذ قراري الجمعية العامة 74/247 و75/282. وترى حكومة مملكة النرويج أن التعاون الدولي أمر أساسي للتصدي للتنامي المستمر لتهديدات الجرائم السيبرانية، وتتطلع حكومة النرويج إلى المشاركة في المفاوضات الرامية لوضع اتفاقية شاملة بشأن هذه المسألة.

**نطاق الاتفاقية**

قررت الجمعية العامة، في قرارها 247/74، تشكيل لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. ولأن القرار يستهدف بوضوح السلوك الإجرامي، ينبغي أن يكون تجريم الجرائم السيبرانية الأساسية جزءاً جوهرياً من الاتفاقية.

وتقع المسائل المتعلقة بالأمن السيبراني والحوكمة السيبرانية خارج نطاق الولاية الممنوحة من الجمعية العامة، ولا ينبغي أن تكون موضوع الاتفاقية. وتخضع هذه المسائل لمحافل وعمليات أخرى تابعة للأمم المتحدة. وسوف تزيد محاولات إدراج أحكام بشأن الأمن السيبراني والحوكمة السيبرانية من صعوبة وضع صك ينال دعماً واسعاً من الدول الأعضاء.

ولطالما شكَّلت الجريمة السيبرانية تحدياً حقيقياً على مدى عقود من الزمن، ومن المشكلات المستمرة أن مرتكبي هذا النوع من الجرائم عادةً ما يسبقون أجهزة إنفاذ القانون الوطنية بخطوة. والجرائم السيبرانية تتطور وتتغير يوماً بعد يوم، وقد ألقت الثورة الرقمية المستمرة على كاهل المجتمع الدولي مهمة شاقة وضخمة. وفي هذا الصدد، من الأهمية بمكان السعي لإدراج مجموعة محدثة ومعاصرة من الجرائم السيبرانية قادرة على الصمود أمام تحدي الزمن.

وعلى الرغم من تطور الجريمة السيبرانية يوماً بعد يوم، تمكنت الأجهزة الوطنية والدولية من تحديد أنواع السلوك الإجرامي الأساسي المتكرر. وهذه الجرائم مُجرمة بالفعل في الوقت الراهن في العديد من الدول الأعضاء. وفي هذا الصدد، تود حكومة مملكة النرويج أن توصي بالنظر على الأقل في الجرائم التالية التي تُرتكب وتُيسر من خلال الفضاء السيبراني:

(أ) الوصول غير المشروع إلى البيانات، أي الوصول إلى حاسوب أو نظام حاسوبي دون الحصول على تصريح بذلك؛

(ب) الاعتراض غير المشروع للبيانات، أي الاعتراض غير القانوني في الوقت الحقيقي لمحتوى الاتصالات أو بيانات الحركة المتعلقة بالاتصالات؛

(ج) التدخل في البيانات أو النظم الرقمية، أي البرمجيات الخبيثة وهجمات حجب الخدمات وفيروسات الفدية وحذف البيانات أو تعديلها؛

(د) إساءة استخدام الأجهزة، أي استخدام بيانات الائتمان وكلمات المرور والمعلومات الشخصية التي تسمح بالوصول إلى الموارد أو الاتجار بها؛

(هـ) الجرائم المتعلقة بالمواد المرتبطة بالاستغلال الجنسي للأطفال؛

(و) الجرائم المتصلة بالاحتيال الميسر من خلال الحاسوب، أي التلاعب بالأنظمة الحاسوبية أو البيانات لأغراض احتيالية مثل التصيد الاحتيالي وتعريض رسائل البريد الإلكتروني التجارية للخطر والاحتيال في المزادات؛

(ز) الجرائم المتعلقة بالتعدي على حقوق النسخ والحقوق ذات الصلة.

وينبغي أن تتضمن الاتفاقية أيضاً أحكاماً بشأن محاولة ارتكاب الجرائم السيبرانية والمساعدة فيها والتحريض عليها والتآمر لتنفيذها وغسل العائدات المُتأتية منها، ومسؤولية الشركات والأشخاص الاعتباريين الآخرين.

وفي ظل استمرار الجريمة السيبرانية في التطور، من المهم أن تضع اللجنة المخصصة اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية تُركز على التقارير المُحدثة

الصادرة عن أجهزة إنفاذ القانون الوطنية والتقارير المماثلة الصادرة عن المنظمات الإقليمية والدولية. ومن المهم أيضاً أخذ الدراسة الشاملة التي أجراها مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية في الاعتبار. وتود حكومة مملكة النرويج أيضاً أن تلفت الانتباه إلى التقييم السنوي لتهديدات الجريمة المنظمة عبر الإنترنت الذي تُجريه اليوروبول بصفته مصدراً مهماً للمعلومات المتصلة بأنواع الجرائم السيبرانية السائدة.

وبالإضافة إلى الأحكام المتعلقة بالتجريم، ينبغي أن تتضمن الاتفاقية أحكاماً بشأن الصلاحيات الإجرائية، ولا سيما الأحكام المتصلة بجمع الأدلة الإلكترونية وتبادلها. ومن الضروري أن تكون هذه الأحكام متسقة مع الأصول القانونية وحماية حقوق الإنسان والحريات الأساسية.

وللتصدي لتحدي الجريمة السيبرانية الحديثة، ينبغي أن تقضي الاتفاقية بأن تدرج الدول الأعضاء في قوانينها الوطنية أحكاماً تتناول الأدلة الإلكترونية على وجه التحديد، مثل القواعد الخاصة بالتعجيل في حفظ البيانات الحاسوبية المُخزنة، والبحث عن البيانات الحاسوبية المُخزنة ومصادرتها، وجمع بيانات الحركة الحاسوبية وبيانات المحتوى الحاسوبي في الوقت الحقيقي في حالات الجرائم الخطيرة. وعلاوةً على ذلك، ينبغي أن تسمح الاتفاقية بالتعاون في جمع الأدلة الإلكترونية والحصول عليها فيما يتعلق بأي نوع من الجرائم وليس الجرائم السيبرانية فحسب.

وعلى وجه الخصوص، ينبغي أن تنظر اللجنة المخصصة في الأحكام المتعلقة بالحصول على الأدلة الإلكترونية مما يسمى منصات "الموارد السحابية". ففي العقد الماضي، كان تخزين البيانات الحاسوبية على منصات الموارد السحابية يُمثل تحدياً شائعاً بالنسبة لأجهزة إنفاذ القانون الوطنية، ويُعزى ذلك على وجه الخصوص إلى المسائل المتصلة بالولاية القضائية والاعتماد على الدول الأخرى. ولذا، ينبغي أن تعكس الاتفاقية المعاصرة والمُحدثة المعنية بالجريمة السيبرانية آليات التعاون فيما بين الدول الأعضاء لتأمين الأدلة المُخزنة على منصات الموارد السحابية في الدول الأخرى.

ومن الضروري أيضاً أن تتضمن الاتفاقية أحكاماً بشأن التعاون الدولي. وفي هذا الصدد، ينبغي للجنة المخصصة أن تستفيد من الخبرات المُكتسبة من المعاهدات القائمة، لاسيما اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد. وينبغي مراعاة الأحكام المتعلقة بتسليم المطلوبين والمساعدة المتبادلة.

ومن المهم أيضاً أن تجسد الاتفاقية القدرات المتفاوتة للدول الأعضاء على الامتثال للأحكام المقترحة، لا سيما الأحكام المتعلقة بالإمكانات وبالبنية التحتية التقنية. ولذا، ينبغي أن تُنشئ الاتفاقية أدوات لبناء القدرات وأن تُوفر سُبلاً للدول الأعضاء للحصول على هذه المساعدة.

وختاماً، ينبغي أن تتناول الاتفاقية كيفية تعاون المواطنين والشركات والمنظمات وأصحاب المصلحة الآخرين مع الحكومات لحماية أنفسهم والمجتمع من الجرائم السيبرانية. وعلى الرغم من أن الأمن السيبراني لا يندرج ضمن نطاق الاتفاقية، فإن منع الجرائم السيبرانية أمر وثيق الصلة بطبيعة الحال وينبغي النظر فيه.

**أهداف الاتفاقية**

ينبغي أن تعمل اللجنة المخصصة على وضع اتفاقية مُحكمة تقضي بأن تعتمد الدول الأعضاء تشريعات وطنية تسهم في تعزيز منع الجرائم السيبرانية والتصدي لها على الصعيد العالمي. وستكون الأحكام المحلية المتعلقة بتجريم أنواع معينة من الجرائم السيبرانية، وكذلك الأحكام المتعلقة بالصلاحيات الإجرائية والتعاون الدولي، ذات أهمية خاصة.

وينبغي أن تستهدف عملية صياغة الاتفاقية وضع صك قادر على الصمود أمام تحدي الزمن ومواكب لجميع الأشكال الحديثة للجرائم السيبرانية والاتجاهات المحتمل ظهورها. وعلاوةً على ذلك، ينبغي السعي لصياغة

صك طموح قادر على التصدي على نحو وافٍ لتحديات الجريمة السيبرانية الأساسية. كما أنه من الضروري أيضاً اعتماد نهج قائم على توافق الآراء.

وتود حكومة مملكة النرويج أيضاً أن تؤكد من جديد أهمية الالتزام بعملية منفتحة وشاملة وشفافة يشارك فيها أصحاب المصلحة المتعددون وتسمح لجميع الدول الأعضاء بالتفاوض بنية صادقة للتوصل إلى حلول عملية مستنيرة، والتي نعتقد أنها ستكون حجر الأساس لضمان انضمام الدول الأعضاء إلى الاتفاقية الجديدة على نطاق واسع.

**هيكل الاتفاقية**

مع أخذ نطاق الاتفاقية وأهدافها المقترحة أعلاه بعين الاعتبار، فإن الأجزاء الرئيسية من الاتفاقية باتت أمراً مسلماً به. وعلى الرغم مما سبق، سيكون من المفيد للجنة المخصصة والدول الأعضاء أن تظل منفتحة فيما يخص هيكل الاتفاقية. وبالرغم من أن الأحكام المتصلة بالتجريم والصلاحيات الإجرائية والتعاون الدولي ينبغي أن تُشكل أجزاءً محورية من الاتفاقية، فقد تُؤثر مسائل أخرى على الهيكل النهائي للاتفاقية. وتُوصي حكومة مملكة النرويج باتباع نهج منفتح فيما يخص هيكل الاتفاقية.

**حقوق الانسان**

ينطبق القانون الدولي لحقوق الإنسان على الأنشطة السيبرانية بقدر انطباقه على أي نشاط آخر. ويجب على الدول أن تمتثل لالتزاماتها في مجال حقوق الإنسان في الفضاء السيبراني كما هو الحال في العالم المادي. ويجب على الدول احترام حقوق الإنسان وحمايتها، ومن هذه الحقوق الحق في حرية التعبير والحق في الخصوصية، وغير ذلك من مبادئ حماية البيانات ذات الصلة.

ومن البديهي أن معايير حقوق الإنسان المنصوص عليها في العهد الدولي الخاص بالحقوق المدنية والسياسية تمثل إطاراً هاماً لأي أحكام جديدة تتصل بالجرائم السيبرانية. وبغض النظر عما سبق، تود حكومة مملكة النرويج أن تؤكد من جديد أهمية حقوق الإنسان في المفاوضات المقبلة، لا سيما فيما يخص الأحكام التي تتطلب تشريعات وطنية بشأن الصلاحيات الإجرائية.

## سلطنة عمان

[الأصل: بالعربية]
[18 تشرين الأول/أكتوبر 2021]

ينبغي تجريم استهداف المنشآت المدنية، لاسيما مرافق البنية التحتية الحيوية، بما في ذلك شبكات الكهرباء والمياه والمؤسسات المالية وقطاع النقل. وينبغي ألا تتحول هذه المنشآت إلى ساحات للصراع بين الدول ولتصفية الحسابات.

## بنما

[الأصل: بالإسبانية]
[28 تشرين الأول/أكتوبر 2021]

يُحتِّم التطور المستمر للتكنولوجيات على الدول أن تعتمد آليات لمنع أشكال الجريمة الجديدة ومكافحتها. وقد أدت جائحة كوفيد-19 إلى تفاقم مشكلة أصبحت بالفعل متزايدة الوضوح، وهي عدم استعدادنا بشكل كافٍ لمكافحة الجرائم السيبرانية والجرائم التي تُرتكب عبر الوسائل التكنولوجية.

ويتطلب الاستعداد لهذه المعركة، من بين أمور أخرى، التوعية بأن التحقيق في الجرائم السيبرانية والجرائم التي تُرتكب عبر الوسائل الرقمية لا يمكن فصله عن البُعد الدولي للموضوع، إذ تتأثر جميع الدول بالأنشطة الإجرامية لأولئك الذين يجدون في الفضاء العابر للحدود أرضاً خصبة لتحقيق أهدافهم غير المشروعة والإفلات من المسؤولية.

وفي ضوء الاعتبارات المذكورة أعلاه، ينبغي أن تكون الاتفاقية الدولية الشاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية أداةً لتيسير تحقيق الدول في هذه الجرائم. ولتحقيق هذه الغاية، من المهم ألا تتناول الاتفاقية الأفعال التي تؤثر بشكل مباشر على المعلومات والنظم الحاسوبية والتكنولوجيات نفسها فحسب، بل وأن تتناول الأفعال المُرتكبة باستخدام الوسائل التكنولوجية أيضاً، بغض النظر عن الحقوق المعنية المحمية قانوناً.

ونعتقد أن هذه الأداة الجديدة ينبغي أن تضع تدابير لتحسين نظم الاتصال الرسمي وغير الرسمي بين الدول من أجل الارتقاء بمستوى التحقيقات في ضوء سرعة تبخر المعلومات.

وتماشياً مع نظام الاتصال المُحسن، ينبغي تناول المفاهيم القانونية التي تحدد تدابير التحقيق مثل مصادرة البيانات والمراسلات، وحفظ البيانات، والتعامل مع الأدلة الإلكترونية.

وبينما ندرك احتمالية وجود مواقف متضاربة بشأن بعض المسائل المعينة، يظل الهدف واحداً، وهو وضع صك يسهم في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

## الاتحاد الروسي

*مذكرة من الأمانة العامة:* يرد الرد المقدم من الاتحاد الروسي في الوثيقة A/75/980، المعنونة "رسالة مؤرخة 30 تموز/يوليه 2021 موجهة إلى الأمين العام من القائم بالأعمال بالنيابة للاتحاد الروسي لدى الأمم المتحدة"، وفي مرفق تلك الرسالة المعنون "مشروع اتفاقية الأمم المتحدة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، الذي أُرسل إلى الجمعية العامة في دورتها الخامسة والسبعين. ويجري إحالته إلى اللجنة المخصصة لوضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية في إطار الآراء المقدمة من الدول الأعضاء بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها) وفق دعوة رئيس اللجنة المخصصة.

## سويسرا

[الأصل: بالإنكليزية]
[28 تشرين الأول/أكتوبر 2021]

أحدثت تكنولوجيات المعلومات والاتصالات أثراً عميقاً على مجتمعاتنا، فهي توفر فرصاً للتنمية على المستويات الاجتماعية والثقافية والاقتصادية، ولكنها تُوفر أيضاً أساساً للأنشطة ذات الأغراض الإجرامية التي تحدث في الفضاء السيبراني. ومع تزايد رقمنة عالمنا، تتزايد الجرائم السيبرانية. وبموجب القرار 74/247، شكَّلت الجمعية العامة لجنة حكومية دولية مخصصة مفتوحة العضوية لوضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. ويوجز الرد الحالي وجهة نظر سويسرا بشأن أهداف هذا الصك ونطاقه وهيكله.

**أهداف الاتفاقية**

ترى سويسرا أن الهدف العام لاتفاقية الأمم المتحدة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية هو حماية مستخدمي تكنولوجيات المعلومات والاتصالات حتى يتمكنوا من استخدامها بحرية والاستمتاع بفوائدها. والواقع أن الطابع العالمي والمفتوح لتكنولوجيات المعلومات والاتصالات إنما هو قوة دافعة لتسريع خطى التقدم على طريق التنمية الاجتماعية والاقتصادية. ولذا، يتمثل الهدف من الاتفاقية في سلامة المستخدمين، وهو ما لا ينبغي أن يعيق حريتهم في استخدام تكنولوجيات المعلومات والاتصالات. ويجب أن يكون المستخدمون قادرين على ممارسة حقوق الإنسان والحريات الأساسية الخاصة بهم على الإنترنت، ومن ثم تحقيق الإمكانات الكاملة لعالم رقمي شامل. ولذا، ينبغي أن تكون الاتفاقية خطوة إلى الأمام نحو ضمان تكنولوجيات معلومات واتصالات مجانية وموثوقة وآمنة.

وقد يساعدنا وضع اتفاقية للأمم المتحدة في بلوغ هذا الهدف العام. وفي سبيل ذلك، ينبغي أن تنص الاتفاقية على نهج منسق في مكافحة الجريمة السيبرانية. ونظراً للطابع العابر للحدود الوطنية لتكنولوجيات المعلومات والاتصالات، فمن المرجح أن تنطوي الجرائم السيبرانية على جناة وضحايا في العديد من الدول. ولذا، يُعد التعاون الدولي عاملاً أساسياً في ضمان أفضل مستوى من الحماية ضد الجرائم السيبرانية. وينبغي أن تهدف الاتفاقية إلى إرساء فهم مشترك للفعل الذي يُشكل جريمة جنائية في سياق تكنولوجيات المعلومات والاتصالات، والجرائم التي ينبغي معاقبة مرتكبيها بموجب القانون الوطني. وهذا الفهم المشترك هو اللبنة الأولى لتمكين أي نوع من أنواع التعاون. وعلى أساس هذا الفهم المشترك والمصطلحات المشتركة، ينبغي أن تهدف الاتفاقية إلى وضع إطار للتعاون الدولي الفعال لحماية مستخدمي تكنولوجيات المعلومات والاتصالات وتحقيق العدالة لضحايا الجرائم السيبرانية.

ولا يمكن تحقيق نهج منسق لمكافحة الجريمة السيبرانية على الصعيد العالمي إلا من خلال عملية شاملة. وينبغي أن تكون جميع الدول الأعضاء قادرة على المشاركة بشكل مثمر، وأن تتاح لها الفرصة لعرض آرائها حول الاتفاقية ومناقشة الآراء التي قدمتها الدول الأخرى خلال الاجتماعات الموضوعية للجنة المخصصة التي ينبغي أن تسعى جاهدة للتوصل إلى توافق في الآراء، كلما أمكن ذلك.

والجريمة السيبرانية عابرة للحدود الوطنية، ولكنها أيضاً بطبيعتها تُهم جهات فاعلة من غير الدول. وإذا أردنا اتفاقية مناسبة للغرض المقصود منها، ينبغي الإنصات لجميع الآراء أثناء عملية وضع الاتفاقية. ولا بد من إشراك جميع أصحاب المصلحة، بما في ذلك المنظمات غير الحكومية ذات الصلة ومنظمات المجتمع المدني والمؤسسات الأكاديمية والقطاع الخاص، في كل خطوة منسقة من عملية وضع الاتفاقية لضمان تحقيق الاتفاقية لأهدافها.[8]

**نطاق الاتفاقية**

ينطبق القانون الدولي على الفضاء السيبراني. ولن تخرج الاتفاقية المستقبلية إلى حيز الوجود بمعزل عن غيرها من الصكوك، ولن تنتقص من أهمية الاتفاقيات الدولية السابقة. وسويسرا مقتنعة بأن هذه الاتفاقية يجب أن تبني على النظام القانوني الحالي وأن تعززه، وينبغي تصميمها لتُكمل المبادرات التي اتخذها المجتمع الدولي بالفعل، وتستفيد من أوجه التآزر القائمة للتصدي بفعالية للجرائم السيبرانية.

وبما أن الاتفاقية ستكون معاهدة من معاهدات القانون الجنائي، ينبغي أن تستند إلى القانون الجنائي الدولي وأن تحترم أحكامه. وتوجد بالفعل أدوات عالمية للتصدي لمسألة الجريمة السيبرانية. فإلى جانب اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تُعد اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية معياراً تقوم بموجبه دول العالم، ومن بينها سويسرا، بتحديث قوانينها الخاصة بالجرائم السيبرانية. كما أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

(8) وفقاً لقرار الجمعية العامة 282/75، الفقرتان 9 و10.

تُمثل خط أساس مهماً للتعاون الدولي في عصر الإنترنت، وينبغي أن تبني اتفاقية الأمم المتحدة على هذه التجربة. وينبغي أن يسترشد عمل اللجنة المخصصة بعمل الأفرقة والمحافل الأخرى، بما في ذلك فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية.

ويجب أن تجسد الاتفاقية قانون حقوق الإنسان وأن تصونه وتعززه على نحو كاف. ولما كانت الجرائم السيبرانية تشكل تهديداً على حقوق الإنسان بالنسبة للأفراد، فإن الجهود المبذولة للتصدي لها يلزم أن تحمي تلك الحقوق، لا أن تقوضها. فالحقوق التي يتمتع بها الأفراد خارج الإنترنت يجب أن تحظى بالحماية أيضاً على الإنترنت. ويجب أن تكون التدابير المتخذة لمكافحة الجرائم السيبرانية متسقة مع القانون الدولي لحقوق الإنسان.

**هيكل الاتفاقية**

ترى سويسرا أن اتباع هيكل صكوك القانون الجنائي الدولي القائمة المُتفاوض بشأنها في سياق الأمم المتحدة هو منهج واعد وفعال لتحقيق الأهداف المذكورة أعلاه. ولذا، يمكن تنظيم الاتفاقية على النحو التالي:

(أ) الأحكام العامة؛

(ب) تدابير المنع؛

(ج) التجريم وإنفاذ القانون؛

(د) التعاون الدولي؛

(هـ) المساعدة التقنية وتبادل المعلومات؛

(و) آليات التنفيذ؛

(ز) الأحكام الختامية.

وترى سويسرا أنه لا حاجة لتكرار تناول الجرائم التي تشملها بالفعل معاهدات معينة (على سبيل المثال، الفساد والاتجار والإرهاب) لمجرد أنها قد تُرتكب (أيضاً) باستخدام تكنولوجيات المعلومات والاتصالات. وبدلاً من ذلك، ينبغي أن تُركز الاتفاقية على الجرائم الخاصة بالفضاء السيبراني، إذ إن إدراج طيف واسع من الجرائم، حتى لو ارتُكبت جميعاً باستخدام نظم حاسوبية، ينطوي على مخاطر التناقض ويجب تحاشيه.

وينبغي تقليص الجرائم المتعلقة بالمحتوى إلى الحد الأدنى، وينبغي دائماً تقييمها من حيث ما تضيفه من قيمة.

وتُشدد سويسرا على ضرورة وأهمية الضمانات الإجرائية التي تكفل شرعية وعدالة الإجراءات وحقوق الأشخاص المتضررين، لا سيما فيما يخص المساعدة القانونية المتبادلة وتبادل المعلومات وتسليم المطلوبين بمقتضى الشروط التي تقرها الدول المعنية. ويجب ضمان الحق في الخصوصية ضماناً كاملاً، وضمان مستوى مناسب من حماية البيانات الشخصية.

ويجب النظر في الظروف والضمانات الملائمة وتضمينها، لا سيما فيما يتعلق بتعزيز حقوق الإنسان والحفاظ عليها، بما في ذلك مبدأ عدم التمييز.

## تركيا

[الأصل: بالإنكليزية]
[4 تشرين الثاني/نوفمبر 2021]

تُولي تركيا أهمية قصوى للاستخدام الحر والمفتوح والآمن لتكنولوجيات المعلومات والاتصالات في شتى ربوع العالم.

ويزيد تطور تكنولوجيات المعلومات والاتصالات من مخاطر إساءة استخدامها للأغراض الإجرامية. وينبغي أن يكون القضاء على هذه المخاطر والتهديدات التي تواجه أمن مرافق البنية التحتية الحيوية والحقوق والحريات الأساسية أولوية من الأولويات القصوى على جدول الأعمال الدولي. ونظراً للطابع عبر الوطني للفضاء السيبراني، قد يصل تأثير الهجمات في هذا المجال إلى المستوى العالمي. ولن يمكن الحد من تأثير هذه الهجمات سوى من خلال التعاون الفعال على الصعيد العالمي.

وفي هذا الصدد، تُولي تركيا أهمية قصوى للتعاون الدولي الفعال من أجل فضاء سيبراني أكثر استقراراً وأماناً على الصعيد العالمي. وفي هذا الشأن، تركيا على استعداد للمساهمة في اللجنة المخصصة لوضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية ودعمها. وفي هذا السياق، نود أن نشارك وجهات نظرنا المبدئية حول نطاق الاتفاقية وأهدافها وهيكلها.

يلزم النظر في القضايا التالية في سياق الاتفاقية:

(أ) إنشاء قنوات للتعاون الفعال بين الدول؛

(ب) تعريف المسائل المتصلة بالاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات تعريفاً واضحاً؛

(ج) إنشاء قنوات اتصال في حالات الطوارئ بين الدول؛

(د) تحسين الموارد اللازمة لجمع المعلومات الاستخبارية عن التهديدات السيبرانية والحصول عليها؛

(هـ) تعزيز تبادل المعلومات الاستخبارية بين المؤسسات ذات الصلة في الدول؛

(و) تبادل المعلومات في القضايا المتصلة بالاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات؛

وبالإضافة إلى ذلك، ينبغي أن تتضمن الاتفاقية تدابير فعالة لمنع التواصل الداخلي بين المجرمين والإرهابيين وأنشطتهم الدعائية.

وقد أدت جائحة كوفيد-19 إلى زيادة استخدام الاتصالات عن بُعد زيادة كبيرة. ولذا، ينبغي أن ننظر أيضاً في آثار الجائحة على الاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات أثناء المفاوضات بشأن الاتفاقية.

وعلاوةً على ذلك، سيكون من المفيد أن ننظر ضمن نطاق الاتفاقية في الاستخدام الآمن لتكنولوجيات الجيل الجديد مثل الحوسبة السحابية والجيل الخامس وسلسلة كتل البيانات وإنترنت الأشياء والذكاء الصناعي في مكافحة الجريمة والهجمات السيبرانية.

## المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[28 تشرين الأول/أكتوبر 2021]

### نطاق الاتفاقية

تعتقد المملكة المتحدة أن الاتفاقية الدولية الجديدة لمكافحة الجريمة السيبرانية ينبغي أن تُركز على تعزيز سُبل التعاون لمواجهة التهديد المتزايد الذي يُشكله النشاط الإجرامي على المواطنين والشركات والحكومات.

وهناك عدد من المعاهدات الإقليمية والدولية القائمة المتعلقة بالجرائم السيبرانية والتي ساهمت بالفعل مساهمة ملموسة في الجهود المبذولة للتصدي للجريمة السيبرانية. ومن المهم البناء على نجاح تلك المعاهدات والاعتراف بالأحكام ذات الصلة في معاهدات العدالة الجنائية مثل اتفاقية الأمم المتحدة لمكافحة الفساد واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

وينبغي أن يشمل نطاق الاتفاقية ما يلي: (أ) التحقيق في الجرائم المحددة في الاتفاقية وملاحقة مرتكبيها؛ و(ب) تطوير القدرات والإمكانات لتمكين جميع الدول الأعضاء من التصدي لهذه الجرائم؛ و(ج) الاعتراف بمنتدى للخبراء يُمكن من خلاله كشف التهديدات الجديدة والناشئة.

وينبغي أن تتناول اتفاقية الأمم المتحدة بشأن مكافحة الجريمة السيبرانية الجرائم التي تُرتكب من خلال الفضاء السيبراني إلى جانب الجرائم التي تُيسر من خلال الفضاء السيبراني والتي يؤدي استخدام أجهزة الحاسوب فيها إلى اتساع نطاق تلك الجرائم وزيادة سرعتها ومداها. ويكون التعاون فعالاً عندما تكون الجرائم الواردة في الاتفاقية مفهومة لدى الجميع ومعترفاً بها من قبل جميع النظم القانونية.

ولا ينبغي أن تقوض الجرائم الواردة في الاتفاقية ممارسة حرية التعبير أو الرأي.

وهذه اتفاقية من اتفاقيات القانون الجنائي، ومن ثم ينبغي أن تُركز على النشاط الذي يجب أن تؤديه الإدارات الوطنية. كما ينبغي أن تنظر الاتفاقية في آلية للتعاون فيما بين المواطنين والمنظمات غير الحكومية ومنظمات المجتمع المدني والمؤسسات الأكاديمية والقطاع الخاص، وفق نهج متعدد أصحاب المصلحة، لحماية أنفسهم من الجرائم السيبرانية.

ويجب أن تتضمن أي اتفاقية ضمانات قوية تشمل احترام الخصوصية وحقوق الإنسان الأخرى، على النحو المنصوص عليه في القانون الدولي لحقوق الإنسان والمعترف به في القرارات ذات الصلة الصادرة عن الجمعية العامة ومجلس حقوق الإنسان.

ويجب صياغة الاتفاقية بطريقة شاملة وشفافة تحترم آراء جميع الدول الأعضاء وبمشاركة نشطة من جانب مجموعة واسعة من أصحاب المصلحة، بما في ذلك المنظمات غير الحكومية ومنظمات المجتمع المدني والمؤسسات الأكاديمية والقطاع الخاص. وعلاوةً على ذلك، ينبغي أن تشجع أحكام الاتفاقية، ومنها على سبيل المثال تلك المتعلقة بالتنفيذ وبناء القدرات، على اتباع نهج شامل للجميع وشفاف للتصدي للجرائم السيبرانية.

وينبغي صياغة الاتفاقية بلغة محايدة من الناحية التكنولوجية لضمان صمودها أمام تحدي الزمن وعدم احتياجها إلى تحديث مستمر.

وينبغي ألا تكرر الاتفاقية العمل الذي نُفذ بالفعل أو المفترض تنفيذه على نحو وافٍ بموجب الصكوك والاتفاقيات الأخرى. وينبغي ألا تمتد الاتفاقية لتشمل مسائل الأمن السيبراني، التي تناولتها بالفعل اللجنة الأولى للجمعية العامة، أو مسائل حوكمة الإنترنت، والتي تناولتها بالفعل محافل مخصصة متعددة أصحاب المصلحة.

**أهداف الاتفاقية**

ينبغي أن يكون الغرض الأساسي من الاتفاقية هو دعم التعاون الفعال بين أجهزة إنفاذ القانون والنيابة العامة الوطنية، على الصعيد الثنائي أو المتعدد الأطراف، في التحقيق في الجرائم المنصوص عليها في الاتفاقية وملاحقة مرتكبيها. ومن شأن وضع اتفاقية تحظى بتأييد واسع النطاق أن يتيح أوسع نطاق ممكن من التعاون الدولي.

ومن أجل دعم التعاون المتبادل الفعال، يجب توفر خيارات للرفض على أساس التجريم المزدوج، والرفض فيما يخص الجرائم السياسية، لا سيما عندما تتصل الجريمة المزعومة بممارسة حرية التعبير، ورفض طلب مُقدم لغرض معاقبة أو اضطهاد الشخص على أساس العرق أو الدين أو الجنس أو غيرها من الخصائص المحمية. وقد يكون من المفيد وجود حد أدنى من المعايير يجب أن تؤكد السلطة الطالبة أنها قد استوفته، مثل أن يكون الطلب ضرورياً ومتناسباً ومقيداً بفترة زمنية ومسموحاً به على مستوى معين.

ويجب أن يخضع استخدام الصلاحيات المُخولة للتحقيق في الجرائم المنصوص عليها في الاتفاقية وملاحقة مرتكبيها، بما في ذلك تلك المستخدمة في الحالات الثنائية أو المتعددة الأطراف، لضمانات فعالة فيما يخص حقوق الإنسان والحريات الأساسية، على النحو المنصوص عليه في القانون الدولي لحقوق الإنسان.

ويجب أن تعترف الاتفاقية بالاستقلال العملياتي لأجهزة التحقيق والنيابة العامة الوطنية، وأن قرار التدخل واتخاذ أية إجراءات يقع على عاتق تلك الأجهزة وحدها دون سواها.

وينبغي أن تدعم الاتفاقية تطوير القدرات على الصعيد العالمي، وأن تدعم بناء القدرات.

ومن المتوقع أن تتغير أشكال وأنماط التهديدات الناجمة عن النشاط الإجرامي في الفضاء السيبراني. ولذا، ينبغي أن تنشئ الاتفاقية عملية حكومية دولية ومتعددة أصحاب المصلحة لتحديد التهديدات المستقبلية، دون المساس بما إذا كانت هذه العملية تُشكل جزءاً من الاتفاقية أم لا.

وبالنظر إلى اختلاف التأثير الناجم على الجرائم السيبرانية باختلاف نوع الجنس، ينبغي أن تكون الاتفاقية شاملة للجنسين من أجل مساعدتنا في التصدي للجرائم السيبرانية على نحو أكثر فعالية. ومن شأن وضع اتفاقية تراعي الآثار الجنسانية المترتبة على أحكامها أن تشجع المزيد من النساء على المشاركة على جميع المستويات وفي جميع العمليات. وسيُثمر ذلك عن حلول أكثر تنوعاً وثراءً وأفضل في نهاية المطاف. وفي اجتماع فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية المنعقد في نيسان/أبريل 2021، اتفقت جميع الدول الأعضاء على أنه حري بها أن تعزز، على وجه الخصوص، مشاركة الخبيرات.

وينبغي أن تعزز الاتفاقية نهج "شامل للمجتمع بأسره" للتصدي للجرائم السيبرانية، وأن تشجع الدول الأعضاء على التعاون مع الجهات الفاعلة غير الحكومية، بما في ذلك الخبراء والصناعات والجمهور، في مجالات مثل التوعية وتحسين التعليم والتدريب على الشؤون الجنسانية وعلى مكافحة الجرائم السيبرانية، ومساندة الضحايا.

**هيكل الاتفاقية**

تعتقد المملكة المتحدة أن الهيكل التالي سيكون وسيلة فعالة لتنظيم الاتفاقية:

(أ) أحكام عامة

ينبغي أن تتضمن الأحكام العامة الأساس الذي تنبني عليه الاتفاقية والغرض المقصود منها، والتعاريف التي ستُستخدم فيها. ويجب أن تكون التعاريف مفهومة ومتفقاً عليها بشكل عام من قبل جميع الأطراف، وأن تكون محايدة من الناحية التكنولوجية، مع مراعاة المصطلحات المُجمع عليها في الصكوك الإقليمية والمستخدمة في أطر العمل القانونية الوطنية؛

(ب) الجرائم الأساسية

يجب أن تشمل الجرائم الأساسية الجرائم التي تُرتكب من خلال الفضاء السيبراني (مثل الوصول غير القانوني للمعلومات)، مع وضع أوصاف وتعاريف مقبولة لجميع الأطراف. وينبغي إدراج الجرائم التي تُيسر من خلال الفضاء السيبراني (مثل الاستغلال الجنسي للأطفال والتحرش بهم أو الاحتيال) متى كانت الجريمة تُرتكب بشكل أساسي عبر الإنترنت وكانت الحواسيب تُغير من حجم الجريمة وسرعتها ومتى كانت تعريفات الجريمة مفهومة لدى الجميع؛

(ج) حقوق الإنسان والضمانات

يجب أن يكون إعمال الاتفاقية وتنفيذها مدعومين بضمانات إجرائية ذات مغزى وسبل حماية متينة لحقوق الإنسان، ومرجعية للقانون الدولي لحقوق الإنسان؛

(د) التدابير الوقائية

كما هو الحال مع اتفاقية مكافحة الفساد واتفاقية الجريمة المنظمة عبر الوطنية، ينبغي أن تنص الاتفاقية على أحكام تحث الدول على تنفيذ تدابير لمنع الجريمة السيبرانية، بما في ذلك من خلال العمل مع جميع أصحاب المصلحة؛

(هـ) أحكام القانون الإجرائي

يجب أن تسمح صلاحيات دعم التحقيقات والملاحقة للسلطات المختصة بالحفاظ على الأدلة الإلكترونية والبحث عنها ومصادرتها فيما يخص أي جريمة تُرتكب باستخدام الحاسوب أو متى كانت الأدلة المتصلة بجريمة ما في شكل إلكتروني، وذلك بالنسبة للتحقيقات المحلية والدولية على حد سواء؛

(و) التعاون الدولي

يجب أن تشمل أحكام التعاون الدولي المساعدة القانونية المتبادلة والمساعدة في حالات الطوارئ، بما في ذلك مطالبة الدول بتوفير جهات اتصال على مدار الساعة وطوال أيام الأسبوع. وإلى جانب التبادل العملي للأدلة، أوضحت التوصيات التي قدمها فريق الخبراء في نيسان/أبريل 2021 رغبة الدول الأعضاء في مواصلة تبادل الخبرات وأفضل الممارسات، فضلاً عن المعلومات المتصلة بالتهديدات الجديدة والمتنامية؛

(ز) المساعدة التقنية وبناء القدرات

ينبغي تشجيع بناء القدرات، مع اضطلاع مكتب الأمم المتحدة المعني بالمخدرات والجريمة بدور محوري في هذا الصدد، وينبغي تنسيق هذا العمل من خلال الهياكل القائمة مثل المنتدى العالمي للخبرة السيبرانية. وتلاحظ المملكة المتحدة العدد الكبير من التوصيات التي اتفق عليها فريق الخبراء في نيسان/أبريل 2021 والتي ركزت على بناء القدرات، بما في ذلك توفير تدريب متخصص ومُحدث للممارسين على التحقيق في الجرائم السيبرانية، والتعامل مع الأدلة الإلكترونية، وسلسلة العهدة، والتحليل الجنائي؛

(ح) التنفيذ

ينبغي وضع خطة واضحة لتنفيذ الاتفاقية.

## الولايات المتحدة الأمريكية

[الأصل: بالإنكليزية]
[28 تشرين الأول/أكتوبر 2021]

يسر حكومة الولايات المتحدة الأمريكية أن تستجيب للدعوة الموجهة إلى الدول الأعضاء لتقديم آرائها بشأن نطاق الاتفاقية الجديدة وأهدافها وهيكلها (عناصرها)، فيما يخص تنفيذ قراري الجمعية العامة 74/247 و75/282. وتتطلع الولايات المتحدة إلى العمل مع الدول الأعضاء الأخرى وأصحاب المصلحة المعنيين لصياغة صك عالمي يُركز على تحسين التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها، بما يتفق مع الحقوق والالتزامات القائمة ويبني عليها. وتؤكد الولايات المتحدة مجدداً أهمية الالتزام بعملية منفتحة وشاملة وشفافة يشارك فيها أصحاب المصلحة المتعددون وتسمح لجميع الدول الأعضاء بالتفاوض بنية صادقة للتوصل إلى حلول عملية مستنيرة وقائمة على توافق الآراء، والتي نعتقد أنها ستشجع الكثير من الدول على الانضمام إلى صك عالمي جديد لمكافحة الجرائم السيبرانية.

ومن شأن الموعد النهائي المقترح لعملنا أن يجعل الجدول الزمني مضغوطاً حتى في الظروف العادية، ولكننا سنبذل جهودنا في ظل الجائحة العالمية الحالية. ولذا، من الضروري للغاية أن نكون مُركزين وفعالين في جهودنا للتفاوض بشأن صك عالمي لمكافحة الجريمة السيبرانية. وللأسف، في الوقت الذي انشغل فيه معظم العالم بمكافحة جائحة كوفيد-19، استغل المجرمون السيبرانيون التحول العالمي للاعتماد على التكنولوجيات الرقمية. وتُمثل الجريمة السيبرانية تهديداً مباشراً لسلامة ورفاه المجتمعات والأشخاص في العالم بأسره. وهناك تعاون منذ وقت طويل من أجل بناء قدرتنا الجماعية على مكافحة هذا الاستغلال، ويمكننا مواصلة البناء على تلك النجاحات مع دراسة الحلول العملية دراسة متأنية. وبالنظر إلى الطابع الملح للتهديد الذي تُشكله الجريمة السيبرانية، فمن الضروري أن نتحلى بالتركيز والتأني في جهودنا للتفاوض بشأن صك عالمي لمكافحة الجريمة السيبرانية.

وينبغي أن يهدف صك مكافحة الجريمة السيبرانية الجديد إلى تعزيز التعاون الدولي، وتوفير الأدوات العملية لتجهيز أجهزة إنفاذ القانون الوطنية للتصدي لتلك الجرائم على غرار ما فعلته صكوك الأمم المتحدة الأخرى فيما يتعلق بالأشكال الأخرى للجريمة عبر الوطنية، بما في ذلك الفساد والاتجار بالمخدرات والاتجار بالبشر وتهريب المهاجرين. كما ينبغي أن يضمن الصك صلاحيات محلية لجمع الأدلة الإلكترونية المتصلة بأي نوع من الجرائم والحصول عليها، وليس فقط الجرائم التي تُرتكب من خلال الفضاء السيبراني، وتعزيز التعاون الدولي في هذه الحالات. وكما هو الحال مع جميع صكوك الأمم المتحدة المعنية بمكافحة الجريمة، ينبغي أن تتضمن تلك الأدوات حدوداً وضمانات مناسبة، في سياق أطر العمل المحلية القائمة، لمراعاة الخصوصية والحريات المدنية والاحترام الكامل لحقوق الإنسان. كما ينبغي أن يتناول صك مكافحة الجريمة السيبرانية الحاجة المتزايدة إلى المساعدة التقنية وأن يُوفر سبلاً تلتمس من خلالها الدول الأعضاء هذه المساعدة.

وبينما تشرع الدول الأعضاء في عملية الصياغة، من الضروري إدراك أننا لا نفعل ذلك بمعزل عن الظروف المحيطة. وبالرغم من أهمية تحديد الجوانب التي ينبغي أن يتناولها هذا الصك، فإن المهم أيضاً تحديد الجوانب التي تقع خارج نطاقه الصحيح. وتضطلع الأمم المتحدة وغيرها من المنتديات الحكومية الدولية والمتعددة أصحاب المصلحة بعمل مستمر وقيّم بشأن المسائل السيبرانية الأخرى التي تتجاوز نطاق الجريمة السيبرانية. ومن المهم ألا نكرر هذا العمل أو نقوضه، وذلك لتجنب تضارب الالتزامات وحتى لا ننحرف عن هدفنا المتمثل في استحداث صك مُحدد الأهداف وعملي لمكافحة الجريمة السيبرانية. وستفضي محاولة تناول جميع المسائل المتصلة بالفضاء السيبراني في هذا الصك المعني بالعدالة الجنائية إلى المخاطرة بإغراق هذه المفاوضات في مناقشات غير مركزة وعرضية لن تحقق نفعاً يُذكر لمكافحة الجريمة السيبرانية وستؤدي فقط إلى إبطاء تقدمنا صوب وضع صك مفيد.

وعلى وجه الخصوص، ينبغي للدول الأعضاء ألا تخوض في موضوعات الحوكمة السيبرانية أو الأمن السيبراني واسعة النطاق في صك معني بالجريمة ومخصص لمكافحة الجريمة السيبرانية. وبالرغم من أنه غالباً ما يُنظر إلى إنفاذ القانون فيما يتعلق بالجرائم السيبرانية والأمن السيبراني باعتبارهما وجهان لعملة واحدة، إلا أن إنفاذ القانون في الأساس مسؤولية حكومية، بينما الأمن السيبراني مسؤولية مجموعة من الجهات الفاعلة العامة والخاصة. وتركز ولاية اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية على وضع صك عدالة جنائية بشأن المسائل الجنائية لتيسير التصدي الدولي للجريمة السيبرانية، وهو ما ينطوي على تعريف السلوك الإجرامي في الفضاء السيبراني وتحديد عقوبات لمرتكبيه. واللجنة المخصصة غير مخولة بإملاء معايير عالمية للسلوك غير الإجرامي عبر الإنترنت. ولن يفي إدراج مفاهيم الحوكمة السيبرانية والأمن السيبراني في اتفاقية تُعنى بمكافحة الجريمة السيبرانية بالهدف المتمثل في وضع صك مبسط وفعال ينال دعماً وتأييداً واسعين من الدول الأعضاء.

وكما شدد قرار الجمعية العامة 75/282، من الضروري ألا تعيق المفاوضات الرامية إلى وضع صك جديد لمكافحة الجريمة السيبرانية الآليات القائمة، بما في ذلك الصكوك المتعددة الجنسيات والإقليمية التي توفر بالفعل مجموعة من الأدوات لمكافحة الجريمة السيبرانية بشكل فعال. والطريقة المثلى التي يُمكننا من خلالها أن نبني توافقاً في الآراء بشأن هذا الصك الجديد وتجنب القضايا السياسية والمثيرة للانقسام هي الاستفادة من الصكوك القائمة التي برهنت على نجاحها. وينبغي أن نسترشد بالإنجازات التي تحققت في تنفيذ معاهدات الأمم المتحدة الأخرى المعنية بالعدالة الجنائية، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي أثبتت أنها في غاية النفع لأنها تستهدف الأنواع الأساسية من أنشطة الجريمة المنظمة، وفي الوقت ذاته تتضمن أحكاماً عامة للتعاون الدولي يمكن تطبيقها على أي نوع من الجرائم الخطيرة التي يرتكبها ثلاثة أشخاص أو أكثر طلباً للربح غير المشروع. ولذا، استخدمت الدول الأطراف هذه الاتفاقية بنجاح آلاف المرات في أغراض تشمل مكافحة الجرائم مثل حوادث فيروسات الفدية والاستغلال الجنسي للأطفال.

وتؤكد الولايات المتحدة مجدداً على أهمية الالتزام بعملية منفتحة وشاملة وشفافة تسمح لجميع الدول الأعضاء وأصحاب المصلحة المهتمين بالتفاوض بنية صادقة للتوصل إلى حلول عملية مستنيرة وقائمة على توافق الآراء، والتي نعتقد أنها أفضل سبيل لتشجيع الكثير من الدول على الانضمام إلى صك عالمي جديد لمكافحة الجريمة السيبرانية.

**تجريم الجرائم السيبرانية الأساسية**

في المقام الأول، ينبغي لأي صك جديد أن يكفل صلاحيات محلية لجمع الأدلة الإلكترونية المتصلة بأي نوع من الجرائم والحصول عليها. وهذه الصلاحيات ضرورية للدول لتمكينها من التحقيق بشكل فعال في جميع أنواع الجرائم تقريباً وملاحقة مرتكبيها، إذ إن عدد الجرائم التي تُرتكب في عصرنا الحالي خارج العالم الرقمي بالكامل قليل للغاية. وينبغي أن يتيح الصك أيضاً التعاون الدولي في تبادل الأدلة الإلكترونية المتصلة بأي نوع من أنواع الجرائم، رهناً بإدراج نص مرن بشأن ازدواجية التجريم على النحو الوارد في اتفاقية مكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد.[9]

وبالإضافة إلى ذلك، يتطلب التعاون الدولي الفعال أن تضع الدول الأعضاء تشريعات محلية كافية تُجرم الجرائم السيبرانية الأساسية. ويُعد وجود فهم مشترك للجرائم الأساسية ودعم الصلاحية الإجرائية بين الدول

(9) انظر الفقرة 9 من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والفقرة 9 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد. وبالرغم من أن الأحكام الواردة في الاتفاقيتين مختلفة إلى حد ما، توفر المادتان سلطة تقديرية واسعة للدول الأطراف المطلوب منها تقديم المساعدة، لاسيما فيما يخص التدابير القسرية.

الأعضاء ضرورة لتجنب إنشاء ملاذات آمنة للمجرمين السيبرانيين. وتُظهر الدراسات التي أجراها مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن الدول تتفق بصفة عامة على السلوك الأساسي الذي ينبغي تجريمه بموجب قوانين الجرائم السيبرانية المحددة، مع وجود العديد من الاتفاقيات المتعددة الجنسيات والقوانين الجنائية الوطنية التي تتضمن أحكاماً مشتركة. وبالمثل، هناك فهم دولي لأنواع الصلاحيات الإجرائية القانونية لدعم التحقيق الفعال في الجرائم السيبرانية. ونتيجة لذلك، يمتلك الممارسون خبرة متراكمة ومتنوعة ممتدة على مدار عقدين من الزمن في مجال التحقيق في الجرائم السيبرانية تُثبت استمرار جدوى أنواع الصلاحيات الموضوعية والإجرائية الشائعة في التحقيق في الجرائم السيبرانية.

ويجب أن يُعرف الصك الجديد لمكافحة الجريمة السيبرانية الجرائم التي تُرتكب من خلال الفضاء السيبراني وأن ينطبق عليها، وهي الجرائم التي تكون فيها الحواسيب أو البيانات أهدافاً للنشاط الإجرامي، بالإضافة إلى مجموعة معينة من الجرائم التي تُيسر من خلال الفضاء السيبراني، أي الجرائم التي تُستخدم فيها الحواسيب لتسهيل ارتكاب الجريمة. وتشمل الفئة الأولى والأساسية من الجرائم المراد تعريفها في الصك الجديد تلك التي يتعذر ارتكابها دون إساءة استخدام الحواسيب أو النظم الشبكية، ومن ثم فهي لم تكن موجودة كجرائم قبل ظهور النظم الحاسوبية. وقد تقع الجرائم التي تُرتكب من خلال الفضاء السيبراني بالكامل داخل العالم الرقمي. وبالنسبة للجرائم التي تُرتكب من خلال الفضاء السيبراني، مثل هجمات حجب الخدمات أو إتلاف الحواسيب والبيانات، يلزم اشتراع قوانين سيبرانية خاصة نظراً لأن معظم الولايات القضائية تُفسر القوانين الجنائية بشكل صارم، في حين أن القوانين التقليدية التي تتناول المفاهيم المألوفة، مثل التعدي على ممتلكات الغير والتخريب المتعمد، غالباً ما تكون غير كافية لتطبيقها على الجرائم السيبرانية. وعلاوةً على ذلك، فإن بعض أحكام القانون الجنائي التي تنطبق على الجرائم المرتكبة خارج الشبكة الحاسوبية قد تنطبق بسهولة على الجرائم المُرتكبة باستخدام الحواسيب.

وفي المقابل، ينبغي أن نحرص على عدم التعامل مع الجرائم التقليدية على أنها "جرائم سيبرانية" لمجرد استخدام مرتكبيها للحواسيب في تخطيط جرائمهم أو تنفيذها. فبالرغم من إساءة استخدام الحواسيب لارتكاب الجريمة، قد تتناول القوانين العامة بعض السلوكيات غير المشروعة لأنه لا يوجد شيء غريب أو فريد في استخدام نظام حاسوبي في هذا السلوك. وعلى النقيض، سيُسهم صك مكافحة الجرائم السيبرانية في التعامل مع بعض الجرائم التي تُيسر من خلال الفضاء السيبراني تعاملاً ملائماً، على سبيل المثال، عندما يزيد استخدام الحواسيب من:

(أ) نطاق الجريمة، على سبيل المثال، من خلال إشراك آلاف الضحايا أو سرقة ملايين من سجلات بيانات الدفع؛

(ب) أو سرعة الهجوم لأن الحاسوب يزيد بشكل كبير من القدرة على ارتكاب الجريمة؛

(ج) أو حجم الضرر أو الإصابة التي لحقت بالضحايا؛

(د) أو إخفاء هوية الجاني.

وعند تطبيق هذه المفاهيم، قد تكون هناك أسباب وجيهة لاعتبار بعض حالات الجرائم التقليدية، مثل الاحتيال والاستغلال الجنسي للأطفال، ضمن نطاق هذه المفاوضات. ومع ذلك، ينبغي للدول الأعضاء أن تتحلى بالحكمة في تحديد نطاق الجرائم التي تُيسر من خلال الفضاء السيبراني التي نسعى لتناولها حتى لا نشوه مفاهيم العدالة الجنائية الراسخة، وحتى لا تفقد القوانين والصكوك الجنائية القائمة منذ أمد طويل إمكانية تطبيقها لمجرد أن الجريمة تنطوي على عنصر "سيبراني".

كما ينبغي أن يدعو الصك العالمي لمكافحة الجرائم السيبرانية الأطراف إلى سن تشريعات تُجرم الجرائم السيبرانية الأساسية بطريقة محايدة من الناحية التكنولوجية، مع كفالة الضمانات الإجرائية. ويضمن تجريم الجرائم بطريقة محايدة من الناحية التكنولوجية (أي تجريم النشاط الذي يؤثر على سرية بيانات حاسوبية وسلامتها وتوفرها

بدلاً من تجريم الشكل أو الطريقة المعينة المستخدمة، مثل التصيد الاحتيالي أو فيروسات الفدية) أن الأحكام الجنائية الموضوعية لا تتناول التكنولوجيات والتقنيات الإجرامية في الوقت الحاضر فحسب، وإنما تشمل التكنولوجيات والتقنيات الإجرامية في المستقبل أيضاً. ولتوضيح مدى سرعة تطور التكنولوجيا، لم يتضمن مشروع الدراسة الشاملة حول الجرائم السيبرانية لعام 2013، على الرغم من العزم الواضح على أن تكون الدراسة شاملة، تفاصيل حول التكنولوجيات أو التقنيات التي لم تكن شائعة الاستخدام أو التي كانت ناشئة للتو في وقت الدراسة، بما في ذلك فيروسات الفدية وإنترنت الأشياء والعملات المشفرة والتطور السريع لتكنولوجيا الهواتف المحمولة وهيمنتها. وتعبيراً عن هذا الشاغل، كان من بين الاستنتاجات والتوصيات التي اتفقت عليها الدول الأعضاء في اجتماع فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية أنه ينبغي للدول الأعضاء أن تضمن أن أحكامها التشريعية تصمد أمام تحدي الزمن فيما يخص التطورات المستقبلية في التكنولوجيات من خلال سن قوانين بصيغ محايدة من الناحية التكنولوجية وتجريم النشاط الذي يعد غير قانوني بدلاً من الوسائل المستخدمة لارتكاب هذا النشاط.[10] وهذا أمر مهم على وجه الخصوص لأننا نحاول صياغة صك دائم قادر على التعامل بشكل مناسب مع تكنولوجيات الغد ويفي باحتياجات الممارسين في مجال إنفاذ القانون في الحاضر والمستقبل.

ومع مراعاة هذه المبادئ، ينبغي أن يتضمن الصك العالمي لمكافحة الجريمة السيبرانية تجريم الأنشطة التالية:

(أ) الوصول غير المشروع إلى البيانات، أي الوصول إلى حاسوب أو نظام حاسوبي دون الحصول على تصريح بذلك؛

(ب) الاعتراض غير المشروع للبيانات، أي الاعتراض غير القانوني في الوقت الحقيقي لمحتوى الاتصالات أو بيانات الحركة المتعلقة بالاتصالات؛

(ج) التدخل في البيانات أو النظم الرقمية، أي البرمجيات الخبيثة وهجمات حجب الخدمات وفيروسات الفدية وحذف البيانات أو تعديلها؛

(د) إساءة استخدام الأجهزة، أي استخدام بيانات بطاقات الائتمان وكلمات المرور والمعلومات الشخصية التي تسمح بالوصول إلى الموارد، أو الاتجار بها؛

(هـ) الجرائم المتعلقة بالمواد المرتبطة بالاستغلال الجنسي للأطفال؛

(و) الجرائم المتصلة بالاحتيال الميسر من خلال الحاسوب، أي التلاعب بالأنظمة الحاسوبية أو البيانات لأغراض احتيالية مثل التصيد الاحتيالي وتعريض رسائل البريد الإلكتروني التجارية للخطر والاحتيال في المزادات؛

(ز) الجرائم المتعلقة بالتعدي على حقوق النسخ والحقوق ذات الصلة؛

(ح) أحكام تتناول محاولة ارتكاب الجريمة والمساعدة فيها والتحريض عليها والتآمر لتنفيذها.

علاوةً على ذلك، ينبغي تجريم غسل العائدات المُتأتية من الجرائم السيبرانية. وختاماً، يجب أن يخضع الأشخاص الاعتباريون لعقوبات جنائية أو مدنية وإدارية في حالة التورط في الجرائم السيبرانية التي يحظرها الصك.

(10) انظر تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية المنعقد في فيينا في الفترة من 6 إلى 8 نيسان/أبريل 2021 (UNODC/CCPCJ/EG.4/2021/2).

**السلطة الإجرائية لجمع الأدلة الإلكترونية وتبادلها**

بالإضافة إلى تجريم الجرائم الأساسية، ينبغي أن يتناول الصك العالمي لمكافحة الجريمة السيبرانية حاجة السلطات القانونية المحلية إلى حفظ الأدلة الإلكترونية وجمعها وتبادلها، بما يتفق مع الأصول القانونية وحماية حقوق الإنسان والحريات الأساسية. وقد لاحظت بعض الدول الأعضاء أنه، بموجب قوانينها المحلية، قد لا تكون المصادر التقليدية للسلطة الإجرائية قابلة للتطبيق على البيانات غير الملموسة أو قد لا تجيز جمع الأدلة الإلكترونية السريعة الزوال بسرعة كافية. وكما هو الحال دائماً، لن تكفي القوانين المتقادمة لمواجهة التحديات العديدة المتصلة بالتحقيق في الجرائم السيبرانية، بما في ذلك التعامل مع التكنولوجيات الجديدة مثل التشفير الواسع النطاق وخدمات الحوسبة السحابية. ولذا، من الضروري وجود مصادر متخصصة للسلطة الإجرائية لجمع الأدلة الإلكترونية. وينبغي صياغة هذه القوانين مع مراعاة المفاهيم التقنية المعمول بها، وكذلك الاحتياجات العملية للمحققين الجنائيين. وبمزيد من التحديد، ينبغي أن تسمح مصادر السلطة الإجرائية هذه بما يلي:

(أ) التعجيل في حفظ البيانات الحاسوبية المُخزنة؛

(ب) أوامر توفير البيانات الحاسوبية؛

(ج) البحث عن بيانات حاسوبية مُخزنة ومصادرتها؛

(د) جمع بيانات الحركة الحاسوبية في الوقت الحقيقي؛

(هـ) جمع بيانات المحتوى الحاسوبي في الوقت الحقيقي في حالات الجرائم الخطيرة.

وبالإضافة إلى ذلك، ينبغي أن يسمح الصك الجديد بالتعاون في جمع الأدلة الإلكترونية والحصول عليها فيما يتعلق بأي نوع من الجرائم، وليس الجرائم السيبرانية فحسب. وتشتمل جميع الجرائم الجنائية الخطيرة تقريباً على أدلة إلكترونية، سواءً في شكل بيانات على الهاتف المحمول أو البريد الإلكتروني أو بيانات المعاملات أو غيرها من البيانات، ذات صلة بالتحقيق في الجرائم وملاحقة مرتكبيها. وكشأن محلي، تحتاج الدول الأعضاء إلى إطار حديث للإثبات القانوني يُجيز قبول الأدلة الإلكترونية في التحقيقات والملاحقات الجنائية، بما في ذلك تبادل الأدلة الإلكترونية مع شركاء إنفاذ القانون على الصعيد الدولي.

**التعاون الدولي**

إلى جانب القوانين المحلية، يعتمد التعاون الدولي الفعال في مجال الجرائم السيبرانية على التعاون الرسمي القائم على المعاهدات، مثل المساعدة القانونية المتبادلة، وسبل التعاون الأخرى، مثل التعاون التقليدي المباشر بين أجهزة الشرطة المأذون به. وينبغي أن يعتمد الصك الجديد لمكافحة الجريمة السيبرانية على أدوات فعالة لزيادة التعاون الدولي المستند إلى المعاهدات القائمة، وأن يكفل عدم تقويض الصكوك القائمة والتعاون الدولي الجاري في مجال مكافحة الجريمة السيبرانية على الصعيد العالمي. وينبغي أن تمتثل أحكام الصك المعني بمكافحة الجرائم السيبرانية المتصلة بالتعاون الدولي، بما في ذلك الأحكام الخاصة بالمساعدة القانونية المتبادلة، وتسليم المطلوبين، ونقل إجراءات الملاحقة، ومصادرة العائدات، بما في ذلك العملات الافتراضية، ورد الموجودات المصادرة إلى الضحايا، وازدواجية التجريم، والتعاون في مجال إنفاذ القانون، امتثالاً صارماً لأحكام اتفاقية مكافحة الجريمة المنظمة عبر الوطنية واتفاقية مكافحة الفساد، بما في ذلك الضمانات وتدابير الحماية المناسبة الواردة فيهما، والتي نفذتها بنجاح الغالبية العظمى من الدول الأعضاء. وبالإضافة إلى ذلك، ينبغي أن ينص الحكم المتصل بالمساعدة القانونية المتبادلة على تقديم مساعدة واسعة في الحصول على الأدلة الإلكترونية المتعلقة بجريمة جنائية، سواءً ارتُكبت الجريمة باستخدام نظام حاسوبي أو بغيره.

**المساعدة التقنية وبناء القدرات**

تشير دراسات مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن أكثر من 75 في المائة من الدول لديها وحدة مخصصة للقضايا المتصلة بالجرائم السيبرانية ضمن أجهزة إنفاذ القانون القائمة، وأن حوالي 15 في المائة لديها جهاز متخصص خاص بالجرائم السيبرانية. وهذا يؤكد الطابع المتخصص للتحقيقات في الجرائم السيبرانية، بما في ذلك الحاجة إلى التدريب المتخصص. وعلاوةً على ذلك، تزايد مستوى تعقيد الجرائم السيبرانية والعناصر الإلكترونية أو الرقمية الداخلة في الجرائم التقليدية تزايداً كبيراً، مما أدى إلى تزايد الطلب على تدريب محققين وخبراء تقنيين متمرسين والحفاظ عليهم.

ونقص القدرات المحلية هو السبب الأكثر شيوعاً لعجز الدول عن التعاون بفعالية على المستوى الدولي. وبالنسبة لمعظم الدول، لا يفشل التعاون الدولي بسبب الافتقار إلى الإرادة، ولكن بسبب القيود سواءً في القانون المحلي أو نتيجة لقصور خبرة أجهزة إنفاذ القانون. ولا تتوفر لدى العديد من الدول الأعضاء موارد كافية فيما يتعلق بقدرة سلطات إنفاذ القانون على مكافحة الجريمة السيبرانية أو التعامل مع الأدلة الإلكترونية. فعلى سبيل المثال، في ضوء الأولويات الوطنية الحالية، تُواجه بعض الدول الأعضاء تحديات في تطوير قدرات المحققين المدربين والمحققين العدليين والاحتفاظ بهم، وكذلك في التعامل مع النقص في الأجهزة والبرمجيات الحاسوبية. وعليه، هناك إجماع دولي واسع النطاق على أن المساعدة التقنية وبناء القدرات لمؤسسات إنفاذ القانون، بما في ذلك المحققون والمدعون العامون والقضاة، لا تزال المتطلبات الأكثر إلحاحاً للاستجابة الدولية الفعالة للجرائم السيبرانية. وعلاوةً على ذلك، ونظراً لأن الأدلة الإلكترونية أصبحت عنصراً في كل نوع من أنواع الجرائم تقريباً، سوف يحتاج حتى ضباط إنفاذ القانون غير المتخصصين إلى امتلاك فهم أساسي للتحقيقات المتعلقة بالنظم الحاسوبية.

وينبغي أن تتضمن أحكام الصك المعني بمكافحة الجرائم السيبرانية المتصلة بالمساعدة التقنية وبناء القدرات الجوانب التالية:

(أ) التدابير التي تتخذها الدول الأعضاء لإطلاق البرامج التدريبية أو تطويرها أو تحسينها لموظفيها المسؤولين عن منع الجريمة السيبرانية ومكافحتها؛

(ب) قيام الدول الأعضاء، حسب قدراتهم، بالنظر في تزويد بعضها البعض بأكبر قدر من المساعدة التقنية، لاسيما لصالح الدول النامية والدول التي قد تواجه تهديدات الجريمة السيبرانية على نحو غير متكافئ، في خططها وبرامجها لمكافحة الجريمة السيبرانية؛

(ج) وضع آليات يمكن من خلالها للتبرعات المالية من الدول الأعضاء أن تدعم تنفيذ صك خاص بمكافحة جرائم الفضاء السيبراني؛

(د) قيام الدول الأعضاء بالنظر في تقديم تبرعات إلى البرنامج العالمي لمكافحة الجريمة السيبرانية التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة وما يتصل به من جهود لبناء القدرات في مجال العدالة الجنائية.

**مشاركة المجتمع والكيانات والمنظمات**

لا يمكن أن تكون مكافحة الجرائم السيبرانية جهداً منفرداً نظراً لتعقيد المشكلة وطابعها المتعدد الأوجه. وينبغي أن يراعي الصك المعني بمكافحة الجريمة السيبرانية أهمية المشاركة النشطة للأفراد والجماعات، مع إيلاء الاعتبار الواجب للمساواة بين الجنسين، مثل المنظمات غير الحكومية ومنظمات المجتمع المدني والمؤسسات الأكاديمية والقطاع الخاص، في منع الجريمة السيبرانية. ويمكن أن تؤدي هذه المشاركة إلى زيادة الوعي العام بشأن تهديدات الجريمة السيبرانية، والتأكد من أن عمل الدول الأعضاء يتم بطريقة شفافة ويتناول المسائل الجوهرية

المتعلقة بالخصوصية والحريات المدنية وحقوق الإنسان. وعلاوةً على ذلك، يعتمد الصك الفعال على مساهمات الأفراد والكيانات من ذوي الخبرة في ميدان الجرائم السيبرانية. ولذا، فإن المشاركة القوية من جانب الخبراء في هذا الميدان ضرورية من أجل تنفيذ صك عملي وفعال لمكافحة الجريمة السيبرانية.

**آليات التنفيذ**

من السابق لأوانه للغاية في هذه المرحلة تحديد مدى الحاجة إلى عملية منفصلة لمراجعة تنفيذ الصك في المستقبل والشكل الذي ينبغي أن تتخذه هذه العملية، في حالة الحاجة إليها. ولكن يوجد العديد من النماذج الناجحة التي يجب مراعاتها. وبالنظر إلى نقص الموارد المتاحة للمساعدة التقنية، ينبغي النظر في الأساليب التي تعتمد على خيارات ملائمة للميزانية لتعظيم مساهمات المانحين في المساعدة التقنية. ومن هذه الأساليب تخويل لجنة منع الجريمة والعدالة الجنائية، المُشكَّلة عملاً بقرار المجلس الاقتصادي والاجتماعي 1/1992، بالنظر في جميع المسائل المتعلقة بأهداف صك معني بمكافحة الجريمة السيبرانية. وثمة سابقة ناجحة لهذا النوع من الإشراف وهي سابقة لجنة المخدرات، التي تشرف على المعاهدات الدولية الثلاثة لمراقبة المخدرات. وكما هو مبين في القسم أعلاه حول مشاركة المجتمع والكيانات والمنظمات، من الضروري مراعاة المشاركة القوية للمجتمع العام والكيانات والمنظمات عند تنفيذ أي مسار عمل ينبثق عن أي صك. ومع ذلك، ينبغي إرجاء المناقشة حول آليات تنفيذ الصك لحين تحديد نطاقه تحديداً أكثر تفصيلاً.