

الولايات المتحدة الأمريكية

يسر حكومة الولايات المتحدة الأمريكية الاستجابة للدعوة الموجهة إلى الدول الأعضاء لتقديم آرائهم حول نطاق وأهداف وهيكل (عناصر) الاتفاقية الجديدة، فيما يتعلق بتنفيذ قراري الجمعية العامة للأمم المتحدة 74/247 و 75/282. وتتطلع الولايات المتحدة إلى العمل مع الدول الأخرى الأعضاء في الأمم المتحدة وأصحاب المصلحة المهتمين لصياغة صك عالمي يركز على تحسين التحقيق والملاحقة القضائية في الجرائم السيبرانية، بما يتفق مع الحقوق والالتزامات القائمة والبناء عليها. وتؤكد الولايات المتحدة مجدداً على أهمية الحفاظ على عملية مفتوحة وشاملة وشفافة ومتعددة أصحاب المصلحة من شأنها أن تسمح لجميع الدول الأعضاء بالتفاوض بحسن نية للتوصل إلى حلول مستنيرة وقائمة على توافق الآراء وعملية، والتي نعتقد أنها ستشجع على الانضمام على نطاق واسع إلى صك عالمي جديد لمكافحة الجرائم السيبرانية.

إن الموعد النهائي المقترح لعملنا يخلق جدولاً زمنياً ضيقاً حتى في الظروف الاعتيادية، لكن جهودنا الحالية سيتم القيام بها على خلفية جائحة عالمية. ولذلك، فمن الضروري للغاية أن نكون أكثر تركيزاً وفعالية في جهودنا للتفاوض من أجل التوصل إلى صك عالمي لمكافحة الجريمة السيبرانية. ولسوء الحظ، بينما عمل معظم العالم على مكافحة جائحة كوفيد-19، قام مجرمو الفضاء السيبراني باستغلال التحول العالمي الناتج عن ذلك والاعتماد على التكنولوجيا الرقمية. إن الجرائم السيبرانية تمثل تهديداً مباشراً لسلامة ورفاهية المجتمعات والأشخاص في جميع أنحاء العالم. لقد كان هناك تعاون طويل الأمد لبناء قدرتنا الجماعية على مكافحة هذا الاستغلال، ويمكننا مواصلة البناء على تلك النجاحات مع دراسة متأنية للحلول العملية. وبالنظر إلى الطابع الفوري للتهديد الذي تشكله الجرائم السيبرانية، فمن الأكثر أهمية أن تكون جهودنا للتفاوض بشأن صك عالمي لمكافحة الجريمة السيبرانية مُركزة ومدروسة.

يجب أن يهدف صك مكافحة الجرائم السيبرانية هذا إلى تعزيز التعاون الدولي وتوفير الأدوات العملية لتجهيز سلطات إنفاذ القانون الوطنية للتصدي للجرائم السيبرانية، كما فعلت صكوك الأمم المتحدة الأخرى للأشكال الأخرى من الجريمة العابرة للحدود الوطنية، بما في ذلك الفساد والاتجار بالمخدرات والاتجار بالبشر وتهريب المهاجرين. وينبغي أيضاً أن يضمن الصك وجود سلطة محلية لجمع الأدلة الإلكترونية ذات الصلة بأي نوع من الجرائم والحصول عليها، وليس فقط الجرائم المعتمدة على الإنترنت، وتعزيز التعاون الدولي في مثل هذه الحالات. وكما هو الحال مع كل صك من صكوك الأمم المتحدة لمكافحة الجريمة، يجب أن تتضمن هذه الأدوات حدوداً وضمانات مناسبة، في سياق الأطر المحلية القائمة، وذلك للتعامل مع الخصوصية والحريات المدنية، مع الاحترام الكامل لحقوق الإنسان. كما يجب أن يتناول صك مكافحة الجرائم السيبرانية الحاجة المتزايدة إلى المساعدة الفنية، ويوفر سبلاً للدول الأعضاء لطلب هذه المساعدة.

ومع بدء الدول الأعضاء عملية الصياغة، فمن الضروري أن ندرك أننا لا نفعل ذلك من فراغ. وعلى الرغم من أهمية تحديد ما يجب أن يغطيه هذا الصك، فمن المهم أيضاً التعرف على ما يقع خارج نطاقه الصحيح. إن هناك عمل مستمر وقيم بشأن القضايا السيبرانية الأخرى التي تتجاوز نطاق الجرائم السيبرانية يجري في الأمم المتحدة وغيرها من المنتديات الحكومية الدولية ومنتديات أصحاب المصلحة المتعددين. ومن المهم ألا نكرر هذا العمل أو نقوضه - وذلك لتجنب تضارب الالتزامات وحتى لا ينتقص ذلك من هدفنا المتمثل في وضع صك هادف وعملي لمكافحة الجرائم السيبرانية. إن محاولة تناول كل قضية متعلقة بالإنترنت في صك العدالة الجنائية هذا تُخاطر بتشتيت هذه المفاوضات في مناقشات غير مركزة وعرضية لن تفعل شيئاً يُذكر لمكافحة الجريمة السيبرانية وتؤدي فقط إلى إبطاء تقدمنا نحو التوصل إلى صك مفيد.

وعلى وجه الخصوص، لا ينبغي للدول الأعضاء الخوض في مواضيع واسعة النطاق تتعلق بالإدارة السيبرانية أو الأمن السيبراني في صك للجريمة مكرس لمكافحة الجريمة السيبرانية. وعلى الرغم من أنه

غالبا ما يُنظر إليهما على أنهما وجهان لعملة واحدة، إلا أن مكافحة الجريمة السيبرانية هي بالأساس مسؤولية حكومية، في حين أن الأمن السيبراني هو مسؤولية مجموعة من الجهات الفاعلة العامة والخاصة. إن تفويض اللجنة المخصصة لوضع الاتفاقية يتركز على وضع صك للعدالة الجنائية بشأن المسائل الجنائية لتسهيل الاستجابة الدولية للجرائم السيبرانية، والتي تتضمن تحديد ومعاينة الفعل الإجرامي في الفضاء السيبراني. ولا تتمتع اللجنة المخصصة لوضع الاتفاقية بصلاحيات إملاء معايير عالمية للسلوك غير الإجرامي الذي يحدث على الإنترنت. إن إدراج مفاهيم الإدارة السيبرانية والأمن السيبراني في معاهدة للجرائم السيبرانية لن يفي بالهدف المتمثل في وضع صك مبسط وفعال يجتذب دعما واسعا من الدول الأعضاء.

وكما تم التأكيد مجددا في قرار الجمعية العامة 75/282، فإنه من الأهمية بمكان ألا تعيق المفاوضات الرامية لوضع صك جديد لمكافحة الجرائم السيبرانية الآليات القائمة، بما في ذلك الصكوك متعددة الجنسيات والصكوك الإقليمية، التي توفر بالفعل مجموعة من الأدوات لمكافحة الجريمة السيبرانية بشكل فعال.¹ ويمكننا بناء توافق في الآراء على أفضل وجه بشأن هذا الصك الجديد وتجنب القضايا السياسية والمثيرة للانقسام من خلال الاستفادة من الصكوك الموجودة التي أثبتت نجاحها. ويجب أن نسترشد بالإنجازات في تنفيذ معاهدات الأمم المتحدة الأخرى للعدالة الجنائية، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. فقد أثبتت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية أنها مفيدة للغاية لأن هذا الصك يستهدف الأنواع الأساسية من أنشطة الجريمة المنظمة، بينما يتضمن أيضا أحكاما عامة للتعاون الدولي يمكن تطبيقها على أي نوع من الجرائم الخطيرة التي يرتكبها ثلاثة أشخاص أو أكثر من أجل الربح. ونتيجة لذلك، استخدمت الأطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بنجاح آلاف المرات، بما في ذلك مكافحة الجرائم، مثل حوادث برمجيات انتزاع الفدية والاستغلال الجنسي للأطفال.

¹ القرار 75/282، مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية. اعتمدهت الجمعية العامة في 26 مايو/ أيار 2021 وهو متاح على الموقع: <https://undocs.org/en/A/RES/75/282>

وتؤكد الولايات المتحدة مجدداً على أهمية الحفاظ على عملية مفتوحة وشاملة وشفافة من شأنها أن تسمح لجميع الدول الأعضاء وأصحاب المصلحة المهتمين بالتفاوض بحسن نية للتوصل إلى حلول مستتيرة وقائمة على توافق الآراء وعملية، والتي نعتقد أنها الطريقة الأفضل للتشجيع على الانضمام على نطاق واسع إلى صك عالمي جديد لمكافحة الجرائم السيبرانية.

تجريم الأفعال الأساسية التي تشكل جرائم سيبرانية

أولاً وقبل كل شيء، يجب أن يضمن أي صك جديد وجود سلطة محلية تقوم بجمع الأدلة الإلكترونية لأي نوع من الجرائم والحصول عليها. وهذه السلطات ضرورية للبلدان حتى تتمكن من التحقيق بشكل فعال في كل نوع من الجرائم تقريباً وملاحقته قضائياً، حيث إن عدداً قليلاً جداً من الجرائم الحالية تُرتكب بالكامل خارج العالم الرقمي. وينبغي أن يتيح الصك أيضاً التعاون الدولي لتبادل الأدلة الإلكترونية لأي نوع من الجرائم رهناً بحكم مرن بشأن ازدواجية التجريم كما هو وارد في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد.²

بالإضافة إلى ذلك، يتطلب التعاون الدولي الفعال أن يكون لدى الدول الأعضاء تشريعات محلية كافية تُجرّم الأفعال الأساسية التي تشكل جرائم سيبرانية. ويعد الفهم المشترك للأفعال الجوهرية والأساسية ودعم السلطات الإجرائية بين الدول الأعضاء أمراً ضرورياً لتجنب إنشاء ملاذات آمنة لمجرمي الفضاء السيبراني. وتُظهر دراسات مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن البلدان تتفق عموماً على الفعل الأساسي الذي ينبغي تجريمه بموجب قوانين محددة للجرائم السيبرانية، مع وجود العديد من الاتفاقيات متعددة الجنسيات والقوانين الجنائية الوطنية التي تحتوي على أحكام مشتركة. وبالمثل فإن الفهم الدولي للسلطات الإجرائية

² الفقرة 9 من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية؛ الفقرة 9 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد، على الرغم من اختلاف الأحكام الواردة في الاتفاقيتين إلى حد ما، فإن كلاهما يوفر حرية تقديرية كبيرة للدول الأطراف المستقبلية في تقديم المساعدة، لا سيما فيما يتعلق بالتدابير القسرية.

القانونية لدعم التحقيقات الفعالة في الجرائم السيبرانية هو أمر قد أستقر. ونتيجة لذلك، يتمتع الممارسون بعقدين من الخبرة المتراكمة والمتنوعة من التحقيق في الجرائم السيبرانية والتي توضح استمرار صلاحية السلطات الهامة والإجرائية المعتمدة بشكل مشترك للتحقيق في الجرائم السيبرانية.

يجب أن يحدد الصك الجديد لمكافحة الجريمة السيبرانية الجرائم التي تعتمد على الإنترنت وان يتم تطبيقه عليها، وهي جرائم يكون فيها الكمبيوتر أو البيانات هدفا للنشاط الإجرامي، بالإضافة إلى بعض الجرائم التي يتم تمكينها سيبرانياً، مثل الجرائم التي يتم استخدام الكمبيوتر فيها لتسهيل الجريمة. هذه الفئة الأولى والرئيسية من الأفعال التي يحددها هذا الصك الجديد هي تلك التي لا يمكن ارتكابها دون إساءة استخدام أجهزة الكمبيوتر أو نظم الشبكات، وبالتالي لم تكن موجودة كجرائم قبل ظهور نظم الكمبيوتر. ويمكن أن تتم الجرائم التي تعتمد على الإنترنت بالكامل في العالم الرقمي. وبالنسبة للأفعال الأساسية التي تشكل جريمة تعتمد على الإنترنت، مثل هجمات رفض الخدمة أو إتلاف أجهزة الكمبيوتر والبيانات، تكون هناك حاجة إلى قوانين خاصة بالإنترنت لأنه في معظم الولايات القضائية يتم تفسير القوانين الجنائية بدقة، وغالباً ما تكون القوانين التقليدية التي تغطي المفاهيم المألوفة، مثل التعدي على ممتلكات الغير والتخريب، غير مناسبة للتطبيق على الجرائم السيبرانية. وعلاوة على ذلك، فإن بعض أحكام القانون الجنائي التي تنطبق على الجرائم التي يتم ارتكابها خارج شبكة الكمبيوتر قد لا يكون من السهل تطبيقها على الفعل المرتكب من خلال أجهزة الكمبيوتر.

وفي المقابل، يجب أن نكون حريصين على عدم التعامل مع الجرائم التقليدية على أنها "جرائم سيبرانية" لمجرد استخدام الكمبيوتر في التخطيط لها أو تنفيذها. وعلى الرغم من إساءة استخدام جهاز الكمبيوتر لارتكاب الجريمة، فإن بعض الأفعال الجرمية قد يتم تغطيتها من خلال القوانين العامة لأنه لا يوجد شيء غريب أو فريد لنظام الكمبيوتر في ذلك الفعل. وفي المقابل، يتم التعامل مع بعض الجرائم التي يتم

تمكينها سبيرانيا بشكل مناسب من خلال صك لمكافحة الجرائم السيبرانية حيث يتزايد، على سبيل المثال، استخدام أجهزة الكمبيوتر.

- نطاق الفعل، على سبيل المثال الآلاف من الضحايا أو سرقة ملايين من بيانات الدفع؛
- سرعة الهجوم لأن الكمبيوتر يزيد بشكل كبير من القدرة على إتمام الفعل؛
- حجم الضرر أو الإصابة التي لحقت بالضحايا؛
- أو عدم الكشف عن هوية الجاني.

من خلال تطبيق هذه المفاهيم، قد يُنظر بشكل منطقي أيضا إلى بعض حالات الجرائم التقليدية، مثل الاحتيال واستغلال الأطفال، على أنها تدخل في نطاق هذه المفاوضات. ولكن، ينبغي على الدول الأعضاء أن تكون حكيمة فيما يتعلق بمدى اتساع نطاق الجرائم التي يتم تمكينها سبيرانيا التي نسعى للتعامل معها حتى لا نشوه مفاهيم العدالة الجنائية الراسخة، ولا تفقد القوانين والصكوك الجنائية الراسخة قابليتها للتطبيق لمجرد أن الفعل ينطوي على بعض العناصر "السيبرانية".

كما ينبغي أن يدعو الصك العالمي لمكافحة الجرائم السيبرانية الأطراف إلى سن تشريعات تُجرّم الأفعال الأساسية التي تشكل جرائم سيبرانية بطريقة محايدة من الناحية التكنولوجية، مع ضمان وجود الضمانات الإجرائية. إن تجريم الأفعال بطريقة محايدة من الناحية التكنولوجية (أي تجريم النشاط الذي يؤثر على سرية بيانات الكمبيوتر وسلامتها وتوافرها بدلاً من تجريم النموذج أو الطريقة المعينة المستخدمة، مثل التصيد الاحتمالي أو برمجيات انتزاع الفدية) يضمن أن الأحكام الجنائية الجوهرية لا تتناول فقط - التكنولوجيا والتقنيات الإجرامية الحالية، ولكن أيضا التكنولوجيا والتقنيات المستقبلية. وكتوضيح لمدى سرعة تطور التكنولوجيا، فإنه حتى مسودة الدراسة الشاملة حول الجرائم السيبرانية من عام 2013، بقصدها الصريح أن تكون شاملة، افتقرت إلى التفاصيل حول التكنولوجيا أو التقنيات التي لم تكن مستخدمة على نطاق

واسع، أو ظهرت للتو، في وقت الدراسة، بما في ذلك برمجيات انتزاع الفدية وإنترنت الأشياء (Internet of Things) والعملات المشفرة والتطور السريع وهيمنة تكنولوجيا الهاتف المحمول. وتعبيراً عن هذا القلق، كان من بين الاستنتاجات والتوصيات التي اتفقت عليها الدول الأعضاء في فريق الخبراء التابع للأمم المتحدة أنه "ينبغي على الدول الأعضاء أن تضمن أن أحكامها التشريعية تصمد أمام اختبار الزمن فيما يتعلق بالتطورات المستقبلية في التكنولوجيا من خلال سن قوانين بصيغ تتسم بالحياد التكنولوجي، وتُجرّم النشاط الذي يعتبر غير قانوني بدلاً من الوسائل المستخدمة".³ إن هذا الأمر مهم بشكل خاص ونحن نحاول صياغة صك دائم يمكن أن يتعامل بشكل مناسب مع تكنولوجيات الغد وفي باحتياجات ممارسي إنفاذ القانون الآن وفي المستقبل.

ومع أخذ هذه المبادئ في الاعتبار، ينبغي أن يتضمن الصك العالمي لمكافحة الجريمة السيبرانية

تجريم ما يلي:

- الوصول غير القانوني، أي الوصول إلى جهاز كمبيوتر أو نظام كمبيوتر بدون تصريح؛
- الاعتراض غير القانوني، أي اعتراض غير قانوني في الوقت الفعلي لمحتوى الاتصالات أو بيانات حركة المعلومات المتعلقة بالاتصالات؛
- التدخل في البيانات أو النظام، أي البرامج الضارة، وهجمات رفض الخدمة، وبرمجيات انتزاع الفدية، وحذف البيانات أو تعديلها؛
- إساءة استخدام الأجهزة، أي الاتجار أو استخدام بيانات بطاقات الائتمان وكلمات المرور والمعلومات الشخصية التي تسمح بالوصول إلى الموارد؛

³ مكتب الامم المتحدة المعني بالمخدرات والجريمة/ لجنة منع الجريمة والعدالة الجنائية/ فريق الخبراء 4/2021/2، تقرير حول اجتماع فريق الخبراء المعني بإجراء دراسة شاملة حول الجريمة السيبرانية الذي عُقد في فيينا من 6 إلى 8 أبريل/ نيسان 2021. وهو متاح على الموقع: <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf>

- الأفعال المتعلقة بمواد الاعتداء الجنسي على الأطفال؛
- الأفعال المتعلقة بالاحتيال الذي يتم بواسطة الكمبيوتر، أي التلاعب بنظم الكمبيوتر أو البيانات لأغراض احتيالية مثل التصيد الاحتيالي، والكشف عن البريد الإلكتروني للأعمال التجارية، والاحتيال في مجال المزادات؛
- الأفعال المتعلقة بالتعدي على حقوق التأليف والنشر والحقوق ذات الصلة؛
- وأحكام تتناول المحاولة والمساعدة والتحريض والتآمر.

علاوة على ذلك، ينبغي أيضا تجريم غسل عائدات الجرائم السيبرانية. وأخيرا، يجب أن يخضع الأشخاص الاعتباريون لعقوبات جنائية أو مدنية وإدارية إذا تورطوا في جرائم سيبرانية يحظرها الصك.

السلطات الإجرائية لجمع الأدلة الإلكترونية وتبادلها

بالإضافة إلى تجريم الأفعال الجوهرية، ينبغي أن يتناول الصك العالمي لمكافحة الجرائم السيبرانية حاجة السلطات القانونية المحلية إلى حفظ الأدلة الإلكترونية وجمعها وتبادلها بما يتفق مع الإجراءات القانونية الواجبة وحماية حقوق الإنسان والحريات الأساسية. لقد لاحظت بعض الدول الأعضاء أنه بموجب قوانينها المحلية، قد لا تنطبق السلطات الإجرائية التقليدية على البيانات غير الملموسة أو قد لا تسمح بجمع الأدلة الإلكترونية سريعة الزوال بالسرعة الكافية. وكما هو الحال دائما، لن تكون القوانين القديمة كافية لمواجهة التحديات العديدة المتعلقة بالتحقيقات في الجرائم الإلكترونية، بما في ذلك التعامل مع التكنولوجيا الجديدة مثل التشفير وخدمات الحوسبة السحابية واسعة الانتشار. لذلك فإن السلطات الإجرائية المتخصصة لجمع الأدلة الإلكترونية ضرورية. ويجب صياغة هذه القوانين مع مراعاة المفاهيم الفنية القابلة للتطبيق وكذلك الاحتياجات العملية للمحققين الجنائيين. وبشكل أكثر تحديدا، يجب أن تسمح هذه السلطات الإجرائية بما يلي:

- الحفظ العاجل لبيانات الكمبيوتر المخزنة؛

- أوامر تقديم بيانات الكمبيوتر؛
- البحث عن بيانات الكمبيوتر المخزنة ومصادرتها؛
- جمع بيانات حركة المعلومات على الكمبيوتر في الوقت الفعلي؛
- وجمع بيانات المحتوى في الوقت الفعلي في حالات الجرائم الخطيرة.

بالإضافة إلى ذلك، ينبغي أن يسمح الصك الجديد بالتعاون في جمع الأدلة الإلكترونية والحصول عليها لأي نوع من الجرائم، وليس فقط الجرائم السيبرانية. إن جميع الجرائم الجنائية المهمة تقريبا تشتمل على أدلة إلكترونية، سواء في شكل بيانات الهاتف المحمول أو البريد الإلكتروني أو بيانات المعاملات أو غيرها من البيانات ذات الصلة بالتحقيق في الجرائم وملاحقة مرتكبيها قضائيا. وكمسألة محلية، تحتاج الدول الأعضاء إلى إطار قانوني حديث للأدلة يسمح بقبول الأدلة الإلكترونية في التحقيقات الجنائية والملاحقات القضائية، بما في ذلك مشاركة الأدلة الإلكترونية مع شركاء إنفاذ القانون على الصعيد الدولي.

التعاون الدولي

خارج إطار القوانين المحلية، يعتمد التعاون الدولي الفعال بشأن الجرائم السيبرانية على التعاون الرسمي القائم على المعاهدات، مثل المساعدة القانونية المتبادلة، وغيرها من الوسائل، مثل التعاون التقليدي والمصرح به بين أجهزة الشرطة. وينبغي أن يستفيد الصك الجديد لمكافحة الجريمة السيبرانية من أدوات فعالة لزيادة التعاون الدولي من المعاهدات القائمة، ويضمن عدم تقويضه للصكوك القائمة والتعاون الدولي الجاري في مكافحة الجريمة السيبرانية. إن أحكام صك مكافحة الجرائم السيبرانية المتعلقة بالتعاون الدولي، بما في ذلك المساعدة القانونية المتبادلة وتسليم المجرمين وتحويل الملاحقة القضائية ومصادرة العائدات بما في ذلك العملات الافتراضية وإعادة الأصول المصادرة إلى الضحايا وازدواجية التجريم والتعاون في مجال إنفاذ القانون، يجب أن تلتزم بعناية بأحكام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة

عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد، بما في ذلك الضمانات والحماية المناسبة الواردة فيهما، والتي تم تنفيذها بنجاح من قبل الغالبية العظمى من الدول الأعضاء في الأمم المتحدة. وبالإضافة إلى ذلك، ينبغي أن تنص الاحكام المتعلقة بالمساعدة القانونية المتبادلة على مساعدة واسعة في الحصول على الأدلة الإلكترونية المتعلقة بجريمة جنائية، سواء ارتكبت الجريمة أو لم ترتكب بمشاركة نظام كمبيوتر.

المساعدة الفنية وبناء القدرات

تشير دراسات مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن أكثر من 75 في المائة من البلدان لديها وحدة مخصصة للقضايا المتعلقة بالجرائم السيبرانية داخل منظمات إنفاذ القانون القائمة، وأن حوالي 15 في المائة لديها وكالة متخصصة ومخصصة للجرائم السيبرانية. وهذا يؤكد الطبيعة المتخصصة للتحقيقات في الجرائم السيبرانية، بما في ذلك الحاجة إلى التدريب المتخصص. علاوة على ذلك، ازداد تعقيد الأفعال التي تشكل جرائم سيبرانية والعناصر الإلكترونية أو الرقمية للجرائم التقليدية بشكل كبير، مما يفرض متطلبات إضافية على تدريب المحققين والخبراء الفنيين ذوي المهارات العالية والحفاظ عليهم.

إن عدم كفاية القدرات المحلية هو السبب الأكثر شيوعاً لاحتمال عدم قدرة البلدان على التعاون بفعالية على الصعيد الدولي. وبالنسبة لمعظم البلدان، لا يُحقق التعاون الدولي بسبب الافتقار إلى الإرادة، بل بسبب القيود سواء في القانون المحلي أو في خبرة وكالات إنفاذ القانون. ولا يتوفر للعديد من الدول الأعضاء موارد جيدة فيما يتعلق بقدرات إنفاذ القانون لمكافحة الجريمة السيبرانية أو التعامل مع الأدلة الإلكترونية. فعلى سبيل المثال، تواجه بعض الدول الأعضاء، في ضوء الأولويات الوطنية الحالية، تحديات في تطوير واستبقاء المحققين المدربين والمفتشين العدليين، فضلاً عن التعامل مع النقص في أجهزة وبرامج الكمبيوتر. وبناءً على ذلك، هناك إجماع دولي واسع على أن المساعدة الفنية وبناء القدرات لمؤسسات إنفاذ القانون، بما في ذلك المحققون والمدعون العامون والقضاة، تظل من المتطلبات الأكثر إلحاحاً للاستجابة الدولية الفعالة

للجرائم السيبرانية. وعلاوة على ذلك، ونظرا لأن الأدلة الإلكترونية أصبحت عنصرا في كل نوع من أنواع الجرائم تقريبا، سيحتاج حتى ضباط إنفاذ القانون "غير المتخصصين" إلى بعض الفهم الأساسي للتحقيقات المتعلقة بالكمبيوتر.

ينبغي أن تتضمن أحكام صك الجرائم السيبرانية المتعلقة بالمساعدة الفنية والقدرات ما يلي:

- الاجراءات التي تتخذها الدول الأعضاء لبدء أو وضع أو تحسين برامج التدريب لموظفيها المسؤولين عن منع الجريمة السيبرانية ومكافحتها.
- نظر الدول الأعضاء، حسب القدرات، في تزويد بعضها البعض بأكثر قدر من المساعدة الفنية، وخاصة لصالح البلدان النامية وتلك البلدان التي قد تواجه بشكل غير متناسب تهديدات الجرائم السيبرانية، في خططها وبرامجها لمكافحة الجريمة السيبرانية.
- إنشاء آليات يمكن من خلالها للمساهمات المالية الطوعية من الدول الأعضاء أن تدعم تنفيذ صك خاص بالجرائم السيبرانية.
- نظر الدول الأعضاء في تقديم تبرعات طوعية إلى البرنامج العالمي المعني بالجريمة السيبرانية التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة وما يرتبط به من جهود لبناء القدرات في مجال العدالة الجنائية.

مشاركة المجتمع والكيانات والمنظمات ككل

لا يمكن أن تكون مكافحة الجريمة السيبرانية جهدا منفردا نظرا لتعدد المشكلة وطبيعتها ذات الجوانب المتعددة. ويجب أن يأخذ صك مكافحة الجرائم السيبرانية في الاعتبار 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 لمثل هذه

المشاركة أن ترفع الوعي العام حول تهديدات الجريمة السيبرانية، وتضمن تنفيذ عمل الدول الأعضاء بطريقة شفافة، وتعالج المسائل الجوهرية المتعلقة بالخصوصية والحريات المدنية وحقوق الإنسان. وعلاوة على ذلك، يعتمد الصك الفعال على مساهمات الأفراد والكيانات من ذوي الخبرة في مجال الجرائم السيبرانية. ولتنفيذ صك عملي وفعال لمكافحة الجريمة السيبرانية، تكون المشاركة القوية للخبراء في هذا المجال أمر ضروري.

آليات للتنفيذ

إن تحديد ما إذا كانت هناك حاجة إلى إجراءات منفصلة لمراجعة التنفيذ المستقبلي للصك، وإذا كان الأمر كذلك، الشكل الذي يجب أن تأخذه، هو أمر مُبكر للغاية في هذه المرحلة. وهناك العديد من النماذج الناجحة التي يمكن النظر فيها. وبالنظر إلى النقص في الموارد المتاحة للمساعدة الفنية، ينبغي النظر في الطرق التي تعتمد على خيارات غير مُكلفة لتعظيم مساهمات المانحين في المساعدة الفنية. وتتمثل إحدى هذه الطرق في السماح للجنة منع الجريمة والعدالة الجنائية، المنشأة بموجب قرار المجلس الاقتصادي والاجتماعي رقم 1992/1، بالنظر في جميع المسائل المتعلقة بأهداف صك مكافحة الجرائم السيبرانية. وهناك سابقة ناجحة لمثل هذا الإشراف تتعلق بلجنة المخدرات التي تشرف على المعاهدات الدولية الثلاث للرقابة على المخدرات. وكما هو موضح في قسم مشاركة المجتمع والكيانات والمنظمات، فمن الضروري مراعاة المشاركة القوية للمجتمع والكيانات والمنظمات ككل عند تنفيذ أي مسار عمل من الصك. ومع ذلك، ينبغي الانتظار على إجراء النقاش حول آليات التنفيذ حتى يتم تحديد نطاق الصك بشكل أكبر.