|  |  |
| --- | --- |
| **ال‍مجلس 2020 جنيف، 19-9 يونيو 2020** |  |
|  |  |
|  |  |
| **بند جدول الأعمال: PL 1.4** | **الوثيقة C20/18-A** |
|  | **30 مارس 2020** |
|  | **الأصل: بالإنكليزية** |
| تقرير من الأمين العام | |
| أنشطة الاتحاد الدولي للاتصالات بشأن تعزيز دوره في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات | |
|  | |

|  |
| --- |
| **ملخص**  يلخص هذا التقرير أنشطة الاتحاد الدولي للاتصالات منذ دورة المجلس التي عُقدت في عام 2019 فيما يتعلق بالقرار 130 (المراجَع في دبي، 2018) ودور الاتحاد بصفته الميسِّر الوحيد لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات وسائر قرارات الأعضاء بشأن تعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات (ICT).  **الإجراء المطلوب**  يُدعى المجلس إلى **الإحاطة علماً** بهذا التقرير.  \_\_\_\_\_\_\_\_\_  **المراجع**  *القرارات*[*71*](https://www.itu.int/en/council/Documents/basic-texts/RES-071-A.pdf) *و*[*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-A.pdf) *و*[*140*](https://www.itu.int/en/council/Documents/basic-texts/RES-140-A.pdf) *و*[*174*](https://www.itu.int/en/council/Documents/basic-texts/RES-174-A.pdf) *و*[*179*](https://www.itu.int/en/council/Documents/basic-texts/RES-179-A.pdf) *(المراجَعة في دبي، 2018)**والقرار*[*181*](https://www.itu.int/en/council/Documents/basic-texts/RES-181-A.pdf) *(غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين،* [*ولوائح الاتصالات الدولية*](http://www.itu.int/pub/S-CONF-WCIT-2012/en) *(المراجَعة في دبي، 2012)، والقرار*[*1306*](https://www.itu.int/md/S15-CL-C-0109/en) *للمجلس، والقرار*[*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(المراجَع في دبي، 2014) والقرارات* [*2 و67 و69*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *(المراجَعة في بوينس آيرس، 2017) للمؤتمر العالمي لتنمية الاتصالات، والهدف 2/النتيجة 2.2 لقطاع تنمية الاتصالات (*[*خطة عمل بوينس آيرس*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*)، والقرارات*[*50*](https://www.itu.int/pub/T-RES-T.50-2016) *و*[*52*](https://www.itu.int/pub/T-RES-T.52-2016) *و*[*75*](https://www.itu.int/pub/T-RES-T.75-2016) *(المراجَعة في الحمامات، 2016) والقرار*[*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(المراجَع في دبي، 2012) للجمعية العالمية لتقييس الاتصالات، ووثائق المجلس الصادرة مؤخراً* [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/en) *و*[*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en) *و*[*C17/18*](https://www.itu.int/md/S17-CL-C-0018/en) *و*[*C18/18*](https://www.itu.int/md/S18-CL-C-0018/en) *و*[*C19/18*](https://www.itu.int/md/S19-CL-C-0018/en) |

# 1 الأنشطة ذات الصلة بالأمن السيبراني ومكافحة الرسائل الاقتحامية

1.1 حظيت تنمية تكنولوجيا المعلومات والاتصالات، القائمة على الأمن والثقة، بالاعتراف بصفتها أمراً أساسياً للتنمية المستدامة. ويبيِّن هذا التقرير، المنظَّم حول الركائز الخمس [للبرنامج العالمي للأمن السيبراني (GCA)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)، الطبيعة التكاملية لبرامج عمل الاتحاد القائمة، ويسهِّل تنفيذ أنشطة مكتب تنمية الاتصالات (BDT) ومكتب تقييس الاتصالات (TSB) ومكتب الاتصالات الراديوية (BR) في هذا المجال.

# 2 التدابير القانونية

1.2 في إطار الهدف 2/الناتج 2.2 لخطة عمل بوينس آيرس يقوم الاتحاد، مراعياً المسألة 3/2 التي تعنى بها لجنة الدراسات 2 لقطاع تنمية الاتصالات (المسألة 22/1 سابقاً)، بمساعدة الدول الأعضاء على فهم الجوانب القانونية للأمن السيبراني من خلال [الموارد القانونية للاتحاد بشأن الجريمة السيبرانية](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx)، من أجل المساعدة في تحقيق تناسق الأطر القانونية لهذه الدول. وفي مجال التدابير القانونية، يتعاون الاتحاد بشكل وثيق مع شركاء من قبيل مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) وغيره من الخبراء.

# 3 التدابير التقنية والإجرائية

1.3 تواصل [لجنة الدراسات 17 لقطاع تقييس الاتصالات (SG-17)](http://www.itu.int/ITU-T/studygroups/com17/)، بصفتها لجنة الدراسات الرئيسية المعنية بالأمن وإدارة الهوية (IdM)، أداء دورها الأساسي في دراسة وتقييس الأمن السيبراني، ومكافحة الرسائل الاقتحامية، وإدارة الهوية، وشهادات التوصية ITU‑T X.509، وإدارة أمن المعلومات، وشبكات الاستشعار الشمولية، والبيانات البيومترية عن بُعد، وأمن الخدمات المتنقلة، وأمن التمثيل الافتراضي في سبيل أمن الحوسبة السحابية، وحماية المعلومات المحدِّدة لهوية الشخص، ومعمارية الأمن، وأمن التطبيقات، وذلك بالتعاون مع المنظمات الخارجية المعنية بوضع المعايير.

2.3 ومنذ أن قدمت لجنة الدراسات 17 تقريرها الأخير إلى المجلس، عقدت اجتماعاً واحداً في سبتمبر 2019، وضعت في إطاره [25 بنداً جديداً من بنود العمل في مجال التقييس](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). ووافقت لجنة الدراسات 17 على أكثر من ثلاثين توصية جديدة أو مراجعة لقطاع تقييس الاتصالات بشأن أمن تكنولوجيا المعلومات والاتصالات، منها ما يلي على وجه التحديد: الطبعة التاسعة من سلسلة التوصيات ITU-T X.500 المتعلقة بالمعايير الأساسية للأمن السيبراني، بشأن البنية التحتية للمفاتيح العمومية، التوصية X.1044 بشأن "المتطلبات الأمنية لإضفاء الطابع الافتراضي على الشبكات"، التوصية X.1045 بشأن "معمارية سلسلة الخدمات الأمنية، الخاصة بالشبكات والتطبيقات"، التوصية X.1059 بشأن "التوجيهات التنفيذية الصادرة للمنظمات المعنية بالاتصالات بشأن إدارة مخاطر أصولها التي يمكن النفاذ إليها عالمياً في الشبكات القائمة على بروتوكول الإنترنت"، التوصية X.1702 بشأن "معمارية مولِّد الأعداد العشوائية للضوضاء الكمومية"، التوصية X.1232 بشأن "الإطار التقني لمكافحة الرسائل الاقتحامية الإعلانية في المعلومات التي يُنتجها المستخدِم"، التوصية X.677 بشأن "آلية تعرُّف هوية المركبات الجوية غير المأهولة باستخدام معرِّف الأشياء"، التوصية X.1402 "التهديدات الأمنية التي تتعرض لها تكنولوجيا سجل الحسابات الموزَّع (DLT) "، التعديل 1 للتوصية X.1197 بشأن "المبادئ التوجيهية المراجَعة المتعلقة بمعايير اختيار خوارزميات التجفير المستخدمة لحماية خدمة تلفزيون بروتوكول الإنترنت ومحتواه"، التصويب 1 للتوصيةX.694 والتصويب 1 للتوصية X.893، بشأن لغة الترميز 1 لقواعد التركيب المجردة (ASN.1)، السلسلة Z.100 المراجَعة المتعلقة بلغة التوصيف والوصف، السلسلة Z.160 المراجعة المتعلقة بالإصدار الثالث من لغة ترميز الاختبار وترميز التحكم في الاختبار (TTCN-3). كما وافقت لجنة الدراسات 17 على إضافة جديدة بشأن حالات استخدام إطار ضمان الاستيقان من كيان (EAA)، وراجعت دليل جهات التنفيذ في سلسلة التوصيات Z.

3.3 ونظمت لجنة الدراسات 17 في 26 أغسطس 2019 [ورشة عمل الاتحاد بشأن "أمن التكنولوجيا المالية"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx) التي دامت ليوم واحد، وأسفرت عن اقتراحات بشأن أنشطة المتابعة المتعلقة بتكنولوجيا DLT، التي تُجريها لجنة الدراسات بالتعاون مع منظمات أخرى محددة من المنظمات المعنية بوضع المعايير وأمن التكنولوجيا المالية، أي الفريق المتخصص المعني بتطبيق تكنولوجيا سجل الحسابات الموزع (FG-DLT) والفريق المتخصص المعني بالعملة الرقمية، بما في ذلك العملة الرقمية الرسمية (FG-DFC) واللجنة التقنية 307 للمنظمة الدولية للتوحيد القياسي (ISO) واتحاد الشبكة العالمية (W3C) بشأن تكنولوجيا الشبكات الموزعة (DLT). ونظمت اللجنة أيضاً في 26 أغسطس 2019 [ورشة عمل مصغَّرة بشأن التحديات الأمنية السيبرانية في القيادة الآلية](file:///\\blue\dfs\pool\TRAD\A\SG\CONSEIL\C20\000\mini%20workshop%20on%20cybersecurity%20challenges%20in%20automated%20driving)، وذلك بالتعاون مع هيئة التعاون التابعة للاتحاد المعنية بوضع معايير الاتصالات الخاصة بأنظمة النقل الذكية (CITS) وفرقة العمل 29 التابعة للجنة الأمم المتحدة الاقتصادية لأوروبا (UNECE).

4.3 ونظراً إلى تفشّي فيروس كورونا، أصبح اجتماع لجنة الدراسات 17 الذي عُقد في الفترة26-17 مارس 2020 أول اجتماع افتراضي كلياً للجان دراسات قطاع تقييس الاتصالات. وقد اضطرت لجنة الدراسات أيضاً إلى تأجيل [ورشة العمل المشتركة بين لجنة الدراسات 17 لقطاع تقييس الاتصالات واللجنة التقنية 307 بالمنظمة الدولية للتوحيد القياسي (ISO TC 307) بشأن "أمن تكنولوجيا سجل الحسابات الموزع وإدارة الهوية والخصوصية"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx)، التي كانت تعتزم تنظيمها في 16 مارس 2020.

5.3 وواصلت لجنة الدراسات 17 العمل على أمن إنترنت الأشياء والتنسيق مع لجنة الدراسات 20 لقطاع تقييس الاتصالات المعنية بموضوع "إنترنت الأشياء وتطبيقاتها بما في ذلك المدن والمجتمعات الذكية (SC&C)".

6.3 وحددت لجنة الدراسات 9 لقطاع تقييس الاتصالات مشاريع خمس توصيات ITU-T J.1012 وITU-T J.1013 وITU-T J.1014 وITU-T J.1015 وITU-T J.1015.1 بشأن السطح البيني المشترك المدمج من أجل حلول النفاذ المشروط/إدارة الحقوق الرقمية (CA/DRM) القابلة للمبادلة.

7.3 ووافقت لجنة الدراسات 13 لقطاع تقييس الاتصالات على التعديل 1 للتوصية ITU-T Y.3053 (2018) بشأن "إطار التوصيل الشبكي الجدير بالثقة مع ميادين شبكية تتمحور حول الثقة: التعديل 1 - معمارية وإجراءات نشر الشبكات الجديرة بالثقة". كما وافقت لجنة الدراسات 13 على التصويب 1 للتوصية ITU-T Y.3514 "الحوسبة السحابية - إطار الحوسبة السحابية البينية الموثوق بها ومتطلباتها" والتوصية ITU-T Y.3517 "الحوسبة السحابية - نظرة عامة عن إدارة الثقة في الخدمات السحابية البينية".

8.3 وتعمل لجنة الدراسات 15 لقطاع تقييس الاتصالات على إعداد إضافة (G.Sup.otnsec) تصف اللغة المستخدمة في طبقات البروتوكول القائمة لشبكة النقل البصرية (OTN) وما يلزم هذه الطبقات من بنية تحتية مشتركة للبيانات تمكنها من استخدام بروتوكولات التجفير المقترحة على نحو مستقل لإيجاد حلول نقل مأمونة بشأن طبقات مختارة من الشبكة OTN.

9.3 ووافقت لجنة الدراسات 20 لقطاع تقييس الاتصالات على التوصية ITU-T Y.4807 بشأن " المرونة من خلال التصميم من أجل أمن أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات المستعملة في إنترنت الأشياء ".

10.3 وفي الوقت الحاضر، تبحث عدة أفرقة متخصصة تابعة للقطاع في إطار عملها جانب الثقة في العديد من التكنولوجيات الناشئة، ومن هذه الأفرقة: (1) [*الفريق المتخصص التابع لقطاع تقييس الاتصالات والمعني بالتعلم الآلي المتصل بشبكات المستقبل بما في ذلك شبكات الجيل الخامس* *(FG-ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx)، (2) [*الفريق المتخصص التابع للقطاع والمعني* بتكنولوجيا شبكات 2030 *(FG NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx)، (3) [*الفريق المتخصص التابع للقطاع والمعني بالذكاء الاصطناعي من أجل الصحة* *(FG* *AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h)، (4) [*الفريق* *المتخصص التابع للقطاع والمعني بالوسائط المتعددة في المركبات* *(FG-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)، (5) [*الفريق* *المتخصص التابع للقطاع والمعني بالذكاء الاصطناعي لأغراض القيادة الذاتية والمساعَدة (FG-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx)، (6) [*الفريق المتخصص التابع للقطاع والمعني بتكنولوجيا المعلومات الكمومية من أجل الشبكات (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*.*

11.3 وبالتعاون المشترك مع مؤسسة بيل وميليندا غيتس ومجموعة البنك الدولي وبنك التسويات الدولية، نظم الاتحاد [ورشة عمل بشأن الأمن والبنى التحتية والثقة في الخدمات المالية الرقمية](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Pages/default.aspx)، عُقدت يومي 4 و5 ديسمبر 2019 في مقر الاتحاد في جنيف، سويسرا.

12.3 ويتواصل عمل قطاع الاتصالات الراديوية على صعيد تقييس الاتصالات الراديوية مواكباً التطور المستمر في مجال شبكات الاتصالات الحديثة. وقد وضع هذا القطاع مبادئ واضحة بشأن أمن شبكات الاتصالات المتنقلة الدولية (من الأجيال الثالث والرابع والخامس) (في التوصيات ITU‑R M.1078 وITU‑R M.1223 وITU‑R M.1457 وITU‑R M.1645 وITU‑R M.2012 وITU‑R M.2083). كما أصدر توصيات بشأن القضايا الأمنية في معمارية إدارة الشبكات للنظم الساتلية الرقمية (التوصية ITU‑R S.1250) وتحسينات الأداء بشأن بروتوكول التحكم في الإرسال عبر الشبكات الساتلية (التوصية ITU‑R S.1711).

# 4 الهياكل التنظيمية

1.4 أجرى الاتحاد الدولي للاتصالات (ITU) تقييمات تقنية لتقدير مدى تأهب 76 بلداً لإنشاء فريق للتصدي للحوادث الحاسوبية (CIRT) بكل منها، ويتخذ حالياً إجراءات المتابعة اللازمة. وقد استُكمل العمل المباشر في 14 نشاطاً من هذه الانشطة. وبتنفيذ مشروع خدمات CIRT وبناء القدرات المتصلة بها، قُدمت المساعدة إلى دولة فلسطين في مجال بناء ونشر القدرات التقنية وما يتعلق بذلك من تدريبات من أجل عمليات فريق CIRT. وتلقت كيريباتي وجزر سليمان المساعدة في إعداد استراتيجيتيهما الوطنيتيْن للأمن السيبراني. وقُدمت إلى بابوا غينيا الجديدة وفانواتو المساعدة في مجال تنمية قدرات فريق CIRT عن طريق [المشروع المشترك بين الاتحاد ووزارة الاتصالات والفنون](https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9RAS18061) الأسترالية (DoCA). وأُجريت في تشاد وليبيريا ورش عمل لتقييم مدى جاهزية فريق CIRT بكل منها. وتلقى أصحاب المصلحة الوطنيون المعنيون بفريق CIRT في غامبيا التدريب على عمليات هذا الفريق. وشُرع في إنشاء أربعة مشاريع تتعلق بفريق CIRT في بوتسوانا وبوروندي وغامبيا وملاوي ولا يزال تنفيذها جارياً. وفي كينيا، يجري العمل على تحسين فريق CIRT القائم (ومن المزمع الانتهاء من هذا العمل في عام 2020).

2.4 كما أجرى الاتحاد 28 [تدريباً سيبرانياً](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) في أكثر من مائة بلد، في: [أوغندا](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Africa-Cyberdrill-2019.aspx) (منطقة إفريقيا، في نوفمبر 2019)؛ [عُمان](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (منطقة الدول العربية، في أكتوبر 2019)؛ [ماليزيا](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) (منطقة آسيا والمحيط الهادئ، في سبتمبر 2019)؛ ورومانيا (منطقة أوروبا وكومنولث الدول المستقلة، في مايو 2019). ويُعتزم إجراء خمسة تدريبات سيبرانية في عام 2020.

# 5 بناء القدرات

1.5 نظم الاتحاد [منتديات الأمن السيبراني الإقليمية](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) لجميع مناطقه من أجل بناء القدرات اللازمة لمختلف برامج/أنشطة مكتب تنمية الاتصالات وتوفير منبر تشغيلي من أجل التعاون الإقليمي والدولي.

2.5 وتنفيذاً لقرار المؤتمر العالمي لتنمية الاتصالات (WTDC) لعام 2017، تواصل لجنة الدراسات 2 لقطاع تنمية الاتصالات خلال الفترة الدراسية 2021-2018 أعمالها بشأن المسألة 3/2 ([تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني](http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)).

3.5 ولا يزال دليل الاتحاد لوضع الاستراتيجيات الوطنية للأمن السيبراني (NCS) يشكل دليلاً للممارسات الجيدة استخدمته البلدان في جميع المناطق. وقد نُظمت بهذا الشأن في عام 2019 ورش العمل التالية: ( أ ) ورشة عمل إقليمية استضافتها وزارة المعلوماتية ووكالة الأمن السيبراني لإندونيسيا في جاكرتا وخُصصت لاستراتيجيات الأمن السيبراني (وشملت النقاشات اللوائح العامة لحماية البيانات)، (ب) ورشة عمل إقليمية استضافتها مقدونيا بشأن تحسين الاستراتيجيات الوطنية في خمس دول في منطقة البلقان، (ج) ورشة عمل إقليمية استضافتها تونس بشأن تحسين الاستراتيجيات الوطنية لبلدان من منطقة إفريقيا ومنطقة الدول العربية. وشارك في ورش العمل هذه عشرون بلداً مشاركة فعّالة. وتلقت ثلاثة بلدان مساعدة مباشرة لوضع استراتيجيات وطنية للأمن السيبراني ومراجعتها باستخدام الدليل.

4.5 وقُدمت إلى السودان خدمة تنمية القدرات والمساعدة التقنية من أجل تحسين استراتيجيته المتعلقة بحماية البنية التحتية للمعلومات الحرجة.

5.5 وخلال الأسبوع الإقليمي للأمن السيبراني لمنطقة الدول العربية، عزز المركز الإقليمي المعني بالأمن السيبراني في المنطقة العربية التابع للاتحاد (ITU-ARCC) تبادل المعلومات وبناء القدرات في مجال الأمن السيبراني. ووفر الأسبوع منصة يجتمع فيها كبار المسؤولين في مجال تكنولوجيا المعلومات والاتصالات والأمن السيبراني من المنطقة بأصحاب المصلحة المعنيين ويناقشون تهديدات الأمن السيبراني وتطوره والفرص والتحديات المرتبطة به.

6.5 وعُقد أسبوع مولدوفا للأمن السيبراني في تشيسيناو، مولدوفا، بدعمٍ من الاتحاد. وأتاح المؤتمر فرصاً للتواصل ومنصة لتبادل الأفكار والمناقشة والتعاون لإدارة استراتيجيات الأمن السيبراني وحلوله العالمية من خلال الابتكار.

7.5 وعُقد حدث "الدرع السيبراني لعام 2019" في أنقرة، تركيا، بدعمٍ من الاتحاد. وتمثلت أهدافه الرئيسية في زيادة القدرات في مجال التصدي للحوادث ومستويات الجاهزية لها، وزيادة الفهم المتبادل للمخاطر السيبرانية والآثار المتصلة بها، وضمان مواصلة جهود التعاون بين أصحاب المصلحة المعنيين بالأمن السيبراني على الصعيد الدولي، وخاصةً الأفرقة الوطنية للتصدي للحوادث الحاسوبية (CIRT)، من أجل التخفيف من وطأة التهديدات السيبرانية. كما نظم الاتحاد دورة تدريبية لقيرغيزستان بشأن كيفية إنشاء مركز لعمليات الأمن السيبراني.

8.5 واشترك الاتحاد ومركز التدريب المتقدم في مجال الاتصالات وكلية العلوم التطبيقية للبريد والاتصالات (كلية تكنولوجيا المعلومات والاتصالات، جمهورية إيران الإسلامية) في تنظيم [تدريب على الأمن السيبراني في مركز التميز لمنطقة آسيا والمحيط الهادئ التابع للاتحاد (طهران، إيران - ديسمبر 2018)](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2018/CybersecurityASPCOE/cybersecurity.aspx).

9.5 ويُثبت الإصدار الثالث من [الرقم القياسي العالمي للأمن السيبراني](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) للاتحاد حدوث تحسن كبير في مستوى الالتزام بقضية الأمن السيبراني في العالم. وقد أُطلق الإصدار الرابع من الاستقصاء المتعلق بالرقم القياسي العالمي للأمن السيبراني، باستبيان ومنهجية محسَّنين. وبالشراكة مع مؤسسة Deloitte، أُجري استعراض للمشهد الأمني السيبراني في كوت ديفوار شمل نتائج الرقم القياسي GCI. وقد ساعد هذا الاستعراض البلد في تحديد أولوياتها من مبادرات الأمن السيبراني من أجل تحسين وضعها الأمني السيبراني.

# 6 التعاون الدولي

1.6 يعمل الاتحاد على إقامة علاقات و[شراكات](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) مع منظمات ومبادرات إقليمية/دولية شتى، بما فيها مبادرة الكومنولث بشأن الجريمة السيبرانية، والوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)، والمنظمة الدولية للشرطة الجنائية (INTERPOL)، والجماعة الاقتصادية لدول إفريقيا الغربية (ECOWAS)، والبنك الدولي، ومنتدى أفرقة التصدي للحوادث وأمن المعلومات (FIRST)، والرابطات الإقليمية لأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)/أفرقة الاستجابة للطوارئ الحاسوبية (CERT) مثل فريق الاستجابة للطوارئ الحاسوبية في منطقة آسيا والمحيط الهادئ (AP CERT) وفريق الاستجابة للطوارئ الحاسوبية في منطقة إفريقيا (Africa CERT) وفريق الاستجابة للطوارئ الحاسوبية لمنظمة التعاون الإسلامي (OIC CERT).

2.6 ويدعم الاتحاد رئاسة مجموعة العشرين لعام 2020 (المملكة العربية السعودية)، بناءً على طلبها، بصفته شريك معرفي في العديد من المسارات، بما فيها المسار المتعلق بالأمن في الاقتصاد الرقمي الذي يحظى بأولوية، وذلك في إطار المسعى المتعلق بأصحاب المصلحة المتعددين الذي تبذله أمانة مجموعة العشرين فيما يتصل بإشراك المنظمات الدولية المعنية في أعمال المجموعة.

3.6 وقام الاتحاد بصفته الميسِّر الرئيسي لخط العمل C5 من خطوط القمة العالمية لمجتمع المعلومات (WSIS) بتنظيم عدة جلسات في [منتدى WSIS لعام 2019](https://www.itu.int/net4/wsis/forum/2019/)، من بينها جلسة رفيعة المستوى بشأن الذكاء الاصطناعي والثقة، فضلاً عن جلسة بشأن أهمية القياس في الأمن السيبراني.

4.6 وتنفيذاً لتكليفات المجلس في دورته لعام 2019، قدم الأمين العام إلى دورة المجلس لعام 2019 (1) تقريراً يوضح كيفية استخدام الاتحاد حالياً لإطار البرنامج العالمي للأمن السيبراني (GCA) و(2) مبادئ توجيهية ملائمة بشأن استخدام الاتحاد لإطار GCA أُعدَّت بمشاركة الدول الأعضاء، وذلك لينظر فيهما المجلس ويوافق عليهما.

# 7 حماية الأطفال على الخط (COP)

1.7 بدأ فريق عمل مكون من خبراء ومتعدد أصحاب المصلحة، يضم أكثر من 50 عضواً من المنظمات والخبراء الأفراد، في استعراض [المبادئ التوجيهية بشأن حماية الأطفال على الخط](https://www.itu.int/en/cop/Pages/guidelines.aspx) التي صدرت أول مرة في عام 2009.

2.7 وفي إفريقيا، بدأت المناقشات مع تشاد وكينيا وملاوي ورواندا بشأن تنفيذ أطر الاستراتيجيات الوطنية. وعلى وجه الخصوص، جمع المنتدى الإقليمي لحماية الأطفال على الخط الذي عُقد في غانا طائفة واسعة من الخبراء من أجل تحليل الحلول والتدابير الممكن اتخاذها. وفي منطقة آسيا والمحيط الهادئ، قُدمت المساعدة لوضع الإطار الإقليمي لرابطة دول جنوب شرق آسيا (ASEAN)بشأن حماية الأطفال على الخط، استناداً إلى المبادئ التوجيهية بشأن حماية الأطفال على الخط، وبالتنسيق مع شركاء آخرين من بينهم كبار المسؤولين في قطاع الاتصالات وتكنولوجيا المعلومات (TELSOM) ووزراء الاتصالات وتكنولوجيا المعلومات (TELMIN). وأُجريت أنشطة أخرى في أوروبا في إطار المبادرة الإقليمية لتعزيز الثقة والأمان في استعمال تكنولوجيا المعلومات والاتصالات.

3.7 ويعمل الاتحاد أيضاً بصفة أمانة لجنة النطاق العريض المعنية بالتنمية المستدامة. وقد أصدر فريق العمل المعني بسلامة الأطفال على الخط، الذي تقوده المؤسسة العالمية للطفولة ومجموعة زين، [تقريره](https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf) الشامل في أكتوبر 2019 في نيويورك. وأُدرجت فيه المبادئ التوجيهية بشأن حماية الأطفال على الخط كمرجع واتُّخذت كأساس لتنفيذ توصيات التقرير.

4.7 وقد صيغَت دراسة إقليمية بشأن النُهُج الوطنية للحفاظ على سلامة الأطفال والشباب على الخط من أجل استعراضها وعرضها للتشاور مع البلدان. كما قُدمت المساعدة إلى جورجيا وأوكرانيا في وضع استراتيجية وطنية لحماية الأطفال على الخط.

5.7 واحتفل الاتحاد باليوم العالمي لإنترنت أكثر أماناً لعام 2020 بإجراء أنشطة مختلفة شملت تعزيز حماية الأطفال على الخط. ونُشرت التميمة الجديدة المتعلقة بحماية الأطفال على الخط في اليوم العالمي لإنترنت أكثر أماناً لعام 2020. و[قصة التميمة وخلفيتها](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) من ابتكار وتصميم أطفال في مطلع يناير 2020.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ