UNODC/CCPCJ/EG.4/2020/L.1/Add.3

27 July 2020
Arabic
Original: English

فريق الخبراء المعني بإجراء دراسة شاملة
عن الجريمة السيبرانية
فيينا، 27-29 تموز/يوليه 2020

مشروع التقرير

إضافة

ثانيا- قائمة التوصيات والاستنتاجات الأولية *(تابع)*

باء- المنع

1- تماشيا مع خطة عمل فريق الخبراء، تتضمن هذه الفقرة تجميعا للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند 3 من جدول الأعمال المعنون "المنع". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أن فريق الخبراء قد أقرها، كما أن ترتيب عرضها لا يعني ضمنا ترتيبا لدرجة أهميتها:

(1) ينبغي التسليم بأن المنع ليس مسؤولية الحكومات وحدها، وإنما يتطلب مشاركة جميع أصحاب المصلحة المعنيين، بما في ذلك أجهزة إنفاذ القانون، والقطاع الخاص، ولا سيما مقدمي خدمات الإنترنت، والمنظمات غير الحكومية، والمدارس، والأوساط الأكاديمية، بالإضافة إلى الجمهور بوجه عام.

(2) أوصي بأن يسهل على الجمهور الوصول إلى أدوات المنع، ومنها المنصات الإلكترونية، والمقاطع الصوتية، والمعلومات البيانية التي تستخدم لغة مبسطة، وكذلك منصات الإبلاغ.

(3) اعتبر من الضروري وضع سلسلة من السياسات العامة الطويلة الأجل المتعلقة بالمنع، وينبغي أن تشمل تلك السياسات تنظيم حملات للتوعية بشأن الاستخدام الآمن للإنترنت.

(4) ينبغي إدراج الوعي بالأمن السيبراني كموضوع في التعليم الابتدائي والثانوي والعالي، للطلاب والمعلمين على حد سواء. وينبغي أن يكون ذلك، في الحالة المثلى، جزءا من استراتيجية وطنية للأمن السيبراني. وينبغي للدول أيضا أن تتبادل الخبرات بشأن كيفية استخدام استراتيجيات الأمن السيبراني لمنع الجريمة السيبرانية. وبالإضافة إلى ذلك، ينبغي للدول أن تولي اهتماما خاصا لتدابير المنع الموجهة إلى أوساط الشباب، بما في ذلك من ارتكبوا جريمة للمرة الأولى، بهدف منع معاودة ارتكابهم للجرائم.

(5) ينبغي للدول، عند منع الجريمة السيبرانية ومكافحتها، أن تولي اهتماما خاصا لمسائل منع العنف الجنساني، والعنف ضد النساء والفتيات، وجرائم الكراهية، والقضاء على تلك الجرائم.

(6) يجب أن تكون الأنشطة المتعلقة بالمنع استباقية ومنتظمة ومستمرة ومناسبة للفئات الضعيفة.

(7) يمكن للتقاطع والتعاون بين كيانات القطاعين العام والخاص التي تمتلك مجموعات بيانات كبيرة أو مراكز بيانات كبيرة أن تكون من المجالات التي تتسم بالضعف الشديد، وبخاصة، على سبيل المثال لا الحصر، في قطاع الصحة، نظرا للجائحة الحالية. وينبغي للدول أن تولي اهتماما خاصا لتنظيم الوصول إلى هذه البيانات على نحو قانوني وحمايتها من هجمات الجرائم السيبرانية.

(8) فيما يتعلق بالجهود في مجال المنع، ينبغي أن يتحمل مقدمو خدمات الإنترنت مزيدا من المسؤولية عن الاحتياطات الأمنية ("على نحو تلقائي") وعن منع الجريمة السيبرانية، وينبغي وضع معايير دولية بشأن محتوى معلومات السجلات والمدة التي يتعين على مقدمي الخدمات الاحتفاظ بها بتلك المعلومات. وعلاوة على ذلك، ينبغي أن تحدد بوضوح مسؤوليات مقدمي الخدمات فيما يتعلق باكتشاف الجرائم السيبرانية ومنعها وتعطيلها.

(9) هناك حاجة إلى إقامة شراكات بين القطاعين العام والخاص في مجال منع الجريمة السيبرانية ومكافحتها، بما في ذلك التعاون مع أصحاب المصلحة في مجال الأمن السيبراني وشركات التكنولوجيا الكبرى بشأن تبادل المعلومات.

(10) ينبغي للدول أن توفر التدريب للقضاة المتخصصين وغيرهم من القضاة الذين يتعاملون مع قضايا الجرائم السيبرانية، وأن تزود هيئات التحقيق بأدوات عالية الأداء لتتبع العملات المشفرة ومعالجة استخدامها لأغراض إجرامية.

(11) ينبغي للدول أن تزيد من استراتيجيات مكافحة استغلال المجموعات الإجرامية التقليدية للأدوات السيبرانية بغرض إخفاء اتصالاتها وأنشطتها.

(12) ينبغي وضع حلول تتيح التعاون المباشر بين السلطات الوطنية ومقدمي خدمات الإنترنت، مع الحفاظ على سيادة القانون وحقوق الإنسان، بما في ذلك متطلبات حماية البيانات.

(13) ينبغي للدول أن تكفل حرية الصحافة عند وضع تدابير منع الجريمة السيبرانية.

(14) أوصي ببناء القدرات الجماعية للمؤسسات المختصة وتغيير ثقافة المنع بحيث تكون استباقية بدلا من أن تكون قائمة على رد الفعل. وأوصي أيضا بإنشاء آلية قوية لحفز وتيسير تبادل المعلومات الاستخبارية بشأن أساليب العمل الإجرامية المحتملة.

(15) تشجع الدول الأعضاء على أن تواصل إدراج تدابير منع فعالة على الصعيدين الوطني والدولي، وتركز على الأنشطة الاستباقية مثل تعزيز الوعي بمخاطر الجريمة السيبرانية؛ وتوجه حملات نحو أساليب العمل من قبيل التصيد الاحتيالي أو البرمجيات الخبيثة (فيروسات الفدية "ransomware")، ونحو مجموعات مختلفة مثل الشباب أو المسنين؛ وترجح احتمال خضوع الجناة للملاحقة القضائية والعقاب وتبذل جهود لمنع الجريمة عن طريق كشف ما يجري من أنشطة إلكترونية غير مشروعة وعرقلتها. ويتعين على أجهزة الشرطة والنيابات العامة أن تستثمر في الكشف عن التهديدات التي تطرحها الجرائم السيبرانية، والتعريف بها والرد عليها. وتجدر الإشارة إلى أن الشراكة بين القطاعين العام والخاص لا غنى عنها في هذا المجال أيضا. ولا تتطلب أنشطة المنع هذه قوانين أو لوائح إضافية.

(16) نظرا لوجود "فجوة رقمية"، فإن بعض البلدان النامية تفتقر إلى القدرة على منع الجرائم السيبرانية وكشفها ومكافحتها، وهي أضعف حالا في مواجهة التحديات التي تمثلها تلك الجرائم.

(17) شُجِّع المكتب المعني بالمخدرات والجريمة بقوة على مواصلة تقديم المساعدة التقنية، عند الطلب، لمنع ومكافحة الجريمة السيبرانية.