برنامج الأمن السيبراني لقطاع تنمية الاتصالات

الإصدار الخامس من الرقم القياسي العالمي للأمن السيبراني - GCIv5
نموذج مرجعي (المنهجية)

جدول المحتويات

التاريخ والخلفية

إن الرقم القياسي العالمي للأمن السيبراني (GCI) الذي نُشر لأول مرة في عام 2015 يساعد البلدان على تحسين التزامها بالأمن السيبراني. ومن خلال البيانات التي جُمعت، يسلط الرقم القياسي العالمي للأمن السيبراني الضوء على التزامات الدول الأعضاء المتعلقة بتنفيذ ما يناسب بيئتها الوطنية، والترويج للممارسات الرشيدة وتعزيز ثقافة عالمية للأمن السيبراني.

ويحدد نطاق الرقم القياسي GCI وإطار عمله في القرار 130 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين للاتحاد، الذي يتناول تعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات (ICT) وعلى وجه التحديد، تدعى الدول الأعضاء إلى "دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك الرقم القياسي العالمي للأمن السيبراني *(GCI)*، من أجل تشجيع الاستراتيجيات الحكومية وتبادل المعلومات عن الجهود المبذولة عبر الصناعات والقطاعات." والهدف النهائي هو تعزيز قيام ثقافة عالمية في الأمن السيبراني وإدماجها في صميم تكنولوجيات المعلومات والاتصالات.

وستتبع الإصدارات السابقة من الرقم القياسي العالمي للأمن السيبراني توصيات القرار 45 (المراجَع في كيغالي، 2022) لقطاع تنمية الاتصالات الذي يحدد بوضوح العمل المنجز من خلال الرقم القياسي العالمي للأمن السيبراني ويوصي مكتب تنمية الاتصالات "بالنظر في نتائج الرقم القياسي العالمي للأمن السيبراني لتوجيه مبادرات مكتب تنمية الاتصالات في مجال الأمن السيبراني، ولا سيما مراعاة الفجوات المحددة من خلال عملية الرقم القياسي العالمي للأمن السيبراني"

وتشمل الإصدارات السابقة ما يلي:

اسم الإصدار	GCIv1	GCIv2	GCIv3	GCI 2020 (GCIv4)
رقم الإصدار	1	2	3	4
البلدان المشاركة	105 بلدان	136 بلداً	155 بلداً	169 بلداً
سنة جمع البيانات	2014-2013	2016	2018-2017	2020
سنة النشر	2015	2017	2019	2021
ملاحظات	بالشراكة مع مؤسسة ABI للبحوث			

والاستبيان الخاص بالرقم القياسي GCI الذي تشتق منه المؤشرات والمؤشرات الفرعية والمؤشرات دون الفرعية، يحدَّث فيما بين الإصدارات بالتشاور مع لجنة الدراسات بقطاع تنمية الاتصالات المعنية بالمسألة: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني لأعضاء الاتحاد.

ونتيجة لاستمرار اهتمام الدول الأعضاء بالرقم القياسي العالمي للأمن السيبراني (GCI)، يقوم الاتحاد بتجميع إصدار خامس (GCIv5) بالتشاور مع فريق خبراء الرقم القياسي العالمي للأمن السيبراني على النحو الموصى به في القرار 45 (المراجَع في كيغالي، 2022).

مجال التطبيق

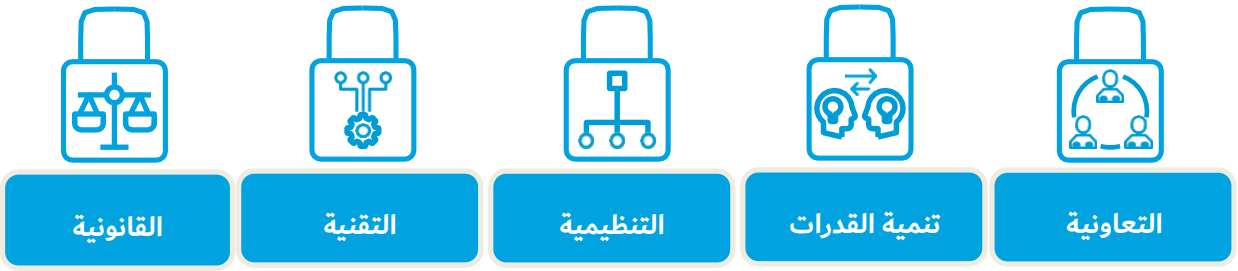
الرقم القياسي العالمي للأمن السيبراني (GCI) هو رقم قياسي مركب يجمع مجموعة متنوعة من مؤشرات الأمن السيبراني في مقاييس، استناداً إلى الدعائم الخمس للبرنامج العالمي للأمن السيبراني (GCA). وهذه الدعائم تشكل الدعائم الخمس للرقم القياسي العالمي للأمن السيبراني. وتتمثل الأهداف الرئيسية للرقم القياسي العالمي للأمن السيبراني (GCI) في قياس ما يلي:

- أنواع ومستويات وتطور الالتزامات الوطنية المتعلقة بالأمن السيبراني بمرور الزمن؛
- التقدم المحرز في الالتزام بالأمن السيبراني من منظور عالمي؛
- التقدم المحرز في الالتزام بالأمن السيبراني من منظور إقليمي؛
- فجوة الالتزام بالأمن السيبراني: الفرق بين البلدان من حيث مستوى التزامها في مبادرات الأمن السيبراني.

ويهدف الرقم القياسي العالمي للأمن السيبراني إلى مساعدة البلدان في تحديد مجالات التحسين في مضمار الأمن السيبراني، مما يساعد على رفع المستوى الإجمالي للأمن السيبراني على الصعيد العالمي. ويجمع الرقم القياسي أيضاً الممارسات الرشيدة التي يمكن للبلدان أن تتعلم منها بغية تحسين ممارساتها في مجال الأمن السيبراني واعتماد نهج أكثر اتساقاً.

الإطار المفاهيمي

يركز الرقم القياسي العالمي للأمن السيبراني على اتباع خمس دعائم باعتبارها مجالات شاملة لالتزامات البلدان بشأن الأمن السيبراني:



التدابير القانونية: وهي الأدوات التشريعية، مثل القوانين واللوائح والسياسات، وتعرِّف الحقوق، والمسؤوليات، والحماية المقدمة بشأن القضايا الرئيسية المتعلقة بالأمن السيبراني، مثل مسألة حظر سلوك جنائي محدد أو فرض الحد الأدنى من المتطلبات التنظيمية.

التدابير التقنية: بدون وجود تدابير وقدرات تقنية مناسبة لكشف الحوادث والتعاطي معها، تظل الدول الأعضاء والكيانات التابعة لها عرضة للمخاطر السيبرانية التي يمكن أن تقوض فوائد التكنولوجيات الرقمية. ومن ثم يتعين على الدول الأعضاء أن تمتلك القدرة على وضع استراتيجيات وتحديد معايير مقبولة للحد الأدنى من الأمن وبرامج اعتماد للتطبيقات والأنظمة البرمجية. ويمكن قياس التدابير التقنية بناءً على مدى وجود المؤسسات والأطر التقنية التي تتعامل مع الأمن السيبراني والتي تقرها أو تستحدثها الدول الأعضاء.

التدابير التنظيمية: التدابير التنظيمية والإجرائية ضرورية من أجل التنفيذ السليم للمبادرات الوطنية. فيجب على الدولة العضو تحديد هدف استراتيجي واسع، مع خطة شاملة من أجل التنفيذ والمتابعة والقياس. ويتعين إنشاء هياكل على غرار الوكالات الوطنية من أجل تنفيذ استراتيجيات الأمن السيبراني وتقييم نجاح أو فشل الخطة. ويمكن قياس الهياكل التنظيمية بناءً على وجود وعدد المؤسسات والاستراتيجيات التي تنظم تطوير الأمن السيبراني على الصعيد الوطني.

تدابير تنمية القدرات: تنمية القدرات عنصر ملازم للتدابير القانونية والتقنية والتنظيمية. ويمكن لفهم التكنولوجيا والمخاطر والتداعيات في مجال الأمن السيبراني أن يساعد على وضع الأفضل من التشريعات والسياسات والاستراتيجيات والتنظيم للأدوار والمسؤوليات المختلفة. وتشمل تنمية القدرات تطوير المعارف والمهارات بين السكان الأساسيين والمهنيين الذين يتطرق عملهم إلى الأمن السيبراني فضلاً عن المتخصصين ضمن القطاع.

التدابير التعاونية: تتكلل جهود الأمن السيبراني بمزيد من النجاح عندما تعتمد على جميع القطاعات والتخصصات المتأثرة ويتعين الاضطلاع بها باتباع نهج شمولي متعدد أصحاب المصلحة. ويعزز التعاون الحوار والتنسيق ويمكن من إيجاد مجال أكثر شمولية لتطبيق الأمن السيبراني. ويمكن أن يشمل التعاون أنشطة من قبيل المبادرات المشتركة وتبادل المعلومات والدورات التدريبية وغيرها من الأنشطة التي تربط بين المهنيين والمسؤولين وسائر الجهات الفاعلة التي تسعى إلى تحسين الأمن السيبراني.

منهجية حسابية

ينقسم الإصدار الخامس لاستبيان الرقم القياسي العالمي للأمن السيبراني (GCI) إلى خمس دعائم هي: التدابير القانونية والتقنية والتنظيمية وتدابير تنمية القدرات والتدابير التعاونية، وهي تشمل ما مجموعه 20 مؤشراً، مع 64 مؤشراً فرعياً و28 مؤشراً دون فرعي، استناداً إلى 83 سؤالاً. وتهدف الأسئلة إلى تحقيق التوازن بين الجزئيات ذات المغزى في التزامات الأمن السيبراني، مع الحفاظ على منظور إجمالي. ويمكن الاطلاع على المؤشرات في استبيان الرقم القياسي العالمي للأمن السيبراني (الملحق A).

وتُختار المؤشرات على أساس:

- صلتها بدعائم البرنامج العالمي للأمن السيبراني؛
- صلتها بمجال تطبيق الرقم القياسي العالمي للأمن السيبراني وإطاره المفاهيمي؛
- قدرة الدول الأعضاء على الإجابة على الأسئلة بدقة؛
- إمكانية التحقق المقابل عبر البيانات الثانوية.

ويستخدم هذا الإصدار إجابات ثلاثية (نعم أو جزئياً أو لا) لإزالة التقييم القائم على رأي وأي تحيز محتمل إزاء أنواع معينة من الردود. وعلاوة على ذلك، يسمح المفهوم الثلاثي البسيط بإجراء تقييم أسرع وأكثر تعقيداً لأنه لا يتطلب إجابات مطولة، مما يؤدي إلى تسريع وتبسيط تقديم الإجابات والمزيد من التقييم. ولا ينبغي للمجيب إلا أن يؤكد وجود أو عدم وجود حلول محددة سلفاً بشأن الأمن السيبراني.

وضماناً للدقة، سيُطلب من البلدان دعم ردها من خلال ميزة تحميل الوثائق وعناوين المواقع الإلكترونية الداعمة. وسيضاف قسم للتعليق إلى كل دعامة للسماح للبلدان بعرض الممارسات الرشيدة التي تروي قصة الآثار الناجمة عن تطورها في مجال الأمن السيبراني.

وبالنسبة لهذا الإصدار الخامس وجميع الإصدارات المستقبلية، ستُعاد هيكلة الرقم القياسي العالمي للأمن السيبراني ضمن مستويات الالتزام وفقاً للقرار 45 الصادر عن المؤتمر العالمي لتنمية الاتصالات، بكيغالي، رواندا، في يونيو 2022، حيث أوصت الدول الأعضاء بأن يعتمد الرقم القياسي العالمي للأمن السيبراني نهجاً من مستويات لفرز البلدان بدلاً من تصنيف مرتباتها لتزويد البلدان بتقييم أكثر دلالة لمجالات القوة والتحسين. وبالتالي، ستُكلَّف اجتماعات فريق خبراء المنهجية بتحديد إطار مناسب للمسويات.

المسار الإجمالي لعملية الرقم القياسي العالمي للأمن السيبراني (GCI)

1 يُراجَع استبيان الرقم القياسي العالمي للأمن السيبراني بأخذ التعليقات الواردة من الدول الأعضاء ومن فريق الخبراء المعني بالرقم القياسي بعين الاعتبار. ويقدَّم الاستبيان إلى اجتماع لجنة الدراسات 2 لمواصلة النقاش بشأنه.

2 وفقاً للقرار 45 لقطاع تنمية الاتصالات (المراجَع في كيغالي، 2022)، سيستدعي الرقم القياسي العالمي للأمن السيبراني مواصلة التماس المشورة من "فريق خبراء الرقم القياسي العالمي للأمن السيبراني" بشأن القضايا المتصلة بالمنهجيات والهيكل والأسئلة وأوزان الترجيح.

3 شُكل فريق عمل بالمراسلة تابع لفريق خبراء الرقم القياسي العالمي للأمن السيبراني (GCI) وهو يتألف من خبراء وممثلين عن الدول الأعضاء الراغبة في تقديم توصيات وتعليقات بشأن الاستبيان.

4 تجري أمانة مكتب تنمية الاتصالات المراجعات المناسبة استناداً إلى المشاورات مع فريق العمل بالمراسلة قبل أن توافق إدارة مكتب تنمية الاتصالات على الاستبيان، أو تقدمه جزئياً أو كلياً، للحصول على مزيد من التعليقات من فريق العمل بالمراسلة.

5 يُرسَل الاستبيان المعتمد كي يترجَم إلى جميع اللغات الرسمية الست (6) للأمم المتحدة.

6 عُقد اجتماعان آخران لفريق خبراء الرقم القياسي العالمي للأمن السيبراني (GCI) للتشاور بشأن المستويات وتوزيع أوزان الترجيح.

7 يدعو مدير مكتب تنمية الاتصالات، من خلال رسالة، جميع الدول الأعضاء في الاتحاد ودولة فلسطين، إلى المشاركة في استقصاء الرقم القياسي العالمي للأمن السيبراني (GCI). وترسل إليها رسائل لإبلاغها بالرقم القياسي العالمي للأمن السيبراني وتلتمس منها تعيين مسؤول اتصال يتولى جمع كل بيانات البلد ذي الصلة وملء استبيان الرقم القياسي العالمي للأمن السيبراني.

8 يُدعى مسؤولو الاتصال المعيّنون رسمياً إلى الرد على الاستبيان عبر بوابة إلكترونية.

9 تقوم أمانة مكتب تنمية الاتصالات بجمع البيانات الثانوية للبلدان التي ترد على الاستبيان، ويشمل ذلك:

- تحديد أي نقص في الردود والوثائق الداعمة والروابط وما إلى ذلك.
- قيام مسؤول الاتصال بتحسين دقة الردود عند الضرورة.
- إرسال مشروع الاستبيان المصحَح إلى كل مسؤول اتصال للموافقة النهائية عليه.
- استخدام الاستبيان المصدَّق لأغراض التحليل والتقييم والتصنيف.

10 تقوم أمانة مكتب تنمية الاتصالات بجمع البيانات الأولية للبلدان التي لا ترد على الاستبيان، ويشمل ذلك:

- قيام الاتحاد بصياغة الرد الأولي على الاستبيان باستعمال البيانات المتاحة للعموم والبحث عبر الإنترنت.
- إرسال مشروع الاستبيان إلى مسؤولي الاتصال لاستعراضه.
- قيام مسؤولي الاتصال بتحسين الدقة وإعادة مشروع الاستبيان.
- إرسال مشروع الاستبيان المصحَح إلى كل مسؤول اتصال للموافقة النهائية عليه.
- استخدام الاستبيان المصدَّق عليه لأغراض التحليل والتقييم والتصنيف.

11 يصدر تقرير يتضمن ملخصات للاتجاهات الرئيسية وأفضل الممارسات مع مراعاة التوصيات بشأن المستويات وأوزان الترجيح التي يضعها فريق خبراء الرقم القياسي العالمي للأمن السيبراني.

ملاحظة: في حال عدم قيام بلد ما بالإفادة بمسؤول اتصال بشأن الاستبيان المتعلق بالرقم القياسي العالمي للأمن السيبراني، سيبادر الاتحاد إلى الاتصال مع مسؤول الاتصال المؤسسي من الدليل العالمي لدى الاتحاد.

الملحق A: تعريف الدعائم والمؤشرات

التدابير القانونية

التشريع من التدابير الحاسمة لتوفير إطار منسق للكيانات لتهيئة نفسها لقاعدة تشريعية وتنظيمية مشتركة، سواء فيما يتعلق بمسألة حظر سلوك جنائي محدد أو فرض الحد الأدنى من المتطلبات التنظيمية.

ويمكن قياس البيئة القانونية انطلاقاً من وجود المؤسسات القانونية والأطر الفعّالة التي تتعامل مع الأمن السيبراني والجريمة السيبرانية. وتشمل مؤشرات الأداء التالية:

1.1 قانون الجريمة السيبرانية

يشير مصطلح القانون الموضوعي إلى جميع فئات القوانين العامة والخاصة، بما في ذلك قوانين العقود والعقارات والضرر والوصية والقانون الجنائي التي تؤسس الحقوق والسلوكيات وتحددها وتنظمها.

2.1 لوائح للأمن السيبراني

اللائحة هي قاعدة أو مبدأ يحكم السلوك أو الممارسة؛ من قبيل توجيه تصدره سلطة ما وتديمه.[1] وهي تستند إلى قواعد وتهدف إلى تنفيذ جزء محدد من تشريع. ولوائح للأمن السيبراني تضع قوانين تتعامل مع حماية البيانات والتبليغ عن الانتهاكات ومتطلبات منح الشهادات/التقييس في مجال الأمن السيبراني وتنفيذ تدابير الأمن السيبراني ومتطلبات مراجعة الأمن السيبراني وحماية الخصوصية وحماية الأطفال على الإنترنت والتوقيعات الرقمية والمعاملات الإلكترونية ومسؤولية مقدمي خدمات الإنترنت.

التدابير التقنية

بدون وجود تدابير وقدرات تقنية مناسبة للكشف عن الحوادث والتصدي لها، تظل الدول الأعضاء والكيانات التابعة لها عرضة للمخاطر السيبرانية التي يمكن أن تحد من الفوائد الناتجة عن اعتماد معلومات التكنولوجيات الرقمية. ومن ثم يتعين على الدول الأعضاء أن تمتلك القدرة على وضع استراتيجيات وتحديد معايير مقبولة للحد الأدنى من الأمن وبرامج اعتماد للتطبيقات البرمجية والأنظمة. ويمكن قياس التدابير التقنية بناءً على مدى وجود المؤسسات والأطر التقنية التي تتعامل مع الأمن السيبراني والتي تقرها الدول الأعضاء أو تستحدثها. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

1.1 أفرقة التصدي للحوادث الحاسوبية الوطنية/الحكومية

إن الأفرقة الوطنية للتصدي للحوادث الحاسوبية (CIRT)/أفرقة التصدي للحوادث الحاسوبية (CSIRT)/ أفرقة التصدي لحالات الطوارئ الحاسوبية (CERT) هي كيانات تنظيمية ملموسة، تكلف بمسؤولية تنسيق ودعم التصدي للأحداث أو الحوادث الأمنية الحاسوبية على الصعيد الوطني. وهي تتحمل المسؤولية الوطنية عن تقديم القدرات اللازمة لتحديد التهديدات السيبرانية والدفاع ضدها والتصدي لها وإدارتها وتعزيز أمن الفضاء السيبراني في الدولة. ويتعين أن تُقترن هذه القدرة بجمع معلومات استخباراتها ذاتياً بدلاً من الاعتماد على الإبلاغ الثانوي عن الحوادث الأمنية سواء من الجهات التي تخدمها أفرقة التصدي للحوادث الحاسوبية أو من مصادر أخرى.

2.1 الأفرقة CERT/CIRT/CSRIT القطاعية

الفريق CIRT/CSIRT/CERT القطاعي هو كيان يتعامل مع حوادث الأمن الحاسوبي أو الأمن السيبراني التي تؤثر على قطاع بعينه. وتشكل الأفرقة CERT القطاعية عادةً من أجل القطاعات الحساسة مثل الرعاية الصحية والمرافق العامة وخدمات الطوارئ والطاقة والهيئات الأكاديمية والقطاع المالي.

---

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation

3.1 الإطار الوطني لتنفيذ معايير الأمن السيبراني

من المهم للغاية اعتماد إطار وطني (أطر وطنية) من أجل تنفيذ معايير الأمن السيبراني المعترف بها دولياً داخل القطاع العام (الوكالات الحكومية) وداخل البنى التحتية الحرجة (حتى ولو كان القطاع الخاص هو من يقوم بتشغيلها). وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تطوير معايير المعلومات المنظمة (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، وIAB، وجمعية الإنترنت (ISOC)، وISG، وISI، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وISF، وRFC، وISA، واللجنة الكهرتقنية الدولية (IEC)، وNERC، وNIST، وFIPS، وPCI، وDSS، وغيرها.

التدابير التنظيمية

التدابير التنظيمية والإجرائية ضرورية من أجل التنفيذ السليم لأي نوع من المبادرات الوطنية. فيتعين على الدولة العضو تحديد هدف استراتيجي واسع، مع خطة شاملة من أجل التنفيذ والمتابعة والقياس. ويتعين إنشاء هياكل على غرار الوكالات الوطنية من أجل تنفيذ الاستراتيجية وتقييم نجاح أو فشل الخطة. ويمكن قياس الهياكل التنظيمية بناءً على وجود وعدد المؤسسات والاستراتيجيات التي تنظم تطوير الأمن السيبراني على الصعيد الوطني. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

1.1 الاستراتيجية/السياسة الوطنية للأمن السيبراني

يمثل وضع سياسات للنهوض بالأمن السيبراني أولوية من الأولويات الوطنية العليا. وينبغي للاستراتيجية الوطنية للأمن السيبراني أن تنص على الحفاظ على وجود البنى التحتية الحيوية الوطنية للمعلومات تتسم بالقدرة على الصمود والاعتمادية، بما في ذلك أمن وسلامة المواطنين؛ وحماية مواد وأصول الملكية الفكرية الخاصة بالمواطنين والمنظمات والدولة العضو؛ والتصدي للهجمات السيبرانية على البنى التحتية الحيوية ومنعها؛ والتقليل بأقصى ما يمكن الأضرار ومن الوقت اللازم للتعافي من الهجمات السيبرانية.

2.1 الوكالة المسؤولة

الوكالة المسؤولة عن تنفيذ الاستراتيجية/السياسية الوطنية للأمن السيبراني يمكن أن تضم لجاناً دائمة أو أفرقة عمل رسمية أو مجالس استشارية أو مراكز متعددة الاختصاصات. وقد تكون هذه الهيئة مسؤولة وحدها عن الفريق الوطني للتصدي للحوادث الحاسوبية.

3.1 مقاييس الأمن السيبراني

وجود أي ممارسات تقييم وطنية أو قطاعية معترف بها رسمياً أو مرجعية تُستعمل في قياس تطور الأمن السيبراني واستراتيجيات تقييم المخاطر وعمليات التدقيق الأمني السيبراني وغيرها من الأدوات والأنشطة الخاصة بقياس أو تقييم الأداء الناتج من أجل إجراء تحسينات في المستقبل. وذلك، على سبيل المثال، طبقاً للمعيار ISO/IEC 27004 المعني بالقياسات المتعلقة بإدارة أمن المعلومات.

4.1 استراتيجيات ومبادرات حماية الأطفال على الإنترنت (COP)

ينبغي أن تتضمن الاستراتيجية الوطنية لحماية الأطفال على الإنترنت خطة عمل لتعزيز البيئات الآمنة للأطفال على الإنترنت في جميع أنحاء العالم. وسيكون من الضروري وضع مجموعة من السياسات ترسي مجموعة من القواعد والأهداف توضح أن أي جريمة وكل جريمة ترتكب ضد أي طفل في العالم الواقعي يمكن، مع مراعاة ما يقتضيه اختلاف الحال، أن ترتكب على الإنترنت أو أي شبكة إلكترونية أخرى.

تدابير تنمية القدرات

تمثل القدرات عنصراً ملازماً للتدابير الثلاثة السابقة (القانونية والتقنية والتنظيمية). ومن شأن فهم التكنولوجيا والمخاطر والتداعيات أن يساعد على وضع الأفضل من التشريعات والسياسات والاستراتيجيات وتحقيق تنظيم أفضل فيما يتعلق بالأدوار والمسؤوليات المختلفة. ويتم تناول مجال الدراسة هذا في معظم الأحوال من منظور تكنولوجي؛ وإنما تنطبق في هذا المجال تداعيات اقتصادية واجتماعية وسياسية عديدة.

وينبغي لأي إطار لتنمية القدرات من أجل النهوض بالأمن السيبراني أن يشمل أنشطة إذكاء الوعي وتوفير الموارد. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

1.1 حملات التوعية العامة بالأمن السيبراني

تشمل التوعية العامة الجهود المبذولة في سبيل تشجيع وصول حملات التوعية إلى أكبر عدد ممكن من المواطنين والاستفادة من المنظمات غير الحكومية والمؤسسات والمنظمات وموردي خدمات الإنترنت والمكتبات ومنظمات التجارة المحلية والمراكز المجتمعية وكليات المجتمعات المحلية وبرامج تعليم الكبار والمدارس ومنظمات أولياء الأمور-المعلمين من أجل توصيل الرسالة إلى الجميع بشأن السلوك الآمن من الناحية السيبرانية على الإنترنت.

2.1 تدريب المهنيين العاملين في مجال الأمن السيبراني

وجود برامج تدريب مهني خاصة بالقطاعات لزيادة الوعي لدى الجمهور العام (أي تخصيص يوم أو أسبوع أو شهر وطني للتوعية بالأمن السيبراني) وتشجيع تثقيف القوة العاملة من مختلف التخصصات (التقنية والعلوم الاجتماعية وغيرها) بالأمن السيبراني وتشجيع منح الشهادات للمهنيين في أي من القطاعين العام أو الخاص.

ويشمل هذا المؤشر أيضاً وجود إطار معتمد (مؤيد) أو أطر معتمدة (مؤيدة) من الحكومة لمنح الشهادات واعتماد المهنيين من خلال معايير معترف بها دولياً للأمن السيبراني. وتشمل هذه الشهادات وأوراق الاعتماد والمعايير على سبيل الذكر وليس الحصر: معارف أمن الحوسبة السحابية (تحالف أمن الحوسبة السحابية) وCISSP وSSCP وCBK وCSSLP والتحليل الجنائي في مجال الأمن السيبراني (ISC^2) وغيرها.

3.1 البرامج التعليمية المتعلقة بالأمن السيبراني كجزء من المناهج الأكاديمية الوطنية

وضع وتشجيع مناهج وبرامج تعليم وطنية لتدريب جيل الشباب على المهارات والمهن المتعلقة بالأمن السيبراني في المدارس والكليات والجامعات ومؤسسات التعلم الأخرى. وتشمل المهن المتعلقة بالأمن السيبراني، على سبيل الذكر وليس الحصر، محللي الشفرات وخبراء الأدلة الجنائية الرقمية والمستجيبين لحالات الحوادث والمعماريين الأمنيين ومختبري الاختراق.

4.1 برامج البحث والتطوير (R&D) في مجال الأمن السيبراني

يقيس هذا المؤشر الاستثمار في برامج البحث والتطوير الوطنية في مجال الأمن السيبراني في المؤسسات التي قد تكون تابعة للقطاع العام أو القطاع الخاص أو أكاديمية أو غير حكومية أو دولية. ويتناول أيضاً وجود هيئة مؤسسية معترف بها على الصعيد الوطني للإشراف على البرامج.

5.1 الصناعة الوطنية للأمن السيبراني

من شأن وجود بيئة اقتصادية وسياسية واجتماعية مؤاتية تدعم تطوير الأمن السيبراني أن يحفز نمو الشركات المعنية بالأمن السيبراني في القطاع الخاص. ووجود حملات للتوعية العامة وتطوير للقوة العاملة وتنمية للقدرات وحوافز حكومية من شأنه أن يدفع بظهور سوق لمنتجات وخدمات الأمن السيبراني. ووجود صناعة داخلية للأمن السيبراني يعد شاهداً على هذه البيئة المؤاتية ويدفع بنمو المشاريع المبتدئة في مجال الأمن السيبراني وأسواق التأمين السيبراني المرتبطة بها.

6.1 آليات تحفيز حكومية

يبحث هذا المؤشر أي جهود تحفيزية تبذلها الحكومة لتشجيع تنمية القدرات في مجال الأمن السيبراني، سواء من خلال الإعفاءات الضريبية وتقديم المنح والتمويل والقروض وتدبير المرافق وغيرها من الحوافز الاقتصادية والمالية، بما في ذلك تخصيص هيئة مؤسسية معترف بها وطنياً للإشراف على أنشطة بناء القدرات في مجال الأمن السيبراني.

التدابير التعاونية

يتطلب الأمن السيبراني مدخلات من جميع القطاعات والتخصصات، ولهذا السبب تلزم معالجته من خلال نهج متعدد أصحاب المصلحة. ويعزز التعاون الحوار والتنسيق ويمكن من إيجاد مجال أكثر شمولية لتطبيق الأمن السيبراني. ويصعب تبادل المعلومات بالشكل الأفضل بين التخصصات المختلفة وداخل شركات التشغيل في القطاع الخاص. ويتضح ذلك بشكل أكبر على الصعيد الدولي. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

1.1 الاتفاقات الثنائية بشأن الأمن السيبراني

تشير الاتفاقات الثنائية (اتفاقات بين طرفين) إلى أي شراكات وطنية أو قطاعية معترف بها رسمياً لتبادل معلومات الأمن السيبراني أو أصوله عبر الحدود بين الحكومة وحكومة أجنبية أخرى أو كيان إقليمي (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيا والموارد الأخرى).

2.1 اتفاقات متعددة الأطراف بشأن الأمن السيبراني

تشير الاتفاقات متعددة الأطراف (اتفاقات بين طرف وأطراف متعددة) إلى أي برامج وطنية أو قطاعية معترف بها رسمياً من أجل تبادل معلومات أو أصول الأمن السيبراني عبر الحدود بين الحكومة وحكومات أجنبية أو منظمات دولية متعددة (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيا والموارد الأخرى).

3.1 اتفاقات المساعدة القانونية المتبادلة بشأن الأمن السيبراني

يجوز أن تشمل أيضاً التصديق على اتفاقات دولية تتضمن بنوداً تتعلق بالمساعدة القانونية المتبادلة والأمن السيبراني.

4.1 الشراكات بين القطاعين العام والخاص

يشير مصطلح الشراكات بين القطاعين العام والخاص (PPP) إلى مشاريع مشتركة بين القطاعين العام والخاص. ويمكن أن تتخذ شكل عقد طويل الأجل بين طرف خاص وكيان حكومي، لتقديم أصول أو خدمة عمومية، يتحمل فيها الطرف الخاص مسؤولية كبيرة عن المخاطر والإدارة، ويكون فيها الأجر مرتبطاً بالأداء.[2] ويُستعمل مؤشر الأداء هذا لقياس عدد الشراكات الوطنية أو القطاعية المعترف بها رسمياً بين القطاعين العام والخاص لتبادل معلومات الأمن السيبراني وأصوله (الأشخاص والعمليات والأدوات) بين القطاعين العام والخاص (أي الشراكات الرسمية للتعاون أو تبادل المعلومات و/أو الخبرات و/أو التكنولوجيا و/أو الموارد)، وطنياً أو دولياً.

5.1 الشراكات بين الوكالات

يشير مؤشر الأداء هذا إلى أي شراكات رسمية بين الوكالات الحكومية المختلفة داخل الدولة العضو (ولا يشير إلى الشراكات الدولية). ويمكن أن يشير إلى الشراكات بشأن تبادل المعلومات أو الأصول بين الوزارات والدوائر والبرامج ومؤسسات القطاع العام الأخرى.

[2] https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships