المسألة 22-1/1: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

1 بيان الحالة

بالنظر إلى

أ) النمو الهائل في نشر واستخدام شبكات تكنولوجيا المعلومات والاتصالات؛

ب) أن الهجمات الإجرامية على الأمن السيبراني آخذة في النّمو ولا توجد تدابير فعّالة بمقدورها وقف هذه الهجمات؛

ج) الحاجة إلى ضمان أمن البُنى التحتية العالمية المترابطة إذا كان الهدف هو تحقيق إمكانات مجتمع المعلومات؛

د) الاعتراف المتزايد على الأصعدة الوطنية والإقليمية والدولية بضرورة بلورة وتعزيز أفضل الممارسات والخطوط التوجيهية والإجراءات التقنية لتقليل مكامن الضعف في شبكات تكنولوجيا المعلومات والاتصالات والحد من الأخطار التي تتهدّدها؛

هـ) ضرورة العمل وطنياً والتعاون إقليمياً ودولياً من أجل بناء ثقافة عالمية للأمن السيبراني تشمل التنسيق الوطني والبنى التحتية القانونية الملائمة وقدرات الإنذار والمراقبة والإصلاح، والشراكات بين القطاعين الحكومي والصناعي، والانفتاح على المجتمع المدني والمستهلكين؛

و) ضرورة اتباع نهج قائم على تعدد أصحاب المصلحة من أجل الاستخدام الفعال لمختلف الأدوات المتاحة لبناء الثقة في استعمال شبكات تكنولوجيا المعلومات والاتصالات،

ز) أن قرار الجمعية العامة للأمم المتحدة 57/239، "إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي" يدعو الدول الأعضاء إلى "تنمية ثقافة أمن الفضاء الحاسوبي في تطبيق واستخدام تكنولوجيا المعلومات، على صعيد المجتمع بكامله"؛

ح) أن أفضل ممارسات الأمن السيبراني يجب أن تحمي وتراعي حقوق الخصوصية وحرية الرأي على النحو المحدد في الأجزاء ذات الصلة من الإعلان العالمي لحقوق الإنسان وإعلان مبادئ جنيف والصكوك الدولية الأخرى المتعلقة بحقوق الإنسان؛

ط) أن إعلان مبادئ جنيف يشير إلى أن "الأمر يتطلب إشاعة ثقافة عالمية للأمن السيبراني وتطويرها وتنفيذها بالتعاون مع جميع أصحاب المصلحة وهيئات الخبرة الدولية". كما أن خطة عمل جنيف لمجتمع المعلومات تشجع تبادل أفضل الممارسات، واتخاذ الإجراءات المناسبة بشأن الرسائل الاقتحامية على الصعيدين الوطني والدولي، كذلك فإن برنامج عمل تونس يعيد التأكيد على ضرورة إشاعة ثقافة عالمية للأمن السيبراني، وتحديداً خط العمل جيم5 (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات)؛

ي) أن القمة العالمية لمجتمع المعلومات، تونس 2005، طلبت في برنامج عملها للتنفيذ والمتابعة، من الاتحاد الدولي للاتصالات أن يكون الميسر/المنسق الأوحد لخط العمل جيم5 **"بناء الثقة والأمن في استعمال تكنولوجيا الاتصالات والمعلومات"**. وقد أجرت قطاعات الاتحاد للتقييس والاتصالات الراديوية والتنمية وأمانته العامة بناءً على هذه المسؤولية واستجابةً للقرارات ذات الصلة التي اعتمدها المؤتمر العالمي لتنمية الاتصالات (الدوحة، 2006)، مع توقع تحديثها في حيدر آباد 2010 هذا العام، ومؤتمر المندوبين المفوضين (أنطاليا، 2006) وكذلك في الجمعية العالمية لتقييس الاتصالات (جوهانسبرغ، 2008)، دراسات كثيرة من أجل تحسين الأمن السيبراني؛

ك) أن نواتج القمة العالمية لمجتمع المعلومات في كلٍّ من جنيف 2003 وتونس 2005 نادت ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

ل) أن القرار 45 [حيدر آباد، 2010] للمؤتمر العالمي لتنمية الاتصالات يدعم تعزيز الأمن السيبراني فيما بين الدول الأعضاء المعنية؛

م) أنه ينبغي للاتحاد أن يضطلع، طبقاً لولايته، بدور في تنظيم لقاءات بين الدول الأعضاء وأعضاء القطاعات والخبراء الآخرين من أجل تبادل الخبرات والتجارب الخاصة بتأمين شبكات تكنولوجيا المعلومات والاتصالات؛

ن) النتائج الممتازة للمسألة 22/1 بعنوان "تقرير عن أفضل الممارسات من أجل نهج وطني للأمن السيبراني: اللبنات الأساسية لتنظيم الجهود الوطنية للأمن السيبراني"، في تقريرها الختامي للفترة 2006-2009، كما هو وارد في الوثيقة 1/249(Rev.1) لهذه المسألة لعام 2009، تُبرّر استمرار هذه المسألة لفترة جديدة أخرى مع توجّهات مختلفة تأخذ في الاعتبار احتياجات البلدان النامية؛

س) أن هناك الكثير من الجهود المبذولة لتسهيل تحسين أمن الشبكات، بما في ذلك العمل الذي تضطلع به الدول الأعضاء وأعضاء القطاعات في أنشطة وضع المعايير داخل قطاع تقييس الاتصالات وفي عملية وضع تقارير أفضل الممارسات داخل قطاع تنمية الاتصالات؛ وما تقوم به أمانة الاتحاد الدولي للاتصالات في إطار البرنامج العالمي للأمن السيبراني (GCA)؛ إضافة إلى العمل الذي يضطلع به قطاع تنمية الاتصالات ضمن أنشطته المتعلقة ببناء القدرات داخل البرنامج 3؛

ع) أن حكومات البلدان النامية وموردي الخدمات والمستعملين النهائيين يواجهون تحديات فريدة من نوعها في وضع سياسات ونُهج الأمن الملائمة لظروف كل منهم؛

ف) أن الدول الأعضاء ومشغلي البُنى التحتية سيستفيدون من أي تقارير أخرى تتناول بالتفصيل الموارد والاستراتيجيات والأدوات المختلفة المتاحة لبناء الثقة في استعمال شبكات تكنولوجيا المعلومات والاتصالات ودور التعاون الدولي في هذا المضمار.

2 المسألة والقضايا المقترحة للدراسة

أ) تحديث ناتج الدورة الماضية على أن يؤخذ في الاعتبار احتياجات البلدان النامية ويعكس النتائج التي توصل إليها الاتحاد ككل (النواتج ذات الصلة من لجنة الدراسات 17/T ولجنة الدراسات 13/T والنواتج ذات الصلة من البرنامج المتخصص للأمن السيبراني في مكتب تنمية الاتصالات وأنشطة الأمانة العامة كمتابعة لخط العمل جيم5 ونواتج فريق الخبراء رفيع المستوى (HLEG) التي أيدها كل خبراء البلدان النامية) إضافة إلى التقدم الذي أحرزته المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC) بشأن الموضوع. كما ستأخذ هذه المراجعة في الاعتبار التقدم الذي أحرزه مشروع IMPACT ومشروع FIRST والمشروعات المشابهة التي تضم الآن في عضويتها الكثير من البلدان النامية.

ب) أن يجري خلال فترة الدراسة المقبلة التوسُّع انطلاقاً من المعلومات الواردة في المرحلة الأولى من تقرير أفضل الممارسات والتي تتناول: (1) وضع استراتيجية وطنية للأمن السيبراني؛ (2) إقامة شراكات بين القطاعين العام والخاص؛ (3) استحداث قدرات وطنية لإدارة الحوادث السيبرانية تقوم بمراقبة الحوادث؛ (4) إرساء ثقافة الوعي العام؛ (5) تحديد أفضل الممارسات للوقاية من البرمجيات الضارة الاقتحامية والتهديدات السيبرانية الأخرى، وذلك على النحو التالي:

(i) بالنسبة لوضع استراتيجية وطنية للأمن السيبراني، أ) وضع نماذج للإدارة الوطنية للأمن السيبراني، ب) تحديد النماذج التنظيمية التي تتّبعها البلدان والتقنيات التي استخدمتها في وضع استراتيجية وطنية للأمن السيبراني، إضافة إلى الدروس المُستفادة، خاصة النماذج التي استخدمتها منظمة التعاون والتنمية في الميدان الاقتصادي أو أي نموذج آخر أوصت به أوروبا ككل.

(ii) فيما يتعلق بالشراكات بين القطاعين العام والخاص، بلورة (1) المبادئ الخاصة بشراكات سليمة بين القطاعين العام والخاص؛ (2) النماذج الهيكلية المختلفة لتحقيق شراكات سليمة بين القطاعين العام والخاص؛ (3) مفهوم الحد من المخاطر بالنسبة للشراكات بين القطاعين العام والخاص والدور الخاص بكل منها.

(iii) بالنسبة لاستحداث قدرات وطنية لإدارة الحوادث السيبرانية، بلورة المعلومات المتعلقة بآليات المراقبة والإنذار والاستجابة والاستعادة وإنشاء أفرقة وطنية للاستجابة للحوادث الأمنية الحاسوبية.

(iv) مع الأخذ في الاعتبار الدراسات الجارية في لجنة الدراسات 17 بقطاع تقييس الاتصالات بشأن توسيع هذه المراكز الوطنية بحيث تغطي جميع الأمور المتعلقة بالأمن السيبراني بوجه عام وعدم قصرها على الإنترنت فحسب، فضلاً عن إنتاج برنامج ذي صلة يتبع قطاع تنمية الاتصالات بشأن أفرقة الاستجابة للحوادث الحاسوبية (CIRT) ويُفضل أن يلبّي الاحتياجات الإقليمية للمناطق الستّ الحالية لمكتب تنمية الاتصالات، مع مراعاة أن نموذجاً وحيداً يصلُحُ لكلّ البلدان النامية يمكن أن يكون الاتجاه الأفضل في هذا المجال[1].

(v) فيما يتعلق بإرساء ثقافة وعي عام بالأمن السيبراني، جمع أفكار من شتى المصادر عن الكيفية التي تقوم بها البلدان ودوائر الأعمال وأفرقة الخبراء بتثقيف الأفراد والكيانات بشأن موضوع الأمن السيبراني وتشجيعها على الإلمام بمستجداته، بما في ذلك حماية الأطفال على الخط واحتياجات المعوقين في مجال الأمن السيبراني.

(vi) فيما يتعلق بتحديد أفضل الممارسات والاستراتيجيات للوقاية من الرسائل الاقتحامية والبرمجيات الضارة: (1) دراسة وتحديد جهود تثقيف المستهلكين وشركات الأعمال على الصعيد الوطني والتي من شأنها بناء الثقة لدى المستعملين من خلال منع الرسائل الاقتحامية والبرمجيات الضارة والحد منها؛ (2) دراسة الدور الذي يمكن أن تضطلع به الحكومات والمنظمات غير الحكومية في النهوض بمنع الرسائل الاقتحامية والبرمجيات الضارة، بما في ذلك النظر فيما يخص كل هذه الحكومات والمنظمات من أفضل الممارسات والمبادئ التوجيهية ومدونات السلوك في هذا الصدد؛ (3) دراسة الطرائق المستخدمة في توعية المستعملين النهائيين بالمخاطر المرتبطة بعمليات الاحتيال والبرمجيات الروبوتية الخبيثة والفيروسات وغيرها من المحتويات الضارة التي قد تضمها الرسائل الاقتحامية، فضلاً عن التدابير الوقائية المستخدمة؛ (4) دراسة التوقعات المأمولة من الآليات المستخدمة في تحسين الأمن السيبراني وتحديد المعلومات والقدرات والأدوات والآليات المتاحة أمام دوائر الأعمال والمستعملين النهائيين الآخرين.

(vii) إجراء استقصاءات، حسبما يتناسب، في المجالات المبينة أعلاه، بغرض تحديد الخطوات المتخذة من جانب البلدان ودوائر الأعمال وأفرقة الخبراء.

(viii) نتيجة لهذه الاستقصاءات، وضع خلاصة وافية بجميع الممارسات الوطنية و/أو الإقليمية ذات الصلة في هذا المجال، تشمل جميع الردود والمعلومات ذات الصلة.

(ix) إجراء دراسة/عملية تقييميّة لتزويد الدول الأعضاء بمعلومات تمكّنها من المفاضلة والمقارنة بين جميع السياسات الحالية الجاري تنفيذها في دول أعضاء أخرى بالاتحاد.

(x) دراسة المعلومات المتاحة عن هذه الموضوعات من مصادر مختلفة، بما في ذلك أصحاب المصلحة المعنيين.

ج) استعمال تقرير أفضل الممارسات إلى جانب المواد الأخرى ذات الصلة لوضع مواد منهج دراسي بشأن الموضوعات المحددة في الفقرات 2ب) (i)-(v) أعلاه للمساعدة في تحليل استراتيجيات الأمن السيبراني الوطنية والتخطيط لبرامج التدريب العملية. ويمكن استعمال مواد هذا المنهج وحدها أو كجزء من ورش العمل والمنتديات الأخرى الخاصة بالخبراء؛

د) استناداً إلى المساهمات المقدمة، تجميع مجموعة من دراسات الحالة القطرية لأغراض المعلومات تقوم بوصف الحالة الراهنة لجهود الأمن السيبراني في هذه البلدان وسياساتها في مجال الأمن السيبراني؛

هـ) وضع إطار للعمل عليه وتنفيذه في إطار البرنامج 2 بمكتب تنمية الاتصالات لزيادة الوعي لدى البلدان النامية بشأن الأمن السيبراني يغطي جميع المستويات الوطنية والإقليمية والدولية، وعلى وجه الخصوص:

---

[1] ملاحظة: رهناً بموافقة المؤتمر العالمي لتنمية الاتصالات لعام 2010 بحيدر آباد على القرار الجديد المقترح الذي يشجّع البلدان النامية على إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية، يجب أن تساعد هذه المسألة في تناول هذا القرار حال الموافقة عليه.

- دور الحكومة/الحكومات، بما في ذلك المركز الوطني للأمن السيبراني؛
- دور المجموعات الحكومية الدولية في الأمن السيبراني الوطني والإقليمي والدولي؛
- دور المجموعات غير الحكومية في الأمن السيبراني الوطني والإقليمي والدولي؛
- وغير ذلك.

حتى يتمكن مكتب تنمية الاتصالات من تنفيذ خطة عمل لإذكاء الوعي بالأمن السيبراني على كل المستويات في البلدان النامية.

و) يمكن لهذه المسألة أن تُشارك بدور ما في تنفيذ القرار 45 المراجَع مؤخراً[2].

3 الناتج المتوقع

(1) تقارير تُرفع للأعضاء بشأن القضايا المحددة في الفقرات 2ب) (i)-(v) أعلاه. وستبرز التقارير المشار إليها أن شبكات المعلومات والاتصالات الآمنة تشكل جزءاً لا يتجزأ من عملية بناء مجتمع المعلومات والتنمية الاقتصادية والاجتماعية لجميع الدول. وتشمل تحديات الأمن السيبراني إمكانية النفاذ غير المخول إلى المعلومات المتداولة عبر شبكات تكنولوجيا المعلومات والاتصالات وتدميرها وتعديلها. بيد أنه يمكن التخفيف من تداعيات هذه التحديات بزيادة الوعي بقضايا الأمن السيبراني وتبادل أفضل الممارسات الناجحة المستخدمة من جانب صانعي السياسات ودوائر الأعمال وعن طريق التعاون مع أصحاب المصلحة الآخرين. وإضافة إلى ذلك، يمكن لثقافة الأمن السيبراني أن تزيد من القناعة والثقة بهذه الشبكات وتحفّز الاستعمال الآمن وتكفل حماية البيانات والخصوصية مع تعزيز النفاذ والتداول وتمكن الدول من تحقيق فوائد التنمية الاقتصادية والاجتماعية لمجتمع المعلومات وذلك بصورة أفضل.

(2) مواد تثقيفية للاستخدام في ورش العمل والحلقات الدراسية وما إلى ذلك.

4 التوقيت

يُقترح أن تستغرق هذه الدراسة أربع سنوات مع تقديم تقارير حالة أولية عن التقدم المحرز بعد 12 شهراً و24 شهراً و36 شهراً.

5 جهة الاقتراح

لجنة الدراسات 1 بقطاع تنمية الاتصالات ولجنة البلدان الأمريكية للاتصالات (CITEL) والدول العربية.

6 مصادر المُدخلات

أ) الدول الأعضاء وأعضاء القطاعات.

ب) الأعمال ذات الصلة التي يجري الاضطلاع بها حالياً في لجان دراسات قطاع تقييس الاتصالات وقطاع الاتصالات الراديوية.

ج) المُخرَجات ذات الصلة من المنظمات الدولية والإقليمية، بما في ذلك المنظمة الدولية للتوحيد القياسي (ISO) ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD).

د) المنظمات غير الحكومية ذات الصلة المعنية بتعزيز الأمن السيبراني وثقافة الأمن.

هـ) الاستقصاءات والموارد المتاحة على الخط.

و) مصادر أخرى، حسب الاقتضاء.

[2] ملاحظة: تعتمد هذه الفقرة على نتائج المؤتمر العالمي لتنمية الاتصالات بحيدر آباد بشأن مراجعة القرار 45.

7 الجمهور المُستهدف

	البلدان المتقدمة	البلدان النامية[3]
صانعو سياسات الاتصالات	نعم	نعم
منظمو الاتصالات	نعم	نعم
مقدمو/مشغلو الخدمات	نعم	نعم
المصنعون	نعم	نعم

أ) الجمهور المستهدف

صانعو السياسات على المستوى الوطني وأعضاء القطاعات، وأصحاب المصلحة الآخرون المعنيون بأنشطة الأمن السيبراني أو المسؤولون عنه، وخصوصاً من البلدان النامية.

ب) الأساليب المقترحة لتنفيذ النتائج

يُركّز برنامج الدراسة على جمع المعلومات وأفضل الممارسات، ولذلك فإنه سيكون إعلامياً في طبيعته ويمكن استعمال هذه المعلومات في زيادة وعي الدول الأعضاء وأعضاء القطاعات بقضايا الأمن السيبراني واسترعاء انتباههم إلى المعلومات، والأدوات وأفضل الممارسات المتاحة، ويمكن استخدام نتائج ذلك في الحلقات الدراسية وورش العمل التي ينظمها مكتب تنمية الاتصالات.

8 الأساليب المقترحة لتناول هذه المسألة أو القضية

سيتم تناول هذه المسألة في نطاق لجنة دراسات على مدى فترة دراسات من أربع سنوات (مع تقديم النتائج المرحلية)، وسيقوم المقرر ونوابه بإدارة المسألة. ومن شأن ذلك أن يتيح للدول الأعضاء وأعضاء القطاعات المساهمة بخبراتهم والدروس التي خرجوا بها بشأن الأمن السيبراني.

9 التنسيق

التنسيق مع قطاع تقييس الاتصالات، وخصوصاً مع لجنة الدراسات 17 أو خليفيتها. ونظراً لمستوى الخبرات التقنية المتاحة بشأن هذه المسألة لدى لجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات، ينبغي إرسال جميع الوثائق (الاستبيانات والتقارير المرحلية ومشاريع التقارير النهائية وغيرها) إلى لجنة الدراسات 17 لإبداء ملاحظاتها وتقديم مدخلاتها قبل تقديمها إلى لجنة الدراسات التابعة لقطاع تنمية الاتصالات للتعليق عليها واعتمادها.

10 جهة الاتصال بمكتب تنمية الاتصالات

البرنامج 2 التابع لقطاع تنمية الاتصالات.

_____

[3] يشمل مصطلح "البلدان النامية" أيضاً أقل البلدان نمواً والدول الجُزُرية الصغيرة النامية والبلدان النامية غير الساحلية والبلدان التي تمر اقتصاداتها بمرحلة انتقالية.