|  |  |
| --- | --- |
| **المجلس 2022جنيف، 31-21 مارس 2022** | A picture containing text, clipart  Description automatically generated |
|  |  |
|  |  |
| **بند جدول الأعمال: PL 1.4** | **الوثيقة C22/32-A** |
| **18 فبراير 2022** |
| **الأصل: بالإنكليزية** |
| تقرير من الأمين العام |
| مشروع المبادئ التوجيهية للاتحاد الدولي للاتصالات لكيفية استخدامه البرنامج العالمي للأمن السيبراني |

|  |
| --- |
| **ملخص**كلَّف المجلس في دورته لعام 2019 الأمين العام بأن يقدم، بالتوازي، إلى دورة المجلس التالية (1) تقريراً يوضح كيف يستخدم الاتحاد حالياً إطار البرنامج العالمي للأمن السيبراني (GCA)، و(2) مبادئ توجيهية مناسبة، تُعدُّ بمشاركة الدول الأعضاء، بشأن كيفية استخدام الاتحاد هذا البرنامج، كي ينظر فيهما المجلس ويوافق على المبادئ التوجيهية (الوثيقتان C19/117 وC19/58).وتنفيذاً لهذه التعليمات، صيغَ مشروع المبادئ التوجيهية بدعم من رئيس القضاة (المتقاعد) السيد شتاين شولبرغ (الرئيس السابق لفريق الخبراء الرفيع المستوى المعني بالأمن السيبراني (HLEG))، والأستاذة سولونج غرناوطي، والسيد نوبورو ناكاتاني، وبمشاركة الدول الأعضاء وأصحاب مصلحة آخرين، وعُرض المشروع، إلى جانب التقرير المقدم من الأمانة (C21/36)، على اجتماع المشاورة الافتراضية لأعضاء المجلس لعام 2021 (C21/VCC-1) كي ينظر فيهما المجلس ويوافق على المشروع (C21/71).وعقب المشاورة الافتراضية لأعضاء المجلس لعام 2021، أحاطت الدول الأعضاء في المجلس علماً بالتقرير المقدم من الأمانة واتخذت بالمراسلة قراراً بشأن مشروع المبادئ التوجيهية بتكليف الأمانة بأن تجري مزيداً من المشاورات مع الدول الأعضاء في المجلس، وتأخذ في اعتبارها المساهمات الواردة والتعليقات المقدمة في هذا الاجتماع. وينبغي للأمانة أن تُعيد إلى المجلس نسخة منقَّحة من الوثيقة لينظر فيها ويوافق عليها في دورته المقبلة.ووفقاً لذلك، عُقدت المزيد من المشاورات مع الدول الأعضاء في المجلس وأُعدَّت النسخة المنقَّحة التالية من مشروع المبادئ التوجيهية، مع أخذ المساهمات الواردة في الاعتبار، إلى جانب وثيقة معلومات داعمة ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)). ومن المهم الإشارة إلى أن هذه الجهود لا تهدف إلى معالجة المسائل المتعلقة بتنقيح البرنامج العالمي للأمن السيبراني، ولن تهدف إلى ذلك.**الإجراء المطلوب**تقدَّم هذه الوثيقة إلى المجلس **لينظر** فيها و**يوافق** عليها، على النحو المناسب.***ملاحظة: تناقش الدول الأعضاء في المجلس مشروع المبادئ التوجيهية هذا حالياً، ويُعتزم إجراء مزيد من المشاورات في مرحلة الاستعدادات النهائية لعقد دورة المجلس لعام 2022 لمناقشة المسائل المعلَّقة (المبيَّنة باستخدام أقواس معقوفة) في هذه الوثيقة.***ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ**المراجع**[*القرار 130 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-A.pdf)[*البرنامج العالمي للأمن السيبراني (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*،* [*الوثيقة C21/36 للمجلس*](https://www.itu.int/md/S21-CL-C-0036/en)*،* *وثائق المجلس* [*C21/36*](https://www.itu.int/md/S21-CL-C-0036/en)*،* [*C21/71*](https://www.itu.int/md/S21-CL-C-0071/en)*،* [*C19/117*](https://www.itu.int/md/S19-CL-C-0117/en)*،* [*C19/58*](https://www.itu.int/md/S19-CL-C-0058/en)*،* [*C22/INF/8*](https://www.itu.int/md/S22-CL-INF-0008/en) |

# القسم 1 مقدمة

**1.1** اعتمد مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات لعام 2018 الذي عُقد في دبي [القرار 130](https://www.itu.int/en/council/Documents/basic-texts/RES-130-A.pdf): *تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات*. وينص القرار، ضمن جملة أمور، *على استخدام إطار البرنامج العالمي للأمن السيبراني (GCA) لمواصلة توجيه عمل الاتحاد بشأن الجهود الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT).*

**2.1** وأثناء المناقشات التي دارت في الجلسة العامة قبيل اعتماد القرار 130، *لاحظ* الأمين العام للاتحاد *بارتياح الاعتراف على نطاق واسع، أثناء المناقشات بشأن مشروع القرار، بقيمة البرنامج العالمي للأمن السيبراني. وناشد الجلسة العامة أن توافق على الاحتفاظ بالفقرة 1.12 من "يقـرر"، مما يسمح للاتحاد بالاستفادة من هذا البرنامج لتوجيه أعماله بشأن الثقة والأمن في تكنولوجيا المعلومات والاتصالات. وقال إنه سيطلب المشورة من المجلس ومن الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالبرنامج العالمي للأمن السيبراني، القاضي شتاين شولبرغ، في هذا الصدد*.[[1]](#footnote-1)

**3.1** وقُدم تقرير الرئيس السابق لفريق الخبراء الرفيع المستوى المعني ب[البرنامج العالمي للأمن السيبراني](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (HLEG) إلى دورة مجلس الاتحاد لعام 2019، الذي يشير إلى أنه يمكن وضع مبادئ توجيهية مناسبة لتحسين الاستفادة من البرنامج العالمي للأمن السيبراني.[[2]](#footnote-2) وفي هذا الاجتماع، كلَّف المجلس الأمين العام بأن يقدم، بالتوازي، إلى دورة المجلس التالية (1) تقريراً يوضح كيفية استخدام الاتحاد حالياً إطار البرنامج العالمي للأمن السيبراني (GCA)، و(2) مبادئ توجيهية مناسبة، معدة بمشاركة الدول الأعضاء، بشأن كيفية استخدامه البرنامج، كي ينظر فيهما المجلس ويوافق على المبادئ التوجيهية.[[3]](#footnote-3)

**4.1** وتنفيذاً لهذه التعليمات، صدرت رسالة معمَّمة [(CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/en) تبيِّن عملية إعداد مشروع المبادئ التوجيهية، وعُقدت في 23 أبريل 2020 و1 مارس 2021 مشاورتان مفتوحتان لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات (WSIS) ليقدموا تعليقات بشأن هذا المشروع (مشاورة مفتوحة). وحضر الاجتماعين أكثر من 160 مشاركاً وقدموا تعقيبات على كل قسم من أقسام مشروع المبادئ التوجيهية. وقد نُشرت في [الموقع الإلكتروني للبرنامج العالمي للأمن السيبراني](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) جميع التعليقات الخطية التي وردت من المشاركين قبل عقد المشاورتين أو بعده.

**5.1** وأعدَّت الأمانة، آخذةً المساهمات الواردة في اعتبارها، التقرير الذي يوضح كيفية استخدام الاتحاد حالياً إطار البرنامج العالمي للأمن السيبراني ([تقرير الأمانة](https://www.itu.int/md/S21-CL-C-0036/en))، وصيغَ مشروع المبادئ التوجيهية لكيفية استخدام الاتحاد هذا البرنامج ([مشروع المبادئ التوجيهية](https://www.itu.int/md/S21-CL-C-0071/en)) بدعم من رئيس القضاة (المتقاعد) السيد شتاين شولبرغ (الرئيس السابق لفريق الخبراء الرفيع المستوى المعني بالأمن السيبراني)، وبمشاركة الدول الأعضاء، كي ينظر فيهما المجلس ويوافق على المشروع. ويعرب الأمين العام عن امتنانه للتوجيه الذي قدمه كل من الأستاذة سولونج غيرناوطي (الفريق السويسري للمشورة والبحوث في مجال الأمن السيبراني، جامعة لوزان)، بشأن القسمين المتعلقين بالركيزتين 2 و4 من البرنامج العالمي للأمن السيبراني، والسيد نوبورو ناكاتاني (المدير التنفيذي السابق للمجتمع العالمي للابتكار التابع للإنتربول)، بشأن القسم المتعلق بالركيزة 3 من هذا البرنامج، ولمساهمتهما في إعداد هذه الأقسام. ومن المهم الإشارة إلى أن هذه الجهود لا تهدف إلى معالجة المسائل المتعلقة بتنقيح البرنامج العالمي للأمن السيبراني، ولن تهدف إلى ذلك.

**6.1** ونظراً إلى وقوع جائحة فيروس كورونا (كوفيد-19(، أُرجئ عرض هذه الوثائق إلى المشاورة الافتراضية لأعضاء المجلس لعام 2021 (VCC 2021) التي عُقدت في الفترة 18-8 يونيو 2021. وعقب المشاورة، أحاطت الدول الأعضاء في المجلس علماً بالتقرير المقدم من الأمانة واتخذت بالمراسلة قراراً بشأن مشروع المبادئ التوجيهية *"بتكليف الأمانة بأن تجري مزيداً من المشاورات مع الدول الأعضاء في المجلس، وتأخذ في اعتبارها المساهمات الواردة والتعليقات المقدمة في هذا الاجتماع. وينبغي للأمانة أن تُعيد إلى المجلس نسخة منقَّحة من* [*الوثيقة 71*](https://www.itu.int/md/S21-CL-C-0071/en) *لينظر فيها ويوافق عليها في دورته المقبلة".*

**7.1** ووفقاً لذلك، عُقدت المزيد من المشاورات مع الدول الأعضاء في المجلس وأُعدَّت وثيقتان، مع أخذ المساهمات الواردة في الاعتبار، هما:

 أ ) وثيقة معلومات ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)) تعرض خلفية وسياق إعداد مشروع المبادئ التوجيهية هذا وتطور المشهد المحيط بإعداده؛

ب) ومشروع المبادئ التوجيهية هذا المبين أدناه الذي أُعدَّ لينظر فيه المجلس في دورته لعام 2022 ويوافق عليه.

وقد أُخذت في الاعتبار عند إعداد هاتين الوثيقتين التوصيات الواردة في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، والأنشطة التي اضطلع بها الاتحاد منذ صدور ذلك التقرير، والتطورات المستجدة في هذا المجال منذ عام 2008[، والمساهمات الواردة من الدول الأعضاء](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) وأصحاب المصلحة الآخرين (عملاً بالرسالتين المعممتين ([CL-20/18](https://www.itu.int/md/S20-SG-CIR-0018/en) و[CL‑20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)).

**8.1** وعلى الرغم من إقرار الترابط المتبادل بين الركائز الخمس، يتناول كل قسم ركيزة محددة من البرنامج العالمي للأمن السيبراني ويقترح مبادئ توجيهية محددة لاستخدامها. ويركز القسم 2 على التدابير القانونية. ويتناول القسم 3 التدابير القانونية والإجرائية. ويعالج القسم 4 بناء القدرات. ويتعلق القسم 5 بالهياكل التنظيمية ويغطي القسم 6 التعاون الدولي. ويتضمن القسم 7 بعض المبادئ التوجيهية الشاملة العامة لاستخدام إطار البرنامج العالمي للأمن السيبراني.

# القسم 2 الركيزة 1 - التدابير القانونية

**2** نظراً إلى التقدم السريع في مجال التكنولوجيا، فإن التدابير التي تتخذها المنظمات والبلدان بحاجة إلى التطور لمواكبة معدل التغير. وهذا يجلب تعقيدات جديدة لتحدي الأمن السيبراني، مما يتطلب دراسة دقيقة من زوايا مختلفة ومتنوعة. وفي هذا السياق، ترد أدناه مبادئ توجيهية مقترحة لاستخدام الركيزة 1:

**أ )** ينبغي للاتحاد أن يواصل بذل جهود [في إطار ولايته] لتيسير النقاش والتعاون فيما بين أصحاب المصلحة المتعددين من أجل معالجة التحديات المقترنة بالأمن السيبراني، ولا سيما تعزيز علاقته مع جميع أصحاب المصلحة الآخرين لتقديم المساعدة إلى الدول الأعضاء في هذا الصدد.

**ب)** وينبغي للاتحاد أن يواصل العمل، في إطار ولايته، مع الشركاء المعنيين من أجل التشجيع على استحداث مراجع لتشريعات الأمن السيبراني والجرائم السيبرانية وعلى الإبقاء على هذه المراجع، لمساعدة الدول الأعضاء على فهم الجوانب القانونية للأمن السيبراني، مع دعم تبادل الخبرات والمعارف بين الدول الأعضاء لدعم جهودها الرامية إلى وضع أطر لهذا الموضوع، [تشمل أُطراً قانونية دولية].

**ج)** وينبغي للاتحاد أن يعمد، بالتعاون مع جميع أصحاب المصلحة [المناسبين]، إلى تعزيز فهم أفضل للتحديات والمخاطر القانونية المتصلة بالأمن السيبراني التي تشكلها التكنولوجيات الناشئة، وتيسير تبادل دراسات الحالة والممارسات الجيدة على المستويات الوطنية والإقليمية والدولية.

**د )** [ولا بد أيضاً لجميع أصحاب المصلحة المعنيين من اتخاذ التدابير القانونية المناسبة لتنفيذ برامج فعّالة لمنع أو حظر نشر المواد الإلكترونية المتعلقة بالاعتداء الجنسي على الأطفال واستغلالهم جنسياً، بما في ذلك اتخاذ إجراءات وقائية لكشف وتعطيل وتفكيك الشبكات أو المنظمات أو الهياكل التي تُستخدم لإنتاج و/أو توزيع مواد على الإنترنت تتعلق بالاعتداء الجنسي على الأطفال واستغلالهم جنساً، ووضع آليات للكشف عن الجناة ومحاكمتهم مع تحديد الضحايا وحمايتهم. وفي هذا الصدد،] ينبغي أن يواصل الاتحاد تعزيز برنامج حماية الأطفال على الإنترنت كمنصة للعمل مع الشركاء وأصحاب المصلحة لتعزيز تبادل المعارف والمعلومات والأنشطة (بما يشمل تلك المتعلقة بالتدابير القانونية) التي يمكن أن تسهل وتدعم الإجراءات القُطرية بشأن هذه القضية الحاسمة.

# القسم 3 الركيزة 2 - التدابير التقنية والإجرائية

**3** لا تزال التوصيات المتعلقة بالركيزة 2 في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 سارية. وفي ضوء ذلك، تُقترح المبادئ التوجيهية التالية من أجل الركيزة 2:

**أ )** ينبغي أن تركز لجان الدراسات التابعة للاتحاد على التكنولوجيات الناشئة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات (ICT)، من أجل دراسة واقتراح مبادئ توجيهية وتوصيات في مجال الأمن السيبراني تتعلق ببناء الثقة والأمن في استخدام هذه التكنولوجيات، وأن توصي الدول الأعضاء بتطبيقها طواعيةً في الوقت المناسب.

**ب)** ينبغي إنشاء آلية للتعاون الوثيق بين مختلف لجان دراسات قطاع تقييس الاتصالات فيما يتعلق بدراسة المسائل المتعلقة بالأمن السيبراني، مع قيام لجنة الدراسات 17 بدور تنسيقي/قيادي، بحيث يتم الحفاظ على أعلى درجة ممكنة من الأمن من طرف إلى طرف طوال عملية تقييس جميع مكونات وواجهات منتجات تكنولوجيا المعلومات والاتصالات.

**ج)** ينبغي تشجيع التنسيق والتعاون الوثيقين، على أساس المعاملة بالمثل التي يقيمها الاتحاد مع المنظمات الأخرى المعنية بوضع المعايير، لضمان الحفاظ على أمن المنتجات من البداية إلى النهاية لمختلف التطبيقات والخدمات طوال دورة حياة المنتجات.

**د )** ينبغي أن يواصل الاتحاد نشر المعايير الأمنية العالمية لتكنولوجيا المعلومات والاتصالات ويعمل، أيضاً، مع غيره من المنظمات المعنية بوضع المعايير (SDO) ومع المجموعات الصناعية الأخرى لتشجيعها على أن تقدم إلى قطاعي تقييس الاتصالات (ITU-T) والاتصالات الراديوية (ITU-R) بالاتحاد معاييرها المتعلقة بالتدابير التقنية والإجرائية للموافقة عليها كتوصيات صادرة عن هذين القطاعين.

**ه‍ )** ينبغي أن يواصل الاتحاد جهوده الرامية إلى وضع توصيات [طوعية] بشأن التدابير التقنية والإجرائية للأمن السيبراني في المجالات التي تدخل في إطار ولايته، بتحفيز أعضائه على زيادة مشاركتهم فيما يضطلع به من أنشطة تقييسية ذات صلة، وإقامة شراكات استراتيجية والتشاور مع الجامعات والمنظمات المعنية بوضع المعايير.

**و )** [ينبغي أن يواصل الاتحاد تشجيع أعضائه على البدء/المشاركة في تنفيذ ترتيبات إصدار الشهادات المتبادلة بهدف إنشاء نظم دولية لإصدار شهادات الأمن السيبراني في العالم تستند إلى معايير منسقة.]

# القسم 4 المبادئ التوجيهية لاستخدام الركيزة 3 - الهياكل التنظيمية

**4** على الرغم من الاعتراف بأن التوصيات الواردة في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 قد عملت بشكل جيد في توجيه جهود الاتحاد في إطار الركيزة 3 لا تزال ذات صلة، يمكن للمبادئ التوجيهية التالية المقترحة، ذات الصلة بشكل خاص بعمل مكتب تنمية الاتصالات (BDT) بالاتحاد، أن تساعد في تعزيز الجهود المبذولة في هذا الصدد:

 **أ )** ينبغي للاتحاد أن يواصل تقديم المساعدة إلى البلدان النامية، وأقل البلدان نمواً، والدول الجزرية الصغيرة النامية (SIDS)، في تصميم وتنفيذ إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية (CIRT) وما يتصل بها من وحدات/منظمات تقنية أخرى.

**ب)** تفادياً لازدواجية الجهود، ينبغي للاتحاد أن يواصل التشجيع على التعاون والتنسيق المنفتحين والشاملين، في إطار ولايته، فيما بين مختلف المنظمات الوطنية أو الإقليمية أو الدولية المشاركة في الجهود الرامية إلى إنشاء هياكل تنظيمية وطنية مستدامة.

**ج)** ينبغي للاتحاد أن يعزز جهوده الرامية إلى قياس الالتزامات المؤسسية للدول الأعضاء، بالاستفادة من أدوات مثل الرقم القياسي العالمي للأمن السيبراني (GCI) لتعزيز الأمن السيبراني كعامل تمكيني، شامل، لجهود هذه الدول الأعضاء في مجال التحول الرقمي.

**د )** فيما يتعلق بالهياكل الوطنية على وجه الخصوص، ينبغي للاتحاد، بناءً على طلب الدول الأعضاء، أن يقدم إليها المساعدة في رسم استراتيجيات لإنشاء إطار تنسيقي يشمل كامل القطاعات الحكومية لتحسين التنفيذ المتسق والشامل للجهود الوطنية المتعلقة بالأمن السيبراني.

**هـ )** ينبغي للاتحاد أن يواصل تعزيز المزيد من التعاون بين الهياكل التنظيمية للأمن السيبراني على الصعيدين الإقليمي والعالمي من خلال أنشطة مثل التدريبات السيبرانية وغيرها.

# القسم 5 المبادئ التوجيهية لاستخدام الركيزة 4 - بناء القدرات

**5** في ضوء ما تقدم، لا يزال البرنامج العالمي للأمن السيبراني والتوصيات الواردة في إطار هذه الركيزة من تقرير الفريق لعام 2008 توفر إطاراً متيناً يعزز ويشجع نهجاً متعدد التخصصات لبناء القدرات. ومع مراعاة ذلك، يُقترح أن يقوم الاتحاد، من خلال مكتبه لتنمية الاتصالات (BDT) بما يلي:

**أ )** مواصلة التشجيع على زيادة الانفتاح والشمول في التعاون والتنسيق فيما بين مختلف المنظمات الوطنية والإقليمية والدولية المشاركة في بناء القدرات في مجال الأمن السيبراني من أجل ضمان التأثير وتجنب ازدواجية الجهود.

**ب)** مواصلة دعم البلدان النامية، وأقل البلدان نمواً، والدول الجزرية الصغيرة النامية، في جهود بناء القدرات في مجال الأمن السيبراني، بدعم من المجتمعات الوطنية والدولية المعنية ببناء القدرات في مجال الأمن السيبراني.

**ج)** مواصلة مساعدة البلدان النامية، وأقل البلدان نمواً، والدول الجزرية الصغيرة النامية، بالتعاون مع الشركاء المهتمين والمجتمعات المعنية بتنمية القدرات، على تحديد استراتيجيات وخطط وسياسات وقدرات وطنية في مجال الأمن السيبراني للاستجابة للحوادث.

**د )** مواصلة جهود بناء القدرات لسد الفجوة التقييسية، وذلك بسبل منها تقديم المساعدة التقنية إلى البلدان بناءً على الطلب.

**هـ )** تعزيز وتيسير تبادل الممارسات الجيدة للدول الأعضاء من أجل مساعدة البلدان المتخلفة عن الركب من حيث الخبرة المتخصصة في مجال الأمن السيبراني على تحسين وضعها في مجال الأمن السيبراني وتقليص الفجوة في القدرات.

**و )** مواصلة تطوير أنشطته في مجال بناء القدرات مع مراعاة الحاجة إلى مهارات جديدة للتكيف مع الفرص والتحديات المقترنة بالتكنولوجيات الناشئة في ميدان الأمن السيبراني. وفي هذا الصدد، ينبغي تعزيز التعاون مع الهيات الأكاديمية والقطاع الخاص والدول الأعضاء.

**ز )** مواصلة التركيز بشكل خاص على احتياجات الفئات الأكثر ضعفاً، كالنساء والأطفال والأشخاص ذوي الإعاقة والأشخاص ذوي الاحتياجات المحددة والأشخاص ذوي الإعاقات المتصلة بالسن، في جهود بناء القدرات.

**ح)** مواصلة تطوير وتعزيز البرنامج العالمي للأمن السيبراني (GCI) بوصفه أداة لبناء القدرات والوعي.

**ط)** [وضع "دليل لإعداد وتنفيذ برنامج التعليم في مجال الأمن السيبراني" بهدف تقديم الدعم إلى الدول الأعضاء في تطوير/اعتماد دورات في مجال الأمن السيبراني للشباب في أنظمة التعليم المهني والابتدائي والثانوي والجامعي وللمهنيين من أجل المساهمة في تدريب مزيد من المهنيين في مجال الأمن السيبراني على الصعيد العالمي وزيادة الوعي بقضايا الأمن السيبراني في جميع التخصصات وفي أوساط جميع مهنيي المستقبل]

**ي)** مواصلة تسهيل تحديد الأنشطة البحثية المتصلة بالأمن السيبراني بين أصحاب المصلحة، خاصةً في مجال التكنولوجيا الناشئة، والاستفادة من أعضاء الاتحاد من الهيئات الأكاديمية والقطاع الخاص.

**ك)** نشر الأدوات والموارد والممارسات الجيدة لفائدة الدول الأعضاء ودوائر الصناعة وأصحاب المصلحة الآخرين بهدف دعم جهودهم الرامية إلى بناء قدرات المؤسسات الصغرى والصغيرة والمتوسطة (MSME) لبناء الثقة والاطمئنان في استخدام تكنولوجيا المعلومات والاتصالات، ومواصلة تعزيز ثقافة الأمن السيبراني.

# القسم 6 المبادئ التوجيهية لاستخدام الركيزة 5 - التعاون الدولي

6 نظراً إلى الطابع الشامل لهذه الركيزة، وبالنظر إلى نطاق التعاون والشراكات في مختلف قطاعات الاتحاد، من المهم أن تعمل جميع قطاعات الاتصالات معاً بشكل وثيق وأن تنسق جهودها، داخلياً وخارجياً باستخدام آليات تنسيق فعّالة ومشتركة بين القطاعات وجهات تنسيق معيّنة. ولا تزال توصيات تقرير الفريق لعام 2008 في هذا الصدد ذات صلة، واستناداً إلى المعلومات المقدمة في القسم أعلاه، تُقترح كذلك المبادئ التوجيهية التالية لاستخدام الركيزة 5:

**أ )** [تقوم الأمم المتحدة بدور فريد في تعزيز التعاون والحوار والتنسيق بين جميع الدول وكذلك مع القطاع الخاص وأصحاب المصلحة الآخرين، بشأن مسائل الأمن السيبراني العالمية. وينبغي للاتحاد، بالنظر إلى مركزه في منظومة الأمم المتحدة بوصفه الوكالة المتخصصة المعنية بتكنولوجيا المعلومات الاتصالات والميسّر الوحيد لخط العمل جيم5 (بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات) أن يواصل القيام بدور رائد، في المجالات التي تدخل في نطاق ولايته، فيما يتعلق بالتطورات ذات الصلة.]

**ب)** [واستناداً إلى عملية القمة العالمية لمجتمع المعلومات، ومع مراعاة جهود الفريق الرفيع المستوى المعني بالتعاون الرقمي والتابع للأمين العام للأمم المتحدة، ولا سيما التوصية 4 (الالتزام العالمي بالثقة والأمن)، ينبغي للاتحاد أن يساعد في تعزيز جهود التيسير في الجمع بين مختلف الأطراف الفاعلة. ويمكن أن يتم ذلك من خلال الآليات المتاحة في إطار العمليات ذات الصلة بخط العمل جيم5 من خلال منتدى القمة العالمية لمجتمع المعلومات، وكذلك تلك التي يوفرها منتدى إدارة الإنترنت وغيرها]

**ج)** في حين ينبغي مواصلة تشجيع الجهات الفاعلة الرئيسية على إجراء مناقشات ثنائية ومتعدد الأطراف فيما بينها، نظراً إلى عالمية طبيعة الأمن السيبراني، من اللازم أيضاً تيسير إجراء مناقشات أوسع نطاقاً فيما بين مجموعات أوسع، تشمل القطاع الخاص وهيئات الأمم المتحدة والهيئات الأكاديمية ومنظمات المجتمع المدني وأصحاب المصلحة الآخرين [، بهدف التوصل إلى تدابير عالمية منصفة وشاملة، قادرة على حسم مختلف التحديات الأمنية السيبرانية]. ويمكن للاتحاد، في المجالات التي تدخل في نطاق ولايته، أن يضطلع بدوري تيسيري في هذا الصدد، من خلال العمل مع الشركاء للمساعدة في جمع أصحاب المصلحة كافة في السياق العالمي الأوسع للأمم المتحدة.

**د )** ينبغي للاتحاد أن يواصل استكشاف آليات مبتكرة ومرنة وسريعة الحركة لبناء الشراكات مع مراعاة قطاع تكنولوجيا المعلومات والاتصالات سريع التطور ومجموعة الكيانات الجديدة الناشئة، ولا سيما المشاريع المبتدئة والشركات الصغرى والصغيرة والمتوسطة.

**ه‍ )** ينبغي للاتحاد أن يواصل العمل مع الوكالات الرئيسية الأخرى داخل منظومة الأمم المتحدة من أجل دعم الجهود الداخلية التي تبذلها أمانة الأمم المتحدة لتنسيق وتبسيط برامجها وأنشطتها المتعلقة بالأمن السيبراني، لكي يكون أكثر فعالية في خدمة المجتمع العالمي.

# القسم 7 المبادئ التوجيهية العامة لإطار البرنامج العالمي للأمن السيبراني

**7** أسفرت عملية وضع مبادئ توجيهية لاستخدام البرنامج العالمي للأمن السيبراني عن عدد قليل من المبادئ التوجيهية الشاملة الواسعة المنطبقة وذات الصلة بجميع أعمال الاتحاد والركائز الخمس للبرنامج العالمي. واعترافاً بالروابط القوية بين الركائز وضرورة أن يعمل الاتحاد وشركاؤه لوضع رؤية عمل كاملة وشاملة بشأن الأمن السيبراني، تُقترح المبادئ التوجيهية العامة أدناه:

**أ )** نظراً إلى انتشار أصحاب المصلحة والمنظمات والشراكات والأماكن التي تعمل بشأن الأمن السيبراني وتدفع مختلف جوانب التقدم، ينبغي للاتحاد أن يواصل تعزيز وتوسيع دائرة تعاونه ومشاركته بما يعود بالفائدة الجماعية على جميع أصحاب المصلحة هؤلاء، من أجل تعزيز تقاسم المعارف وتبادل المعلومات والخبرات مع تجنب ازدواجية الجهود أيضاً.

**ب)** ينبغي للاتحاد أن يكون بمثابة مستودع للمعلومات لمختلف الأنشطة والمبادرات والمشاريع العالمية المنفذة في مختلف جوانب الأمن السيبراني من جانب أصحاب المصلحة الآخرين والمنظمات الأخرى النشطة في هذا المجال، والتي يمكن أن يكون لها ولاية ودور و/أو مسؤوليات رائدة في تلك الجوانب المحددة لتمكين المجتمع الدولي من الوصول بسهولة إلى جميع هذه الموارد.

**ج)** ينبغي أن تسترشد جميع الأعمال التي يضطلع بها الاتحاد عملاً بالبرنامج العالمي للأمن السيبراني بتقييم عالمي لاحتياجات وأهداف أعضائه باستخدام أدوات مثل الرقم القياسي العالمي للأمن السيبراني (GCI)، كما ينبغي أن تسترشد بالنواتج المطلوبة لتلبيتها، وتتفق مع المقاييس والقياسات المناسبة المصممة خصيصاً لهذا الغرض.

**د )** ينبغي للاتحاد أن يواصل متابعة تطوير واستخدام تكنولوجيات المعلومات والاتصالات الجديدة والناشئة من أجل توجيه الدول الأعضاء وأصحاب المصلحة بشأن الجوانب الأمنية لهذه التكنولوجيات في المجالات التي تدخل في نطاق ولايته وعند الاقتضاء تطبيقها المحتمل لمكافحة التهديدات السيبرانية.

**ه‍ )** ونظراً إلى أثر الأمن السيبراني العابر للحدود الوطنية والشامل لعدة قطاعات بطبيعته، ينبغي للاتحاد أن يشجع الأنشطة والمبادرات والمشاريع التي يمكن أن تساعد الدول الأعضاء في تعزيز نهج حكومي شامل لمعالجة هذه المسألة.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

1. محضر الجلسة العامة السابعة عشرة لمؤتمر المندوبين المفوضين، دبي، الخميس 15 نوفمبر 2018، متاح في الموقع التالي:
<https://www.itu.int/md/S18-PP-C-0174/en>. [↑](#footnote-ref-1)
2. إحالة التقرير المقدم من الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالبرنامج العالمي للأمن السيبراني (الوثيقة C19/58)، الاتحاد الدولي للاتصالات، 8 مايو 2019، وهو متاح في الموقع التالي <https://www.itu.int/md/S19-CL-C-0058/en>. [↑](#footnote-ref-2)
3. محضر الجلسة العامة السادسة (الوثيقة C19/117)، الاتحاد الدولي للاتصالات، 20 يونيو 2019، متاح في الموقع التالي
<https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)