|  |  |
| --- | --- |
| **المجلس 2020جنيف، 19-9 يونيو 2020** |  |
|  |  |
|  |  |
| **بند جدول الأعمال: PL 1.4** | **الوثيقة C20/65-A** |
|  | **5 مايو 2020** |
|  | **الأصل: بالإنكليزية** |
| تقرير من الأمين العام |
| المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني |
|  |

|  |
| --- |
| ملخصكلّف 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) شتاين شولبرغ، النرويج (الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالأمن السيبراني)، وبمشاركة الدول الأعضاء، 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-20/18))](https://www.itu.int/md/S20-SG-CIR-0018/en)، عُقدت مشاورة مفتوحة لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات في 23 أبريل 2020 لتقديم تعليقات على مشروع المبادئ التوجيهية.الإجراء المطلوببما أن تعليقات أصحاب المصلحة خلال المشاورات المفتوحة أبرزت الحاجة إلى إجراء مزيد من المشاورات بشأن مشروع المبادئ التوجيهية، فإن المجلس مدعوّ إلى النظر في هذه الوثيقة **وتقديم توجيهات** بشأن سبل المضي قدماً.\_\_\_\_\_\_\_\_\_\_\_\_المراجع*القرار* [*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf) *(المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين*[*البرنامج العالمي للأمن السيبراني (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*،* [*الوثيقة C20/36*](https://www.itu.int/md/S20-CL-C-0036/en)*،* [*الوثيقة C20/INF/11*](https://www.itu.int/md/S20-CL-INF-0011/en) |

**جدول المحتويات**

[**القسم 1 مقدمة** 3](#_Toc41495922)

[خلفية 3](#_Toc41495923)

[السياق 4](#_Toc41495924)

[استمرار أهمية وانطباق البرنامج العالمي للأمن السيبراني كإطار عالمي للعمل 6](#_Toc41495925)

[**القسم** **2 الركيزة 1: التدابير القانونية** 7](#_Toc41495926)

[مقدمة 7](#_Toc41495927)

[تطور المشهد القانوني منذ عام 2008 7](#_Toc41495928)

ال[مبادئ توجيهية لاستخدام الركيزة 1 – التدابير القانونية 9](#_Toc41495931)

[**القسم3 الركيزة 2: التدابير التقنية والإجرائية** 10](#_Toc41495932)

[مقدمة 10](#_Toc41495933)

[تطور مشهد التدابير التقنية والإجرائية منذ عام 2008 11](#_Toc41495934)

ال[مبادئ توجيهية لاستخدام الركيزة 2 – التدابير التقنية والإجرائية 12](#_Toc41495936)

[**القسم 4 الركيزة 3: الهياكل التنظيمية** 13](#_Toc41495937)

[مقدمة 13](#_Toc41495938)

[تطور مشهد الهياكل التنظيمية منذ عام 2008 13](#_Toc41495939)

[المبادئ التوجيهية لاستخدام الركيزة 3 – الهياكل التنظيمية 14](#_Toc41495940)

[**القسم 5 الركيزة 4: بناء القدرات** 15](#_Toc41495941)

[مقدمة 15](#_Toc41495942)

[تطور مشهد بناء القدرات منذ عام 2008 15](#_Toc41495943)

ال[مبادئ التوجيهية لاستخدام الركيزة 4 – بناء القدرات 16](#_Toc41495944)

[**القسم 6 الركيزة 5: التعاون الدولي** 17](#_Toc41495945)

[مقدمة 17](#_Toc41495946)

[تطور مشهد التعاون الدولي منذ عام 2008 17](#_Toc41495947)

ال[مبادئ التوجيهية لاستخدام الركيزة 5 – التعاون الدولي 19](#_Toc41495951)

[**القسم** **7** **المبادئ التوجيهية لإطار البرنامج العالمي للأمن السيبراني**  20](#_Toc41495952)

[ا**لملحق 1 بعض الأمثلة للتطورات الإقليمية والعالمية منذ عام 2008**  21](#_Toc41495953)

# 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.*

**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) 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، النرويج (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 البروفيسور سولانج غيرناوتي (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 لإنتربول) 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** وفقاً لعملية إعداد مشروع المبادئ التوجيهية الواردة في [الرسالة المعممة (CL-20/18)](https://www.itu.int/md/S20-SG-CIR-0018/en)، عُقدت مشاورة مفتوحة لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات في 23 أبريل 2020 لتقديم تعليقات بشأن مشروع المبادئ التوجيهية (مشاورة مفتوحة). وحضر الاجتماع أكثر من 160 مشاركاً وقدموا تعليقات بشأن كل قسم في مشروع المبادئ التوجيهية. وأُعرب عن آراء مختلفة في المشاورة المفتوحة وجُسدت في ملخص موجز للمشاورة المفتوحة أعدته أمانة الاتحاد (الوثيقة [C20/INF/11](https://www.itu.int/md/S20-CL-INF-0011/en)). وبالإضافة إلى ذلك، نُشرت أي تعليقات واردة من المشاركين كتابةً بعد المشاورة المفتوحة مباشرةً في [الموقع الإلكتروني](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) أيضاً. ومن بين هذه التعليقات، أبرز المشاركون الحاجة إلى مزيد من المشاورات مع أصحاب المصلحة.

## خلفية

**6.1** 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).

**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[[6]](#footnote-6) (تقرير الفريق HLEG لعام (2008. 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** في 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 – ولدى فيسبوك مثلاً أكثر من 2,5 مليار مستعمل نشط شهرياً (ديسمبر 2019).[[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 يسلط وباء COVID-19 في 2020 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 COVID-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** واعتباراً من 2019، وقّع أكثر من 125 بلداً و/أو صدق 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) التي صدقت عليها 65 دولة (مارس 2020)، والبروتوكول الإضافي الثاني للاتفاقية بشأن الأمن السيبراني الذي بدأت المفاوضات بشأنه في 2017.[[11]](#footnote-11) كما نشر [دليل تالين 2.0](https://ccdcoe.org/research/tallinn-manual/) في 2017، الذي يشير إلى أن تغطية القانون الدولي الذي يحكم الحرب السيبرانية تنطبق أيضاً على الأنظمة القانونية في وقت السلم.[[12]](#footnote-12) وفي إطار اللجنة الأولى للجمعية العامة للأمم المتحدة، يواصل فريق من الخبراء الحكوميين (CGE)[[13]](#footnote-13) وفريق عمل مفتوح العضوية (OEWG)[[14]](#footnote-14) دراسة التهديدات التي يطرحها استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي مع التركيز أيضاً على كيفية التصدي لهذه التهديدات.

**20.1** إن تكنولوجيات المعلومات والاتصالات المبتكرة مثل الحوسبة السحابية والشبكات المعرّفة بالبرمجيات (SDN)، والتمثيل الافتراضي لوظائف الشبكة (FVN)، 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.

**21.1** 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 لإنتربول (IGCI)، والمركز العالمي للأمن السيبراني للتابع للمنتدى الاقتصادي العالمي وغيرها.

**22.1** 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 وانطباق البرنامج العالمي للأمن السيبراني كإطار عالمي للعمل

**23.1** 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.

**24.1** وقد عزّز 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.[[15]](#footnote-15)

**25.1** وبغية تعزيز الجهود الرامية إلى الاستفادة من البرنامج العالمي للأمن السيبراني، يُقدم مزيد من التوجيهات في الأقسام اللاحقة. ولدى وضع هذه التوجيهات، أُخذت في الاعتبار التوصيات الواردة في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، وأنشطة الاتحاد منذ ذلك الحين، والتطورات في المجال منذ عام 2008[، والمساهمات الواردة من الدول الأعضاء](https://www.itu.int/md/S20-GCA-C/en) (عملاً ب[الرسالة المعممة (CL-20/18)](https://www.itu.int/md/S20-SG-CIR-0018/en))

**26.1** وفيما يتعلق بالجمهور المستهدف من المبادئ التوجيهية، تقدم بعض المبادئ التوجيهية العامة توجيهات إلى أعضاء الاتحاد وأصحاب المصلحة فيه وشركائه، بشأن تحسين استخدام البرنامج العالمي للأمن السيبراني عملاً بدور الاتحاد كجهة ميسرة لخط العمل جيم5، ويقدم البعض الآخر التوجيه إلى أمانة الاتحاد أثناء الاضطلاع بأنشطتها في هذا الصدد عملاً بقرارات الاتحاد ذات الصلة. وهذا مماثل للنسق المتبع في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008.

**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** البعد القانوني للأمن السيبراني أمر أساسي لضمان احتفاظ الناس من جميع الدول بالثقة في استخدام تكنولوجيا المعلومات والاتصالات.

**2.2** يشير 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 بالمبادرات الإقليمية ذات الصلة كمرجع، بما في ذلك على سبيل المثال لا الحصر اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001.

## تطور المشهد القانوني منذ عام 2008

**3.2** وضعت المنظمات الإقليمية العديد من الاتفاقيات والإعلانات والاتفاقات والمبادئ التوجيهية بعد 2008 بشأن الأمن السيبراني (انظر الملحق 1). وكما ذُكر أعلاه، وقّع أكثر من 125 بلداً و/أو صدّق على اتفاقيات أو إعلانات أو مبادئ توجيهية أو اتفاقات مختلفة بشأن الأمن السيبراني مما أسفر، إلى حد ما، عن التجزؤ والتنوع على الصعيد الدولي.

**4.2** وكانت هناك اقتراحات بشأن استجابة أكثر تنسيقاً وتنظيماً على الصعيد الدولي للتصدي للطائفة الواسعة من التحديات المتصلة بالأمن السيبراني العالمي، وكذلك بشأن أي مبادئ توجيهية تتعلق بالتدابير القانونية لإدراج مبادئ لتنسيق القوانين بشأن عدة قضايا عالمية[[16]](#footnote-16). وبالإضافة إلى ذلك، اقترح البعض وضع مبادئ لصياغة إطار دولي للفضاء السيبراني لأغراض التنسيق العالمي[[17]](#footnote-17).

التدابير القانونية والتكنولوجيات الجديدة

**5.2** اقترح بعض الخبراء أن يشمل القانون الجنائي[[18]](#footnote-18) التكنولوجيا الجديدة وأساليب السلوك في الفضاء السيبراني ذا القصد الإجرامي. وقد اعتمدت بلدان كثيرة أو تستعد لوضع قوانين جديدة تشمل بعض تلك السلوك. ويرد فيما يلي بعض الأمثلة للتكنولوجيات والاتجاهات الحديثة والناشئة التي يمكن أن تؤثر على التدابير القانونية.

 أ ) الهجمات السيبرانية العالمية

تظهر الهجمات السيبرانية العالمية ضد البنى التحتية الحيوية للاتصالات والمعلومات كتهديد للأمن الوطني. وكانت الحكومات والمنظمات الدولية والمؤسسات الخاصة جميعها أهدافاً لهجمات سيبرانية عالمية. ولذلك، يقترح بعض الخبراء أن تشمل الجهود الرامية إلى مواءمة التدابير القانونية في مختلف المجالات الجوانب المتصلة بالأمن السيبراني[[19]](#footnote-19)

ب) السلوك الإجرامي في الشبكات الاجتماعية

هناك دعوات إلى اتخاذ تدابير لمكافحة السلوك غير القانوني، 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.[[20]](#footnote-20) ففي 2016، تعرضت البنية التحتية الإلكترونية في جميع أنحاء العالم، في واحدة من أكبر الهجمات الإلكترونية على الإطلاق، لهجوم من جانب شبكة روبوتية من الأجهزة الموصولة المقرصنة، بدءاً من كاميرات الويب إلى المسيّرات. وأثيرت مخاوف على الصعيد العالمي في هذا الصدد، وعلى سبيل المثال، في 2017، أكد مكتب التحقيقات الفيدرالي الأمريكي على الفرص المختلفة المتاحة لمرتكبي الجرائم السيبرانية للنفاذ إلى إنترنت الأشياء وأجهزة أخرى إلى جانب المعلومات المرفقة بهذه الشبكات[[21]](#footnote-21). ومع ظهور تكنولوجيات جديدة من قبيل الجيل الخامس، والأجهزة الموصولة بينياً في كل مكان التي أصبحت حقيقة واقعة، من المرجح أن تزداد المخاطر[[22]](#footnote-22).

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.[[23]](#footnote-23)

ه‍ ) الاستغلال الجنسي للأطفال 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 الجنسي والاعتداء الجنسي 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.[[24]](#footnote-24) 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 التكنولوجيا ت المماثلة.

القوانين الإجرائية – المبادئ العامة

**6.2** اعتُبر اعتماد القوانين الإجرائية اللازمة لتحديد سلطات وإجراءات مقاضاة السلوك الإجرامي في الفضاء السيبراني إجراءً قانونياً رئيسياً في مجال الأمن السيبراني لمنع الجريمة السيبرانية والتحقيق فيها وملاحقتها قضائياً على الصعيد العالمي. غير أن بعض الخبراء لاحظوا أن هذه السلطات والإجراءات يمكن أن تكون ضرورية أيضاً لمكافحة الجرائم الجناية الأخرى المرتكبة بواسطة نظام حاسوبي، ويمكن أن تنطبق اللوائح على جمع الأدلة في شكل إلكتروني لجميع الجرائم الجنائية[[25]](#footnote-25). وينبغي أن تكون جميع القوانين الإجرائية متسقة مع الالتزامات والمعايير المحددة بموجب القانون الدولي لحقوق الإنسان.

## المبادئ توجيهية لاستخدام الركيزة 1 – التدابير القانونية

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

**8.2** منذ 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 ومستودع الجريمة السيبرانية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html). 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.

|  |
| --- |
| **9.2** 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 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 )** وتُحث الدول الأعضاء على تصميم وتطوير أي تدابير قانونية مناسبة وفقاً لالتزاماتها في مجال حقوق الإنسان.**هـ )** وتُشجع الدول الأعضاء على التعاون والعمل مع أصحاب المصلحة الآخرين للبحث عن أرضية عالمية مشتركة بشأن التدابير القانونية المتعلقة بالأمن السيبراني، مع ملاحظة ونمذجة الأطر القائمة مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001، والعمل الجاري في إطار الجمعية العامة للأمم المتحدة.[[26]](#footnote-26)**و )** تُشجع الدول الأعضاء على مواصلة اتخاذ التدابير القانونية لحماية بنيتها التحتية الحيوية للاتصالات والمعلومات (وأي أصول أو أنظمة ذات صلة أو جزء منها) الضرورية للحفاظ على الوظائف المجتمعية الحيوية مثل الصحة أو السلامة أو الأمن أو الرفاه الاقتصادي أو الاجتماعي للناس، ومنع أي خلل أو تدمير قد يسبب أثراً كبيراً لهذه البنى التحتية الحيوية وفشل تشغيلها.**ز )** ويتعين على الدول الأعضاء أيضاً اتخاذ التدابير القانونية المناسبة لتنفيذ برامج فعالة لمنع أو حظر نشر المواد الإلكترونية المتعلقة بالاعتداء الجنسي على الأطفال، 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، 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.**ح)** مع ملاحظة أن مبدأ سيادة الدول ينطبق على الفضاء السيبراني، تُشجع الدول الأعضاء على استكشاف الآليات التي تحمي الحقوق الأساسية للمواطنين وسلامتهم مع تيسير النفاذ المشروع إلى محتوى الاتصالات حيث تم تنفيذ التشفير من طرف إلى طرف.[[27]](#footnote-27) |

# 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 متسق 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 السيطرة على المخاطر السيبرانية من خلال التدابير التكنولوجية والإجرائية 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** وتعد أنشطة التقييس أمراً أساسياً كي تعمل جميع البنى التحتية والتطبيقات والخدمات. ويوفر الاتحاد، مع أعضائه من أصحاب المصلحة المتعددين، منصة فريدة لتقييس تكنولوجيا المعلومات والاتصالات على الصعيد العالمي.

**5.3** تمثل 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[[28]](#footnote-28) معايير أمن تكنولوجيا المعلومات والاتصالات من أجل النفاذ العام، التي تضم 2600 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 و OneM2Mوغيرها.

**6.3** على 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*"[[29]](#footnote-29).

**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*".[[30]](#footnote-30) 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** أبرز 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"*[[31]](#footnote-31). 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 جميع التوصيات المتعلقة بالركيزة 2 في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008 صالحة. وفي ضوء ما تقدم، تُقترح المبادئ التوجيهية التالية من أجل الركيزة 2:**أ )** ينبغي أن تركز لجان الدراسات التابعة للاتحاد على تكنولوجيات الأمن الناشئة من أجل دراسة وصياغة مبادئ توجيهية لاستخدام التكنولوجيات ذات الصلة، وتوجيه الدول الأعضاء بشأن تطبيق هذه التقنيات 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 الاخرى المعنية بوضع المعايير، لضمان الحفاظ على أمن المنتجات من البداية إلى النهاية لمختلف التطبيقات والخدمات طوال دورة حياة المنتجات.**د )** ينبغي أن يواصل الاتحاد جمع 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 )** تُشجَّع الدول الأعضاء على الالتزام برؤية عالمية مشتركة للأمن السيبراني ، ومواصلة تنفيذ هذه التوصيات، ودعم الاتحاد ليصبح "مركز التميز العالمي" لوضع توصيات بشأن التدابير التقنية والإجرائية للأمن السيبراني في المجالات التي تندرج في إطار ولايته (على النحو المشار إليه في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008).**و )** تُشجَّع الدول الأعضاء على المشاركة في ترتيبات إصدار الشهادات المتبادلة من أجل وضع إطار عالمي لإدارة الأمن السيبراني يستند 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 وتقابلها.

**2.4** ومن الضروري على الصعيد الوطني وضع آليات، وهياكل مؤسسية، فعالة للتعامل مع التهديدات والحوادث السيبرانية 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 مهم في إيجاد الحلول الناجعة.

## 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** تشمل بعض الأمثلة على المبادرات الوطنية والإقليمية أفريبول وأميريبول وشرطة مجلس التعاون الخليجي (GCCPO)، 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).

**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.[[32]](#footnote-32)

**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، ما يقرب من 80 تقييماً لمدى تأهب أفرقة الاستجابة للحوادث الحاسوبية من أجل مساعدة البلدان في تقييم قدرتها الوطنية في مجال التأهب للأمن السيبراني والاستجابة للحوادث.[[33]](#footnote-33) وقدم الاتحاد الدعم لإنشاء/تعزيز 14 فريقاً وطنياً للاستجابة للحوادث الحاسوبية للدول الأعضاء في الاتحاد.[[34]](#footnote-34) 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://www.thegfce.com/) 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.

• يقدم [مركز التميز المعني بالدفاع الحاسوبي التعاوني (CCDCOE) التابع لمنظمة حلف شمال الأطلسي](https://ccdcoe.org/research/tallinn-manual/)، الذي أطلق في تالين في 2008، نتائج أبحاثه بشأن تدابير الدفاع السيبراني ويعزز الأمن السيبراني من خلال تمارين تستهدف الخبراء التقنيين والموظفين العسكريين والدول الأعضاء المعنية بوصع القرار.

• أطلق المنتدى الاقتصادي العالمي [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 المؤشر العالمي للأمن السيبراني، لتعزيز الأمن السيبراني كعامل تمكيني شامل للتحول 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** تواجه جميع البلدان وجميع المنظمات الحاجة إلى أن تتوفر لها الموارد والمهارات البشرية الكافية والضرورية من أجل:

• تنفيذ تدابير استراتيجية وتشغيلية للأمن السيبراني؛

• السيطرة على المخاطر؛

• إدارة الأزمات المتعلقة بوقوع حوادث أمنية (الهجمات السيبرانية)؛

• تعزيز متانة البنى التحتية وقدرتها على الصمود؛

• تطوير سلوكيات 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 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 ويتعامل مع مجموعة كبيرة من القضايا – مثل استخدامات تكنولوجيا المعلومات والاتصالات أو إساءة استخدامها، والتدابير التقنية والقضايا الاقتصادية والقانونية والسياسية – من المهم تطوير ثقافة عالمية للأمن السيبراني لتعزيز مستوى الفهم لكل جهة فاعلة في سلسلة الأمن السيبراني. وعند تطوير ثقافة الأمن السيبراني وتصميمها، يتمثل أحد التحديات الرئيسية المطروحة في أن تُحدد بشكل صحيح القضايا العالمية والدولية والاحتياجات المحلية المحددة. ولا يمكن للمعايير الدولية أن تساهم إلا في تحديد القضايا العالمية والعامة الرئيسية المتعلقة بثقافة الأمن السيبراني، إذ تعتمد الثقافات بشكل أساسي على العوامل المحلية والزمنية التي تستجيب للعديد من خلفيات المستعملين النهائيين ووجهات نظرهم واحتياجاتهم لهذا الغرض.

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.[[35]](#footnote-35) وكل ما يمكن توصيله يمكن قرصنته.. 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 على أتم استعداد لمواجه التحدي المتمثل في بناء مجتمع معلومات شامل.

7.5 لا 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 لإدارة أفرقة الاستجابة للحوادث الحاسوبية (CIRT) وتطوير الموارد لحماية الأطفال على الخط.

9.5 فعلى سبيل المثال، من المهم الاعتراف بمساهمة [المؤشر 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 المؤشر العالمي للأمن السيبراني، من خلال تركيزه على زيادة الوعي، يقدم الدعم للدول الأعضاء لتحسين موقفها 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 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.[[36]](#footnote-36)

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. وتفيد التقارير بأنه سيكون هناك ما يصل إلى 3,5 مليون فرصة عمل ذات صلة بالأمن السيبراني بحلول عام 2021.[[37]](#footnote-37) 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.[[38]](#footnote-38)

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 الاهتمام إلى بناء قدرات المؤسسات الصغرى والصغيرة والمتوسطة (MSME) التي أصبحت الآن جهات فاعلة رئيسية في الاقتصاد الرقمي المتنامي من خلال تعزيز ثقتها في استخدام تكنولوجيا المعلومات والاتصالات (بما في ذلك النطاق العريض والإنترنت) والحد من التعرض للهجمات.

|  |
| --- |
| 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 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 )** 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.**هـ )** 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.**و )** مواصلة التركيز بشكل خاص على احتياجات الفئات الأكثر ضعفاً – كالنساء والأطفال والأشخاص ذوي الإعاقة والأشخاص ذوي الاحتياجات المحددة وكبار السن – في جهود بناء القدرات.**ز )** مواصلة تطوير وتعزيز البرنامج العالمي للأمن السيبراني بوصفه أداة لبناء القدرات.**ح)** وضع "دليل بشأن تنفيذ 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.**ط)** 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 كما حدث على سبيل المثال من خلال القمة العالمية بشأن الذكاء الاصطناعي من أجل تحقيق الصالح العام التي ينظمها الاتحاد سنوياً.**ي)** 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 هذه الشركات لتكنولوجيا المعلومات والاتصالات.**ك)** 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[[39]](#footnote-39)

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، وبعضها الآخر بدأته جهات معنية أخرى، مثل عملية لندن، واللجنة العالمية المعنية باستقرار الفضاء السيبراني، ومجموعات مثل مجموعة العشرين إلى جانب مختلف المحافل الدولية والإقليمية الأخرى.**

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 القيام بدور ريادي، في إطار ولايته، في التطورات ذات الصلة.**

6.6 **على الرغم من اقتراح عقد "مؤتمر عالمي" في التوصية** 15.1 **من تقرير الفريق لعام** 2008،**[[40]](#footnote-40) 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 لنهج يشمل الحكومة بأسرها مع إنشاء 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، منها على سبيل المثال الحوارات المشتركة رفيعة المستوى بين الولايات المتحدة والصين،[[41]](#footnote-41) والحوار بين روسيا والولايات المتحدة،[[42]](#footnote-42) والحوار بين الهند والمملكة المتحدة بشأن الأمن السيبراني،[[43]](#footnote-43) والحوار بين جمهورية كوريا وأستراليا بشأن السياسات السيبرانية،[[44]](#footnote-44) والحوار بين الاتحاد الأوروبي واليابان[[45]](#footnote-45) وما إلى ذلك.**

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 مع أكثر من 30 بلداً من جميع مجموعات 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 وجامعة ومنظمة دولية وإقليمية مما يبرز الطبيعة المتغيرة بسرعة للمجتمع الرقمي اليوم**.

تحسين التنسيق داخل منظومة الأمم المتحدة

12.6 **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.**

13.6 **ومع ذلك، يتعين على مختلف وكالات الأمم المتحدة أن تعمل وفقاً للمؤشرات التي توفرها عضويتها المعنية، ولا يمكن لمزيد من قنوات الحوار الدولي إلا أن يساعد البلدان في التوصل إلى فهم أكثر شمولاً وأكثر شيوعاً للقضايا المعنية.**

14.6 **ومن 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 **واتُخذت 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[[46]](#footnote-46) 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 إطار ولايته، في التطورات 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 بما في ذلك منظمو مختلف العمليات. 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 أن يضطلع بدوري تيسيري في هذا الصدد – من خلال العمل مع الشركاء لمساعدة الدول الأعضاء وأصحاب المصلحة الآخرين 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 قيادة الجهود المبذولة بالتعاون مع الوكالات الرئيسية الأخرى داخل أسرة الأمم المتحدة، لتنسيق الجهود الداخلية للأمم المتحدة وتبسيط برامجها وأنشطتها المتعلقة بالأمن السيبراني، لكي يكون أكثر فعالية في خدمة المجتمع العالمي. |

# القسم 7 المبادئ التوجيهية 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، والنواتج المطلوبة لتلبيتها، وأن تكون وفقاً للمقاييس 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 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. **و )** واعترافاً بالتحدي الملح الذي يشكله الأمن السيبراني على الصعيدين الوطني والدولي، تُشجع البلدان على مواصلة الارتقاء بمسألة الأمن السيبراني إلى أعلى قنوات وضع السياسات والإدارة داخل حكوماتها. |

# الملحق 1 بعض الأمثلة للتطورات الإقليمية والعالمية منذ عام 2008[[47]](#footnote-47)

**1** صدّقت ووقّعت 65 دولةً على **اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لعام 2001** ولكن لم يعقبها تصديق من جانب 3 دول (مارس (2020.وبدأت المفاوضات بشأن **البروتوكول الإضافي الثاني للاتفاقية بشأن الجريمة السيبرانية** في 2017 بهدف استكمالها في عام 2020.[[48]](#footnote-48) وصدر في 19 مارس 2018بيان عن تعزيز التعاون الدولي بشأن الجريمة السيبرانية والأدلة الإلكترونية: *نحو بروتوكول لاتفاقية بودابست*[[49]](#footnote-49)يفيد بما يلي: *المسائل التي يتعين حلها مقعدة وقد يكون من الصعب التوصل إلى توافق في الآراء بشأن الخيارات المطروحة حالياً. ومع ذلك، ما لم يتم الاتفاق على حلول، قد تكون الحكومات أقل قدرة على الحفاظ على سيادة القانون لحماية الأفراد وحقوقهم في الفضاء السيبراني*.

**2** وضعت **المنظمات الإقليمية** اتفاقيات أو إعلانات أو اتفاقات أو مبادئ توجيهية بعد عام 2008 بشأن الأمن السيبراني والجريمة السيبرانية، وبعضها على النحو التالي:

• اتفاق بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون بشأن التعاون الدولي في مجال ضمان أمن المعلومات (2009)؛

• اتفاقية جامعة الدول العربية بشأن مكافحة جرائم تكنولوجيا المعلومات (2010)؛

• الاتحاد الدولي للاتصالات والمفوضية الأوروبية – دعم وضع سياسات منسقة لسوق تكنولوجيا المعلومات والاتصالات في دول إفريقيا والبحر الكاريبي والمحيط الهادئ (2012)؛

• توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (2013)؛

• اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (2014)؛

• خطة العمل الاستراتيجية لفريق العمل المعني بالاتصالات والمعلومات (TEL) التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) للفترة 2020-2016 (2015)؛

• توجيه الاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات (NIS 2016)؛

• منظمة حلف الشمال الأطلسي – دليل تالين 2.0: القانون الدولي المنطبق على العمليات السيبرانية (2017)؛

• إعلان رابطة أمم جنوب شرق آسيا لمنع الجريمة السيبرانية ومكافحتها (2017)؛

• لائحة الاتحاد الأوروبي العامة لحماية البيانات (2018)؛

• إعلان الكومنولث السيبراني (2018).

**3** وضعت **منظمات مختلفة** إعلانات واتفاقات أو مبادئ توجيهية منها:

**1.3** [**منتدى باريس للسلام لعام 2018**](https://parispeaceforum.org/) الذي يتضمن إعلاناً أطلقه الرئيس إيمانويل ماكرون، فرنسا، في 12 نوفمبر 2018، بعنوان *دعوة باريس بشأن الثقة والأمن في الفضاء السيبراني* وتضمن البيان التالي: *ندرك أن خطر الإجرام السيبراني يتطلب بذل المزيد من الجهود لتحسين أمن المنتجات التي نستخدمها، وتعزيز دفاعاتنا ضد المجرمين وتعزيز التعاون بين جميع أصحاب المصلحة داخل الحدود الوطنية وعبرها، وأن اتفاقية بودابست بشأن الجريمة السيبرانية أداة رئيسية في هذا الصدد*. وكان الهدف من هذا الإعلان رفيع المستوى وضع مبادئ توجيهية مشتركة لتأمين الفضاء السيبراني. وقد وقّع 78 بلداً على *دعوة باريس بشأن الثقة والأمن في الفضاء السيبراني* (أبريل (2020.[[50]](#footnote-50)

**2.3** **إعلان الكومنولث السيبراني**[[51]](#footnote-51)الذي اتفق عليه بالإجماع اجتماع رؤساء حكومات الكومنولث في 2018 في لندن،
20-16 أبريل 2018. وقرر قادة 53 بلداً في الإعلان مكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني الجيد، معترفين بأهمية التعاون الدولي *ومدركين للتهديدات التي يتعرض لها الاستقرار في الفضاء السيبراني وسلامة البنية التحتية الحيوية، ومؤكدين التزامهم المشترك بالامتثال الكامل لمبادئ ومقاصد ميثاق الأمم المتحدة للتخفيف من هذه المخاطر*.

**3.3** [**إعلان جوهانسبرغ لقمة بريكس (BRICS)**](https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration) في 26 يوليو 2018 من جانب البرازيل وروسيا والهند والصين وجنوب إفريقيا.

**4.3** [**إعلان قادة قمة مجموعة العشرين لعام 2018 (بوينس آيرس، الأرجنتين): بناء التوافق في الآراء من أجل التنمية العادلة والمستدامة**](http://www.g20.utoronto.ca/2018/2018-leaders-declaration.html) الذي اعتُمد في 1 ديسمبر 2018 وأكد من جديد أهمية معالجة قضايا الأمن في استخدام تكنولوجيا المعلومات والاتصالات وأيد التدفق الحر للمعلومات والأفكار والمعرفة مع احترام الأطر القانونية المعمول بها، والعمل على بناء ثقة المستهلك والخصوصية وحماية البيانات وحماية حقوق الملكية الفكرية.

**5.3** [**اتفاقية تكنولوجيا الأمن السيبراني لعام 2018**](https://cybertechaccord.org/?utm_source=t.co&utm_medium=referral) التي أطلقت في 17 أبريل 2018 من قبل شركات تكنولوجيا المعلومات العالمية تحت قيادة مايكروسوفت وفيسبوك. واتفاق تكنولوجيا الأمن السيبراني هو *"التزام عام بين أكثر من 30 شركة عالمية بحماية المدنيين وتمكينهم على الخط لتحسين أمن الفضاء السيبراني واستقراره ومرونته"*. ويشمل العدد الحالي للموقعين 143 شركة (أبريل 2020).[[52]](#footnote-52)

**6.3** اعتمد اجتماع رؤساء حكومات الكومنولث الذي عُقد في لندن في الفترة 20-16 أبريل 2018 [**إعلان الكومنولث السيبراني**](http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf). وقرر قادة 53 بلداً في الإعلان مكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني الجيد. ويعترف القادة بأهمية التعاون الدولي في التصدي للجريمة السيبرانية وتعزيز الاستقرار في الفضاء السيبراني، ويلتزمون التزاماً تاماً بمبادئ ومقاصد ميثاق الأمم المتحدة.

**7.3** يرمي [**حوار جنيف حول السلوك المسؤول في الفضاء السيبراني**](https://genevadialogue.ch/) الذي أطلق في ربيع عام 2018 إلى رسم خريطة لأدوار ومسؤوليات الجهات الفاعلة في المساهمة في تحقيق المزيد من الأمن والاستقرار في الفضاء السيبراني في سياق السلام والأمن الدوليين. وسيركز الحوار الذي يجري حالياً في مرحلته الثانية على أدوار ومسؤوليات الجهات الفاعلة في قطاع الأعمال. ويرمي المشروع إلى ما يلي: دعوة الجهات الفاعلة في قطاع الأعمال التجارية العالمية إلى مناقشة السلوك المسؤول في الفضاء السيبراني؛ ومساعدة قطاع الأعمال في تنمية قدراته على فهم السياسات الدولية والعمليات الدبلوماسية ومتابعتها والإسهام فيها بشكل مفيد؛ وتسهيل الحوار بين الشركات العالمية من أجل تشكيل المبادئ وخطة العمل التي تسهم في الجهود العالمية في إطار الأمم المتحدة وأماكن أخرى.

**8.3** أكد الاتحاد الأوروبي ودوله الأعضاء، من خلال [**إعلان الممثل السامي بالنيابة عن الاتحاد الأوروبي – دعوة إلى تعزيز السلوك المسؤول في الفضاء السيبراني وإدارته**](https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/)، التزامه بمواصلة تعزيز السلوك المسؤول في الفضاء السيبراني من خلال تطبيق القانون الدولي وقواعد السلوك المسؤول، وتدابير بناء الثقة الإقليمية ومن خلال إطار الاتحاد الأوروبي للرد الدبلوماسي المشترك على الأنشطة السيبرانية الخبيثة.

4 التطورات في الأمم المتحدة:

**1.4** [**قرار الجمعية العامة للأمم المتحدة المؤرخ 2 نوفمبر 2018 بعنوان**](http://undocs.org/A/C.3/73/L.9/Rev.1): *مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.* صوتت 85 دولة لصالح اعتماد القرار وصوتت 55 دولة ضد اعتماده وامتنعت 29 دولة عن التصويت. ويطلب القرار أن يلتمس الأمين العام آراء الدول الأعضاء بشأن التحديات التي تواجهها في التصدي لاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية ويقدم تقريراً بناءً على تلك الآراء لتنظر فيه الجمعية العامة في دورتها الرابعة والسبعين.

**2.4 الجمعية العامة للأمم المتحدة** تعتمد قرارين:[[53]](#footnote-53)

 أ ) "**الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي"** (الوثيقة A/C.1/73/L.37) (اعتُمد بأغلبية 139 صوتاً مؤيداً مقابل 11 صوتاً معارضاً مع امتناع 18 دولة عن التصويت). وبموجب هذا النص، ستطلب الجمعية العامة إلى الأمين العام، بمساعدة فريق من الخبراء الحكوميين سيتم إنشاؤه في 2019، مواصلة دراسة التدابير التعاونية الممكنة للتصدي للتهديدات القائمة والمحتملة في مجال أمن المعلومات، بما في ذلك، معايير وقواعد ومبادئ السلوك المسؤول للدول.

ب) **"التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي"** (الوثيقة A/C.1/73/L.27.Rev.1) (اعتُمد بأغلبية 109 أصوات مؤيدة مقابل 45 صوتاً معارضاً مع امتناع 16 دولة عن التصويت). وبموجب هذا النص، ستقرر الجمعية العامة عقد اجتماع لفريق عمل مفتوح العضوية في 2019 يعمل على أساس توافق الآراء لمواصلة تطوير قواعد ومعايير ومبادئ السلوك المسؤول للدول.

**3.4 قرار الجمعية العامة للأمم المتحدة الصادر في 27 ديسمبر 2019**: *مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية* (اللجنة الثالثة). قررت الجمعية العامة إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وعند القيام بذلك، ستأخذ الجمعية العامة في الاعتبار الكامل الصكوك والجهود العالمية المبذولة حالياً لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما في ذلك على وجه الخصوص، عمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية. واعتمدت الجمعية العامة القرار بأغلبية 79 صوتاً مؤيداً مقابل 60 صوتاً معارضاً مع امتناع 30 دولة عن التصويت.[[54]](#footnote-54)

5 بعض الأمثلة على بيانات ودعوات رؤساء الدول وكبار الوزراء

**1.5** في أعقاب الهجوم الإرهابي على صحيفة شارلي إيبدو الفرنسية في 7 يناير 2015، وبناء على دعوة من **برنار كازنوف، وزير داخلية الجمهورية الفرنسية**، اجتمع في 11 يناير في باريس **وزراء الداخلية و/أو العدل من لاتفيا، ريهاردز كوزلوفسكيس، الرئيس المؤقت لمجلس وزراء الاتحاد الأوروبي ومن ألمانيا، توماس دي مايزير ومن النمسا، يوهانا ميكل-ليتنر، ومن بلجيكا، يان جامبون ومن الدانمارك، ميتي فريديركسن ومن إسبانيا، وخورخي فرنانديز دياز ومن إيطاليا، أنجلينو ألفانو، ومن هولندا، إيفو أوبستلتن، ومن بولندا، تيريزا بيوتروسكا، ومن المملكة المتحدة، تيريزا ماي ومن السويد، أندرز يجمان**، واعتمدوا البيان التالي بحضور **المفوض الأوروبي للهجرة والشؤون الداخلية ديميتريس أفراموبولوس، والنائب العام للولايات المتحدة إريك هولدر الابن، ونائب وزير الأمن الداخلي في الولايات المتحدة أليخاندرو مايوركاس، وستيفن بلاني، وزير السلامة العامة في كندا، والمنسق الأوروبي لمكافحة الإرهاب جيل دي كريشوف:**[[55]](#footnote-55)

*نشعر بالقلق إزاء الاستخدام المتزايد للإنترنت لتأجيج الكراهية والعنف ونبدي تصميمنا على ضمان عدم إساءة استخدام الإنترنت لهذا الغرض، مع ضمان أن تظل، مع الاحترام الدقيق للحريات الأساسية، مجالاً لحرية التعبير، مع الاحترام الكامل للقانون.*

**2.5** أدلت **رئيسة الوزراء تيريزا ماي، المملكة المتحدة** البيان التالي بشأن الهجوم الإرهابي على جسر لندن الذي أسفر عن مقتل 11 شخصاً وإصابة 48 شخصاً في 3 يونيو 2017:[[56]](#footnote-56)

*يجب أن نعمل مع الحكومات الديمقراطية المتحالفة لإبرام اتفاقات دولية تنظم الفضاء السيبراني لمنع انتشار التطرف والتخطيط للإرهاب. ويجب علينا أن نفعل كل ما في وسعنا في الداخل للحد من خطر التطرف عبر الإنترنت.*

**3.5** [**نداء كرايستشيرش**](https://www.christchurchcall.com/): أدلت **رئيسة الوزراء جاسيندا أردرن، نيوزيلاندا** ببيان بشأن الهجوم الإرهابي على المسجد في كرايستشيرش الذي أسفر عن مقتل 50 شخصاً في 15 مارس 2019:[[57]](#footnote-57)

*"سنبحث أيضاً الدور الذي تقوم به وسائل التواصل الاجتماعي والخطوات التي يمكننا اتخاذها، بما في ذلك على مستوى الساحة الدولية، وبالتعاون مع شركائنا. ولا يمكننا ببساطة أن نبقى مكتوفي الأيدي ونقبل بأن هذه المنصات موجودة فقط وأن ما يتداول فيها ليس مسؤولية المكان الذي تُنشر فيه. فالناشر مسؤول وليس فقط ساعي البريد. ولا يمكن أن تكون هناك حالة توجد فيها فوائد دون مسؤوليات".*

دعا الرئيس إيمانويل ماكرون، فرنسا، ورئيسة الوزراء جاسيندا أردرن مجموعة من القادة رفيعي المستوى من 17 بلداً وشركات تكنولوجيا المعلومات مثل أمازون وفيسبوك وغوغل ومايكروسوفت إلى اجتماع في باريس في 15 مايو 2019.[[58]](#footnote-58) وكان الهدف من هذه القمة الجمع بين البلدان وشركات التكنولوجيا في محاولة لوضع حد للقدرة على استخدام وسائل التواصل الاجتماعي لتنظيم وتعزيز الإرهاب والتطرف. وتعهد قادة العالم وشركات التكنولوجيا *"بالقضاء على المحتوى الإرهابي المتطرف والعنيف على الإنترنت".* ووقّع 17 بلداً في البداية على الاتفاق غير الملزم تلاها 31 بلداً آخر في 23 سبتمبر من العام نفسه. ويشمل التعهد ثلاثة أقسام أو التزامات: واحد للحكومات، وواحد لمقدمي الخدمات الإلكترونية وآخر للطرق التي يمكن أن يعمل بها الاثنان معاً.

**4.5 قمة النفاذ القانوني لعام 2019**

عقدت وزارة العدل الأمريكية قمة النفاذ القانوني في 4 أكتوبر 2019[[59]](#footnote-59) لمسؤولي إنفاذ القانون على مستوى الولايات والمستوى الاتحادي حول موضوع *"الإبقاء على التشفير في حالة صدور أمر قضائي"*. وكان الهدف هو مناقشة ضرورة فتح شركات التكنولوجيا لأنظمة التشفير الخاصة بها للشرطة في حالة التحقيق في الجرائم. وسُلط الضوء على إحدى المشاكل: *هل حولت أنظمة التشفير الإنترنت إلى فضاء بدون إطار قانوني؟*[[60]](#footnote-60)

قدم وزير الشؤون الداخلية الأسترالي بيتر دوتون في القمة قانون مكافحة التجفير الذي تم سنه في أستراليا في ديسمبر 2018. عندما اعتمدت أستراليا قانون تعديل الاتصالات وتشريعات أخرى (المساعدة والنفاذ) لعام 2018.[[61]](#footnote-61) وكان الغرض من ذلك أيضاً ضمان أن تتمكن الوكالات من النفاذ بشكل قانوني إلى محتوى اتصالات واضح، حيث كان من المقدر أنه بحلول عام 2020، سيتم تجفير جميع الاتصالات الإلكترونية ذات القيمة التحقيقية.

وفي 4 أكتوبر 2019، اتفقت حكومتا الولايات المتحدة والمملكة المتحدة أيضاً على اتفاق بشأن قانون الحوسبة السحابية.[[62]](#footnote-62)

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، 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 اعتباراً من الربع الأخير من 2019، 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. مجلس أوروبا، مفاوضات بشأن البروتوكول، متاح في الموقع التالي: <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>. [↑](#footnote-ref-11)
12. على الرغم من أنها ليست اتفاقات دولية، فإن دليل تالين وتالين 2.0 الأكثر شمولاً وثائق مهمة يرعاها مركز التميز المعني بالدفاع الحاسوبي التعاوني التابع للناتو. [↑](#footnote-ref-12)
13. فريق الخبراء الحكوميين، متاح في الموقع التالي: <https://www.un.org/disarmament/group-of-governmental-experts/>. [↑](#footnote-ref-13)
14. فريق عمل مفتوح العضوية، متاح في الموقع التالي: <https://www.un.org/disarmament/open-ended-working-group/>. [↑](#footnote-ref-14)
15. 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/2020/Pages/default.aspx>.

- تقرير مقدم إلى المجلس في دورته لعام 2020 بشأن استخدام الاتحاد للبرنامج العالمي للأمن السيبراني، متاح في الموقع التالي: <https://www.itu.int/md/S20-CL-C-0036/en>. [↑](#footnote-ref-15)
16. القاضي شتاين شولبرغ، 2018 والقاضي شتاين شولبرغ 2019، متاح في الموقع التالي: <https://www.cybercrimelaw.net/Cybercrimelaw.html>. [↑](#footnote-ref-16)
17. براد سميث، الحاجة إلى اتفاقية جنيف الرقمية، 14 فبراير 2017، متاح في الموقع التالي: [*https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/*](https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/). [↑](#footnote-ref-17)
18. شتاين شولبرغ، تاريخ الجريمة السيبرانية، (الطبعة الثالثة، فبراير 2020). [↑](#footnote-ref-18)
19. المرجع نفسه. [↑](#footnote-ref-19)
20. 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-20)
21. .FBI Tech Tuesday بناء الدفاع الرقمي ضد إنترنت الأشياء (IOT)، 12 ديسمبر 2017، متاح في الموقع التالي: <https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday---building-a-digital-defense-against-the-internet-of-things-iot>. [↑](#footnote-ref-21)
22. نظمت حكومة اليابان مؤتمراً بعنوان [Cyber3 Conference](https://yosihiro.com/speech/files/2015-11-07-program.pdf) في أوكيناوا، في 8-7 نوفمبر 2015، ركز أيضاً على عدة أمور منها العوامل البشرية والبعد الأخلاقي لإنترنت الأشياء. [↑](#footnote-ref-22)
23. 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-23)
24. 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-24)
25. المرجع نفسه الوارد في الرقم 16. [↑](#footnote-ref-25)
26. هذا يشمل العمل الذي يضطلع به حالياً فريق الخبراء الحكوميين وفريق العمل مفتوح العضوية. [↑](#footnote-ref-26)
27. يستند هذا المبدأ التوجيهي إلى التوصيات 9.1 و12.1 و14.1 الواردة في تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008. [↑](#footnote-ref-27)
28. 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>. [↑](#footnote-ref-28)
29. 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-29)
30. 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-30)
31. تقرير فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني لعام 2008، الفقرة2، الصفحة 9، نفس المرجع السابق الذي يحيل إلى رقم 6. [↑](#footnote-ref-31)
32. 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-32)
33. المرجع نفسه. [↑](#footnote-ref-33)
34. المرجع نفسه. [↑](#footnote-ref-34)
35. 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-35)
36. غيرناوتي، *Cyberpower, Crime, Conflict and Security in Cyberspace*، قسم EPFL Press، 2013. [↑](#footnote-ref-36)
37. لورانس برادفورد، *Cybersecurity needs women: Here’s why*، متاح في الموقع التالي: <https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8>. [↑](#footnote-ref-37)
38. المرجع نفسه. [↑](#footnote-ref-38)
39. انظر الملحق 1 لمزيد من المعلومات. [↑](#footnote-ref-39)
40. 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-40)
41. يُتاح مزيد من المعلومات في الموقع التالي:

 <https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.> [↑](#footnote-ref-41)
42. بيان حقائق التعاون بين الولايات المتحدة وروسيا بشأن تكنولوجيا المعلومات والاتصالات، متاح في الموقع التالي: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>. [↑](#footnote-ref-42)
43. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.gov.uk/government/news/the-4th-uk-india-cyber-dialogue>. [↑](#footnote-ref-43)
44. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.minister.defence.gov.au/minister/lreynolds/statements/australia-republic-korea-foreign-and-defence-ministers-22-meeting-2019>. [↑](#footnote-ref-44)
45. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.mofa.go.jp/files/000495346.pdf>. [↑](#footnote-ref-45)
46. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.un.org/en/digital-cooperation-panel/>. [↑](#footnote-ref-46)
47. قام القاضي شتين شجولبرغ، الرئيس السابق لفريق الخبراء رفيع المستوى المعني بالأمن السيبراني بتجميع المعلومات في هذا الملحق. والهدف هو تقديم بعض الأمثلة وهي ليست شاملةً في طبيعتها. وتُقدم هنا لأغراض العلم فقط.  [↑](#footnote-ref-47)
48. مجلس أوروبا، مفاوضات البروتوكول، متاح في الموقع التالي: <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>. [↑](#footnote-ref-48)
49. مجلس أوروبا، تعزيز التعاون الدولي بشأن الجريمة السيبرانية والأدلة الإلكترونية: نحو بروتوكول لاتفاقية بودابست، متاح في الموقع التالي: <https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713>. [↑](#footnote-ref-49)
50. يُتاح مزيد من المعلومات في الموقع التالي: <https://pariscall.international/en/>. [↑](#footnote-ref-50)
51. إعلان الكومنولث السيبراني، متاح في الموقع التالي: <http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf>. [↑](#footnote-ref-51)
52. يُتاح مزيد من المعلومات في الموقع التالي: <https://cybertechaccord.org/accord/>. [↑](#footnote-ref-52)
53. توافق اللجنة الأولى التابعة للأمم المتحدة على 27 نصاً، اثنان منها يقترحان إنشاء أفرقة جديدة لوضع قواعد للدول بشأن السلوك المسؤول في الفضاء السيبراني، متاح في الموقع التالي: <https://www.un.org/press/en/2018/gadis3619.doc.htm>. [↑](#footnote-ref-53)
54. **لم يؤيد** [**بيان الاتحاد الأوروبي الصادر في 15 يناير 2020**](https://eeas.europa.eu/delegations/council-europe_en/73052/EU%20Statement%20in%20support%20of%20the%20Council%20of%20Europe%20Convention%20on%20Cybercrime) **قرار الجمعية العامة للأمم المتحدة:** *يلاحظ الاتحاد الأوروبي الحاجة إلى مزيد من الإجراءات المحايدة من الناحية التكنولوجية وتدابير بناء القدرات من أجل مكافحة هذا النوع من الجرائم بفعالية. ومع ذلك، لا يوجد توافق في الآراء بشأن الحاجة إلى معاهدة دولية جديدة يتم التفاوض بشأنها في إطار الأمم المتحدة ولا يمكن أن يكون الحل أداة يمكن أن تخفض معايير حماية حقوق الإنسان والحريات الأساسية، وتزيد من الفجوة الرقمية وتؤيد سيطرة الدولية على الإنترنت. ويؤكد الاتحاد الأوروبي من جديد دعمه للمعايير العالية المنصوص عليها بالفعل في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. ويدعو جميع الدول التي لم تفعل ذلك إلى الانضمام إلى هذه الاتفاقيات في أقرب وقت ممكن.* [↑](#footnote-ref-54)
55. يُتاح مزيد من المعلومات في الموقع التالي: <https://in.ambafrance.org/Charlie-Hebdo-joint-statement-of>. [↑](#footnote-ref-55)
56. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.gov.uk/government/speeches/pm-statement-following-london-terror-attack-4-june-2017>. [↑](#footnote-ref-56)
57. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/prime-minister-jacinda-arderns-house-statement-on-christchurch-mosques-terror-attack/>. [↑](#footnote-ref-57)
58. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.christchurchcall.com/> [↑](#footnote-ref-58)
59. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.justice.gov/olp/lawful-access> [↑](#footnote-ref-59)
60. انظر أيضاً: رسالة مفتوحة من وزير الداخلية – فضلاً عن وزير العدل الأمريكي بار، ووزير الأمن الداخلي (بالنيابة) ماكلينان، ووزير الداخلية الأسترالي دوتون – إلى مارك زوكربيرج، 23 ديسمبر 2019، متاحة في الموقع التالي:

 <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f>. [↑](#footnote-ref-60)
61. يُتاح مزيد من المعلومات في الموقع التالي: https://www.justice.gov/dag/page/file/1153466/download. [↑](#footnote-ref-61)
62. يُتاح مزيد من المعلومات في الموقع التالي: <https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists>. [↑](#footnote-ref-62)