|  |  |
| --- | --- |
| **المجلس 2021المشاورة الافتراضية لأعضاء المجلس، 18-8 يونيو 2021** |  |
|  |  |
|  |  |
| **بند جدول الأعمال: PL 1.4** | **الوثيقة C21/71-A** |
| **22 أبريل 2021** |
| **الأصل: بالإنكليزية** |
| تقرير من الأمين العام |
| المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني |
|  |

|  |
| --- |
| **ملخص**كلّف المجلس في دورته لعام 2019 الأمين العام بأن يقدم، بالتوازي، إلى دورة المجلس التالية (1) تقريراً يوضح كيف يستعمل الاتحاد حالياً إطار [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 بدعم من رئيس القضاة (المتقاعد) السيد شتاين شولبرغ (الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالأمن السيبراني)، والأستاذة سولونج غرناوطي، والسيد نوبورو ناكاتاني، وبمشاركة الدول الأعضاء وأصحاب مصلحة آخرين، كي ينظر فيها المجلس ويوافق عليها. ومن المهم الإشارة إلى أن هذه الجهود ليس المقصود منها أن تعالج المسائل المتعلقة بمراجعة البرنامج العالمي للأمن السيبراني، ولن تقوم بذلك.ووفقاً لعملية وضع مشروع المبادئ التوجيهية، الواردة في [الرسالة المعممة CL-20/55))](https://www.itu.int/md/S20-SG-CIR-0055/en)، عُقدت مشاورتان مفتوحتان لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات (WSIS) في 23 أبريل 2020 و1 مارس 2021 ليقدموا تعليقات بشأن هذا المشروع. وقد أُعدّت في الأصل نسخة سابقة من هذه الوثيقة بالرمز [C20/65](https://www.itu.int/md/S20-CL-C-0065/en) لتقديمها إلى المجلس في دورته لعام 2020 لكنها لم تُستعرض في تلك الدورة.**الإجراء المطلوب**تقدَّم هذه الوثيقة إلى المجلس **لينظر فيها** و**يوافق عليها**، على النحو المناسب.\_\_\_\_\_\_\_\_\_**المراجع**[*القرار 130 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf)[*البرنامج العالمي للأمن السيبراني (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*،* [*الوثيقة C21/36*](https://www.itu.int/md/S21-CL-C-0036/en) *للمجلس* |

**جدول المحتويات**

**الصفحة**

[**القسم 1 مقدمة 3**](#_Toc73431778)

[خلفية 4](#_Toc73431779)

[السياق 4](#_Toc73431780)

[استمرار أهمية وسريان البرنامج العالمي للأمن السيبراني كإطار عالمي للعمل 7](#_Toc73431781)

[**القسم 2 الركيزة 1: التدابير القانونية 7**](#_Toc73431782)

[مقدمة 7](#_Toc73431783)

[تطور المشهد القانوني منذ عام 2008 8](#_Toc73431784)

[المبادئ توجيهية لاستخدام الركيزة 1 – التدابير القانونية 10](#_Toc73431785)

[**القسم3 الركيزة 2: التدابير التقنية والإجرائية 11**](#_Toc73431786)

[مقدمة 11](#_Toc73431787)

[تطور مشهد التدابير التقنية والإجرائية منذ عام 2008 11](#_Toc73431788)

[المبادئ توجيهية لاستخدام الركيزة 2 – التدابير التقنية والإجرائية 13](#_Toc73431789)

[**القسم 4 الركيزة 3: الهياكل التنظيمية 13**](#_Toc73431790)

[مقدمة 13](#_Toc73431791)

[تطور مشهد الهياكل التنظيمية منذ عام 2008 14](#_Toc73431792)

[المبادئ التوجيهية لاستخدام الركيزة 3 – الهياكل التنظيمية 15](#_Toc73431793)

[**القسم 5 الركيزة 4: بناء القدرات 15**](#_Toc73431794)

[مقدمة 15](#_Toc73431795)

[تطور مشهد بناء القدرات منذ عام 2008 16](#_Toc73431796)

[المبادئ توجيهية لاستخدام الركيزة 4 – بناء القدرات 17](#_Toc73431797)

[**القسم 6 الركيزة 5: التعاون الدولي 18**](#_Toc73431798)

[مقدمة 18](#_Toc73431799)

[تطور مشهد التعاون الدولي منذ عام 2008 18](#_Toc73431800)

[المبادئ توجيهية لاستخدام الركيزة 5 – التعاون الدولي 20](#_Toc73431801)

[**القسم 7 المبادئ التوجيهية العامة لإطار البرنامج العالمي للأمن السيبراني 21**](#_Toc73431802)

# 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/action/cybersecurity/PublishingImages/Lists/resolutions/AllItems/Res%20130.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 رفيع 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) 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، كي ينظر فيها المجلس ويوافق عليها.[[4]](#footnote-4) وأعرب الأمين العام عن امتنانه لتوجيهات ومساهمة الأستاذة سولونج غيرناوطي (الفريق السويسري للمشورة والبحوث في مجال الأمن السيبراني، جامعة لوزان) بشأن الأقسام المتعلقة 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 البرنامج العالمي للأمن السيبراني. ومن المهم الإشارة إلى أن هذه الجهود ليس المقصود منها أن تعالج المسائل المتعلقة بمراجعة البرنامج العالمي للأمن السيبراني، ولن تقوم بذلك.

**5.1** ووفقاً لعملية إعداد مشروع المبادئ التوجيهية، الواردة في [الرسالة المعممة (CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/en)، عُقدت مشاورتان مفتوحتان لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات (WSIS) في 23 أبريل 2020 و1 مارس 2021 لتقديم تعليقات بشأن هذا المشروع (مشاورة مفتوحة). وحضر الاجتماع أكثر من 160 مشاركاً وقدموا تعليقات بشأن كل قسم في 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 المشاورتين أو بعدهما.

خلفية

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

**7.1** وفي القمة العالمية لمجتمع المعلومات، عهد رؤساء الدول وقادة العالم إلى الاتحاد بأداء دور الميسّر لخط العمل جيم5 في 2005، "*بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات*".[[5]](#footnote-5) واستجابةً لذلك، أطلق الاتحاد البرنامج العالمي للأمن السيبراني في 2007 كإطار للتعاون الدولي في هذا المجال.

**8.1** ويشمل البرنامج خمس ركائز أو مجالات عمل هي: التدابير القانونية؛ والتدابير التقنية والإجرائية؛ والهياكل التنظيمية؛ وبناء القدرات؛ والتعاون الدولي. وهو مصمم من أجل التعاون والكفاءة بين أصحاب المصلحة المتعددين، من خلال تشجيع التعاون مع جميع الشركاء ذوي الصلة وفيما بينهم والبناء على المبادرات القائمة لتجنب تكرار الجهود.

**9.1** 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. وترأس هذا الفريق شتاين شيولبرغ، رئيس القضاة (المتقاعد).

**10.1** والفريق هو فريق خبراء عالمي مستقل متعدد أصحاب المصلحة يضم 100 خبير من جميع أنحاء العالم. وقدّم الفريق المشورة للأمين العام بشأن جميع الركائز الخمس في تقرير مقدم من الرئيس أُعد في أغسطس 2008 (تقرير الفريق HLEG لعام (2008[[6]](#footnote-6). وأكد رئيس الفريق ما يلي:

 *التكاليف المرتبطة بالهجمات السيبرانية كبيرة – من حيث خسائر الإيرادات، وفقدان البيانات الحساسة، وتلف المعدات وهجمات منع الخدمة وانقطاع الشبكة. إن النمو المستقبلي لمجتمع المعلومات على الخط وإمكاناته في خطر بسبب تزايد التهديدات السيبرانية. وعلاوةً على ذلك، لا حدود للفضاء السيبراني: يمكن للهجمات السيبرانية أن تسبب أضراراً لا حصر لها في بلدان مختلفة في دقائق معدودة. وتشكِّل التهديدات السيبرانية مشكلة عالمية يلزم التوصل إلى حل شامل لها يشمل جميع أصحاب المصلحة.*

**11.1** وفي عام 2008، كان العمل المتعلق بالركائز الخمس للبرنامج ابتكاراً رئيسياً في النهج العالمي المتصل بقضايا الأمن السيبراني. ولقد مر أكثر من عقد من الزمان 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.

السياق

**12.1** 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 وتحديداً المبادئ الواردة في خط العمل جيم5. وإن التوصيات ذات الصلة التي يتضمنها تقرير الفريق لعام 2008 لا تزال مهمة اليوم[[7]](#footnote-7) باستثناء بضعة جوانب محددة يمكن أن تعتبر متقادمة أو قد تجاوزتها أحداث أخرى.

**13.1** وبطبيعة الحال لقد تغيّر مشهد تكنولوجيا المعلومات والاتصالات بشكل جذري منذ عام 2008، إذ إن تكنولوجيات المعلومات والاتصالات تشكل الآن أساس كل قطاع من قطاعات المجتمع، والجزء الأكبر من البنية التحتية[[8]](#footnote-8) ويشهد العالم ظهور تكنولوجيات جديدة واعتمادها بوتيرة سريعة، ومن أمثلة ذلك ما يلي:

• التوسع في اعتماد إنترنت الأشياء مع وجود عشرات إن لم يكن مئات المليارات من الأجهزة الجديدة الموصولة بينياً مما يفتح الباب أمام عدد كبير من نقاط الضعف الجديدة المحتملة؛

• نمو الذكاء الاصطناعي كأداة للاستفادة من البيانات لا سيما البيانات الضخمة للسماح للبشر باتخاذ قرارات أكثر استنارة فضلاً عن تمكين الآلات من اتخاذ قرارات مستقلة وذكية كما يُطلق عليها ودون تدخل الإنسان، مما يثير تحديات تتعلق بالأمن والثقة، إلى جانب حماية حقوق الإنسان؛

• والتكنولوجيات والمعايير الجديدة للاتصالات من قبيل الجيل الخامس (5G) الذي يُتيح الاتصال بسرعة تفوق أضعافاً مضاعفة ما يمكن تحقيقه حالياً؛

• والحوسبة الكمومية التي توفر سرعات حاسوبية تتجاوز القدرات الحالية مما يُتيح فرصاً كبيرة ولكن يعرّض أيضاً خوارزميات التشفير الحالية وغيرها للخطر.

• تكنولوجيات الأمن الجديدة مثل تكنولوجيات السجلات الموزعة (تعد سلاسل الكتل من التطبيقات الأكثر شيوعاً) التي توفر وسائل أفضل بكثير للحفاظ على الأنظمة والبيانات ذات الصلة بها. ويتوجه عدد متزايد من البلدان في العالم أيضاً نحو اعتماد أنظمة الهوية الرقمية بصورة متزايدة.

**14.1** وبالإضافة إلى ذلك، فإن النظام الإيكولوجي العالمي لتكنولوجيا المعلومات والاتصالات تَشكّل إلى حد كبير منذ عام 2008 مع الاعتماد واسع النطاق للشبكات الاجتماعية على الصعيد العالمي. ولدى بعض الشبكات الاجتماعية عدد من المستخدمين أكبر من عدد سكان العديد من البلدان مجتمعةً، فلدى ’فيسبوك‘، مثلاً، حتى عام 2020 نحو 2,8 مليار مستعمل نشط شهرياً.[[9]](#footnote-9) وقد أدت وسائل التواصل الاجتماعي دوراً محورياً في توصيل الناس عبر العالم، وطمس الحدود الجغرافية، وإتاحة سهولة الوصول إلى المعلومات والفرص على نطاق وسرعة غير مسبوقين. كما أنها جلبت شواغل كبيرة تتعلق بالثقة – فيما يخص خصوصية وأمن المستعملين والبيانات التي يولدونها، وموثوقية المعلومات المتاحة على الشبكات الاجتماعية وجدارتها بالثقة ونشر المحتوى المحرّض على الكراهية وما إلى ذلك.[[10]](#footnote-10)

**15.1** وعلاوة على ذلك، استمرت عوامل أخرى، مثل ظهور شبكة الويب المظلمة، في إثارة شواغل متزايدة في جميع أنحاء العالم بشأن النشاط الإجرامي في الفضاء السيبراني، ولا سيما بشأن جوانب مثل النفاذ إلى الأدوات والخدمات والمحتويات الخبيثة.

**16.1** ونظراً إلى هذه التطورات، كان هناك اعتراف متزايد بين جميع أصحاب المصلحة، بما في ذلك الحكومات، بتنوع الإجراءات العاجلة التي يتعين اتخاذها للنهوض بالأمن السيبراني، بدءاً من حماية البنية التحتية الحيوية إلى حماية خصوصية المستعمل. وكقضية يمكن أن تشكل تهديداً للأمن الوطني لجميع البلدان، وصل الأمن السيبراني إلى برامج أعلى المستويات السياسية للحكومات التي تستثمر بشكل متزايد في التدابير التسييرية والإدارية لدفع استجابة الحكومة بأكملها من أجل تعزيز قدرتها الوطنية على الصمود في المجال السيبراني.

**17.1** ولم تسلط جائحة فيروس كورونا (كوفيد-19) سوى المزيد من الضوء على أهمية تكنولوجيا المعلومات والاتصالات بالنسبة للصحة والسلامة والحفاظ على تقدم اقتصادنا ومجتمعنا. وتوفر خدمات تكنولوجيا المعلومات والاتصالات وبنيتها التحتية النفاذ المستمر إلى الاحتياجات الحرجة بدءاً من العمل عن بُعد والتجارة الإلكترونية إلى الطب عن بُعد والتعلم عن بُعد. وزادت أزمة كوفيد-19 أيضاً من الحاجة إلى التصدي لتحديات الأمن السيبراني الحرجة والسريعة التطور التي يفرضها اعتماد المجتمع بدرجة عالية على تكنولوجيا المعلومات والاتصالات.

**18.1** وفي إطار البرنامج العالمي للأمن السيبراني، تطورت كل ركيزة من الركائز الخمس بطريقتها الخاصة على مدى العقد الماضي.

**19.1** وحتى عام 2020، كان أكثر من 125 بلداً قد وقّع و/أو صدّق على اتفاقيات أو إعلانات أو مبادئ توجيهية أو اتفاقات مختلفة بشأن الأمن السيبراني والجريمة السيبرانية مثل [اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185) (اتفاقية بودابست)، [والاتفاق بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون من أجل التعاون في ميدان ضمان أمن المعلومات الدولي](http://eng.sectsco.org/documents/) (عام 2009)، و[اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (عام 2014)](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).

**20.1** وعملاً بقرارات الجمعية العامة للأمم المتحدة (UNGA)، عمد فريق خبراء حكوميين (GGE)[[11]](#footnote-11) وفريق عمل مفتوح العضوية (OEWG)[[12]](#footnote-12) إلى دراسة عدة قضايا تتعلق باستخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، *من بينها* الارتقاء بسلوك الدول المسؤول في الفضاء السيبراني، ومدى وجوب تطبيق القانون الدولي على أنشطة الفضاء السيبراني، وبناء القدرات، وضرورة تنفيذ تدابير لبناء الثقة في الفضاء السيبراني ووضع المزيد من هذه التدابير.

**21.1** إن تكنولوجيات المعلومات والاتصالات المبتكرة مثل الحوسبة السحابية والشبكات المعرّفة بالبرمجيات (SDN)، والتمثيل الافتراضي لوظائف الشبكة (NFV)، والجيل الخامس (5G)، والبيانات الضخمة والذكاء الاصطناعي وما إلى ذلك، تزيل الحواجز السوقية والجغرافية، مما يجعل النظام الإيكولوجي للأمن السيبراني دينامياً ومعقداً على نحو متزايد. ويمكن أن تتسبب التكنولوجيات والجهات الفاعلة التجارية الجديدة في التعرض لمواطن ضعف وتهديدات جديدة، لا سيما وأن تركيز القطاع الخاص على الأداء، وحصة السوق، والتكاليف كثيراً ما يعطى الأولوية على الاستثمارات في الأمن في مرحلة التصميم. وهناك عدد من القضايا التي تطرح تحديات كبيرة عند التعامل مع هذه التكنولوجيات، مثل إيجاد طريقة للحد من عدد نقاط الضعف والسيطرة عليها عن طريق ضمان الأمن من خلال التصميم (حيث لا تزال المنتجات ضعيفة منذ مرحلة التصميم ذاتها)، وتعزيز الثقة في المنتجات والخدمات خلال دورة حياتها من خلال خطط وبروتوكولات ومعايير الاعتماد، والاستخدام المشروع للبيانات التي يولدها المستعمل مع حماية خصوصية المستعمل. ويمكن أن تساعد عمليات التقييس والاعتماد/الإقرار الدوري على الحدد من أوجه الضعف وأثرها من خلال المساهمة في تطوير ثقافة الأمن عن طريق التصميم، وبالتالي بناء الثقة في هذه التكنولوجيات. بيد أن توحيد المعايير الأمنية أي وضع تدابير تقنية وإجرائية للأمن، لا يزال هدفاً متحركاً لأن ذلك يستلزم صناعة متقدمة من الناحية التكنولوجية ومنظمين بارعين في مجال التكنولوجيا وهيئات إنفاذ مقتدرة، حسب الاقتضاء.

**22.1** وقد أنشئ عدد من المنظمات الوطنية والإقليمية والدولية لمعالجة مسألة الأمن السيبراني. ومن الأمثلة على المبادرات الوطنية والإقليمية أفريبول وأميريبول وشرطة مجلس التعاون الخليجي (GCCPO)، ومركز أوقيانوسيا للأمن السيبراني (OCSC)، والمركز الأسترالي للأمن السيبراني (ACSC)، والمركز الأوروبي للجرائم السيبرانية (EC3)، ومركز التنسيق الوطني الروسي المعني بحوادث الحاسوب، ومركز تنسيق الجرائم السيبرانية في الهند (I4C). وفيما يتعلق بالكيانات الدولية، تشمل الجهود المبذولة مؤخراً المركز العالمي للقدرات الأمنية السيبرانية (GCSCC)، والمنتدى العالمي للخبرة السيبرانية (GFCE)، والمجمع العالمي للابتكار التابع للإنتربول (IGCI)، والمركز العالمي للأمن السيبراني للتابع للمنتدى الاقتصادي العالمي (WEF)، وبرنامج الأمن السيبراني التابع للجنة البلدان الأمريكية لمكافحة الإرهاب (CICTE) التابعة لمنظمة الدول الأمريكية (OAS)، والمجموعة الاقتصادية لدول غرب إفريقيا (ECOWAS)، والجماعة الإنمائية للجنوب الإفريقي (SADC)، وغيرها.

**23.1** وعلاوةً على ذلك، فإن الافتقار إلى المهارات والخبرة في الأبعاد التقنية والقانونية والتنظيمية والبشرية للأمن السيبراني يمكن أن يؤثر سلباً على البنى التحتية الوطنية الحيوية. ومن المرجح ألا يفهم العديد من المستعملين النهائيين لتكنولوجيا المعلومات والاتصالات في الوقت الحالي قضايا الأمن السيبراني فهماً تاماً أو أن يكون لديهم المهارات أو الأدوات اللازمة لحماية بياناتهم وخصوصيتهم وأصولهم على أفضل وجه، مع تعرض المستعملين الأكثر ضعفاً بمن فيهم النساء والأطفال للخطر بشكل خاص. ولا يزال بناء المهارات والكفاءات والتدابير التي من شأنها أن تساهم في تحقيق ثقافة فعّالة للأمن السيبراني تشكل تحدياً حاسماً.

استمرار أهمية وسريان البرنامج العالمي للأمن السيبراني كإطار عالمي للعمل

**24.1** تتطور الأنشطة المنفذة باستخدام إطار البرنامج العالمي للأمن السيبراني مع مراعاة المشهد المتغير لتكنولوجيا المعلومات والاتصالات بما في ذلك الأنشطة التي يضطلع بها الاتحاد ضمن ولايته ووفقاً لدوره كجهة ميسِّرة لخط العمل جيم5 للقمة.

**25.1** وقد عَزّز البرنامج العالمي للأمن السيبراني الجهود التي يبذلها الاتحاد في سبيل بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات. وكإطار، فإنه يطبق على المستويات العالمية والإقليمية والوطنية، وينبغي مواصلة تنفيذه على هذا النحو. ويعمل الاتحاد ضمن ولايته ومسترشداً بإطار البرنامج العالمي للأمن السيبراني للجمع بين أصحاب المصلحة المختلفين من أجل التعاون بشأن عدد من المبادرات التي تشمل مساعدة الدول الأعضاء في تحديد استراتيجياتها الوطنية بشأن الأمن السيبراني وتعزيز بنيتها التحتية من خلال تطوير وتنفيذ معايير الأمن الدولية وإنشاء أفرقة الاستجابة للحوادث الحاسوبية ونشر المبادرات لحماية الأطفال على الخط وبناء القدرات والمهارات البشرية اللازمة. وأُطلقت في إطار البرنامج العالمي للأمن السيبراني عدة مبادرات لأصحاب المصلحة المتعددين كمبادرة حماية الأطفال على الخط.[[13]](#footnote-13)

**26.1** وبغية تعزيز الجهود الرامية إلى الاستفادة من البرنامج العالمي للأمن السيبراني، تقدم الأقسام التالية المزيد من التوجيهات. وقد أُخذت في الحسبان لدى إعداد هذه التوجيهات التوصيات الواردة في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، وأنشطة الاتحاد منذ ذلك الحين، 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)).

**27.1** 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

مقدمة

**1.2** يشكلالبعد القانوني للأمن السيبراني أحد العوامل الرئيسية لتحقيق الثقة في استخدام تكنولوجيا المعلومات والاتصالات.

**2.2** ويشير تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 إلى أن الركيزة 1 من البرنامج العالمي للأمن السيبراني تسعى إلى تعزيز التعاون وتقديم المشورة الاستراتيجية للأمين العام للاتحاد بشأن الاستجابات التشريعية لمعالجة القضايا القانونية المتطورة في مجال الأمن السيبراني، بما في ذلك كيفية التعامل مع الأنشطة الإجرامية المرتكبة عبر تكنولوجيا المعلومات والاتصالات من خلال التشريعات بطريقة متوافقة دولياً. وأشارت المناقشات إلى أن الاتحاد يمكن أن يضع استراتيجيات لتطوير تشريعات نموذجية بشأن الجرائم السيبرانية كمبادئ توجيهية. وأوصى التقرير أيضاً بالاسترشاد بالمبادرات الإقليمية ذات الصلة كمرجع.

تطور المشهد القانوني منذ عام 2008

**3.2** وضعت المنظمات الإقليمية العديد من الاتفاقيات والإعلانات والاتفاقات والمبادئ التوجيهية بعد 2008 بشأن الأمن السيبراني. وكما ذُكر أعلاه، وقّع العديد من البلدان و/أو صدّق على اتفاقيات أو إعلانات أو مبادئ توجيهية أو اتفاقات مختلفة بشأن الأمن السيبراني مما أسفر عن التجزؤ والتنوع على الصعيد الدولي.

**4.2** وفي منظومة الأمم المتحدة، أنشأت الجمعية العامة للأمم المتحدة أيضاً، كما ذُكر سابقاً في القسم 1، عمليتين لمناقشة قضية الأمن في استخدام تكنولوجيا المعلومات والاتصالات، ألا وهما فريق الخبراء الحكوميين (GGE) وفريق العمل المفتوح العضوية (OEWG). ومنذ عام 2004، أنشأت الجمعية العامة للأمم المتحدة ستة أفرقة للخبراء الحكوميين تُعنى بدراسة ما قد يشكله استخدام تكنولوجيا المعلومات والاتصالات من تهديدات للأمن الدولي وكيف ينبغي التصدي لهذه التهديدات، كان آخرها [فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي](https://www.un.org/disarmament/group-of-governmental-experts/)، للفترة 2021/2019 ([القرار 73/266](https://undocs.org/ar/A/RES/73/266)). واتفق فريق الخبراء الحكوميين للفترة 2015/2014 في النتائج التي توصل إليها على أن الالتزامات القائمة للدول بموجب القانون الدولي واجبة التطبيق على استخدامها لتكنولوجيا المعلومات والاتصالات، وأنه يجب على الدول الوفاء بالتزاماتها تجاه احترام حقوق الإنسان وحرياته الأساسية وحمايتها. وفي عام 2018، أُنشئ [فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي](https://www.un.org/disarmament/open-ended-working-group/) (القرار 73/27)، الذي يضم ’جميع الدول المهتمة‘، ليناقش التهديدات القائمة والمحتملة فيما يتعلق بأمن المعلومات وما يمكن اعتماده من تدابير للتعاون للتصدي لها؛ ومسألة مواصلة وضع قواعد ومعايير ومبادئ السلوك المسؤول للدول؛ وكيفية تطبيق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات؛ ومسألة بناء القدرات؛ وإمكانية إطلاق حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة. واعتمد فريق العمل المفتوح العضوية للفترة 2021‑2019 [تقريره الموضوعي النهائي](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) بتوافق الآراء في مارس 2021، الذي أكد مجدداً وجوب تطبيق أحكام القانون الدولي، ولا سيما ميثاق الأمم المتحدة، في أنشطة الفضاء السيبراني، وأوصى كذلك بأن تدعم الدول جهود بناء القدرات في مجالات القانون الدولي والتشريعات الوطنية والسياسات لأن ذلك سيمكّن جميع الدول من الإسهام في بناء فهم مشترك لكيفية تطبيق القانون الدولي على استخدامها لتكنولوجيا المعلومات والاتصالات. ومن المتوقع أن يواصل فريق العمل المفتوح العضوية أعماله، ذلك أن القرار 75/240 أنشأ فريق عمل مفتوح العضوية يُعنى بأمن تكنولوجيا المعلومات والاتصالات وتحقيق الأمن في استخدامها، للفترة 2021-2025.

**5.2** وقد شرُع أيضاً في تنفيذ عدة مبادرات وعمليات داخل منظومة الأمم المتحدة للمساعدة في تحديد التحديات القانونية التي يطرحها الأمن السيبراني عالمياً والتصدي لها. فعلى سبيل المثال، أُجيز عدد من قرارات الجمعية العامة للأمم المتحدة في هذا الصدد من قبيل [قرار الجمعية العامة للأمم المتحدة المؤرخ 27 ديسمبر 2019 بشأن *مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية* (القرار 74/247)](https://undocs.org/pdf?symbol=en/A/RES/74/247)، الذي تقرر فيه إنشاء لجنة خبراء حكومية دولية مخصّصة مفتوحة العضوية، تمثل جميع مناطق العالم، لصياغة اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

**6.2** وفي ضوء ما تقدم، تتناقش الدول حالياً في هذه المحافل المختلفة بشأن ضرورة تعزيز التعاون فيما بينها ومع أصحاب المصلحة الآخرين من أجل البحث عن أرضية عالمية مشتركة في فهم القانون الدولي وتفسيره وإعلاء سلطته في سياق الفضاء السيبراني، ولا سيما بتيسير زيادة تبادل المعلومات وأفضل الممارسات.

**التدابير القانونية والتكنولوجيات الجديدة**

**7.2** اقترح بعض الخبراء أن يشمل القانون الجنائي[[14]](#footnote-14) التكنولوجيا الجديدة وأساليب السلوك في الفضاء السيبراني ذات القصد الجنائي. وقد اعتمدت بلدان كثيرة أو تستعد لاعتماد قوانين جديدة تشمل بعض تلك السلوكيات. ومن المهم أن يتفق جميع ما قد يوضع من تدابير قانونية مناسبة في هذا الصدد مع التزامات هذه البلدان المتعلقة بحقوق الإنسان. ويرد أدناه بعض الأمثلة للتكنولوجيات والاتجاهات الحديثة والناشئة التي يمكن أن تؤثر على التدابير القانونية:

**أ ) الهجمات السيبرانية العالمية**

ظهرت الهجمات السيبرانية العالمية على البنى التحتية الحيوية للاتصالات والمعلومات كتهديد للأمن الدولي والوطني. وقد كانت الحكومات والمنظمات الدولية والمؤسسات الخاصة جميعها أهدافاً لهذه الهجمات السيبرانية العالمية التي تقتضي وضع أُطر قانونية وطنية متينة للتصدي لهذا التحدي.

**ب) السلوك الإجرامي على الشبكات الاجتماعية**

هناك دعوات إلى اتخاذ تدابير لمكافحة السلوكيات غير القانونية، مثل خطاب الكراهية في الشبكات الاجتماعية. وقد ظهرت مبادرات جديدة – مثل [المنتدى العالمي للإنترنت لمكافحة الإرهاب](https://www.gifct.org/about/) بالشراكة بين الأمم المتحدة وشركات التكنولوجيا فيسبوك ومايكروسوفت ويوتيوب – لمعالجة مثل هذه القضايا.

**ج) إنترنت الأشياء (IoT)**

إن التكنولوجيا الذكية تغير الطريقة التي يعيش بها سكان العالم ويتفاعلون ويعملون.[[15]](#footnote-15) فقد وقعت مؤخراً حالات عديدة لتعرض البنى التحتية الإلكترونية في جميع أنحاء العالم لهجوم من جانب شبكة روبوتية من الأجهزة الموصولة المقرصنة، بدءاً من كاميرات الويب إلى المسيّرات. ومع ظهور تكنولوجيات جديدة من قبيل تكنولوجيا الجيل الخامس، والأجهزة الموصولة بينياً في كل مكان التي أصبحت حقيقة واقعة، من المرجح أن تزداد المخاطر.

**د ) الذكاء الاصطناعي (AI)**

إن الشفافية الخوارزمية، بما في ذلك إمكانية تتبع الإجراءات المتخذة، عامل مهم جداً في تحديد المساءلة والمسؤولية عن القرارات التي تتخذها الأنظمة المؤتمتة جزئياً أو كلياً وبالتالي ضمان الثقة في تطبيقات وخدمات تكنولوجيا المعلومات والاتصالات. وقد لاحظ الخبراء أنه بالنسبة إلى عدة أنواع من تقنيات الذكاء الاصطناعي، مثل التعلم العميق، من الصعب توضيح كيفية الوصول إلى النتائج. ومع تزايد انتشار عمليات وضع القرار الآلية في تطبيقات وخدمات المستهلكين والأعمال التجارية، ستبرز الحاجة إلى مزيد من الوضوح بشأن الجوانب القانونية المتعلقة بالمساءلة والمسؤولية عن التحليلات والقرارات التي تقدمها هذه العمليات.[[16]](#footnote-16)

**ه‍ ) الاعتداء الجنسي على الأطفال واستغلالهم جنسياً عبر الإنترنت**

اعتُمدت [اتفاقية الأمم المتحدة لحقوق الطفل (CRC)](https://www.ohchr.org/en/professionalinterest/pages/crc.aspx) في 1989. وتلزم المادة 34 من الاتفاقية الدول الأطراف باتخاذ التدابير المناسبة لحماية الأطفال من جميع أشكال الاستغلال والاعتداء الجنسيين وفي 2002، دخل حيز النفاذ [بروتوكول اختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية](https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx). وقد انتشر الاعتداء الجنسي على الأطفال عبر الإنترنت مع نمو الإنترنت ووسائل التواصل الاجتماعي. وقد دعا الخبراء إلى اتباع نهج شامل إزاء منع هذه الانتهاكات.[[17]](#footnote-17) ويشمل ذلك تدابير لمنع تطوير المواقع الإلكترونية التي تحتوي على محتوى يتعلق بالاعتداء الجنسي على الأطفال والنفاذ إليها، بما في ذلك حجب هذه المواقع الإلكترونية أو تصفيتها أو غيرها من التكنولوجيات المماثلة. وفي مارس 2021، اعتمدت لجنة حقوق الطفل [تعليقها العام رقم 25 (2021) بشأن حقوق الطفل فيما يتعلق بالبيئة الرقمية](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en)، الذي يوضح كيف ينبغي للدول الأطراف في اتفاقية حقوق الطفل تنفيذ الاتفاقية فيما يتعلق بالبيئة الرقمية، ويقدم توجيهات بشأن التدابير التشريعية والسياساتية وغيرها من التدابير ذات الصلة.

## 8.2 القوانين الإجرائية – المبادئ العامة

اعتُبر اعتماد القوانين الإجرائية اللازمة لتحديد سلطات وإجراءات المقاضاة على السلوك الإجرامي في الفضاء السيبراني تدبيراً قانونياً رئيسياً لمنع الجريمة السيبرانية والتحقيق فيها والمقاضاة عليها على الصعيد العالمي ولضمان الأمن السيبراني. غير أن بعض الخبراء لاحظوا أن هذه السلطات والإجراءات يمكن أن تكون ضرورية أيضاً لمكافحة الجرائم الجنائية الأخرى المرتكبة بواسطة أي نظام حاسوبي، ويمكن أن تنطبق اللوائح على جمع الأدلة في شكل إلكتروني لجميع الجرائم الجنائية[[18]](#footnote-18). وينبغي أن تكون جميع القوانين الإجرائية متسقة مع الالتزامات والمعايير المحددة بموجب القانون الدولي لحقوق الإنسان. وفي هذا الصدد، وبالإشارة إلى سريان مبدأ سيادة الدول في الفضاء السيبراني، فقد ترددت أيضاً طلبات ونقاشات تتعلق ببحث آليات يمكنها أن تيسّر النفاذ المشروع إلى محتوى الاتصالات المُجفَّر من طرف إلى طرف، وتضمن في الوقت ذاته حماية حقوق المواطنين الأساسية وسلامتهم.[[19]](#footnote-19) وقد حذّر بعض أصحاب المصلحة من أن أي آليات من هذا النوع يمكن أن تُضعف أمن الإنترنت وتزيد من احتمالات تعرّض الاقتصاد العالمي والخدمات الحيوية التي يعوّل عليها الكثيرون وحياة المواطنين للضرر.

**9.2** وفي ضوء الأقسام الواردة أعلاه، من الواضح أنه ينبغي للبلدان أن تواصل اتخاذ التدابير القانونية المناسبة لحماية بُناها التحتية الحيوية للاتصالات والمعلومات (وأي أصول أو أنظمة متصلة بها أو أي أجزاء من هذه الأصول أو الأنظمة) التي لا بد من وجودها للحفاظ على الوظائف المجتمعية الحيوية مثل الصحة أو السلامة أو الأمن أو الرفاه الاقتصادي أو الاجتماعي للناس، ولمنع وقوع أي خلل أو أعمال تدمير قد يؤثران على هذه البنى التحتية الحيوية تأثيراً بالغاً ويؤديان إلى تعطّلها.

المبادئ توجيهية لاستخدام الركيزة 1 – التدابير القانونية

**10.2** كما أُقر سابقاً، فإن الركائز الخمس للبرنامج العالمي للأمن السيبراني مترابطة وتغطي الركيزة المتعلقة بالتدابير القانونية هذه الركائز جميعها.

**11.2** ومنذ إطلاق البرنامج العالمي للأمن السيبراني، يركز الاتحاد على مجالات الأمن السيبراني التي تندرج ضمن اختصاصاته وخبراته الأساسية، وتحديداً الجوانب التقنية والتنموية، مع استبعاد المجالات المتعلقة بتطبيق الدول الأعضاء لمبادئ قانونية أو سياساتية تتعلق بالدفاع والأمن الوطنيين والمحتوى والجريمة السيبرانية والتي تشملها الحقوق السيادية لهذه الدول. ولذلك، فيما يتعلق بالأنشطة المندرجة في إطار الركيزة 1، ركز الاتحاد في المقام الأول على تيسير العمل التعاوني باستخدام آليات مثل مذكرات التفاهم، مع المنظمات الدولية وأصحاب المصلحة الآخرين ذوي الصلة (مثل إنتربول ومكتب الأمم المتحدة المعني بالمخدرات والجريمة) الذين قد تكون لهم ولاية قيادية في هذا المجال لتقديم المساعدة إلى البلدان. وشمل ذلك مساعدة الدول الأعضاء على فهم الجوانب القانونية للأمن السيبراني من خلال موارد مثل [موارد تشريعات الجرائم السيبرانية للاتحاد](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html) [ومستودع الجريمة السيبرانية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة](https://sherloc.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo). وجرى العمل أيضاً لمساعدة الدول الأعضاء في منطقة البحر الكاريبي، وإفريقيا جنوب الصحراء الكبرى، وجزر المحيط الهادئ في مواءمة اللوائح والتشريعات المتعلقة بتكنولوجيات المعلومات والاتصالات بما في ذلك الأطر القانونية المتعلقة بالجريمة السيبرانية.

|  |
| --- |
| **12.2** 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 جهوده لتيسير المناقشات والتعاون بين أصحاب المصلحة المتعددين بشأن التحديات المرتبطة بمعالجة مسألة الأمن السيبراني، ولا سيما تعزيز علاقته مع الشركاء وأصحاب المصلحة الآخرين لتقديم المساعدة إلى الدول الأعضاء في هذا الصدد.**ب)** وينبغي للاتحاد أن يواصل العمل مع الشركاء، في نطاق ولايته، لتطوير الموارد والحفاظ عليها مثل موارد تشريعات الجرائم السيبرانية، لمساعدة الدول الأعضاء على فهم الجوانب القانونية للأمن السيبراني، مع دعم تبادل الخبرات والمعارف بين الدول الأعضاء لدعم جهودها الرامية إلى وضع أطر بشأن هذا الموضوع بما في ذلك التشريعات.**ج)** وينبغي للاتحاد أن يعمد، بالتعاون مع الشركاء المناسبين، إلى تعزيز فهم أفضل للتحديات والمخاطر المتصلة بالأمن السيبراني التي تشكلها التكنولوجيات الناشئة بشأن التدابير القانونية الحالية، 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 فعالة 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 والنتائج بشأن جميع الجوانب بما في ذلك التدابير القانونية التي يمكن أن تسهل وتدعم الإجراءات القطرية بشأن هذه القضية الحاسمة. |

# القسم3 الركيزة 2: التدابير التقنية والإجرائية

مقدمة

**1.3** لقد وجّه البرنامج العالمي للأمن السيبراني وضع مختلف المبادرات وتنفيذها مما أسهم في نضج النقاش بشأن الأمن السيبراني على المستويات الدولية والإقليمية والوطنية. وينبغي تلبية الحاجة إلى تدابير تتسم بالفعالية والكفاءة في مجال الأمن السيبراني، سواء على مستوى استراتيجي أو تشغيلي، في إطار نهج متماسك لا يزال يشكل تحدياً رئيسياً.

**2.3** واليوم، قد يبدو أن الأبعاد التي حددتها ركائز البرنامج العالمي للأمن السيبراني 1 و3 و4 و5 تزداد أهمية في مجال الدبلوماسية السيبرانية والحوار الدولي، وغالباً ما تكون لها الغلبة على الركيزة 2. ومع ذلك، يمكن أن تكون القضايا التقنية أساس جميع الركائز الأخرى في كثير من الأحيان. ولا تزال إدارة المخاطر السيبرانية من خلال التدابير التكنولوجية والإجرائية (كالتدابير الإدارية أو التشغيلية أو الإدارية العليا) ذات أهمية قصوى، خاصة في سياق البنى التحتية الحيوية. ونظراً للدور الذي يضطلع به الاتحاد منذ وقت طويل، بصفته وكالة متخصصة تابعة للأمم المتحدة ومنظمة عالمية معنية بوضع المعايير (SDO)، فهو في وضع جيد يسمح له بالنهوض بمجال المعايير والتدابير التقنية ذات الصلة بالأمن.

تطور مشهد التدابير التقنية والإجرائية منذ عام 2008

**3.3** إن التكنولوجيات (الحالية والناشئة) والممارسات الرقمية الناتجة عنها تتطور باستمرار. وهذا البعد التقني الدينامي مستقل نوعاً ما عن الركائز الأخرى للبرنامج العالمي للأمن السيبراني، ويتطور إلى حد كبير بمفرده، مع مراعاة محدودة للاحتياجات والآثار على موضوع الركائز الأربع الأخرى.

**4.3** ووضع معايير وتنفيذها مسألة أساسية كي تعمل جميع البنى التحتية والتطبيقات والخدمات. وفضلاً عن ذلك، من المهم عند وضع المعايير أن تؤخذ أيضاً في الاعتبار الالتزامات المتعلقة بحقوق الإنسان، ذات الصلة بهذه المعايير.

**5.3** ويشكل الاتحاد الدولي للاتصالات، بأعضائه من أصحاب المصلحة المتعددين، منصةً عالمية فريدة لوضع المعايير العالمية لتكنولوجيا المعلومات والاتصالات لتعتمدها طواعيةً الدول الأعضاء فيه. وتمثل لجنة الدراسات 17 لتقييس الاتصالات داخل الاتحاد، لجنة الدراسات الرئيسية المعنية بمعايير الأمن – حيث نشرت أكثر من 200 معيار يركز على الأمن. وتعمل حالياً على مجموعة متنوعة من مجالات التكنولوجيات الناشئة، منها أمن التكنولوجيات المالية، وأمن إنترنت الأشياء (بما في ذلك أمن الإنترنت الصناعية)، وأمن نظام النقل الذكي، والتوزيع الكمومي للمفاتيح، والتعلم الآلي لمكافحة الرسائل الاقتحامية، وأمن الجيل الخامس، وحوسبة الحواف، وحماية المعلومات القابلة للتعرّف الشخصي، والحوسبة متعددة الأطراف، والمبادئ التوجيهية لإنشاء مراكز الدفاع السيبراني وتشغيلها وأتمتتها من بين عدة مجالات أخرى. وعند تنفيذ توصيات تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني لعام 2008، بشأن "التعاون" (مثل التوصيات 1.2 و6.2 و7.2 و10.2 و12.2 و(16.2، تقوم لجنة الدراسات 17. بجمع وتحديث قاعدة بيانات[[20]](#footnote-20) معايير أمن تكنولوجيا المعلومات والاتصالات من أجل النفاذ العام، التي تضم 2 600 معيار من معايير أمن تكنولوجيا المعلومات والاتصالات القائمة والجارية من 13 منظمة رئيسية معنية بوضع المعايير منها 3GPP وATIS وETSI وIEEE وIEFT وISO/IEC JTC 1 والاتحاد الدولي للاتصالات، وOASIS وOneM2Mوغيرها.

**6.3** وعلى الرغم من أن لجنة الدراسات 17 لتقييس الاتصالات لا تزال تشكل لجنة الدراسات الرئيسية المعنية بالمعايير الأمنية، فإن معظم لجان الدراسات الأخرى – إن لم يكن كلها – تتناول أيضاً الجوانب المتصلة بالأمن في مجالات الدراسة الخاصة بكل منها، مثل لجنة الدراسات 20 المعنية بإنترنت الأشياء وتطبيقاتها (بما في ذلك المدن والمجتمعات الذكية)، أو لجنة الدراسات 13 المعنية بشبكات الجيل التالي، أو لجنة الدراسات 16 المعنية بتشفير الوسائط المتعددة وأنظمتها وتطبيقاتها وغيرها. كما أن الأفرقة المتخصصة المختلفة المعنية بالتكنولوجيات الناشئة مثل الذكاء الاصطناعي والصحة، والتعلم الآلي والجيل الخامس، وتكنولوجيات السجلات الموزعة، وتكنولوجيا المعلومات الكمومية للشبكات وغيرها، تعالج التحديات المتصلة بالأمن. ومن المهم تطوير التعاون الوثيق بين الأفرقة المختلفة، مع اضطلاع لجنة الدراسات 17 بدور تنسيقي/قيادي بحيث يتم الحفاظ على أعلى درجة ممكنة من الأمن من طرف إلى طرف طوال عملية تقييس دورة تطوير منتجات/خدمات تكنولوجيا المعلومات والاتصالات.

**انتشار مبادرات التقييس والحاجة إلى مزيد من التعاون**

**7.3** يطرح التقييس الدولي للأمن السيبراني تحديات بسبب مجموعة التكنولوجيات وظهور جهات فاعلة متنوعة عبر القطاعات، والصعوبة التي تواجهها البلدان النامية بشكل خاص والتي قد تفتقر إلى القدرات التشغيلية والمهارات التقنية في مجال الأمن السيبراني.

**8.3** وفي هذا الصدد، فإن التوصية 1.2 من تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 لا تزال صحيحة الآن أكثر من أي وقت مضى: "*فيما يتعلق بفرص تعزيز التعاون مع العمل الحالي بشأن الأمن السيبراني خارج الاتحاد، ينبغي للاتحاد أن يعمل مع مراكز الخبرة الخارجية القائمة لتحديد وتشجيع وتعزيز اعتماد إجراءات أمنية وتدابير تقنية معززة*"[[21]](#footnote-21).

**9.3** وعلاوة على ذلك، وكما هو محدد في التوصية 2.2 من تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، يعتبر الاتحاد "*مركز التميز العالمي*".[[22]](#footnote-22) للتعامل مع عملية التقييس والمعايير الدولية المتصلة بالتدابير التقنية والإجرائية. ولتحقيق ذلك، ينبغي تحفيز البلدان الأكثر تقدماً من الناحية التكنولوجية وقطاعاتها الخاصة على المشاركة في أنشطة الاتحاد والتعاون لوضع المعايير التقنية والإجرائية بما فيها المعايير المتصلة بالأمن.

**10.3** ومن المهم مواصلة تعزيز التنسيق والتعاون مع المنظمات الأخرى المعنية بوضع المعايير على أساس المعاملة بالمثل، بحيث يتم ضمان الأمن من طرف إلى طرف والأمن عن طريق التصميم، وتقييم المخاطر، وإمكانية التشغيل البيني طوال دورة حياة المنتج.

**11.3** وأبرز تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 أهمية *"التدابير الرئيسية للتصدي لمواطن الضعف في منتجات البرمجيات، بما في ذلك خطط الاعتماد والبروتوكولات والمعايير"*[[23]](#footnote-23). وفي هذا الصدد، ينبغي للاتحاد أن يواصل تكييف عمله مع مراعاة التكنولوجيات والمتطلبات الجديدة. وبالنسبة لكل من هذه التكنولوجيات/المجالات، ينبغي مراعاة المتطلبات التالية:

• الحاجة إلى الأمن عن طريق التصميم/الأمن بالتغيب في كل عنصر وواجهة في نظام إيكولوجي غير متجانس لتكنولوجيا المعلومات والاتصالات في مرحلة التصميم؛

• الحاجة إلى مقاييس مناسبة لتحديد مستوى الأمن في مرحلة التنفيذ؛

• الحاجة إلى عملية (عمليات) تقييم وإصدار شهادات دورية للمصادقة على مستوى أمن مجموعة البيانات/ المنتجات/الأنظمة/الخدمات طوال دورة حياتها بعد النشر.

المبادئ توجيهية لاستخدام الركيزة 2 – التدابير التقنية والإجرائية

|  |
| --- |
| **12.3** لا تزال التوصيات المتعلقة بالركيزة 2 في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 سارية. وفي ضوء ما تقدم، تُقترح المبادئ التوجيهية التالية من أجل الركيزة 2:**أ )** ينبغي أن تركز لجان الدراسات التابعة للاتحاد على التكنولوجيات الناشئة من أجل دراسة وصياغة مبادئ توجيهية أمنية لاستخدام التكنولوجيات ذات الصلة، وأن توصي الدول الأعضاء بتطبيقها طواعيةً في الوقت المناسب لمواجهة التهديدات الإلكترونية المتغيرة والمتصاعدة.**ب)** ينبغي إنشاء آلية للتعاون الوثيق بين مختلف لجان دراسات قطاع تقييس الاتصالات فيما يتعلق بدراسة المسائل المتعلقة بالأمن، 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. وتُشجع المنظمات الأخرى المعنية بوضع المعايير ومجموعات الصناعة على تقديم معاييرها بشأن التدابير التقنية والإجرائية لقطاع تقييس الاتصالات لاعتمادها كتوصيات صادرة عن قطاع تقييس الاتصالات.**ه‍ )** ينبغي أن يواصل الاتحاد جهوده الرامية إلى تحوله إلى "مركز التميز العالمي" لوضع التوصيات المتعلقة بالتدابير التقنية والإجرائية للأمن السيبراني في المجالات التي تدخل في نطاق ولايته (على النحو المشار إليه في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008)، وذلك بسبل *منها* تحفيز أعضائه على زيادة مشاركتهم فيما يضطلع به من أنشطة تقييسية ذات صلة، وإقامة شراكات استراتيجية.**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 الركيزة 3: الهياكل التنظيمية

مقدمة

**1.4** يمكن تحليل الهياكل التنظيمية على المستويات التنسيقية الوطنية والإقليمية والدولية استناداً إلى ما إذا كان الغرض من التعاون فيما بينها استراتيجياً أم تشغيلياً. ففي هيكل استراتيجي، تركز المؤسسات على إقامة علاقة تعاونية أكثر مما تركز على تنفيذ العمليات المشتركة في حالة وقوع حادث سيبراني. ومن ناحية أخرى، في هيكل تشغيلي، تشكل المنظمات أنظمة وثيقة لتقاسم المعلومات من أجل تبادل المعلومات بسرعة للاستجابة بسرعة للحوادث السيبرانية. ويمكن أن يكون هذا التمييز مفيداً عند مقارنة الهياكل التنظيمية المختلفة في العالم.

**2.4** ومن الضروري على الصعيد الوطني وضع آليات، وهياكل مؤسسية، فعالة للتأهب لمواجهة التهديدات والحوادث السيبرانية والتصدي لها، على نحو موثوق. ويطرح غياب هذه المؤسسات والافتقار إلى القدرات الوطنية تحديات في التصدي للهجمات السيبرانية على نحو ملائم وفعال. وتقوم أفرقة الاستجابة للحوادث الحاسوبية (CIRT) بدور حيوي في تحسين مستوى التأهب وزيادة القدرة على الصمود على الصعيد الوطني.

تطور مشهد الهياكل التنظيمية منذ عام 2008

**3.4** لقد أُحرز تقدم كبير في العقد الماضي من حيث الركيزة 3. وتم إنشاء العديد من المنظمات الوطنية والإقليمية والدولية لمعالجة مسألة الأمن السيبراني.

**4.4** ومن أمثلة المبادرات الوطنية والإقليمية أفريبول (AFRIPOL) وأميريبول (AMERIPOL) وشرطة مجلس التعاون الخليجي (GCCPOL)، ومركز أوقيانوسيا للأمن السيبراني (OCSC)، ومركز الأمن السيبراني الأسترالي (ACSC)، والمركز الأوروبي للجرائم الإلكترونية (EC3)، ومركز تنسيق الجرائم الإلكترونية في الهند (I4C)، وبوابة الإبلاغ عن الجرائم الإلكترونية، والمركز الوطني الياباني للاستعداد للحوادث واستراتيجية الأمن السيبراني، ومركز التحكم في الجرائم السيبرانية (JC3)، والوكالة الوطنية الماليزية للأمن السيبراني (NACSA)، والوكالة الوطنية الفرنسية للأمن السيبراني (ANSSI)، والمركز الوطني للأمن السيبراني في ليتوانيا (NCSC)، والمركز الوطني للأمن السيبراني في سويسرا، والمركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC)، وخلية تنسيق الجرائم السيبرانية الدولية في الولايات المتحدة (IC4)، ومركز التنسيق الوطني الروسي بشأن الحوادث الحاسوبية، وكذلك مركز التنسيق الاستشاري لمنظمة معاهدة الأمن الجماعي للاستجابة للحوادث الحاسوبية (CCC CSTO)، ولجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية (CICTE)، وبرنامج الأمن السيبراني، والهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (NCA)، والهيئة الوطنية للأمن السيبراني في رواندا.

**5.4** وعلى الرغم من الاستثمار المتزايد للدول الأعضاء في أفرقة الاستجابة للحوادث الحاسوبية والتوعية الإقليمية والدولية المستقلة بشأن هذه الأفرقة، ما زال 85 بلداً يفتقر لفريق وطني للاستجابة للحوادث الحاسوبية – وهي حالة تثير قلقاً كبيراً نظراً للطبيعة العالمية للتهديدات السيبرانية.[[24]](#footnote-24)

**6.4** ويعمل الاتحاد من خلال مكتبه، مع الدول الأعضاء والشركاء والمنظمات الإقليمية/الدولية لبناء القدرات على الصعيدين الوطني والإقليمي، ونشر القدرات والمساعدة في إنشاء وتعزيز الأفرقة الوطنية للاستجابة للحوادث الحاسوبية. وأجرى الاتحاد، حتى اليوم أكثر من 80 تقييماً لمدى تأهب أفرقة الاستجابة للحوادث الحاسوبية من أجل مساعدة البلدان في تقييم قدرتها الوطنية في مجال التأهب للأمن السيبراني والاستجابة للحوادث.[[25]](#footnote-25) وقدم الاتحاد الدعم لإنشاء/تعزيز 22 مشروعاً لإنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية للدول الأعضاء في الاتحاد.[[26]](#footnote-26) ولإجراء هذه التقييمات للبلدان، يتعاون الاتحاد مع شركائه مثل منتدى أفرقة الأمن والاستجابة للحوادث (FIRST) والمركز العالمي لقدرات الأمن السيبراني وغيرها.

**7.4** وبالنسبة للمنظمات الدولية، كانت هناك عدة مبادرات، وفيما يلي بعض الأمثلة عليها:

• [المركز العالمي لقدرات الأمن السيبراني (GCSCC)](https://www.oxfordmartin.ox.ac.uk/cyber-security/) هو مركز دولي للبحوث المتعلقة ببناء القدرات الكفؤة والفعالة في مجال الأمن السيبراني، وقد تعاون المركز مع الاتحاد في تطوير [دليل لوضع استراتيجية وطنية للأمن السيبراني (NCS)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx)، يجري استخدامه حالياً لتقديم تدريبات عملية بشأن الاستراتيجيات الوطنية للأمن السيبراني، فضلاً عن التدريب على الممارسات الجيدة للبلدان بشأن وضع إطار استراتيجي وطني فعال للأمن السيبراني.

• يهدف [المنتدى العالمي للخبرة السيبرانية (GFCE)](https://thegfce.org/) الذي أنشئ في 2015 إلى تبادل الممارسات الجيدة وتقديم الخبرة في مجال بناء القدرات السيبرانية للبلدان والمنظمات الدولية والقطاع الخاص. والمنتدى والاتحاد هما مبادران مشاركان في [مبادرة نضج أفرقة الاستجابة للحوادث الأمنية الحاسوبية](https://cybilportal.org/projects/csirt-maturity-initiative-3/)، وقد تعاونا بشأن أنشطة الأمن السيبراني مثل "[مجموعة أدوات مكافحة الجرائم السيبرانية](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf)".

• يوفر [المجمع العالمي للابتكار التابع للإنتربول (IGCI)](https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors) الذي افتُتح في 2015 في سنغافورة، الدعم والتدريب التشغيليين المتخصصين في مجال إنفاذ القانون الوطني استجابةً للوجه المتغير للجريمة. وفي 2018، وقّع الاتحاد وإنتربول اتفاق تعاون لإنشاء إطار رسمي لإنتربول والاتحاد من أجل التعاون لما فيه مصلحتهما المشتركة وفي نطاق ولاية وموارد كل منها، في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

• أطلق المنتدى الاقتصادي العالمي (WEF) [مركزاً عالمياً جديداً للأمن السيبراني](https://www.weforum.org/centre-for-cybersecurity/) في 2018 بهدف إنشاء منصة عالمية للحكومات والشركات والخبراء ووكالات إنفاذ القانون من أجل التعاون بشأن تحديات الأمن السيبراني. وفي العام نفسه، وافق الاتحاد والمنتدى الاقتصادي العالمي على التعاون بشأن تعزيز مشاريع ومبادرات الأمن السيبراني التي تهدف إلى التخفيف من التهديدات السيبرانية، وكذلك استكشاف المزيد من الفرص للتعاون بشأن تعزيز الأمن السيبراني.

المبادئ التوجيهية لاستخدام الركيزة 3 – الهياكل التنظيمية

|  |
| --- |
| **8.4** 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 مساعدة البلدان النامية في تنفيذ الأفرقة الوطنية للاستجابة للحوادث الحاسوبية والوحدات/المنظمات التقنية الأخرى ذات الصلة.**ب)** ينبغي للاتحاد أن يعطي الأولوية للبلدان التي لم تُنفذ فيها بعد الهياكل التنظيمية السليمة للأمن السيبراني.**ج)** ينبغي للاتحاد أن يشجع تعاوناً أكثر انفتاحاً وشمولاً إلى جانب التنسيق بين مختلف المنظمات الوطنية أو الإقليمية أو الدولية المشاركة في الجهود الرامية إلى إنشاء هياكل تنظيمية وطنية مستدامة، من أجل ضمان الدعم الفعّال وتجنب ازدواجية الجهود.**د )** ينبغي للاتحاد أن يعزز جهوده الرامية إلى قياس الالتزامات المؤسسية للدول الأعضاء، بالاستفادة من أدوات مثل الرقم القياسي العالمي للأمن السيبراني، لتعزيز الأمن السيبراني كعامل تمكيني، شامل، لجهود هذه الدول الأعضاء في مجال التحول الرقمي.**هـ )** فيما يتعلق بالهياكل الوطنية على وجه الخصوص، ينبغي للاتحاد أن يساعد الدول الأعضاء في وضع استراتيجيات لتطوير إطار تنسيقي يشمل كامل القطاعات الحكومية لتحسين التنفيذ المتسق والشامل للجهود الوطنية المتعلقة بالأمن السيبراني.**و )** 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 الركيزة 4: بناء القدرات

مقدمة

**1.5** يعدّ تطوير ونشر المهارات المناسبة وثقافة الأمن السيبراني والممارسات الجيدة بين جميع أصحاب المصلحة من المسائل الحاسمة.

**2.5** وتواجه جميع البلدان وجميع المنظمات الحاجة إلى أن تتوفر لها الموارد والمهارات البشرية الكافية والضرورية من أجل:

• تنفيذ تدابير استراتيجية وتشغيلية للأمن السيبراني؛

• إجراء تقييمات وطنية للمخاطر الأمنية السيبرانية؛

• إدارة الأزمات المتعلقة بوقوع حوادث أمنية سيبرانية؛

• تعزيز متانة البنى التحتية والخدمات الرقمية وقدرتها على الصمود؛

• إعداد عمليات ومهارات وممارسات متسقة.

**3.5** ومن المهم الإشارة أيضاً إلى أنه نظراً إلى التقدم السريع في مجال تكنولوجيا المعلومات والاتصالات، والمسائل القائمة بالفعل المتعلقة بالنفاذ والتوصيلية، يمكن أن يكون المستعملون النهائيون، ولا سيما السكان مثل النساء والأطفال وكبار السن والأشخاص ذوو الإعاقة والاحتياجات المحددة، أكثر عرضة للتهديدات والحوادث الأمنية السيبرانية في كثير من الأحيان. ولذلك، فإن برامج التثقيف المتصلة بالأمن السيبراني، بالإضافة إلى زيادة الوعي بتهديدات الأمن السيبراني ذات الصلة بالمستعملين النهائيين الضعفاء يمكن أن تكون أساسية للحد من مخاطر الأمن السيبراني بالنسبة للمجتمع ككل.

تطور مشهد بناء القدرات منذ عام 2008

4.5 نظراً لأن للأمن السيبراني بعداً عالمياً ولأنه يتعامل مع مجموعة كبيرة من القضايا، مثل استخدامات تكنولوجيا المعلومات والاتصالات أو إساءة استخدامها، والتدابير التقنية والقضايا الاقتصادية والقانونية والسياسية، من المهم بناء ثقافة عالمية للأمن السيبراني لتعزيز مستوى فهم كل جهة فاعلة في سلسلة الأمن السيبراني. وعند بناء ثقافة الأمن السيبراني، يتمثل أحد التحديات الرئيسية المطروحة في أن تُحدد بشكل صحيح القضايا العالمية والدولية والاحتياجات المحلية الخاصة لأن الثقافات تعتمد أساساً على العاملَين المكاني والزماني. ويمكن للمعايير التقنية الدولية أن تساهم في تحديد القضايا العالمية والعامة الرئيسية المتعلقة بالبعد التقني والإجرائي لثقافة الأمن السيبراني.

5.5 ومن المهم وجود استجابة جماعية لحماية البنى التحتية الرقمية. ويزداد هذا الأمر إلحاحاً حيث إن التغيير التكنولوجي يسير نحو توصيل بيني أكبر ودائم عبر تكنولوجيا المعلومات والاتصالات.[[27]](#footnote-27) وكل ما يمكن توصيله يمكن المساس به. وعلاوةً على ذلك، فإن تصغير المكونات بسبب تكنولوجيا النانو، بما في ذلك الأنواع المختلفة من الرقائق الذكية والمستقلة، أدى إلى دمج هذه الرقائق في تكنولوجيات تمس جميع أنشطتنا.

6.5 وقد كان البرنامج العالمي للأمن السيبراني بمثابة إطار مبتكر وفعال متعدد التخصصات لجهود بناء القدرات يمكن من خلاله للجهات الفاعلة ذات الصلة أن تواصل تطوير إجابات عالمية وقابلة للجدولة ومحددة من أجل التعاون بفعالية. وإطار البرنامج العالمي للأمن السيبراني إطار محكم الإنشاء لدعم التحدي المتمثل في بناء مجتمع معلومات مأمون وشامل للجميع.

7.5 ولا تزال التوصيات الواردة في هذا الصدد في تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني لعام 2008 ذات صلة بالموضوع حتى اليوم. ومع مراعاة العمل الذي قام به الاتحاد، لا سيما منذ صدور أول منشور بعنوان "[دليل الأمن السيبراني للبلدان النامية](https://www.itu.int/pub/D-STR-SECU-2006)" في 2006، واستناداً إلى الإطار العالمي للأمن السيبراني وتقرير الفريق لعام 2008، جرى العمل على نطاق واسع عبر الدول الأعضاء بشأن بناء القدرات، بما في ذلك أنشطة التدريب والتوعية والتعليم على المستويات الوطنية والإقليمية والدولية.

8.5 وباستخدام إطار البرنامج العالمي للأمن السيبراني، يواصل الاتحاد مساعدة البلدان، ولا سيما في بناء القدرات والمهارات البشرية اللازمة، وتحديد استراتيجياتها الوطنية للأمن السيبراني، وتنمية مهارات إدارة أفرقة الاستجابة للحوادث الحاسوبية (CIRT)، وكذلك في تطوير الموارد لحماية الأطفال على الخط.

9.5 فعلى سبيل المثال، من المهم الاعتراف بمساهمة [الرقم القياسي العالمي للأمن السيبراني (GCI)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) من حيث زيادة الوعي. ومنذ إطلاقه لأول مرة في 2015، أُنتجت للمؤشر العالمي للأمن السيبراني، الذي يقيس مدى التزام الدول الأعضاء بالأمن السيبراني – ثلاثة منشورات ناجحة نتيجة الطلبات القوية المقدمة من الدول الأعضاء، والقطاع الخاص، والهيئات الأكاديمية، وغيرها. ولا يزال الرقم القياسي العالمي للأمن السيبراني، من خلال تركيزه على زيادة الوعي، يقدم الدعم للدول الأعضاء لتحسين مواقفها بشأن الأمن السيبراني من خلال تبادل الممارسات الجيدة لتنفيذ الأمن السيبراني على نحو فعال. وقد أثبت المؤشر العالمي أنه أداة قيّمة في مجال بناء الوعي والقدرات وينبغي مواصلة الاستفادة منه وتعزيزه.

المبادئ توجيهية لاستخدام الركيزة 4 – بناء القدرات

10.5 ينبغي اتخاذ إجراءات محددة على الصعيد الوطني لبناء أو تحسين قدرات مختلف أصحاب المصلحة في مجال الأمن السيبراني للتمكن من معالجة قضايا الأمن السيبراني الوطنية والدولية. وبما أن أنشطة بناء القدرات تحدث بشكل أساسي على الصعيد الوطني، ينبغي تخصيص الموارد المناسبة للجهات الفاعلة الوطنية.[[28]](#footnote-28)

11.5 وعلاوة على ذلك، ومن منظور عالمي، يتطلب تمكين الموارد البشرية إطاراً تعليمياً عاماً ونمطياً ومرناً في مجال الأمن السيبراني للاستجابة لاحتياجات زيادة الوعي العام، وتوفير مناهج تعليمية مصممة خصيصاً لمهنيين محددين. وينبغي إيلاء اهتمام خاص للفجوة بين الجنسين في هذا المجال. وهناك الكثير من رأس المال البشري غير المستغل الذي يمكن جلبه للمساهمة في مجال الأمن السيبراني، بما في ذلك النساء اللاتي ما زلن لا يمثلن سوى %20 من القوى العاملة في مجال الأمن السيبراني.[[29]](#footnote-29)

12.5 إن جودة التعليم الرسمي في المدرسة أو الجامعة وزيادة الوعي العام تعتمد إلى حد ما على جودة البحث ونضجه وأهميته.

13.5 وبالإضافة إلى ذلك، من المهم إيلاء اهتمام لبناء قدرات المؤسسات الصغرى والصغيرة والمتوسطة (MSME) التي أصبحت الآن إحدى الجهات الفاعلة الرئيسية في الاقتصاد الرقمي المتنامي، وذلك بتمكينها من تحديد المخاطر السيبرانية وإدارتها واستخدام أصول تكنولوجيا المعلومات والاتصالات (بما فيها النطاق العريض والإنترنت) استخداماً مأموناً ومستداماً.

|  |
| --- |
| 14.5 في ضوء ما تقدم، لا يزال البرنامج العالمي للأمن السيبراني والتوصيات الواردة في إطار هذه الركيزة من تقرير الفريق لعام 2008 توفر إطاراً يعزز ويشجع نهجاً متعدد التخصصات لبناء القدرات. ومع مراعاة ذلك، يُقترح أن يقوم الاتحاد، من خلال مكتبه لتنمية الاتصالات (BDT) بما يلي:**أ )** مواصلة تعزيز المزيد من التعاون المفتوح والشامل، وكذلك التنسيق 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 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، بالتعاون مع الشركاء المهتمين والمجتمعات الأخرى 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 وتشجيع 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 الاحتياجات الأمنية للتكنولوجيات الناشئة. 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 وكبار السن، في جهود بناء القدرات.**ح)** مواصلة تطوير وتعزيز البرنامج العالمي للأمن السيبراني 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 أو الحوارات البحثية المتصلة بالأمن السيبراني بين مختلف أصحاب المصلحة، لا سيما في مجال التكنولوجيا الناشئة، والاستفادة من أعضاء الاتحاد من الهيئات الأكاديمية والقطاع الخاص كما حدث على سبيل المثال من خلال القمة العالمية بشأن الذكاء الاصطناعي من أجل تحقيق الصالح العام التي ينظمها الاتحاد سنوياً.**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 للتصدي للتحديات الأمنية وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.**ل)** مواصلة تعزيز ثقافة الأمن السيبراني. |

# القسم 6 الركيزة 5: التعاون الدولي

مقدمة

1.6 من الواضح أنه منذ العقد الماضي، لا يمكن لأي كيان أو منظمة بمفردها أن تتصدى لكامل التحديات الحالية والناشئة في مجال الأمن السيبراني. ويمكن التصدي لهذه التحديات من خلال الشراكات التي تنطوي على التعاون والتنسيق الوثيقين بين جميع أصحاب المصلحة من أجل المساعدة في بناء نظام إيكولوجي لتكنولوجيا المعلومات والاتصالات متاح للجميع ومفتوح وآمن وجدير بالثقة.

2.6 **ولذلك فإن الركيزة** 5 **بشأن التعاون الدولي هي ركيزة شاملة للبرنامج العالمي للأمن السيبراني – إذ تشكل الأساس لكل جانب من جوانب بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات. وفي تقرير الفريق لعام** 2008**، تسعى هذه الركيزة إلى وضع استراتيجية للتعاون والحوار والتنسيق على الصعيد الدولي في التعامل مع التهديدات السيبرانية.**

تطور مشهد التعاون الدولي منذ عام 2008

**حوارات عالمية رفيعة المستوى**

3.6 **تجري المناقشات بشأن الجوانب المختلفة للأمن السيبراني، بما في ذلك الجوانب التقنية والجريمة السيبرانية والخصوصية وحماية البيانات وغيرها، في العديد من المنتديات والعمليات. وقد استضافت وكالات الأمم المتحدة المختلفة بما في ذلك الاتحاد الدولي للاتصالات أو المنظمات الدولية الأخرى بعض هذه المناقشات، بينما شرع أصحاب مصلحة آخرون، إلى جانب مختلف المحافل الدولية والإقليمية الأخرى، في إجراء بعضها الآخر.**

4.6 **وعلى الرغم من أن جميع المنتديات والعمليات تقوم بعمل جيد في مجال إذكاء الوعي وتحسين الفهم، من المهم تحديد أوجه التآزر بين هذه الجهود المختلفة حتى يتمكن المجتمع الدولي من التكاتف وإيجاد الحلول الناجعة.**

5.6 **ومنصة الأمم المتحدة، بما تتمتع به من قدرة كبيرة على عقد الاجتماعات، في وضع جيد لتعزيز التعاون والحوارات والتنسيق على الصعيد الدولي بين جميع أصحاب المصلحة من جميع الدول بشأن التصدي للتحديات المتصلة بالفضاء السيبراني. وكما جاء في تقرير الفريق لعام** 2008**، يمكن للاتحاد، بالنظر إلى مركزه في منظومة الأمم المتحدة بوصفه الوكالة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات، أن يواصل الاضطلاع بدور مهم، في نطاق ولايته، في ميادين التطورات ذات الصلة.**

6.6 **على الرغم من اقتراح عقد "مؤتمر عالمي" في التوصية** 15.1 **من تقرير الفريق لعام** 2008،**[[30]](#footnote-30) يمكن أيضاً الاستفادة على نحو أفضل من المؤتمرات والمنتديات العالمية الحالية المنبثقة عن عملية القمة العالمية لمجتمع المعلومات والمعززة فيما بعد –** [منتدى القمة العالمية لمجتمع المعلومات](https://www.itu.int/net4/wsis/forum/2020/) لأغراض التنمية و[منتدى إدارة الإنترنت](https://www.intgovforum.org/multilingual/) لأغراض الإدارة. ويقدم منتدى القمة العالمية لمجتمع المعلومات، وهو أكبر تجمع سنوي لمجتمع تكنولو**جيا المعلومات والاتصالات لأغراض التنمية، عدة آليات للجمع بين المجتمع العالمي لمناقشة حلول ملموسة وتحديدها للتصدي للتحديات الإنمائية المتعلقة ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (خط العمل جيم**5**) بما في ذلك مسار الجهات الميسرة لخطوط العمل، والحوارات رفيعة المستوى وجلسات أصحاب المصلحة المستهدفة وغيرها.**

7.6 **ومن التطورات الهامة التي حدثت في العقد الماضي الاعتراف بالأهمية الحاسمة للأمن السيبراني على أعلى المستويات السياسية للحكومات الوطنية. ويتجلى ذلك في اعتماد الكثير من البلدان استراتيجية للتحول الرقمي تعتمد نهجاً يشمل الحكومة بأسرها ويُنشئ آليات تنسيق مركزية شاملة لعدة قطاعات تكون عادة مسؤولة مباشرة أمام رؤساء الدول والحكومات.**

8.6 **ومن التطورات الأخرى ذات الصلة العدد الكبير من المناقشات الثنائية الجارية بين البلدان والمناطق المتقدمة تكنولوجياً.**

**الشراكات الدولية لأصحاب المصلحة المتعددين**

9.6 **حقق الاتحاد نجاحات مختلفة في تعزيز التعاون الدولي من خلال دوره** بصفته الميسِّر الوحيد لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات.

10.6 **وقد أقام الاتحاد مجموعة من الشراكات بين أصحاب المصلحة المتعددين، من خلال ما يلي:**

• آليات رسمية مثل مذكرات التفاهم أو ترتيبات مماثلة (من قبيل أفرقة التصدي للحوادث وأمن المعلومات (FIRST)، والإنتربول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، والمنتدى الاقتصادي العالمي وغير ذلك)؛

• مبادرات مثل مبادرة حماية الأطفال على الخط، بالشراكة[[31]](#footnote-31) مع أكثر من 80 كياناً من جميع فئات أصحاب المصلحة؛

• آليات مثل الأفرقة المتخصصة، منها الأفرقة المتخصصة المعنية بتكنولوجيات السجلات الرقمية، والتكنولوجيات الكمومية، والذكاء الاصطناعي، والصحة وما إلى ذلك، التي توفر منصة لجميع أصحاب المصلحة لمناقشة القضايا المتعلقة بالثقة في التكنولوجيات الناشئة**.**

11.6 والاتحاد، من خلال التوسع الكبير في عضويته متعددة أصحاب المصلحة في العقد الماضي، ولا سيما مجموعة شركات القطاع الخاص والمؤسسات الأكاديمية، يستفيد من عضوية واسعة تضم 193 دولة عضواً وما يقرب من 900 شركة من القطاع الخاص وجامعة ومنظمة دولية وإقليمية مما يبرز الطبيعة المتغيرة بسرعة للمجتمع الرقمي اليوم.

**تحسين التنسيق داخل منظومة الأمم المتحدة**

12.6 **كما سبق أن ذُكر في الفقرتين** 4.2 **و**5.2 **من هذه الوثيقة، أنشأت الجمعية العامة للأمم المتحدة عدداً من عمليات الأمم المتحدة، التي تستهدف المساعدة في التصدي لتحديات ضمان الأمن الدولي في الفضاء السيبراني، وتشمل هذه العمليات أعمال فريق الخبراء الحكوميين** (GGE) **وفريق العمل المفتوح العضوية** (OEWG)**. وقد خلص** [**التقرير الموضوعي النهائي لفريق العمل المفتوح العضوية**](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) **للفترة** 2021-2019**، ضمن استنتاجات أخرى، إلى** **أن أي حوار مؤسسي قد يُجرى في المستقبل بانتظام ينبغي ألا يكرر ولايات الأمم المتحدة وجهودها وأنشطتها الحالية المركِّزة على الأبعاد الرقمية للقضايا الأخرى، وأن أي آلية مستقبلية للحوار المؤسسي المنتظم تحت رعاية الأمم المتحدة ينبغي أن تكون عملية ذات منحى عملي ومحددة الأهداف، تنطلق من النتائج السابقة، وتكون شاملة للجميع وشفافة ومدفوعة بتوافق الآراء وقائمة على النتائج. وبأخذ ذلك في الاعتبار، من المهم أن تكمّل أعمال الاتحاد اتجاهات العمل الجارية حالياً بهذا الخصوص داخل منظومة الأمم المتحدة، ولا سيما العمليات المذكورة أعلاه التي أنشأتها الجمعية العامة للأمم المتحدة.**

13.6 **إن الصياغة المعقدة لولاية منظومة الأمم المتحدة يمكن أن تعرقل في بعض الأحيان اتباع نهج منسق عملي وفعال. ولذلك من الضروري أن تواصل أسرة الأمم المتحدة العمل من أجل تنسيق جهودها بما في ذلك تبسيط البرامج والأنشطة المتعلقة بالأمن السيبراني لكي تكون أكثر فعالية.**

14.6 **ولذلك، من المهم العمل على بناء تفاهم مشترك داخل الأمم المتحدة بشأن الاحتياجات والمتطلبات اللازمة لوضع البرامج والمبادرات التي من شأنها أن تدعم بفعالية الجهود التي تبذلها الحكومات ودوائر الصناعة وجميع أصحاب المصلحة الآخرين المعنيين.**

15.6 **وقد اتُخذت خطوة أولى مهمة في عام** 2010**. نحو تعزيز التنسيق الداخلي بين وكالات الأمم المتحدة في مساعدتها للدول الأعضاء فيما يتعلق بالأمن السيبراني.** وقاد 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، صدق عليه مجلس الرؤساء التنفيذيين (CEB) في نوفمبر 2013.

16.6 **وعلى الرغم من أنها خطوة رئيسية، هناك حاجة إلى مزيد من التغييرات المنهجية لضمان التنسيق الفعّال. ويتيح تحديد الأمين العام للأمم المتحدة لأوليات التعاون الرقمي[[32]](#footnote-32) فرصة لتلبية حاجة أسرة الأمم المتحدة ككل إلى مواصلة تحسين التنسيق والتعاون الداخليين من خلال استعمال مختلف الآليات المشتركة بما فيها مجلس الرؤساء التنفيذيين.**

المبادئ توجيهية لاستخدام الركيزة 5 – التعاون الدولي

|  |
| --- |
| 17.6 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 السيبرانية 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 رفيع 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)** وفي حين ينبغي مواصلة تشجيع المناقشات الثنائية ومتعدد الأطراف بين الجهات الفاعلة الرئيسية، نظراً للطابع العالمي للتهديدات السيبرانية، من المهم أيضاً تيسير إجراء مناقشات أوسع نطاقاً بين مجموعات أوسع، بما في ذلك القطاع الخاص وأصحاب المصلحة الآخرين. 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 )** وينبغي للاتحاد أن يواصل استكشاف آليات مبتكرة ومرنة وسريعة الحركة لبناء الشراكات مع مراعاة قطاع تكنولوجيا المعلومات والاتصالات سريع الطور ومجموعة الكيانات الجديدة الناشئة، ولا سيما المشاريع المبتدئة والشركات الصغرى والصغيرة والمتوسطة.**ه‍ )** وينبغي للاتحاد أن يواصل العمل بنشاط مع الوكالات الرئيسية الأخرى داخل منظومة الأمم المتحدة، لتنسيق الجهود الداخلية لأمانة الأمم المتحدة وتبسيط برامجها وأنشطتها المتعلقة بالأمن السيبراني، لكي يكون أكثر فعالية في خدمة المجتمع العالمي. |

# القسم 7 المبادئ التوجيهية العامة لإطار البرنامج العالمي للأمن السيبراني

|  |
| --- |
| 1.7 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)
4. لمزيد من المعلومات بشأن العملية، وللحصول على المساهمات الواردة من الدول الأعضاء وأصحاب المصلحة الآخرين، يرجى زيارة الموقع التالي: <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. الوثائق الختامية للقمة العالمية لمجتمع المعلومات، 2005، متاحة في الموقع التالي: <https://www.itu.int/net/wsis/outcome/booklet.pdf>. [↑](#footnote-ref-5)
6. القاضي شتاين شيولبرغ: تقرير مقدم من رئيس فريق الخبراء رفيع المستوى المعني بالأمن السيبراني (HLEG)، 2008، متاح في الموقع التالي: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-6)
7. تقدم التوصيات الواردة في تقرير الفريق HLEG لعام 2008 مع موجز مشروح للآراء والمناقشات التي جرت خلال الاجتماع فيما يتعلق بكل بتوصية. وعلى الرغم من أن أعضاء الفريق لم يحققوا توافقاً كاملاً في الآراء بشأن كل توصية، فإن معظم خبراء الفريق كانوا مع ذلك متفقين على نطاق واسع بشأن العديد من التوصيات. [↑](#footnote-ref-7)
8. حل [توجيه البرلمان الأوروبي ومجلس الاتحاد الأوروبي المؤرخ 12 أغسطس 2013 بشأن الهجمات على أنظمة المعلومات محل القرار الإطاري للمجلس (2005)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040) ويعرّف البنية التحتية الأساسية على النحو التالي: *أصل أو نظام أو جزء منه موجود في الدول الأعضاء وهو ضروري لحالات الحفاظ على الوظائف المجتمعية الحيوية أو الصحة أو السلامة أو الأمن أو الرفاه الاقتصادي أو الاجتماعي للناس، والذي سيكون لتعطيله أو تدميره تأثير كبير على دولة عضو نتيجة لعدم الحفاظ على تلك الوظائف*. [↑](#footnote-ref-8)
9. عدد مستعملي فيسبوك النشطين شهرياً في جميع أنحاء العالم حتى الربع الأخير من عام 2020، متاح في الموقع التالي:
<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. [↑](#footnote-ref-9)
10. مارك زوكربيرغ: *الإنترنت بحاجة إلى قواعد جديدة. دعونا نبدأ في هذه المجالات الأربعة*، واشنطن بوست، 30 مارس 2019، متاح في الموقع التالي: <https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html>. [↑](#footnote-ref-10)
11. فريق الخبراء الحكوميين، متاح في الموقع التالي: <https://www.un.org/disarmament/group-of-governmental-experts/>. [↑](#footnote-ref-11)
12. فريق العمل المفتوح العضوية، متاح في الموقع التالي: <https://www.un.org/disarmament/open-ended-working-group/>. [↑](#footnote-ref-12)
13. لمزيد من المعلومات، يرجى الرجوع إلى ما يلي:

- تقرير الأنشطة السنوية للاتحاد المقدم إلى مجلس الاتحاد بشأن بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات، متاح في الموقع التالي: <https://www.itu.int/en/council/2021/Pages/default.aspx>.

- تقرير مقدم إلى المجلس في دورته لعام 2021 بشأن استخدام الاتحاد للبرنامج العالمي للأمن السيبراني، متاح في الموقع التالي: <https://www.itu.int/md/S21-CL-C-0036/en>. [↑](#footnote-ref-13)
14. شتاين شولبرغ، تاريخ الجريمة السيبرانية، (الطبعة الثالثة، فبراير 2020). [↑](#footnote-ref-14)
15. أطلقت مفوضية الاتحاد الأوروبي برنامجاً يسمى [Horizon 2020](https://ec.europa.eu/programmes/horizon2020/en) لتطوير إمكانات إنترنت الأشياء، وبرنامج العمل 2016-2017 لدعم التجريب والابتكار. ويُدعى إلى تقديم مقترحات بشأن العديد من المواضيع، منها أيضاً: أمن وخصوصية إنترنت الأشياء. والمفاهيم المتقدمة بشأن الأمن من طرف إلى طرف في بيئات إنترنت الأشياء الموزعة بشكل كبير وغير المتجانسة والدينامية. ويجب أن تكون المناهج شمولية وأن تتضمن تحديد الهوية والاستيقان وحماية البيانات والوقاية من الهجمات السيبرانية على مستويات الأجهزة والأنظمة. ويجب أن تتناول عناصر الأمن والخصوصية ذات الصلة مثل السرية، والوعي والتحكم في بيانات المستخدم، والنزاهة، والمرونة، والتفويض (انظر قرار المفوضية الأوروبية C (2015) 6776 المؤرخ 13 أكتوبر 2015). [↑](#footnote-ref-15)
16. ت. باليل، *التحديات القانونية للذكاء الاصطناعي: نمذجة السمات الثورية للتكنولوجيات الناشئة وتقييم تأثيرها القانوني المحتمل*، مراجعة القانون الموحد، المجلد 24، الإصدار 2، يونيو 2019، الصفحات 314-302، متاح في الموقع التالي:
<https://doi.org/10.1093/ulr/unz018>. [↑](#footnote-ref-16)
17. يمكن أن يكون الإطار القانوني النموذجي هو [التوجيه 2011/92/EU للبرلمان الأوروبي والمجلس المؤرخ 13 ديسمبر 2011](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en)، بشأن مكافحة الاعتداء الجنسي على الأطفال واستغلالهم جنسياً واستغلالهم في المواد الإباحية. [↑](#footnote-ref-17)
18. القاضي شتاين شولبرغ، 2018 والقاضي شتاين شولبرغ، 2019، متاح في الموقع التالي:
<https://www.cybercrimelaw.net/Cybercrimelaw.html> [↑](#footnote-ref-18)
19. على سبيل المثال، https://www.justice.gov/olp/lawful-access. [↑](#footnote-ref-19)
20. مشهد معايير الاتحاد، متاح في الموقع التالي:
‑[https://www.itu.int/net4/ITU‑T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance](https://www.itu.int/net4/ITUT/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance). [↑](#footnote-ref-20)
21. تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، الفقرة 1.2، الصفحة 9، نفس المرجع السابق الذي يحيل إلى رقم 6. [↑](#footnote-ref-21)
22. تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، الفقرة 2.2، الصفحة 9، نفس المرجع السابق الذي يحيل إلى رقم 6. [↑](#footnote-ref-22)
23. تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، الفقرة 2، الصفحة 9، نفس المرجع السابق الذي يحيل إلى رقم 6. [↑](#footnote-ref-23)
24. الأفرقة الوطنية للاستجابة للحوادث الحاسوبية، الاتحاد الدولي للاتصالات، متاح في الموقع التالي:
<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>. [↑](#footnote-ref-24)
25. *المرجع نفسه*. [↑](#footnote-ref-25)
26. *المرجع نفسه*. [↑](#footnote-ref-26)
27. Tim Berners-Lee، *30 years on, what’s next #ForTheWeb?*، 12 مارس 2019. (متاح في الموقع التالي: <https://webfoundation.org/2019/03/web-birthday-30/>) في الذكرى السنوية الثلاثين للويب، في رسالة مفتوحة، تشير إلى أنه *على الرغم من أن الويب أتاحت الفرصة للفئات المهمشة، وأعطتها صوتاً وجعلت حياتنا اليومية أسهل، فقد أتاحت الفرصة أيضاً للمحتالين وأعطت صوتاً لمن ينشرون الكراهية وجعلت من السهل ارتكاب جميع أنواع الجرائم.* [↑](#footnote-ref-27)
28. غيرناوطي، *Cyberpower, Crime, Conflict and Security in Cyberspace*، قسم EPFL Press، 2013. [↑](#footnote-ref-28)
29. لورنس برادفورد، *Cybersecurity needs women: Here’s why*، 18 أكتوبر 2018، متاح في الموقع التالي:
[https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity‑needs‑women‑heres‑why/#5a7a3cc447e8](https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurityneedswomenhereswhy/#5a7a3cc447e8) [↑](#footnote-ref-29)
30. تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني لعام 2008، الفقرة 15.1، الصفحة 9، نفس المرجع السابق الذي يحيل إلى رقم 6. [↑](#footnote-ref-30)
31. تُتاح المزيد من المعلومات في الموقع التالي: <https://www.itu.int/en/cop/Pages/partners.aspx> [↑](#footnote-ref-31)
32. تُتاح المزيد من المعلومات في الموقع التالي: <https://www.un.org/en/digital-cooperation-panel/>. [↑](#footnote-ref-32)