|  |  |
| --- | --- |
| **المجلس 2021المشاورة الافتراضية لأعضاء المجلس، 18-8 يونيو 2021** |  |
|  |  |
|  |  |
| **بند جدول الأعمال: PL 1.4** | **الوثيقة C21/36-A** |
| **22 أبريل 2021** |
| **الأصل: بالإنكليزية** |
| تقرير من الأمين العام |
| تقرير يوضح كيفية استخدام الاتحاد حالياً لإطار [البرنامج العالمي للأمن السيبراني](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (GCA) |

|  |
| --- |
| ملخصكلّف المجلس في دورته لعام 2019 الأمين العام بأن يقدم، بالتوازي، إلى دورة المجلس التالية (1) تقريراً يوضح كيفية استعمال الاتحاد حالياً لإطار [البرنامج العالمي للأمن السيبراني](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (GCA)، و(2) مبادئ توجيهية مناسبة، معدة بمشاركة الدول الأعضاء، بشأن استعمال الاتحاد للبرنامج العالمي للأمن السيبراني، كي ينظر فيها المجلس ويوافق عليها (الوثيقتان [C19/117](https://www.itu.int/md/S19-CL-C-0117/en) و[C19/58](https://www.itu.int/md/S19-CL-C-0058/en)).ووفقاً لهذه التوجيهات، تمت صياغة مشروع المبادئ التوجيهية لاستعمال الاتحاد للبرنامج العالمي للأمن السيبراني بدعم من رئيس القضاة (المتقاعد) شتاين شولبرغ (الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالأمن السيبراني)، وبمشاركة الدول الأعضاء وأصحاب المصلحة الآخرين، وكي ينظر فيها المجلس (انظر الوثيقة C21/71).وبالتوازي مع ذلك، يُقدم هذا التقرير الذي يوضح كيفية استخدام الاتحاد حالياً للبرنامج العالمي للأمن السيبراني كي ينظر فيه المجلس. وقد أُعدِّت في الأصل النسخة السابقة من هذا التقرير في الوثيقة [C20/36](https://www.itu.int/md/S20-CL-C-0036/en) لتقديمها إلى دورة المجلس لعام 2020ـ ولكنها لم تُستعرض.الإجراء المطلوبيُدعى المجلس إلى **الإحاطة علماً** بالتقرير.ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــالمراجع[البرنامج العالمي للأمن السيبراني (GCA)](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)؛ [الوثيقة C21/71](https://www.itu.int/md/S21-CL-C-0071/en) الصادرة عن المجلس |

# 1 مقدمة

**1.1** اعتمد مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات لعام 2018 الذي عُقد في دبي، القرار 130: *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)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) *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 (المراجَع في دبي، 2018)، *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 رفيع المستوى المعني بالبرنامج العالمي للأمن السيبراني (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) وكلف المجلس الأمين العام بأن يقدم، بالتوازي، إلى دورة المجلس التالية (1) تقريراً يوضح كيفية استعمال الاتحاد حالياً لإطار البرنامج العالمي للأمن السيبراني (GCA)، و(2) مبادئ توجيهية مناسبة، معدة بمشاركة الدول الأعضاء، بشأن استعمال الاتحاد للبرنامج العالمي للأمن السيبراني، كي ينظر فيها المجلس ويوافق عليها.[[3]](#footnote-3)

**4.1** ووفقاً لهذه التوجيهات تمت صياغة مشروع المبادئ التوجيهية لاستعمال الاتحاد للبرنامج العالمي للأمن السيبراني بدعم من رئيس القضاة (المتقاعد) شتاين شولبرغ (الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالأمن السيبراني)، وبمشاركة الدول الأعضاء، وكي ينظر فيها المجلس[[4]](#footnote-4) ويوافق عليه. وبالتوازي مع ذلك، أعد الأمين العام هذا التقرير الذي يوضح كيفية استخدام الاتحاد حالياً للبرنامج العالمي للأمن السيبراني كي نظر فيه المجلس.

# 2 خلفية

**1.2** يتمثل الدور الأساسي للاتحاد، استناداً إلى توجيهات القمة العالمية لمجتمع المعلومات (WSIS) ومؤتمر المندوبين المفوضين للاتحاد، في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT).

**2.2** وفي القمة العالمية لمجتمع المعلومات، عهد رؤساء الدول وقادة العالم إلى الاتحاد بأداء دور الميسّر لخط العمل جيم5، "*بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات*". واستجابةً لذلك، أطلق الاتحاد البرنامج العالمي للأمن السيبراني في 2007 كإطار للتعاون الدولي في هذا المجال.

**3.2** أُطلق البرنامج العالمي للأمن السيبراني في 2007– وهو مصمم للتعاون والكفاءة وتشجيع التعاون مع جميع أصحاب المصلحة وفيما بينهم. ويشمل البرنامج خمس ركائز أو مجالات عمل هي: التدابير القانونية؛ والتدابير التقنية والإجرائية؛ والهياكل التنظيمية؛ وبناء القدرات؛ والتعاون الدولي.

**4.2** وفي وقت لاحق، أُنشئ فريق الخبراء رفيع المستوى المعني بالبرنامج العالمي للأمن السيبراني (HLEG) في أكتوبر 2007 لمساعدة الأمين العام للاتحاد في إعداد مقترحات استراتيجية للدول الأعضاء بشأن تعزيز الأمن السيبراني. ويترأس هذا الفريق شتاين شيولبرغ، رئيس القضاة (المتقاعد).

**5.2** ويتألف الفريق من فريق خبراء عالمي مستقل متعدد أصحاب المصلحة يضم ما يقرب من 100 فرد من جميع أنحاء العالم. وقدّم الفريق المشورة للأمين العام بشأن جميع الركائز الخمس الواردة في تقرير الرئيس في أغسطس 2008.[[5]](#footnote-5)

**6.2** في 2008، كان العمل المتعلق بركائز البرنامج ابتكاراً رئيسياً في النهج العالمي المتصل بقضايا الأمن السيبراني. ولقد مر أكثر من عشر سنوات منذ تقديم تقرير الفريق HLEG. وعموماً هناك اعتراف عالمي بتكنولوجيات المعلومات والاتصالات كأداة حيوية لتحقيق أهداف التنمية المستدامة (SDG) للأمم المتحدة، وبحقيقة أنه لكي تحقق تكنولوجيا المعلومات والاتصالات هذا الدور، من المهم أن يشعر الجميع في كل مكان بالاطمئنان والثقة في استخدام تكنولوجيا المعلومات والاتصالات. ولذلك فإن هدف *"بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات"* هو هدف أساسي، أكثر من أي وقت مضى، لتحقيق أهداف التنمية المستدامة.

**7.2** حظي الإطار الذي توفره الركائز الخمس للبرنامج بالتقدير على نطاق واسع من جانب أعضاء الاتحاد وقد صمد عموماً أمام تجارب الزمن ولا يزال يوفِّر إطاراً واسعاً للتعاون الدولي بشأن الأمن السيبراني في إطار الوثائق الختامية للقمة العالمية لمجتمع المعلومات ولا سيما المبادئ الواردة في خط العمل جيم5. ولا تزال جميع أنشطة الاتحاد في هذا المجال مهمة تتمحور حول الركائز الخمس للبرنامج العالمي للأمن السيبراني.

**8.2** ومنذ إطلاق البرنامج، دأب الاتحاد على إبلاغ المجلس بأنشطته المتعلقة ببناء الأمن والثقة في استخدام تكنولوجيا المعلومات والاتصالات من خلال تقرير سنوي يتمحور حول الركائز الخمس، مما يبين الطبيعة التكميلية لبرامج عمل الاتحاد الحالية ويسهِّل تنفيذ أنشطة مكتب الاتصالات الراديوية (BR) ومكتب تقييس الاتصالات (TSB) ومكتب تنمية الاتصالات (BDT) في هذا المجال.

**9.2** وتتاح معلومات تفصيلية بشأن هذه الأنشطة في الوثائق [C08/33](https://www.itu.int/md/S08-CL-C-0033/en) و[C09/50](https://www.itu.int/md/S09-CL-C-0050/en) و[C10/12](https://www.itu.int/md/S10-CL-C-0012/en) و[C11/54](https://www.itu.int/md/S11-CL-C-0054/en) و[C12/29](https://www.itu.int/md/S12-CL-C-0029/en) و[C13/23](https://www.itu.int/md/S13-CL-C-0023/en) و[C14/23](https://www.itu.int/md/S14-CL-C-0023/en) و[C15/18](https://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) و[C20/18](https://www.itu.int/md/S20-CL-C-0018/en) و[C21/18](https://www.itu.int/md/S21-CL-C-0018/en). وتتضمن الفقرات التالية بعض الأمثلة لأنشطة الاتحاد المنفذة في إطار البرنامج العالمي للأمن السيبراني.

# 3 بعض الأمثلة لأنشطة الاتحاد

**1.3** يستفيد الاتحاد، بوصفه ميسّر خط العمل جيم5، من إطار البرنامج العالمي للأمن السيبراني من أجل الجمع بين مختلف أصحاب المصلحة لمساعدة البلدان في التصدي للمخاطر المرتبطة بتكنولوجيا المعلومات والاتصالات ويعمل عن كثب في شراكة مع منظمات أخرى عبر قطاعاته وأنشطته، لبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

**2.3** واعترافاً بالترابط المتبادل بين الركاز الخمس، يُسلط الضوء على أمثلة لأنشطة الاتحاد بشأن كل ركيزة في الأقسام أدناه. والغرض من هذه الأمثلة تقديم لقطات عن بعض الأنشطة مع مزيد من التفاصيل المتاحة في التقارير السنوية الفردية المقدمة إلى المجلس منذ عام 2008 (انظر الفقرة 9.2 أعلاه).

**3.3** أُدرج قسم منفصل بشأن مبادرة حماية الأطفال على الإنترنت كمثال لمبادرة شاملة تشمل جميع الركائز الخمس للبرنامج.

## 4.3 الركيزة 1 للبرنامج: التدابير القانونية

 أ ) يعتبر اعتماد تشريعات مناسبة لمكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية ومواءمتها مع السياسات والممارسات الإقليمية والدولية عنصراً لا يتجزأ من أي استراتيجية وطنية للأمن السيبراني.

ب) وفي مجال التدابير القانونية، يتعاون الاتحاد بشكل وثيق مع شركاء من قبيل مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC). ويواصل الاتحاد، بالتعاون مع شركائه، مساعدة الدول الأعضاء على فهم الجوانب القانونية للأمن السيبراني من خلال [الموارد القانونية للاتحاد بشأن الجريمة السيبرانية](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) التي تهدف إلى المساعدة على مواءمة أطرها القانونية.

## 5.3 الركيزة 2 للبرنامج: التدابير التقنية والإجرائية

 أ ) توفر [لجان الدراسات التابعة للاتحاد](https://www.itu.int/en/mediacentre/backgrounders/Pages/itu-study-groups.aspx) منصة عالمية محايدة لأعضاء الاتحاد للالتقاء والعمل بشأن أنشطة التقييس المتصلة بالأمن بخصوص مجموعة متنوعة من المواضيع هي: الهياكل والأطر الأمنية؛ وأمن تطبيقات وخدمات التكنولوجيات الحالية والناشئة مثل تكنولوجيات السجلات الموزعة (التي تعد سلسلة الكتل تنفيذاً لها)، والحوسبة السحابية، والبيانات الضخمة، والذكاء الاصطناعي، والتعلم الآلي، والشبكات الموجهة بالبرمجيات، والجيل الخامس، وإنترنت الأشياء، وأنظمة النقل الذكية، والشبكات الذكية، والأسس الأمنية مثل مؤشرات الأداء الرئيسية، وإدارة الهوية والاستيقان، والأمن السيبراني (بما في ذلك تبادل المعلومات عن التهديدات السيبرانية).

ب) أما [لجنة الدراسات 17 لقطاع تقييس الاتصالات](https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx) فهي لجنة الدراسات المسؤولة عن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات. ويشمل ذلك دراسة العديد من التكنولوجيات المتعلقة بالأمن السيبراني. وهي لجنة الدراسات الرئيسية المعنية بالأمن وإدارة الهوية (IdM)، وتواصل أداء دور أساسي في دراسة وتقييس الأمن السيبراني، ومكافحة الرسائل الاقتحامية، وإدارة الهوية، والبنية التحتية للمفاتيح العمومية (شهادات 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. وقد وضعت لجنة الدراسات حتى الآن أكثر من 200 معيار. وتعمل حالياً بشأن مواضيع منها الأمن القائم على الحوسبة الكمومية ووضعت مواصفات التوصية X.1701 بشأن "معمارية مولِّد الأعداد العشوائية للضوضاء الكمومية".

ج) وتعمل لجان الدراسات الأخرى مثل لجنة الدراسات 9 ولجنة الدراسات 13 ولجنة الدراسات 15 ولجنة الدراسات 20 (إنترنت الأشياء) بشأن المعايير المتصلة بالأمن أيضاً.

د ) وشكّل الأمن والثقة أيضاً عنصراً لا يتجزأ من المناقشات في إطار العديد من [الأفرقة المتخصصة التابعة لقطاع تقييس الاتصالات](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx) (FG)، ومنها ما يلي: [*الفريق المتخصص المعني بالذكاء الاصطناعي من أجل الصحة (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h)،[*الفريق المتخصص المعني بالوسائط المتعددة في المركبات (FG-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*، و*[*الفريق المتخصص المعني بالذكاء الاصطناعي لأغراض القيادة الذاتية والمساعَدة (FG-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx)*، و*[*الفريق المتخصص المعني بتكنولوجيا المعلومات الكمومية من أجل الشبكات (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*، و*[*الفريق المتخصص المعني بالذكاء الاصطناعي لإدارة الكوارث الطبيعية (FG-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx)*، و*[*الفريق المتخصص المعني بالشبكات المستقلة (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx)*.*

ﻫ ) 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).

## 6.3 الركيزة 3 للبرنامج: الهياكل التنظيمية

 أ ) من الضروري على الصعيد الوطني وضع آليات، وهياكل مؤسسية، فعالة للتعامل مع التهديدات والحوادث السيبرانية على نحو موثوق. ويشكل غياب هذه المؤسسات والافتقار إلى القدرات الوطنية مشكلة حقيقية في التصدي للهجمات السيبرانية على نحو ملائم وفعّال. وتؤدي [الأفرقة الوطنية للاستجابة للحوادث الحاسوبية (CIRT)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) دوراً مهماً في إيجاد الحلول الناجعة.

ب)وحتى اليوم، تلقّى أكثر من 80 بلداً المساعدة في تقييم قدراتها الوطنية في مجال التأهب الأمني السيبراني والاستجابة للحوادث. وقد نفذ الاتحاد 22 مشروعاً تتعلق بالأفرقة الوطنية للاستجابة للحوادث الحاسوبية، منها 7 مشاريع قيد التنفيذ و4 مشاريع في طور الانتهاء.

ج) ويضطلع الاتحاد بتمارين [التدريبات السيبرانية](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) على الصُعُد الأقاليمي والإقليمي ودون الإقليمي والوطني لتعزيز قدرة البلدان على التصدي للتهديدات، وبالتالي تعزيز التعاون الوطني والدولي بين الدول الأعضاء في الاتحاد لمكافحة التهديدات السيبرانية والهجمات السيبرانية. وقد نظم الاتحاد حتى اليوم 31 [تدريباً سيبرانياً](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) شارك فيها أكثر من 100 بلد.

## 7.3 الركيزة 4 للبرنامج: بناء القدرات

 أ ) 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.

ب) يساعد الاتحاد الدولي الأعضاء في وضع استراتيجيات وطنية فعّالة في مجال الأمن السيبراني وتحسينها. ولا يزال [الدليل لوضع الاستراتيجيات الوطنية للأمن السيبراني (NCS)](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf)، الذي وُضع من خلال عملية تعاونية متعددة أصحاب المصلحة، يشكل دليلاً للممارسات الجيدة ومجموعة أدوات وظيفية استخدمتها البلدان في جميع المناطق لوضع وتحسين استراتيجياتها في مجال الأمن السيبراني. ومنذ إطلاقه في سبتمبر 2018، نُظمت ورش عمل وطنية وإقليمية في أكثر من عشرين بلداً، تلقت ثلاثة منها مساعدة مباشرة لوضع وتنقيح الاستراتيجيات الوطنية للأمن السيبراني باستخدام الدليل. وعملية تحديث الدليل جارية، ومن المتوقع انتهاؤها في أكتوبر 2021.

ج) وفي عام 2015، أنشأ الاتحاد [مؤشر الأمن السيبراني العالمي (GCI)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) الذي أصبح مرجعاً موثوقاً يقيس التزام البلدان بالأمن السيبراني على المستوى العالمي – لزيادة الوعي بأهمية المسألة وأبعادها المختلفة. ويتم تقييم مستوى التنمية أو الالتزام لكل بلد على أساس الركائز الخمس للبرنامج التي توفر الأساس والإطار العام للمبادرة. واستناداً إلى نهج ومبادرة أصحاب المصلحة المتعددين، يستفيد مؤشر الأمن السيبراني العالمي من قدرات وخبرات منظمات مختلفة بهدف تحسين نوعية الدراسة الاستقصائية وتعزيز التعاون الدولي وتشجيع تبادل المعارف بشأن هذا الموضوع. وسيصدر تقرير النسخة الرابعة من مؤشر الأمن السيبراني العالمي في عام 2021. ويُعتزم بدء الأعمال المتعلقة بالنسخة الخامسة منه في الربع الثالث من عام 2021.

د ) وعن طريق [أكاديمية الاتحاد](https://academy.itu.int/training-courses/full-catalogue?search_api_fulltext=&field_taxon_registration=All&field_course_fee=All&field_taxon_region=All&field_taxon_type=All&field_taxon_topics=109&field_taxon_languages=All&date_start=&date_end=&items_per_page=10)، يواصل الاتحاد وشركاؤه تقديم الأنشطة وورش العمل التدريبية في مختلف مجالات الأمن السيبراني.

هـ ) ويشارك الاتحاد حالياً أيضاً، مع شركائه، في عدد من الأنشطة المتعلقة بالأمن السيبراني التي تركز على المساواة بين الجنسين وعلى الشباب، كمبادرة "[الشباب في مجال الأمن السيبراني (Youth4Cyber)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Youth-for-Cyber/Youth4Cyber.aspx)" والبرنامج الإرشادي "[النساء في مجال الأمن السيبراني](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx)".

## 8.3 الركيزة 5 للبرنامج: التعاون الدولي

 أ ) يقوم البرنامج العالمي للأمن السيبراني على التعاون الدولي ويسعى جاهداً لإشراك جميع أصحاب المصلحة المعنيين في جهد منسق لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

ب) ويواصل الاتحاد إقامة علاقات وشراكات مع منظمات ومبادرات إقليمية/دولية شتى والحفاظ عليها، بما فيها المنتدى الاقتصادي العالمي (WEF)، ومبادرة 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). وتيسر هذه الشراكات التعاون بين أصحاب المصلحة المتعددين بشأن الأنشطة التي تشمل جميع ركائز البرنامج.

ج) ويستفيد الاتحاد، بصفته ميسّر خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، من عملية القمة، بما فيها المنتدى السنوي للقمة العالمية لمجتمع المعلومات، للمساعدة في تيسير الحوار بين أصحاب المصلحة المتعددين. وينظم الاتحاد حوارات رفيعة المستوى، واجتماعات الميسّرين لخط العمل جيم5 بشأن موضوع الأمن السيبراني في [منتدى القمة العالمية لمجتمع المعلومات](https://www.itu.int/net4/wsis/forum/2019/) كل عام.

د ) وإدراكاً لأهمية العمل من **أجل بناء تفاهم مشترك داخل الأمم المتحدة بشأن الاحتياجات والمتطلبات اللازمة لوضع البرامج والمبادرات التي من شأنها أن تدعم بفعالية الجهود التي يبذلها جميع أصحاب المصلحة الآخرين المعنيين، اتُخذت خطوة أولى مهمة في عام** 2010**. نحو تعزيز التنسيق الداخلي بين وكالات الأمم المتحدة في مساعدتها للدول الأعضاء فيما يتعلق بالأمن السيبراني.** وبناءً على طلب مجلس الرؤساء التنفيذيين المعني بالتنسيق (CEB) التابع للأمم المتحدة، قاد الاتحاد ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، بالتعاون مع 33 وكالة أخرى تابعة للأمم المتحدة، جهداً لمدة سنتين لوضع إطار لمنظومة الأمم المتحدة ككل بشأن الأمن السيبراني والجريمة السيبرانية أقره مجلس الرؤساء التنفيذيين في نوفمبر 2013. وواصل الاتحاد منذ ذلك الحين الإسهام في العديد من المبادرات ذات الصلة التي تهدف إلى تحسين التنسيق الداخلي والتعاون داخل منظومة الأمم المتحدة.

## 9.3 مبادرة حماية الأطفال على الإنترنت

 أ ) أطلق الاتحاد [مبادرة حماية الأطفال على الإنترنت (COP)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) في نوفمبر 2008 كجهد متعدد أصحاب المصلحة في إطار البرنامج العالمي للأمن السيبراني. وتجمع المبادرة بين شركاء من جميع قطاعات المجتمع الدولي بهدف وضع استراتيجيات الأمن السيبراني وتعزيز البيئات الآمنة على الإنترنت للأطفال في جميع أنحاء العالم.

ب) وتتمثل الأهداف الرئيسية لمبادرة حماية الأطفال على الإنترنت في (أ) تحديد المخاطر وأوجه الضعف أمام الأطفال في الفضاء السيبراني، و(ب) زيادة الوعي بهذه المخاطر، و(ج) استحداث أدوات عملية للمساعدة في التقليل إلى أدنى حد من المخاطر و(د) تبادل المعارف والخبرات.

ج) تتبع مبادرة حماية الأطفال على الإنترنت نهجاً شاملاً لتعزيز سلامة الأطفال على الإنترنت وتضع استراتيجيات تشمل الركائز الخمس للبرنامج:

● **التدابير القانونية**: من الضروري وضع إطار قانوني شامل يكون أداة أساسية لتعزيز بيئة داعمة وأكثر أمناً على الإنترنت للأطفال والشباب. وتتبع مبادرة الأطفال على الإنترنت النهج المتبعة في مختلف البلدان ذات الأنظمة القانونية المختلفة وتضع مبادئ توجيهية الهدف منها مساعدة الدول الأعضاء على تحقيق أهدافها.

● **التدابير التقنية والإجرائية**: تضع مبادرة حماية الأطفال على الإنترنت توصيات ومعايير رئيسية لدعم حماية الأطفال على الإنترنت من جانب جميع أصحاب المصلحة الرئيسيين.

● **الهياكل التنظيمية**: تشجع مبادرة حماية الأطفال على الإنترنت تطبيق إطار وطني نموذجي للمساعدة في تهيئة بيئة إيجابية على الإنترنت للأطفال والشباب. وتشجع على إنشاء وحدات لحماية الأطفال على الإنترنت على المستوى الوطني وتضع مجموعة من المؤشرات للمساعدة في قياس التقدم المحرز في تنفيذ المبادرات المتعلقة بحماية الأطفال على الإنترنت على المستويات العالمية والإقليمية والوطنية.

● **بناء القدرات**: تدعم مبادرة حماية الأطفال على الإنترنت البلدان في تنفيذ الأطر الوطنية لحماية الأطفال على الإنترنت وتنظم أحداثاً استراتيجية على المستويين الإقليمي والعالمي لدعم هذه العمليات.

● **التعاون الدولي**: تعزز المبادرة تهيئة ثقافة عالمية بشأن "المواطنة الرقمية" وتشجع على وضع ترتيبات تعاونية لتبادل المعلومات من أجل تجنب المخاطر التي يتعرض لها الأطفال والشباب على الإنترنت أو التخفيف منها.

د ) جرى الاضطلاع بمجموعة متنوعة من الأنشطة في إطار مختلف ركائز البرنامج العالمي للأمن السيبراني، يمكن الاطلاع على تفاصيلها في [الموقع الإلكتروني لمبادرة حماية الأطفال على الإنترنت](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) وكذلك في التقارير السنوية المقدمة إلى المجلس منذ إطلاق المبادرة. وتشمل هذه الأنشطة تطوير أدوات وموارد مثل المبادئ التوجيهية لكل من الأطفال، والآباء والمعلمين، ودوائر الصناعة المعنية، وواضعي السياسات. وقد أُنشئ فريق عمل يتألف من خبراء تابعين لأصحاب مصلحة متعددين ويضم أكثر من 50 خبيراً من المنظمات والأفراد، استعرض المجموعات الأربع من [المبادئ التوجيهية بشأن حماية الأطفال على الإنترنت](https://www.itu.int/en/cop/Pages/guidelines.aspx) لواضعي السياسات، ودوائر الصناعة المعنية، والآباء والمعلمين، وكذلك للأطفال، وأصدر مجموعة منقحة منها في عام 2020.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

1. محضر الجلسة العامة السابعة عشرة لمؤتمر المندوبين المفوضين، دبي، الخميس 15 نوفمبر 2018. [↑](#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، <https://www.itu.int/md/S19-CL-C-0058/en>. [↑](#footnote-ref-2)
3. محضر موجز للجلسة العامة السادسة (الوثيقة C19/117)، الاتحاد الدولي للاتصالات، 20 يونيو 2019،
<https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)
4. لمزيد من المعلومات، يُرجى زيارة الموقع الإلكتروني التالي:
<https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. انظر القاضي شتاين شيولبرغ: تقرير مقدم من رئيس فريق الخبراء رفيع المستوى المعني بالأمن السيبراني (HLEG):
<https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-5)