مكتب تنمية الاتصالات (BDT)

المرجع: الرسالة المعممة BDT/DNS/CYB/054 جنيف، 27 أغسطس 2020

- الدول الأعضاء
- أعضاء قطاع تنمية الاتصالات
- الهيئات الأكاديمية
- جهات الاتصال التابعة للاتحاد المعنية بالأمن السيبراني العالمي

الموضوع: دعوة للانضمام إلى التكرار الرابع لفريق الخبراء المعني بالرقم القياسي العالمي للأمن السيبراني (GCI)

حضرات السادة والسيدات،

تحية طيبة وبعد،

يدعوكم الاتحاد الدولي للاتصالات (ITU) إلى ترشيح خبير للمشاركة في التكرار الرابع لفريق الخبراء المعني بتحديد أوزان عناصر الرقم القياسي العالمي للأمن السيبراني (GCI).

وبالنسبة إلى عملية التكرار الرابعة هذه للرقم القياسي GCI، سيتبع الاتحاد نهجاً متعدد أصحاب المصلحة يستند إلى الاستفادة من مجموعة واسعة من الخبرات المتعلقة بالأمن السيبراني بهدف تحسين جودة الرقم القياسي العالمي للأمن السيبراني، وتعزيز التعاون الدولي وتشجيع تبادل المعارف.

وسيطلب من الخبراء تقديم مدخلات بشأن دعامة (دعائم) الرقم GCI الأكثر صلة بمجال خبراتهم وتحديد أوزان لأسئلة التكرار الرابع للرقم طبقاً لأهمية الأسئلة بالنسبة إلى مبادئ الأمن السيبراني. ودعائم الرقم GCI هي التدابير القانونية والتقنية والتنظيمية والتدابير المتعلقة بتطوير القدرات والتعاون الدولي. ويمكن الاطلاع على مزيد من المعلومات في الاختصاصات المرفقة، وعلى الموقع الإلكتروني للرقم القياسي GCI.

في حال قبولكم لهذه الدعوة وترشيح خبير، ينبغي لهذا الخبير المشاركة في الاجتماع الافتراضي لفريق الخبراء المعني بتحديد أوزان عناصر الرقم القياسي العالمي للأمن السيبراني يوم **15 أكتوبر 2020**، حيث سيكون الخبراء، من خلال المناقشات والتوجيهات، على استعداد لتقديم مدخلاتهم المتعلقة بتحديد الأوزان على جدول بيانات بنسق excel سيكون متاحاً بحلول **31 أكتوبر 2020**. وسيتم دمج مدخلات جميع أعضاء فريق الخبراء في جدول بيانات لتحديد الأوزان، سيستخدم في تقييم ردود البلدان على استبيان الرقم القياسي GCI.

يرجى العلم أنه سترسل نسخة من هذه الرسالة إلى جهة الاتصال المعنية بالرقم القياسي GCI في بلدكم. وسنكون ممتنين للغاية لو وصلنا رد منكم أو من جهة الاتصال الخاصة ببلدكم في موعد أقصاه **30 سبتمبر 2020** على العنوان gci@itu.int. ويمكن إرسال أي استفسارات بشأن الرقم القياسي GCI أيضاً إلى نفس عنوان البريد الإلكتروني.

أود أن أشكر الدول الأعضاء وأعضاء قطاع تنمية الاتصالات وأفرقة الخبراء السابقة التي شاركت في منهجية التكرارات السابقة لفريق الرقم القياسي العالمي للأمن السيبراني.

اتطلع إلى مواصلة التعاون بيننا.

وتفضلوا بقبول فائق التقدير والاحترام.

[الأصل عليه توقيع]

دورين بوغدان-مارتن
المديرة

الملحق 1 - الاختصاصات

برنامج الأمن السيبراني لمكتب تنمية الاتصالات/الاتحاد الدولي للاتصالات

فريق الخبراء المعني بتحديد أوزان عناصر الرقم القياسي العالمي للأمن السيبراني

الاختصاصات

أغسطس 2020

الرقم القياسي العالمي للأمن السيبراني (GCI)

يساعد الرقم القياسي العالمي للأمن السيبراني (GCI) الذي صدر للمرة الأولى في 2015 البلدان في تحديد مجالات التحسين في ميدان الأمن السيبراني، وتحفيزها من أجل اتخاذ إجراءات لتحسين ترتيبها، وهو ما يؤدي بدوره إلى زيادة المستوى العام للأمن السيبراني في العالم أجمع. ومن خلال ما يتم تجميعه من بيانات، يسلط الرقم القياسي GCI الضوء على الممارسات التي يمكن للدول الأعضاء اتباعها والتي تناسب بيئتها الوطنية، مع تشجيع الممارسات الجيدة وبناء 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). والاستبيان الخاص بالرقم القياسي GCI الذي تشتق منه المؤشرات والمؤشرات الفرعية والمؤشرات دون الفرعية، يتم إعداده والموافقة عليه من خلال عملية تشاورية في إطار المسألة 3 التابعة للجنة الدراسات 2: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني لأعضاء الاتحاد.

فريق الخبراء المعني بتحديد أوزان عناصر الرقم القياسي العالمي للأمن السيبراني

الهدف من إنشاء فريق الخبراء هذا تحديد أوزان المؤشرات والمؤشرات الفرعية والمؤشرات دون الفرعية للرقم القياسي GCI واقتراح تغييرات لإدخالها على استبيان الرقم القياسي GCI من أجل التكرارات المستقبلية.

وقد تم تعيين أعضاء هذا الفريق لتقديم توصيات وافية وغير منحازة من أجل توزيع النقاط داخل نموذج الرقم القياسي GCI. وينبغي لتوصيات فريق الخبراء بشأن أوزان المؤشرات والمؤشرات الفرعية أن تعكس أهمية كل مؤشر بالنسبة إلى التزام الأمن السيبراني العام لأي دولة من الدول الأعضاء. وتشمل الأنشطة المحددة لفريق الخبراء ما يلي:

- تقديم مدخلات لحساب المؤشرات الرئيسية والمؤشرات الفرعية، الموضحة في الملحق B بهذه الوثيقة؛
- تقديم مدخلات من أجل التكرارات المستقبلية المحتملة للرقم القياسي GCI.

ويمكن لفريق الخبراء في حالات استثنائية وبموافقة الأغلبية أن يوصي بمراجعة أسئلة من أجل التكرار التالي للرقم القياسي GCI.

وسيعمل الاتحاد كأمانة لفريق الخبراء. وباب المشاركة في فريق الخبراء مفتوح للدول الأعضاء في الاتحاد وأعضاء القطاع، إضافةً إلى الخبراء الذين شاركوا في التكرارات السابقة للرقم القياسي GCI.

وينبغي أن يعكس تشكيل فريق الخبراء التنوع الإقليمي والجنساني وتنوع الخبرات فضلاً عن التوازن بين أصحاب المصلحة المختلفين، بما في ذلك الحكومات والقطاع الخاص والهيئات الأكاديمية.

عملية تحديد الأوزان

تتبع عملية التقييم الشامل الخطوات التالية:

1 يزود الاتحاد كل عضو من أعضاء فريق الخبراء بجميع المواد ذات الصلة، وتحديداً:

أ) جدول بيانات تحديد الأوزان مع أسئلة الرقم القياسي GCI

ب) الاختصاصات، فيما يتعلق بكيفية التوجيه وشرح للمؤشرات (هذه الوثيقة)

2 سيعقد اجتماع لفريق الخبراء المعني بالرقم GCI يوم **15 أكتوبر 2020** لمناقشة العملية والإجابة على الأسئلة.

3 بعد الاجتماع الأولي، سيقوم كل عضو من أعضاء فريق الخبراء بشكل مستقل بملء جدول البيانات Excel الخاص بتحديد الأوزان مع التوصية الخاصة بتحديد وزن كل مؤشر ومؤشر فرعي ومؤشر دون فرعي، وإرساله إلى العنوان gci@itu.int في موعد أقصاه **31 أكتوبر 2020.**

4 بعد إرسال أعضاء فريق الخبراء جميع التوصيات، سيتم حساب متوسط لتوصيات تحديد الأوزان وتجميعها في جدول بيانات واحد لتحديد الأوزان.

5 يتم عرض متوسط توصيات تحديد الأوزان على أعضاء فريق الخبراء.

الملحق A: كيفية توزيع الأوزان

ينبغي أن تراجع فقط أوزان الدعائم التي أعلنت عن تمتعك بخبرات فيها. ولن ينظر في أي أوزان توزعها لدعائم لم تعلن عن تمتعك بخبرات بشأنها.

يقوم الرقم القياسي GCI على نموذج تراتبي متداخل. وسيشار إلى كل "فرع" من النموذج فيما بعد باسم "مجموعة"، مثل مجموعة المؤشرات ومجموعة المؤشرات الفرعية ومجموعة المؤشرات دون الفرعية.

ويمكنك أن توزع داخل كل مجموعة 10 نقاط. وينبغي أن توزع المزيد من النقاط للمؤشرات/المؤشرات الفرعية/المؤشرات دون الفرعية ذات الأهمية الأكبر، بناءً على خبراتك.

مثال	النقاط الموزعة
المؤشر الفرعي A	4
المؤشر دون الفرعي X	8
المؤشر دون الفرعي Y	2
المؤشر الفرعي B	3
المؤشر الفرعي C	3

مجموع النقاط لهذه المجموعة من المؤشرات دون الفرعية 10

مجموع النقاط لهذه المجموعة من المؤشرات الفرعية 10

كيف تستخدم جدول بيانات تحديد الأوزان

تتعلق هذه التعليمات بجدول البيانات *GCI-Questionnaire-weightage-calculation.xlsx*.

وقد صمم هذا الملف كي يستخدم بالنسق Microsoft Excel. وقد لا تعمل بعض الوظائف مع برامج أخرى.

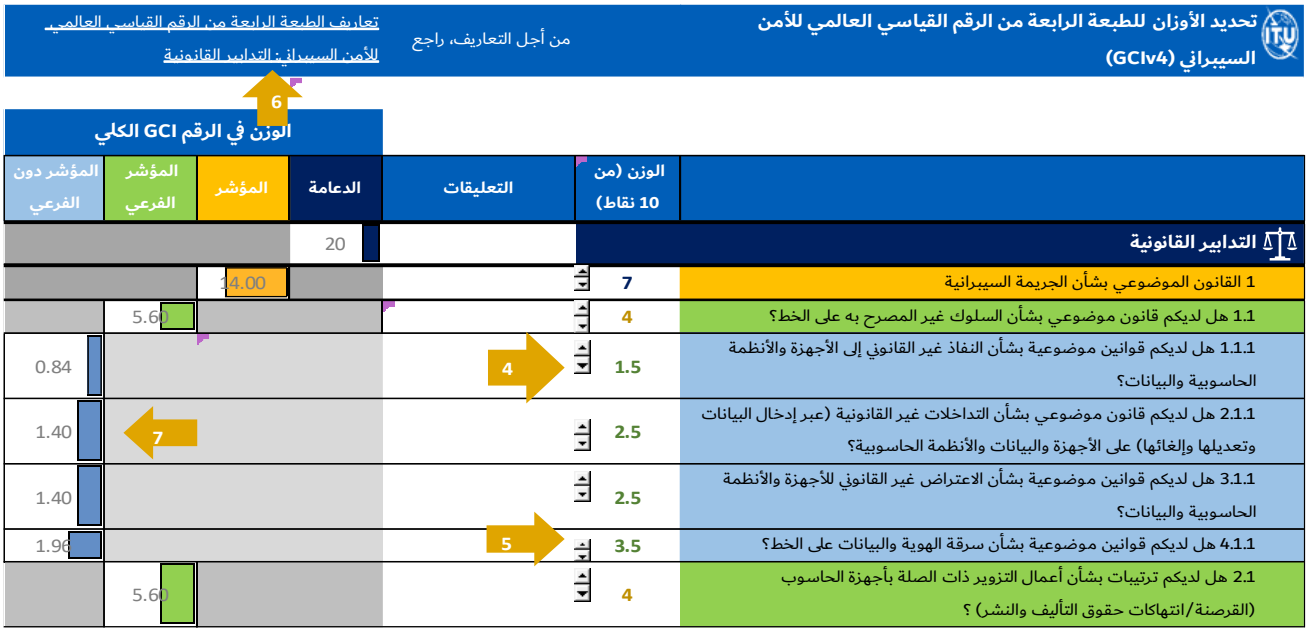
معلومات أولية

1 أدخل اسمك.

2 أختر الدعائم التي ستقوم بتحديد الأوزان بشأنها. ينبغي أن يتطابق ذلك مع ما أعلنت عنه من مجالات خبرة.

3 يمكنك النقر على اسم كل دعامة أو أيقونتها للدخول إلى الدعامة التي تود أن تقدم مدخلات بشأنها.

إدخال الأوزان



4 غير وزن أي مؤشر أو مؤشر فرعي أو مؤشر دون فرعي إما بكتابة الرقم في الخلية أو باستخدام زري التمرير لزيادة الأرقام أو إنقاصها.

أ) لديك 10 نقاط لتوزيعها على أي مجموعة. إذا زاد أو نقص عدد النقاط الموزعة عن 10 نقاط، ستتحول جميع الخلايا في المجموعة إلى اللون الأحمر، كما هو مبين أدناه:

ب) ستغير أسهم التمرير لأعلى ولأسفل الرقم بأرقام صحيحة كاملة.

ج) ولإدخال الكسور، أبدأ الرقم بالرمز =. مثلاً 1/3= من أجل الكسر ⅓.

د) إذا كنت لا تريد توزيع النقاط العشر بالكامل أو ترغب في توزيع عدد أكبر من النقاط، يرجى إبداء ملاحظة في التعليقات. وستخضع أوزانك لإعادة التوازن من 10 عندما يتم حساب المتوسط الحسابي لردود الخبراء.

5 يمكنك إبداء أي تعليقات على تحديد الوزن للمؤشر أو المؤشر الفرعي أو المؤشر دون الفرعي في عمود التعليقات.

6 يمكنك النقر على رابط *تعاريف التكرار الرابع للرقم القياسي GCI* لزيادة فهم المقصود من أي مؤشر.

7 ويبين *الوزن في قسم الرقم GCI الإجمالي* كم سيساوي هذا المؤشر، استناداً إلى درجة تقييمك، في الرقم القياسي GCI النهائي. لا يمكنك تعديل أو تغيير هذه الخلايا.

إنهاء العملية

1 عند الانتهاء، أنقر "Save As" (للاطلاع على المعلومات المتعلقة بكيفية تنفيذ هذه الوظيفة، طالع تعليمات Microsoft Support instructions)، مع وضع اسمك في نهاية الملف.

مثال: *GCI-Questionnaire-weightage-calculations-**NAME**.xlsx*

2 أرفق جدول البيانات الخاص بك برسالة بريد إلكتروني إلى العنوان gci@itu.int في غضون التاريخ المحدد.

الملحق B: 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:

- **القانون الموضوعي بشأن 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.

- **لوائح للأمن السيبراني**

اللوائح عبارة عن قواعد يستند إليها أو يقصد بها تنفيذ جزء محدد من التشريعات.

التدابير التقنية

بدون وجود تدابير وقدرات تقنية مناسبة للكشف عن الحوادث والتعاطي معها، 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 التي تصدق عليها الدول الأعضاء أو تطورها. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

- **أفرقة الاستجابة للحوادث الوطنية/الحكومية**

أفرقة الاستجابة للحوادث الحاسوبية، المعروفة بالأفرقة CIRT/CSIRT/CERT هي كيانات تنظيمية ملموسة، تكلف بمسؤولية تنسيق ودعم الاستجابة للأحداث أو الحوادث الأمنية الحاسوبية على الصعيد الوطني.

- **الأفرقة CERT/CIRT/CSRIT القطاعية**

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

- **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 تقدم معايير المعلومات المهيكلة (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وفريق التداخل بين الرموز (ISI)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وقوات الأمن الداخلي (ISF)، وRFC، والمعايير الدولية لمراجعة الحسابات (ISA)، واللجنة الكهرتقنية الدولية (IEC)، والمجلس الوطني للبحوث البيئية (NERC)، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، ومعايير معالجة المعلومات الفيدرالية (FIPS)، ومعلومات التحكم بالبروتوكول (PCI)، وخدمة أمن الدفاع (DSS)، وغيرها.

- **حماية الأطفال على الخط (COP)**

يقيس هذا المؤشر مدى وجود وكالة وطنية مكرسة لحماية الأطفال على الخط ومدى تيسر رقم هاتف ساخن للإبلاغ عن القضايا المرتبطة بوجود الأطفال على الخط، وأي آليات وقدرات تقنية أخرى يتم نشرها للمساعدة في حماية الأطفال على الخط.

التدابير التنظيمية

التدابير التنظيمية والإجرائية ضرورية من أجل التنفيذ السليم لأي نوع من المبادرات 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 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:

- **الاستراتيجية/السياسة الوطنية للأمن السيبراني**

وضع سياسات للنهوض بالأمن السيبراني كأولوية من الأولويات الوطنية الملحة. وينبغي للاستراتيجية الوطنية للأمن السيبراني أن تنص على الحفاظ على وجود بنى تحتية حرجة وطنية للمعلومات تتسم بالقدرة على الصمود والاعتمادية، بما في ذلك أمن وسلامة المواطنين؛ وحماية مواد وأصول الملكية الفكرية الخاصة بالمواطنين والمنظمات والدولة العضو؛ والتعاطي مع الهجمات السيبرانية على البنى التحتية الحرجة ومنعها؛ وتدنية الأضرار والتقليل للحد الأدنى لزمن الاستعادة من الهجمات السيبرانية.

- **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 يتولى كيان كهذا أيضاً المسؤولية المباشرة للفريق CIRT الوطني.

- **مقاييس الأمن السيبراني**

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

تدابير تطوير القدرات

بناء القدرات عنصر ملازم للتدابير الثلاثة السابقة (القانونية والتقنية والتنظيمية). ومن شأن فهم التكنولوجيا والمخاطر والتداعيات أن يساعد على وضع الأفضل من التشريعات والسياسات والاستراتيجيات والتنظيم للأدوار والمسؤوليات المختلفة. ويتم تناول مجال الدراسة هذا في معظم الأحوال من منظور تكنولوجي؛ كما تنطبق على هذا المجال تداعيات اقتصادية-اجتماعية وسياسية عديدة.

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

- **حملات التوعية العامة بالأمن السيبراني**

تشمل التوعية العامة الجهود التي تبذل 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 الخط.

- **تدريب مهنيي 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 قوة العمل 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 CSSLP والتحليل الجنائي في مجال الأمن السيبراني (ISC)² وغيرها.

- **برامج تعليمية أو مناهج أكاديمية وطنية**

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.

- **برامج البحث والتطوير 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.

- **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 لقوة العمل وبناء 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.

- **آليات تحفيز**

يبحث هذا المؤشر أي جهود تحفيزية تبذلها الحكومة لتشجيع بناء 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

يحتاج الأمن السيبراني إلى مدخلات من جميع القطاعات والتخصصات، ولهذا السبب يجب 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 مشغلي القطاع الخاص. بيد أنه يتزايد على الصعيد الدولي. وتتألف المجموعة الفرعية من مؤشرات الأداء التالية:

- **الاتفاقات الثنائية**

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).

- **المشاركة في الآليات الدولية (المنتديات)**

قد تشمل أيضاً التصديق على اتفاقات دولية بخصوص الأمن السيبراني، مثل اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية واتفاقية بودابست بشأن الجريمة السيبرانية وغيرها.

- **اتفاقات متعددة الأطراف**

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).

- **الشراكات بين القطاعين العام والخاص**

يشير مصطلح الشراكات بين القطاعين العام والخاص (PPP) إلى مشاريع مشتركة بين القطاعين العام والخاص. ويمكن قياس مؤشر الأداء هذا من خلال 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.

- **شراكات بين الوكالات**

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