نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني (GOAT)

المنتدى العالمي
للخبرات السيبرانية

المؤلفون

أعد هذه الوثيقة المنتدى العالمي للخبرات السيبرانية (GFCE)، على يد فريق العمل A – وهو فريق المهام المعني بالاستراتيجية والتقييمات، كمشروع في إطار خطة عمله لعام 2020. والأعضاء في فريق المشروع هم:

- Carolin Weisser Harris، من المركز العالمي لقدرات الأمن السيبراني (GCSCC)
- Ian Wallace، رئيس فريق العمل المعني بالاستراتيجية والسياسات التابع للمنتدى العالمي للخبرات السيبرانية (GFCE)
- James Boorman، مركز أوقيانوسيا للأمن السيبراني (OCSC)
- Orhan Osmani ومروان بن راشد، الاتحاد الدولي للاتصالات (ITU)
- Melissa Hathaway وFrancesca Spidalieri، معهد Potomac لدراسات السياسات العامة (PIPS)
- Radu Serrano، أكاديمية الحوكمة الإلكترونية (eGA)
- Kerry-Ann Barrett، منظمة الدول الأمريكية (OAS).

ويود فريق المشروع أن يعرب عن تقديره لمعهد السياسات الاستراتيجية الأسترالية (API)، ووكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) وشركة MITRE والبنك الدولي لتعليقاتهم ومساهماتهم، وكذلك للسيدة Kathleen Bei من أمانة المنتدى العالمي للخبرات السيبرانية (GFCE) لما تفضلت به من تصاميم ودعم لوجستي وتنظيمي. والشكر موجه أيضاً للاتحاد الدولي للاتصالات لقيامه باستعراض هذه الوثيقة وتنقيحها وترجمتها إلى اللغات العربية والفرنسية والروسية والإسبانية."

جدول المحتويات

مقدمة

يبذل المجتمع العالمي جهوداً متزايدة لفهم أوضاع الأمن السيبراني في البلدان من أجل تشخيص الفجوات واتخاذ قرارات أكثر استنارة بشأن التدخلات والاستثمارات اللازمة لتعزيز القدرات السيبرانية. وقد وضعت مؤسسات البحوث والمنظمات الإقليمية والشركات أطراً ونماذج وأرقاماً قياسية وطبقتها في جميع أنحاء العالم، مشيدةً قاعدة معرفية تبين أين تقف البلدان من حيث النضوج السيبراني ومدى استعدادها في مواجهة تزايد التهديدات السيبرانية على الحكومات ودوائر الصناعة ومصالح الأعمال والمواطنين.

وأبرزت الملاحظات التقييمية الإيجابية الواردة من الجلسة بشأن تقييم القدرات السيبرانية التي نُظمت في الاجتماع الخامس للمنتدى العالمي للخبرات السيبرانية في أبريل 2020 الحاجة إلى إذكاء الوعي بأدوات تقييم القدرات السيبرانية القائمة وتقديم تفاصيل بشأن منهجياتها ومخرجاتها وتأثيرها من أجل مساعدة مجتمع المنتدى (أي المستفيدين والممولين والمنفذين) في تحديد الأدوات والنهج المناسبة الموجهة نحو الاحتياجات والثغرات القائمة في المعارف.

وعليه، تهدف هذه الوثيقة إلى المساعدة في عملية صنع القرار من خلال تقديم لمحة عامة شاملة عن مختلف الأدوات ونهجها وفوائدها ومخرجاتها، وماذا ينبغي عمله والجهة التي يتعين الاتصال بها إذا رغب بلد ما في أن يُختبر بتقييم.

ويعمل فريق مهام الاستراتيجية والتقييم لدى المنتدى العالمي للخبرات السيبرانية على تقييم القدرات السيبرانية للبلدان. وعلى هذا الأساس، أُدرجت الأدوات التالية:

- مكافحة الجريمة السيبرانية: أداة بناء القدرات، البنك الدولي
- النضج السيبراني في منطقة آسيا والمحيط الهادئ، المعهد الأسترالي للسياسات الاستراتيجية (ASPI)
- الرقم القياسي 2.0 للاستعداد السيبراني (CRI) ومعهد Potomac لدراسات السياسات (PIPS)
- نموذج نضج قدرات الأمن السيبراني للأمم المتحدة (CMM)، المركز العالمي لقدرات الأمن السيبراني (GCSCC)
- إطار وضع الاستراتيجيات السيبرانية وتنفيذها (CSDI)، شركة MITRE
- الرقم القياسي العالمي للأمن السيبراني (GCI)، الاتحاد الدولي للاتصالات (ITU)
- إطار تقييم القدرات الوطنية (NCAF)، وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA)
- الرقم القياسي الوطني للأمن السيبراني (NCSI)، أكاديمية الحوكمة الإلكترونية (eGA)

وستضاف أدوات أخرى تفي بالمعيار أعلاه إلى الوثيقة عند تحديدها.

ولأغراض هذه الوثيقة، أرسل استبيان إلى المنظمات المسؤولة عن كل أداة، للحصول على معلومات بشأن ما يلي:

- معلومات عن جهة (جهات) التنفيذ والاتصال
- المَحاور والمواضيع
- المؤشرات
- المنهجية وجمع البيانات ومراقبة الجودة
- المخرجات والعرض
- التأثير والفوائد
- الدور في تنسيق أنشطة بناء القدرات السيبرانية وعملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية.

مكافحة الجريمة السيبرانية: أداة تقييم بناء القدرات

البنك الدولي

أنشئت *أداة تقييم بناء القدرات* ("أداة التقييم") التي وضعها البنك الدولي لمكافحة الجريمة السيبرانية تحت رعاية مشروع مكافحة الجريمة السيبرانية لدعم البلدان النامية في تحديد المجالات ذات الأولوية لتسهيل توزيع مواردها الشحيحة في مجال بناء القدرات.

وتختلف أداة التقييم عن أطر التقييم الأخرى من حيث كونها أداة للتشخيص الذاتي تشمل تسعة أبعاد هي: (1) الإطار غير ذي الصلة بالقانون؛ (2) الإطار القانوني؛ (3) القانون الأساسي؛ (4) القانون الإجرائي؛ (5) الأدلة الإلكترونية؛ (6) الولاية القضائية؛ (7) التدابير الاحترازية؛ (8) التعاون الدولي؛ (9) بناء القدرات.

ويمكن استخدام أداة التقييم سواء بالنسبة لنشاط قائم بذاته ينفذه البلد لأغراضه الخاصة وكذلك كأداة ضرورية لإيلاء العناية الواجبة تمكّن أفرقة المهام التشغيلية من تقييم مدى استعداد البلد لمكافحة الجريمة السيبرانية.

نظرة عامة

تاريخ آخر تحديث للأداة	استُكمل آخر تحديث للمنشور في عام 2017. ونحن الآن بصدد تحديث أداة التقييم الحالية المقرر إنجازه بحلول يوليو 2021.
ما اسم أداة التقييم؟	مكافحة الجريمة السيبرانية: أداة تقييم بناء القدرات
ما اسم المنظمة التي تحتفظ بالأداة؟	البنك الدولي
من هم منفذو التقييمات؟	هذه الأداة متاحة كمنفعة عامة عالمية. ويمكن لأي شخص التوجه إلى الموقع (انظر أدناه) وتحميل الأداة واستخدامها. وهي مصمَمة لإجراء تقييم ذاتي.
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	https://www.combattingcybercrime.org/
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	السيد David Satola، كبير مستشاري نيابة الرئاسة القانونية، البنك الدولي
التغطية الجغرافية	عالمية
من الذي يستطيع استخدام الأداة؟	• واضعو السياسات • المشرّعون • سلطات إنفاذ القانون • المجتمع المدني في البلدان النامية • أي أفراد مهتمين
ما هي المَحاور أو المواضيع المشمولة؟	من ناحية المفاهيم، ينظَّم التقييم حول الأبعاد التسعة التالية: • **الإطار غير ذي الصلة بالقانون**، يشمل الاستراتيجيات والسياسات الوطنية والمسائل الأخرى ذات الطابع غير ذي الصلة بالقانون مثل التعاون مع القطاع الخاص؛ • **الإطار القانوني**، الذي يغطي القانون الوطني وما إذا كان البلد قد انضم إلى معاهدة أم لا؛ • **القانون الأساسي**، الذي يعالج الأنشطة الخاضعة للتجريم؛ • **القانون الإجرائي**، الذي يعالج المسائل الاستقصائية أساساً؛ • **الأدلة الإلكترونية**، التي تركز على مقبولية الأدلة الرقمية ومعالجتها في سياق الجريمة السيبرانية؛ • **الولاية القضائية**، التي تركز على كيفية تحديد الولاية القضائية المعنية بالجريمة؛

	• **التدابير الاحترازية**، التي تركز على ثلاثة عناصر هي "المحاكمة وفق الأصول المرعية" وحماية البيانات وحرية التعبير؛ • **التعاون الدولي**، الذي يركز أولاً على تسليم المطلوبين وثانياً على المستوى الرسمي وغير الرسمي للمساعدة القانونية المتبادلة؛ • **بناء القدرات**، الذي ينظر إلى بناء القدرات المؤسسية (مثل: أكاديميات التدريب على إنفاذ القانون) وبناء القدرات البشرية التي تركز على احتياجات التدريب لإنفاذ القانون والمقاضاة والشؤون القضائية.
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☐ تدابير وأعراف بناء الثقة ☐ الدبلوماسية السيبرانية ☒ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☐ التقاط الحوادث وتحليلاتها ☐ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☐ معايير الإنترنت المفتوحة ☐ إنترنت الأشياء
نوع المؤشرات	المؤشرات الكمية والنوعية على السواء
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	تتألف أداة التقييم من **115** مؤشراً مجمعة في تسعة أبعاد: الإطار غير ذي الصلة بالقانون، والإطار القانوني، والقانون الأساسي، والقانون الإجرائي، والأدلة الإلكترونية؛ والولاية القضائية، والتدابير الاحترازية؛ والتعاون الدولي، وبناء القدرات. وتتقسم الأبعاد التسعة في جدول التقييم إلى أربعة مستويات. ويشير **المستوى 1** إلى كل مجال موضوع (البُعد). ويحدد **المستوى 2** إطاراً عاماً لكل سؤال يُسأل عنه في **المستوى 3** وتمكن مواصلة تحسينه في **المستوى 4**. ويتضمن العمود الأخير (المؤشر) رداً "بنعم/لا" أو خياراً واحداً من بين إجابات مختلفة.
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	**خاص بحالة معينة**: يُجري فريق مكافحة الجريمة السيبرانية تقييماً أولياً للبلد العميل بناءً على بحوث مكتبية، ثم يُطلع السلطات الحكومية المسؤولة في البلد العميل على النتائج ويتحقق من التقييمات ويقر صحتها.
أسلوب جمع البيانات الأولي	• المعلومات المتيسرة لعامة الناس • الوثائق غير المنشورة • الاستبيانات والاستطلاعات • عمليات الرصد • الوثائق والسجلات • المقابلات الشخصية

هل لديكم جمع بيانات ثانوية؟	نعم. وبعد إجراء بحوث مكتبية أولية، يقوم الفريق بزيارة للبلد العميل وبالتشاور مع السلطات الحكومية المسؤولة للتحقق من التقييم الأولي وإقرار صحته. • عمليات الرصد • الوثائق والسجلات
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	أعضاء فريق مكافحة الجريمة السيبرانية، الذي يقوده مستشار رئيسي في مجال تكنولوجيا المعلومات والاتصالات في البنك الدولي، وتتوفر له عادةً خلفية/خبرة في مجال الجريمة السيبرانية ومعالجة مختلف مسائل تكنولوجيا المعلومات والاتصالات في البنك الدولي. وعلاوةً على ذلك، تقوم الهيئات الحكومية في بلدان العملاء بالتحقق من التقييم الأولي الذي يجريه أعضاء الفريق وإقرار صحته لضمان دقة البيانات المجمعة.
ما هي المخرجات الرئيسية للتقييم؟	ينشأ "تقرير تقييم بناء القدرات البشرية في مكافحة الجريمة السيبرانية" عن كل بلد عميل في كل عملية تكرارية.
نسق عرض مخرجات التقييم	• تقرير تقييم بناء القدرات في مكافحة الجريمة السيبرانية (PDF) • أداة العرض المرئي (المخططات البيانية عبر برمجية Excel)
هل يمكن نشر مخرجات التقييم؟	نعم. غير أن بلد العميل هو الذي يقرر نشر نتائج التقييم
كيف يمكن النفاذ إلى التقارير السابقة؟	يترك النفاذ إلى التقارير السابقة لتقدير البلد العميل
ما الدليل على التأثير؟	أجرى الفريق تقييمات لبناء قدرات البلدان العميلة في منطقتي إفريقيا وآسيا والمحيط الهادئ، بما في ذلك ناميبيا وإثيوبيا وكينيا وولايات ميكرونيزيا الموحدة وميانمار. وبالإضافة إلى ذلك، تلقى الفريق طلبات تقييم جديدة من 22 بلداً (بنن وبوروندي وجمهورية الكونغو الديمقراطية وغامبيا وليبيريا ومالي والنيجر ونيجيريا وجمهورية الكونغو وسيراليون وتنزانيا وأوغندا وزامبيا وبوركينا فاصو وكابو فيردي وجزر القمر والمغرب والكاميرون وموريتانيا ورواندا والسنغال). وعلاوةً على ذلك، اعتمد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، وهو واحد من المنظمات الشريكة لنا، أداة التقييم باعتبارها منهجية تقييم حصرية لتقييم التأهب للتعامل مع الجريمة السيبرانية. وأخيراً، عرض الفريق أداة التقييم في الأحداث التالية: الاجتماع السنوي للمنتدى العالمي للخبرات السيبرانية (GFCE) في سنغافورة (2018) واجتماعات أفرقة العمل في لاهاي (2018 و2019)؛ والاجتماع السنوي لمجلس أوروبا (CoE) في ستراسبورغ (2019)؛ والمؤتمرين السنويين للرابطة الدولية لأعضاء النيابة العامة (IAP) في جنوب إفريقيا (2018) والأرجنتين (2019)؛ والاجتماع المشترك لمراكز التميز والاتحاد الإفريقي (AU) بشأن بناء القدرات من أجل مكافحة الجريمة السيبرانية في إفريقيا (2018)؛ والندوة بشأن القانون الدولي في هونغ كونغ، الصين (2019).
ما هي فوائد إجراء تقييم ما؟	تتيح أداة التقييم إجراء تقييم فعّال وقابل للتطبيق عالمياً لاستعداد الدولة للتعامل مع الجريمة السيبرانية من خلال ضمان الموضوعية والوفرة وإمكانية النفاذ. والجمع بين هذه السمات الثلاث لأداة التقييم يضع صانعي السياسات والقانون وأصحاب القرار في وضع يمكنهم من تحديد أفضل طريقة لتوزيع الموارد. • **الموضوعية** تتحقق بجعل الرد على كل سؤال في أداة التقييم رداً إثنينياً أي "نعم/لا" إلى أقصى حد ممكن أو رداً ينحصر في خيار واضح ضمن نطاق ضيق من الخيارات • و**الوفرة** تتحقق "بترجيح" كل معيار. إذ تستخدم أداة التقييم نحو 115 مؤشراً مجمعة في تسعة مواضيع محورية (أو أبعاد). • و**سهولة الفهم** تتحقق من خلال تمثيل بياني للتقديرات في مخطط "عنكبوتي" واحد. ويساعد الرسم البياني البلد العميل على تحديد ما إذا كانت ممارسته الحالية تتماشى مع الممارسات الدولية السليمة. ويمكن أيضاً التعمق في كل بُعد من أبعاد المخطط العام إلى مستوى أكثر تفصيلاً يظهر الأداء في كل معيار من المعايير الفرعية المختلفة.
هل لديكم عملية حساب للترجيحات؟	نعم. ولكن لا يُفصَح للمستعملين عن عملية محددة لحساب الترجيح لمنع التلاعب بأداة التقييم.

هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	كلا. لا يوجد إسناد درجات أو مراتب للنتائج.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• هل توجد استراتيجيات وسياسات وطنية قائمة للأمن السيبراني؟ **(الإطار غير ذي الصلة بالقانون)** • هل توجد أي تشريعات محلية بشأن الجريمة السيبرانية؟ هل انضم البلد إلى معاهدات بشأن الجريمة السيبرانية؟ **(الإطار القانوني)** • هل يجرِّم البلد الجرائم التقليدية التي تُرتكب عن طريق الأنشطة المتصلة بالحاسوب أو الجرائم السيبرانية الناشئة حديثاً؟ **(القانون الأساسي)** • هل توجد قوانين إجرائية تنظم التحقيق في الجرائم السيبرانية ومقاضاتها؟ **(القانون الإجرائي)** • هل ينفذ البلد قواعد خاصة بقبول ومعالجة الأدلة الإلكترونية؟ **(الأدلة الإلكترونية)** • كيف يحدد البلد الولاية القضائية للجريمة السيبرانية؟ **(الولاية القضائية)** • هل يضمن البلد "المحاكمة وفق الأصول المرعية" (حماية البيانات وحرية التعبير) لمواطنيه؟ **(التدابير الاحترازية)** • هل ينفذ البلد إجراءات تسليم المطلوبين أو مبادئ المساعدة القانونية المتبادلة (MLA) الرسمية/غير الرسمية على الصعيد الدولي؟ **(التعاون الدولي)** • هل توجد مؤسسات أو برامج لبناء القدرات في مجال مكافحة الجريمة السيبرانية لمسؤولي إنفاذ القانون والمدعيين العامين والقضاة؟ **(بناء القدرات)**
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	• التمهيد • تقدير وتحليل • وضع الاستراتيجية • التنفيذ • المراقبة والتقييم ويتيح الاستعمال الأول لأداة التقييم خط الأساس، بينما ييسر التحديث الدوري للنتائج باستخدام الأداة مراقبة التقدم الحاصل.
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	تعمل أداة التقييم على تحديد المجالات ذات الأولوية في البلد ضمن الأبعاد التسعة مما يسهل بدوره التركيز والاستهداف في توزيع الموارد النادرة لبناء القدرات من أجل وضع استراتيجية وطنية لبناء قدرات البلد في مجال مكافحة الجريمة السيبرانية. ومن ثم، يمكن استخدام أداة التقييم سواء في نشاط قائم بذاته ينفذه البلد أو كأداة ضرورية لإيلاء العناية الواجبة تمكِّن أفرقة المهام التشغيلية من تقييم وتقدير التأهب للتعامل مع الجريمة السيبرانية في بلد ما.
ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية (GFCE)؟	ستساهم أداة التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية بتقديم خط أساس صلب وموضوعي يمكن من خلاله تخطيط وتنفيذ أنشطته في مجال بناء القدرات السيبرانية.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	كما ذُكر أعلاه، ثبتت فوائد أداة التقييم من خلال الأداء الناجح لتقييمات بناء القدرات في مجال الجريمة السيبرانية في عدد من البلدان العميلة، والإقرار بنجاعتها من منظمة شريكة لنا هي مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) الذي يستخدم أداة التقييم الآن كمنهجية تقييم حصرية لتقييم التأهب للتعامل مع الجريمة السيبرانية.
ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	• قيَّمت المنظمات الشريكة لنا أداة التقييم وأقرت صحتها، ومن بينها مراكز التميز (CoE) والاتحاد الدولي للاتصالات (ITU) ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) ومؤتمر الأمم المتحدة للتجارة والتنمية (الأونكتاد)، ومكتب النيابة العامة العليا بجمهورية كوريا (KSPO)، والمركز العالمي لقدرات الأمن السيبراني (GCSCC) (جامعة أكسفورد). • وساهم فريق مستقل من الخبراء في تحديد ترجيحات كل مؤشر في أداة التقييم.

النضج السيبراني في منطقة آسيا والمحيط الهادئ

المعهد الأسترالي للسياسات الاستراتيجية (ASPI)

يتناول تقرير سنوي صادر عن المعهد الأسترالي للسياسات الاستراتيجية (ASPI) *النضج السيبراني في منطقة آسيا والمحيط الهادئ*، وهو يتفحص اتجاهات النضج السيبراني عبر آسيا والمحيط الهادئ. ويستقصي شريحة جغرافية واقتصادية واسعة للمنطقة تشمل 25 بلداً من جنوب وشمال وجنوب شرق آسيا وجنوب المحيط الهادئ وأمريكا الشمالية.

وتقيِّم منهجية "مقياس النضج السيبراني" أوجه القدرات السيبرانية المختلفة لدى الدول. وقد صُقل هذا النموذج من خلال التعاون مع الخبراء وأصحاب المصلحة في منطقة آسيا والمحيط الهادئ بحيث يقيّم بفعالية التغيرات في نُهج الدول والتطورات التكنولوجية. ويتجلى "النضج" في هذا السياق بوجود الهياكل والسياسات والتشريعات والمنظمات ذات الصلة بالأمن السيبراني وتنفيذها وتشغيلها على نحو فعّال. وتغطي مؤشرات النضج السيبراني هذه السياسة العامة بأكملها للحكومة والهياكل التشريعية، وإجراءات التصدي للجريمة السيبرانية المالية، والمنظمات العسكرية، ومصالح الأعمال والقوة الاقتصادية الرقمية، ومستويات الوعي السيبراني الاجتماعية.

وقد اقتصر تجميع قاعدة البحوث التي تقوم عليها كل من مجموعات المؤشرات هذه على المعلومات المتاحة في المجال العام؛ وبعبارة أخرى، تستند استنتاجات التقرير إلى المواد المفتوحة المصدر حصراً.

نظرة عامة

تاريخ آخر تحديث للأداة	2017
ما اسم أداة التقييم؟	النضج السيبراني في منطقة آسيا والمحيط الهادئ
ما اسم المنظمة التي تحتفظ بالأداة؟	المعهد الأسترالي للسياسات الاستراتيجية (ASPI)
من هم منفذو التقييمات؟	المعهد الأسترالي للسياسات الاستراتيجية (ASPI)
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	السيدة Danielle Cave، نائبة مدير المركز الدولي لسياسات الأمن السيبراني، ASPI السيد Tom Uren، كبير المحللين، المركز الدولي للسياسات السيبرانية، ASPI السيد Bart Hogeveen، رئيس قسم بناء القدرات السيبرانية، ASPI
التغطية الجغرافية	إقليمية
من الذي يستطيع استخدام الأداة؟	أي شخص، والتقرير متاح للعموم.
ما هي المَحاور أو المواضيع المشمولة؟	**1 الإدارة** يتناول موضوع الإدارة النهج التنظيمي للدولة إزاء القضايا السيبرانية، بما في ذلك تشكيل الوكالات الحكومية المشاركة في هذه المسائل، ومقاصد الدولة التشريعية وقدراتها، وانخراط الدولة في مسائل السياسة السيبرانية الدولية مثل إدارة الإنترنت، وتطبيق القانون الدولي، وإعداد الأعراف أو المبادئ. وتقدم هذه المؤشرات التوجيه للانخراط الدبلوماسي والحكومي والتنموي ولانخراط سلطات إنفاذ القانون والقطاع الخاص في دول آسيا والمحيط الهادئ. **2 الإنفاذ بحق الجرائم السيبرانية المالية** الجريمة السيبرانية المالية مسألة حرجة بالنسبة لجميع الدول في منطقة آسيا والمحيط الهادئ. وأثر الجريمة السيبرانية على الأشخاص العاديين في المنطقة جدير بالاعتبار ويكبد خسائر مالية كبيرة. ويمكن لفهم قدرة الدولة على التصدي للجريمة السيبرانية المالية أن يوجه مسألة المشاركة في الإنفاذ توجيهاً يشمل تبادل المعلومات والمساعدة في تنمية القدرات المقدمة من القطاعين العام والخاص.

	3 التطبيق العسكري يتناول هذا الموضوع الهيكل التنظيمي العسكري للدولة (إن وجد) المتعلق بالفضاء السيبراني وآراء الدولة المعروفة بشأن استخدام قواتها المسلحة للفضاء السيبراني. ويمكن لذلك أن يرشد مشاركة الأطراف العسكرية بين الدول فضلاً عن المشاركة الدبلوماسية والسياسية العسكرية. فالاستعمالات العسكرية للفضاء السيبراني، ولا سيما القدرات الوطنية في هذا الصدد، موضوع حساس لجميع بلدان آسيا والمحيط الهادئ، ولذلك يتطلب هذه المجال دراسة متأنية قبل أن تسعى الدول إلى، أو توافق على، التعامل فيما بينها بشأنه. **4 الاقتصاد الرقمي ومصالح الأعمال الرقمية** يُعتبر مستوى إدراك الدولة لأهمية الفضاء السيبراني والاقتصاد الرقمي، وكيفية فهمها لأهميته الاقتصادية، مؤشراً للنضج السيبراني. ويمكن لذلك أن يوجه المشاركة في بناء القدرات وروابط مصالح الأعمال الإقليمية والتعامل بين الحكومة ومصالح الأعمال فيما يتعلق بالأمن السيبراني. **5 المشاركة الاجتماعية** يشير الوعي العام بالقضايا السيبرانية والانخراط فيها، مثل قضايا إدارة الإنترنت والرقابة على الإنترنت والجريمة السيبرانية، إلى مدى نضج الحوار العام بين الحكومة والمواطنين. ويمكن أن تشير البرامج التعليمية بشأن القضايا السيبرانية وتكنولوجيا المعلومات والاتصالات أيضاً إلى مستوى عال من الفهم التقني القائم على هذه القضايا. وتشير نسبة سكان الدولة المزودين بتوصيلية الإنترنت إلى نوع انخراط مصالح الأعمال والانخراط الشخصي في الفضاء السيبراني وجودة البنية التحتية لتكنولوجيا المعلومات والاتصالات ومستوى ثقة المواطنين في التجارة الرقمية. ويمكن لذلك أن يرشد وكالات التنمية التي تسعى إلى بناء اقتصادات ومصالح أعمال إقليمية ترغب في تطوير التجارة في المنطقة.
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☒ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☒ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☐ التقاط الحوادث وتحليلاتها ☐ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☐ التدريب على التعامل مع الجريمة السيبرانية ☐ منع الجريمة السيبرانية

	الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☐ معايير الإنترنت المفتوحة ☐ إنترنت الأشياء
نوع المؤشرات	المؤشرات الكمية والمؤشرات النوعية
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	يتضمن "مقياس النضج السيبراني" 10 مؤشرات. وجرى ترجيح المؤشرات وفقاً لأهميتها بالنسبة للنضج السيبراني للدولة. وقد رجحتها مجموعة من الخبراء وأصحاب المصلحة المعنيين بالأمن السيبراني من الوكالات الحكومية والقطاع الخاص على مكيال يتراوح بين 1 و10، حيث يعتبر 1 "غير مهم البتة" و10 "بالغ الأهمية". ثم حُسبت متوسطات ترجيحات هؤلاء الخبراء في كل فئة لإنتاج عامل ترجيح يمكن استخدامه في حساب الدرجة الإجمالية. ثم صُنف كل بلد في الخطوة النهائية قياساً بالعوامل العشرة على مكيال يتراوح بين 0 و10 (10 هو أعلى مستوى من النضج). واستندت التقييمات إلى بحوث واسعة مفتوحة المصدر بشأن النوعية والكمية، وحيثما أمكن، استندت إلى مقارنة مع البحوث والنتائج خلال الأعوام 2014 و2015 و2016. وكانت الدرجة الإجمالية لكل بلد هي مجموع الدرجات مقابل كل عامل مرجَّح بمتوسط الأهمية المحسوبة. وللمساعدة في التفسير، جرى تحويل الدرجات الإجمالية إلى نسبة مئوية من أعلى درجة ممكنة في ضوء الترجيحات المخصصة: $$\overline{S} = 10 \times \frac{\sum_i S_i w_i}{\sum_i w_i}$$ حيث $\overline{S}$ = الدرجة المرجَّحة، وS = الدرجة وw = الترجيح.
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	المقارنة، بحسب الترتيب
أسلوب جمع البيانات الأولي	معلومات المصادر المفتوحة
هل لديكم جمع بيانات ثانوية؟	• المقابلات • الاستبيانات والاستطلاعات • عمليات الرصد • الأفرقة المتخصصة

ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	تدعى السفارات والمفوضيات العليا للبلدان التي يغطيها التقرير إلى التحقق من وقائع البيانات الوصفية لبلادها.
ما هي المخرجات الرئيسية للتقييم؟	• البيانات العامة لفرادى البلدان • ترتيب المقارنة على الصعيد الإقليمي • نظرة عامة على الاتجاهات الإقليمية • تقييم فرص الانخراط الدولي.
نسق عرض مخرجات التقييم	تقرير
هل يمكن نشر مخرجات التقييم؟	نعم، وتنشر النتائج مع تقرير.
كيف يمكن النفاذ إلى التقارير السابقة؟	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2014
ما الدليل على التأثير؟	انظر الجواب بشأن "التزكيات" أدناه
ما هي فوائد إجراء تقييم ما؟	انظر الجواب بشأن " أي مرحلة من دورة حياة الاستراتيجية" أدناه
هل لديكم عملية حساب للترجيحات؟	نعم. انظر الجواب بشأن "المؤشرات وكيفية تطبيقها" أعلاه
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	نعم. انظر الجواب بشأن "المؤشرات وكيفية تطبيقها" أعلاه

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	ما هي الاتجاهات الإقليمية للنضوج السيبراني في منطقة آسيا والمحيط الهادئ؟ كيف تقارَن بلدان آسيا والمحيط الهادئ عبر خمسة مواضيع سياساتية تشكل النضوج السيبراني؟ ما هي فرص الانخراط الدولي المتاحة مع بلدان آسيا والمحيط الهادئ؟
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	ينظر هذا المقياس إلى منطقة آسيا والمحيط الهادئ من منظور مقارن. ولوضع استراتيجية وطنية للأمن السيبراني، تكون التقارير أنسب ما تكون في مراحل التمهيد والتقدير والمراقبة والتقييم (M&E). وعند وضع نهج إقليمي، أو رسم "صورة" إقليمية، تكون الأداة مناسبة لوضع جداول الأعمال، وتحليلات على المستوى الاستراتيجي، ومقارنة الممارسات الوطنية. والدورة السنوية للتقرير تكسبه قيمة كبيرة في تحليل المراقبة والتقييم (M&E) وتحليل الاتجاهات.
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	يقدم التقرير مصدراً موثوقاً للتحليل الواقعي القائم على الأدلة بما يعود بالفائدة على واضعي السياسات على الصعيدين الوطني والإقليمي وللقطاعين العام والخاص.

ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية (GFCE)؟	يقدم التقرير المنطلقات المحتملة للمحادثات بين المستفيدين من بناء القدرات السيبرانية ومقدميه.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	تميل وسائل الإعلام إلى تلقف التقرير: • https://www.zdnet.com/article/only-us-tops-australia-in-asia-pacific-cyber-maturity-aspi/ • https://www.theaustralian.com.au/commentary/opinion/threat-posed-by-evil-nations-and-criminals-in-cyberland-is-rising/news-story/fdebd93f3dc0206afe0705e6f6ec045c • https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in-asiapacific-region-379580.vov • https://theaseanpost.com/article/cyberattack-malaysia-imminent-or-imagined ويُستشهد بالتقرير في الكلمات التي يدلى بها كبار المسؤولين السياسيين (الأستراليين): • https://www.rusi.org.au/resources/Documents/2015_10_05%20Brodtman.pdf ويستخدم التقرير كمصدر في منشورات السياسات العامة والمنشورات الأكاديمية الأخرى مثل: • https://www.austcyber.com/resources/sector-competitiveness-plan/executive-summary • https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Maurer_Tim_Web.pdf • https://www.standards.org.au/getmedia/952ea009-ffc2-490a-905f-8f731fa84a52/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx
ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	كمركز فكر معترف به، يدار مركز ASPI بموجب ميثاقه الذي ينص على الاستقلالية وعدم الانحياز. وعلاوةً على ذلك، يُكتب التقرير على أساس مصادر مفتوحة يمكن التحقق منها. لا تخضع الملاحظات أو الاستنتاجات لموافقة أي حكومة أو مقدم تمويل ويتبّع الممارسة المعمول بها في معايير التشدد التحليلي.
ترجى إضافة أي معلومات إضافية	نُشر التقرير آخر مرة في ديسمبر 2017 في انتظار تمويل جديد وإعادة تقييم لمخرجات البحوث المحتملة.

الرقم القياسي للتأهب السيبراني 2.0 (CRI)

معهد بوتوماك لدراسة السياسات العامة (PIPS)

يوفر *الرقم القياسي للتأهب السيبراني 2.0* (CRI) منهجية شاملة ومقارنة وقائمة على الخبرات لتقييم التزام البلدان ونضجها فيما يتعلق بتأمين البنية التحتية الرقمية الوطنية والخدمات التي يعتمد عليها نموها الاقتصادي وقدرتها الوطنية على الصمود. وأُنشِأ الرقم القياسي للتأهب السيبراني 2.0 انطلاقاً من نظيره 1.0 لعام 2013 الذي كان أول إطار منهجي متاح لتقييم التأهب السيبراني. ويمكن أن تساعد أداة تقييم الرقم القياسي للتأهب السيبراني البلدان على تحديد الفجوات الحالية، وتعزيز وضعها الحالي المتعلق بالأمن السيبراني، وتحسين إدارة المخاطر السيبرانية على المستوى الوطني.

ومنذ عام 2013، طُبّق الرقم القياسي للتأهب السيبراني على أكثر من 100 بلد، وانتُهي من إعداد 14 تقريراً متعمقاً.

نظرة عامة

تاريخ آخر تحديث للأداة	نُضيف أسئلة ومؤشرات جديدة، على نحو منتظم، لكل عنصر من العناصر الأساسية السبعة للأداة.
ما اسم أداة التقييم؟	الرقم القياسي للتأهب السيبراني 2.0
ما اسم المنظمة التي تحتفظ بالأداة؟	معهد بوتوماك لدراسة السياسات العامة (PIPS)
من هم منفذو التقييمات؟	أعضاء فريق التأهب السيبراني (السيدة Melissa Hathaway والسيدة Francesca Spidalieri)
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	• الموقع الإلكتروني لمعهد بوتوماك لدراسة السياسات العامة: https://www.potomacinstitute.org/academic-centers/cyber- readiness-index • بوابة "Cybil" الإلكترونية: https://cybilportal.org/tools/cyber-readiness-index-2-0/
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	• Melissa Hathaway، زميلة أولى في معهد بوتوماك لدراسة السياسات العامة ومحققة رئيسية في فريق الرقم القياسي للتأهب السيبراني: hathawayglobal@icloud.com • Francesca Spidalieri، محققة رئيسية مشاركة في فريق الرقم القياسي للتأهب السيبراني: francescaspidalieri@gmail.com
التغطية الجغرافية	عالمية
من الذي يستطيع استخدام الأداة؟	• القادة العالميون • الحكومات الوطنية/الإقليمية • الوزارات/الوكالات الحكومية • وكالات الأمن السيبراني/واضعو السياسات • الهيئات الأكاديمية • خبراء الأمن السيبراني • الباحثون الفرادى

ما هي المَحاور أو المواضيع المشمولة؟	يستخدم الرقم القياسي للتأهب السيبراني 2.0 أكثر من 70 مؤشراً فريداً في العناصر السبعة الأساسية لتمييز الأنشطة الجاهزة تشغيلياً وتحديد مجالات التحسين في الفئات التالية: 1 **الاستراتيجية الوطنية**: نشر استراتيجية وطنية. تعيين سلطة مختصة؛ وتحديد الكيانات الحكومية الرئيسية والكيانات التجارية الرئيسية المسؤولة عن التنفيذ؛ والآليات المتبعة لتأمين البنية التحتية الحيوية؛ وتحديد الخدمات الحرجة؛ وتحديد المعايير الوطنية لاستمرارية الخدمة. 2 **الاستجابة للحوادث**: نشر خطة الاستجابة للحوادث. وتحديد التبعات عبر القطاعات؛ وتقديم أدلة على ممارسة الخطة وتحديثها؛ ونشر تقييم التهديد السيبراني؛ وإنشاء فريق الاستجابة للحوادث الأمنية الحاسوبية (CSIRT)؛ والموارد المالية والبشرية. 3 **الجرائم الإلكترونية وإنفاذ القانون**: التصديق على المعاهدة الدولية بشأن الجرائم السيبرانية؛ والجهود المبذولة للحد من الجرائم الإلكترونية؛ والقدرة المؤسسية على مكافحة الجريمة السيبرانية؛ والالتزام باستعراض القوانين والآليات القائمة؛ والجهود المبذولة لتنظيف البنية التحتية المصابة؛ التدريب على إنفاذ القانون وتنمية القدرات. 4 **تبادل المعلومات**: سياسة تبادل المعلومات؛ والهيكل المؤسسي لتبادل المعلومات مع الوكالات الحكومية و/ أو قطاع الصناعة؛ وأدلة على آليات التنسيق بين القطاعات وبين أصحاب المصلحة؛ وقدرة الحكومة وعملياتها فيما يتعلق برفع السرية عن المعلومات الاستخباراتية. 5 **الاستثمار في البحث والتطوير والتعليم والقدرات**: آليات تحفيز حكومية لتشجيع الابتكار والاستثمار في مجال الأمن السيبراني؛ والموارد المالية والبشرية من أجل البحث والتطوير ونقل التكنولوجيا؛ برامج مانحة للشهادة في مجال الأمن السيبراني؛ ورعاية حملات التوعية بالأمن السيبراني والبرامج التعليمية. 6 **الدبلوماسية والتجارة**: تحديد الأمن السيبراني كعنصر أساسي في السياسة الخارجية والمفاوضات الاقتصادية الدولية؛ وتكوين موظفين متخصصين في مجال الدبلوماسية السيبرانية في وزارة خارجية بلد ما؛ والمشاركة في اتفاقات دولية ومتعددة الجنسيات وإقليمية بشأن الأمن السيبراني وإنفاذها. 7 **الدفاع والاستجابة للأزمات**: إنشاء مؤسسة عسكرية و/ أو غير عسكرية على المستوى الوطني في مجال الدفاع السيبراني؛ وأدلة على إجراء تمارين سيبرانية على المستوى الوطني مع شركاء تجاريين و/ أو دوليين؛ ووضع معايير لسلوك الدولة المسؤول في الفضاء السيبراني؛ وإنشاء آليات لتقديم المساعدة السريعة. وللحصول على وصف كامل لكل عنصر أساسي، يرجى الرجوع إلى المنهجية الكاملة على العنوان التالي: https://www.potomacinstitute.org/images/CRIndex2.0.pdf

ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☒ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☒ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☒ التقاط الحوادث وتحليلاتها ☒ تمارين الأمن السيبراني ☒ حماية البنية التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/ أو الوطنية
نوع المؤشرات	يتسم جمع البيانات في إطار الرقم القياسي للتأهب السيبراني 2.0 بكونه نوعياً، ويُقيّم كل مؤشر عبر أربع فئات رئيسية: (1) البيانات/الاستراتيجيات/السياسات؛ (2) والمنظمة/السلطة المختصة؛ (3) والموارد؛ (4) والتنفيذ.
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	يستعمل مستخدمو الرقم القياسي للتأهب السيبراني 2.0 أكثر من 70 مؤشراً في العناصر السبعة الأساسية لتقييم نضج الأمن السيبراني لبلد ما، وتحديد المجالات التي تشتغل بكامل طاقتها أو تشتغل جزئياً أو لا تتوفر فيها أدلة كافية. وتتقاسم جميع مؤشرات الرقم القياسي للتأهب السيبراني 2.0 هيكلاً مشتركاً. إن الأسئلة المطروحة في إطار إصدار واحد من المنهجية قابلة للمقارنة بأسئلة مماثلة في إصدارات سابقة أو مستقبلية. ويحظى كل مؤشر بنفس القدر من الأهمية ثم يوصف في تقرير قُطري كجزء من سياق أوسع يعتمد على احتياجات البلد وقدراته وأولوياته وأهدافه.
أسلوب جمع البيانات الأولي	يستخدم الرقم القياسي للتأهب السيبراني 2.0 المصادر الأولية، بما في ذلك الاستراتيجيات والسياسات والتشريعات الوطنية والبيانات الرسمية للقادة والتقييمات والتقارير الوطنية، وما إلى ذلك، من أجل تقييم الأمن السيبراني للبلدان وتطوير ملفات تعريف قُطرية متعمقة. ⇐ لم تُرتَب البلدان فيما بينها.

هل لديكم جمع بيانات ثانوية؟	• معلومات مفتوحة المصدر • وثائق سرية رسمية أو غير منشورة • مقابلات/ملاحظات • وثائق وسجلات
هل لديكم عملية لجمع البيانات الثانوية؟	نعم. تُجرى عملية جمع البيانات الثانوية لتأكيد المعلومات التي تم جمعها أو تصحيحها أو توسيع نطاقها أثناء تحليلنا للمصادر الأولية والمقابلات مع مسؤولين وخبراء في بلد ما.
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	تستند جميع أبحاثنا إلى مصادر أولية ووثائق رسمية، وتحظى بعد ذلك بدعم مسؤولين داخل بلد ما و/أو خبراء في مجال ما.
ما هي المخرجات الرئيسية للتقييم؟	تُنشر تقارير قُطرية متعمقة على الموقع الإلكتروني لمعهد بوتوماك لدراسة السياسات العامة، وتُتاح للجمهور بجميع لغات الأمم المتحدة الست. ويمكن أن تساعد هذه التقارير الحكومات في تطوير ممارساتها وسياساتها في مجال الأمن السيبراني، ووضع مخطط قابل للتنفيذ بشأن الأولويات المطلوبة من أجل تعزيز وضع الأمن السيبراني الخاص بها، مما يمكّنها من التعرف على الإجراءات التي يجب اتخاذها لتقليل المخاطر بغض النظر عن خبراتها الداخلية الحالية.
نسق عرض مخرجات التقييم	• تقارير قُطرية متعمقة • أداة التصور (الرسم البياني الراداري ومخطط "كرات هارفي") • عرض تقديمي باستخدام برنامج PowerPoint، إذا طلب البلد ذلك
هل يمكن نشر مخرجات التقييم؟	نعم. تتاح جميع التقارير القُطرية بشأن الرقم القياسي للتأهب السيبراني للجمهور على الصفحة الخاصة بالرقم القياسي للتأهب السيبراني في الصفحة الإلكترونية لمعهد بوتوماك لدراسة السياسات العامة: https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
كيف يمكن النفاذ إلى التقارير السابقة؟	انظر أعلاه.
ما الدليل على التأثير؟	أثّر الرقم القياسي للتأهب السيبراني بشكل مباشر على سياسات التأهب السيبراني والتفكير القيادي في البلدان والمنظمات التالية: أستراليا، أذربيجان، بنغلاديش، البوسنة والهرسك، بلغاريا، كندا، الصين، الجمهورية التشيكية، مصر، إستونيا، فرنسا، جورجيا، ألمانيا، أيسلندا، الهند، إندونيسيا، إسرائيل، إيطاليا، اليابان، الأردن، قيرغيزستان، ليتوانيا، المكسيك، هولندا، نيوزيلندا، عُمان، الفلبين، بولندا، رومانيا، المملكة العربية السعودية، صربيا، سلوفاكيا، جنوب إفريقيا، السويد، سويسرا، أوكرانيا، المملكة المتحدة؛ المنتدى الإفريقي لأفرقة الاستجابة للطوارئ الحاسوبية (Africa CERT)، فريق الاستجابة للطوارئ الحاسوبية لمنطقة آسيا والمحيط الهادئ (APCERT)، الاتحاد الدولي للاتصالات، مصرف التنمية للبلدان الأمريكية (IDB)، منظمة حلف شمال الأطلسي (الناتو)، مجلس دول الشمال، منظمة الدول الأمريكية (OAS) والبنك الدولي. ويواصل الرقم القياسي للتأهب السيبراني تأثيره على الصعيد العالمي، وقد عززت ميليسا هاثاواي، المحققة الرئيسية في فريق الرقم القياسي للتأهب السيبراني، عملية تثقيف القادة في جميع أنحاء العالم بشأن هذه المسائل. وعادةً ما تُدعى للمشاركة في الالتزامات والمناقشات الدولية رفيعة المستوى، وتظهر في العديد من المنشورات الدولية وتواصل إبلاغ القادة الوطنيين بشأن التطبيق العملي لاستخدام الرقم القياسي للتأهب السيبراني 2.0 كأداة للتخطيط/ المقارنة المرجعية وضمان مشاركة مختلف أصحاب المصلحة في جهود الأمن السيبراني الوطنية والعمليات، وزيادة التمويل لبناء القدرات في مجال الأمن السيبراني.

ما هي فوائد إجراء تقييم ما؟	يمكن أن يساعد تقييم الرقم القياسي للتأهب السيبراني 2.0 البلدان في تحديد الفجوات بين الوضع الحالي للأمن السيبراني والقدرات السيبرانية الوطنية اللازمة لدعم مستقبلها الرقمي ويمكن استخدام الأداة أيضاً لتقييم موضع بلد ما في منحنى النضج من منظور الحكومة بأكملها والشعب برمته. ويمكن أن تساعد المؤشرات، عند جمعها معاً، الحكومات في تقييم مبادراتها الأمنية الرقمية والوطنية ومواءمتها. ويمكن أيضاً للرقم القياسي للتأهب السيبراني 2.0، من خلال البيانات التي تم جمعها، أن يسلط الضوء على أفضل الممارسات التي يمكن أن تنفذها البلدان لتسهيل جهود التأهب السيبراني والمساعدة في توجيهها عبر الصناعات والقطاعات أيضاً. ويؤكد الرقم القياسي للتأهب السيبراني 2.0 على الأدوات التي يمكن للقادة الوطنيين الاستفادة منها، بما في ذلك السياسات والتشريعات واللوائح والمعايير وحوافز السوق والمبادرات الأخرى، لحماية قيمة استثماراتهم الرقمية ومعالجة التآكل الاقتصادي المستمر الناجم عن انعدام الأمن السيبراني. وقد يساعد هذا التقييم القادة الوطنيين على إدراك أن تحقيق الإمكانات الكاملة للاقتصاد الرقمي من حيث النمو الاقتصادي وزيادة الإنتاجية والكفاءة وتعزيز مهارات القوى العاملة وتحسين الوصول إلى الأعمال والمعلومات، يتطلب مواءمة استراتيجيات التنمية الاقتصادية مع أولويات الأمن القومي. ويوضح التقييم كيف يمكن لتكنولوجيا المعلومات والاتصالات أن تحقق النمو الاقتصادي، وذلك في حالة واحدة تتمثل في وضع سياسات وعمليات وتكنولوجيات صحيحة لحماية وتأمين البنية التحتية والخدمات السيبرانية التي يعتمد عليها المستقبل الرقمي للبلد ونموه.
هل لديكم عملية حساب للترجيحات؟	نعم. في قاعدة البيانات الداخلية الخاصة بنا، نمنح درجة 5.0 للمؤشرات التي تشتغل بكامل طاقتها، و3.0 إلى المؤشرات التي تشتغل جزئياً، و1.0 عند تصنيف عناصر محددة أو لا توجد أدلة كافية على وجودها أو تنفيذها. ويُستخدم حساب الترجيح فقط لإنشاء رسوم بيانية رادارية وصور مرئية أخرى، ولكن ليس لترتيب البلدان.
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	يوفر الرقم القياسي للتأهب السيبراني 2.0 درجة نضج لكل عنصر أساسي، ولكنه لا يرتب البلدان.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• هل تتماشى الأهداف القصيرة والطويلة الأمد للبلد، بما في ذلك البرنامج الرقمي والسياسات الصناعية والأهداف الاقتصادية وأولويات الأمن القومي، مع استراتيجيتها الوطنية في مجال الأمن السيبراني؟ • ما نوع التهديدات السيبرانية التي يمكن أن تعرض هذه الأهداف إلى الخطر أو تعطل تحقيقها؟ • ما هي عناصر التبعية الرقمية الأكثر أهمية في البلد (مثل الشركات والخدمات والبنية التحتية والأصول) التي، إذا تعرضت إلى الضرر، سيكون لها عواقب وخيمة على الاقتصاد والأمن القومي؟ • هل هناك خطوط واضحة للمساءلة والمسؤولية من أجل ضمان تحقيق أهداف البلد وتنفيذ تدابير الحد من المخاطر؟ • هل كانت اعتبارات الأمن السيبراني والقدرة على الصمود جزءاً أساسياً من عملية التخطيط؟ • ما هي الخطوات التي يمكن أن يتخذها البلد ليصبح أكثر قدرةً على الصمود في المجال الرقمي؟ ويمكن الإشارة أيضاً إلى الرقم القياسي للتأهب السيبراني 2.0 كمعيار للبلدان لتحديد الفجوات بين الوضع الحالي للأمن السيبراني والقدرات السيبرانية الوطنية اللازمة لتصحيح أوجه القصور ودعم الأولويات الاقتصادية والأمنية المستقبلية للبلد. وقد يستخدم القادة الحكوميون الرقم القياسي للتأهب السيبراني 2.0 لتسهيل جهود التأهب السيبراني والمساعدة في توجيهها عبر الصناعات والقطاعات أيضاً، وبالتالي، الحفاظ بشكل متواصل على التركيز على الصلة بين الاستراتيجيات الرقمية والصناعية والأولويات الأمنية الوطنية.
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	ينبغي أن تكون منهجية الرقم القياسي للتأهب السيبراني جزءاً من دورة حياة الاستراتيجية بأكملها، ويمكن استخدام أداة التقييم الخاصة بالرقم القياسي قبل وضع استراتيجية وطنية للأمن السيبراني و/أو بعدها، بما في ذلك أثناء مراحل: البدء/الجرد والتحليل/إنتاج الاستراتيجية/التنفيذ/المراقبة والتقييم/ تحديث الاستراتيجية.
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	يربط الرقم القياسي للتأهب السيبراني 2.0 النمو الاقتصادي والتنمية بسياسات الأمن القومي، وبالتالي، يمكن أن يساعد البلدان على تحقيق مواءمة أفضل لاستراتيجيتها الوطنية في مجال الأمن السيبراني مع استراتيجياتها في مجالي الرقمنة والنمو.
ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية (GFCE)؟	يمكن أن يدعم الرقم القياسي للتأهب السيبراني 2.0 أو يكّمل أدوات التقييم الأخرى التي يقدمها مجتمع المنتدى العالمي للخبرة السيبرانية (GFCE)، بما في ذلك Oxford CMM والرقم القياسي للاتحاد بشأن الأمن السيبراني العالمي.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	إضافةً إلى جميع البلدان والمنظمات الدولية المذكورة أعلاه التي استخدمت الرقم القياسي للتأهب السيبراني لتوجيه سياساتها واستراتيجياتها، تم الاستشهاد بالرقم القياسي أو استخدامه في العديد من المقالات والخطابات والإحاطات والتقارير والمنشورات المشتقة. وعلى سبيل المثال، استخدمت منظمة الدول الأمريكية ومصرف التنمية للبلدان الأمريكية منهجية الرقم القياسي للتأهب السيبراني وقاعدة البيانات لتأكيد صحة تقريرهما الدوليين بشأن مستوى القدرة السيبرانية للبلدان الأعضاء ودرجة تأهبها (الأمن السيبراني: هل نحن مستعدون في أمريكا اللاتينية ومنطقة البحر الكاريبي؟). وعمل فريق الرقم القياسي للتأهب السيبراني بنشاط مع الاتحاد لتبادل البيانات ومواءمة الجهود وتوسيع نطاق الآثار والمساهمة في مشروعين من المشاريع الأخيرة بشأن الأمن السيبراني - وضع النسخة الثانية من الرقم القياسي للاتحاد بشأن الأمن السيبراني العالمي، وإنشاء دليل متعدد الشركاء بقيادة الاتحاد لوضع الاستراتيجيات الوطنية للأمن السيبراني. ويمكن العثور على تغطية إعلامية إضافية للرقم القياسي للتأهب السيبراني 2.0 تحت عنوان "التأهب السيبراني في الأخبار": https://www.potomacinstitute.org/academic- centers/cyber-readiness-index
ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	تستند التقارير القُطرية إلى بيانات المصادر الأولية، ويتحقق فريق الخبراء الخاص بنا من صحتها بشكل مستقل.

نموذج نضج قدرات الأمن السيبراني للدول (CMM)

المركز العالمي لقدرات الأمن السيبراني (GCSCC)، جامعة أكسفورد وشركاؤها

يعمل *نموذج نضج قدرات الأمن السيبراني للأمم* (CMM) الذي طوره المركز العالمي لقدرات الأمن السيبراني في جامعة أكسفورد، على قياس قدرة الأمن السيبراني للبلد من خلال خمسة أبعاد، وبالتالي تمكين الدول من الاضطلاع بالتقييم الذاتي، وتخطيط الاستثمارات والاستراتيجيات الوطنية للأمن السيبراني وتحديد الأولويات بشكل أفضل من أجل تنمية القدرات. ومنذ عام 2015، انتُهي من أكثر من 110 استعراض لنموذج نضج قدرات الأمن السيبراني للدول في أكثر من 80 بلداً في جميع أنحاء العالم.

ويحدد المركز العالمي لقدرات الأمن السيبراني وشركاؤه قدرة الأمن السيبراني على نطاق واسع لتشمل السياسات والاستراتيجيات والعوامل الاجتماعية والثقافية والتعليم والتدريب والقانون والتنظيم والتكنولوجيات السيبرانية والمعايير. وتمشياً مع هذا التعريف، فإن منهج المركز العالمي البحثي منهجٌ متعدد التخصصات، ويتناول قدرة الأمن السيبراني في جميع أبعاده من وجهات نظر أكاديمية متعددة.

ووُضع نموذج نضج قدرات الأمن السيبراني للدول بهدف البحث عن الفروق الدقيقة في بناء القدرات في هذه الأبعاد المتعددة وداخلها؛ وأنواع الأنشطة التي يمكن أن تقدم القدرة وتعززها؛ وحيث توجد أفضل الممارسات؛ والشروط التي ينبغي في ظلها السعي إلى تعزيز القدرة؛ والطرائق التي ترتبط بها الأبعاد وتعتمد على بعضها البعض لتحقيق النجاح. وتحقيقاً لهذا الهدف، يوفر نموذج نضج قدرات الأمن السيبراني للدول أيضاً إطاراً يدعم المقارنة بين قدرات الأمن السيبراني عبر دول مختلفة في العالم وبمرور الوقت. وتُستخدم منهجية نموذج النضج لجمع الرؤى من مختلف الجهات الفاعلة ومجموعات أصحاب المصلحة من أجل التعبير عن رؤية واسعة لقدرة الأمن السيبراني في كل دولة.

نظرة عامة

تاريخ آخر تحديث للأداة	مارس 2021
ما اسم أداة التقييم؟	نموذج نضج قدرات الأمن السيبراني للدول، نسخة 2021
ما اسم المنظمة التي تحتفظ بالأداة؟	المركز العالمي لقدرات الأمن السيبراني (GCSCC) مركز أوقيانوسيا للأمن السيبراني (OCSC) مركز قدرات الأمن السيبراني للجنوب الإفريقي (C3SA)
من هم منفذو التقييمات؟	المركز العالمي لقدرة الأمن السيبراني (GCSCC)، ومركز أوقيانوسيا للأمن السيبراني (OCSC)، ومركز قدرات الأمن السيبراني للجنوب الإفريقي (C3SA)، ومنظمة الدول الأمريكية (OAS)، والبنك الدولي، وشركة NRD للأمن السيبراني شركاء التنفيذ: الاتحاد الدولي للاتصالات (ITU)؛ والمنتدى العالمي للخبرات السيبرانية (GFCE)؛ ومنظمة الكومنولث للاتصالات (CTO)؛ ومركز معلومات شبكة آسيا والمحيط الهادئ (APNIC)؛ وجماعة آسيا والمحيط الهادئ للاتصالات (APT)؛ والمعهد النرويجي للشؤون الدولية (NUPI)؛ والمؤسسة الألمانية للتعاون الدولي GmbH (GIZ)، ألمانيا
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	https://gcscc.ox.ac.uk/the-cmm
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	المركز العالمي لقدرات الأمن السيبراني، عالمي، السيدة Carolin Weisser Harris: carolin.weisser@cs.ox.ac.uk مركز أوقيانوسيا للأمن السيبراني، منطقة أوقيانوسيا، السيد James Boorman: james.boorman@ocsc.com.au مركز قدرات الأمن السيبراني للجنوب الإفريقي، منطقة إفريقيا، السيدة Nthabiseng Pule: npule@researchictafrica.net

التغطية الجغرافية	عالمية
من الذي يستطيع استخدام الأداة؟	أي شخص نموذج نضج قدرات الأمن السيبراني للدول هي وثيقة متاحة للجمهور. وإجراءً لاستعراض بواسطة النموذج، يوصى بالعمل مع إحدى الجهات المنفذة ذات الدراية بمنهجية النموذج.
ما هي المَحاور أو المواضيع المشمولة؟	يتناول نموذج نضج قدرات الأمن السيبراني قدرة الأمن السيبراني من خلال الأبعاد الخمسة الحاسمة لبناء قدرة الأمن السيبراني لبلد ما:  **البُعد 1 (*سياسة واستراتيجية الأمن السيبراني*)**: يستكشف قدرة البلد على وضع استراتيجية للأمن السيبراني وتنفيذها وتعزيز قدرة صمود أمنها السيبراني من خلال تحسين الاستجابة للحوادث والدفاع السيبراني وقدرات حماية البنية التحتية الحيوية. ويُراعي هذا البُعد الاستراتيجيات والسياسات الفعّالة عند توفير القدرة الوطنية للأمن السيبراني، مع الحفاظ على فوائد فضاء سيبراني حيوي للحكومة وقطاع الأعمال التجارية الدولية والمجتمع عموماً. **البُعد 2 (*ثقافة ومجتمع الأمن السيبراني*)**: يستعرض العناصر المهمة لثقافة الأمن السيبراني المسؤولة، مثل فهم المخاطر المتعلقة بالفضاء السيبراني في المجتمع، ومستوى الثقة في خدمات الإنترنت، وخدمات الحكومة الإلكترونية والتجارة الإلكترونية، وفهم المستخدمين لمسألة حماية المعلومات الشخصية عبر الإنترنت. وعلاوةً على ذلك، يستكشف هذا البُعد وجود آليات للإبلاغ تعمل كقنوات موجهة إلى المستخدمين من أجل الإبلاغ عن الجرائم السيبرانية. وبالإضافة إلى ذلك، يستعرض هذا البُعد دور وسائل الإعلام ووسائل التواصل الاجتماعي في تشكيل قيم ومواقف وسلوكيات في مجال الأمن السيبراني. **البُعد 3 (*بناء المعارف والقدرات في مجال الأمن السيبراني*)**: يستعرض مدى توافر البرامج وجودتها واستيعابها لمختلف مجموعات أصحاب المصلحة، بما في ذلك الحكومة والقطاع الخاص والسكان ككل، ويتعلق ببرامج إذكاء الوعي بالأمن السيبراني وبرامج التعليم الرسمي للأمن السيبراني، وبرامج التدريب المهني. **البُعد 4 (*الأطر القانونية والتنظيمية*)**: يدرس قدرة الحكومة على تصميم وسنّ التشريعات الوطنية التي تتعلق بشكل مباشر وغير مباشر بالأمن السيبراني، مع التركيز بشكل خاص على موضوعات المتطلبات التنظيمية للأمن السيبراني، والتشريعات المتعلقة بالجرائم السيبرانية والتشريعات ذات الصلة. وتُفحص القدرة على إنفاذ مثل هذه القوانين من خلال إنفاذ القانون والملاحقة والهيئات التنظيمية وصلاحيات المحاكم. وعلاوةً على ذلك، يلاحظ هذا البُعد قضايا مثل أطر التعاون الرسمية وغير الرسمية لمكافحة الجريمة السيبرانية.

	البعد 5 ***(المعايير والتكنولوجيات)***: يتناول الاستخدام الفعّال والواسع النطاق لتكنولوجيا الأمن السيبراني لحماية الأفراد والمنظمات والبنية التحتية الوطنية. ويبحث هذا البُعد تحديداً في تنفيذ معايير الأمن السيبراني والممارسات الجيدة، ونشر العمليات والضوابط وتطوير التكنولوجيات والمنتجات من أجل تقليل مخاطر الأمن السيبراني.
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☒ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☐ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☒ التقاط الحوادث وتحليلاتها ☒ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/ أو الوطنية
نوع المؤشرات	مؤشرات نوعية
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	يشمل نموذج نضج قدرات الأمن السيبراني للدول حوالي 600 مؤشر لتقييم النضج للخمسة أبعاد الحاسمة لبناء قدرة الأمن السيبراني لبلد ما: *سياسة واستراتيجية الأمن السيبراني؛ وثقافة ومجتمع الأمن السيبراني؛ وبناء المعرفة والقدرات في مجال الأمن السيبراني؛ والأطر القانونية والتنظيمية؛ والمعايير والتكنولوجيات.* ويتضمن كل ***بُعد*** من أبعاد نموذج نضج قدرات الأمن السيبراني للدول مجموعةً من ***العوامل*** التي تصف وتحدد ما يعنيه امتلاك قدرة للأمن السيبراني. وتُقسم معظم العوامل إلى عدة ***جوانب***. ويحتوي كل عامل/جانب على سلسلة من ***المؤشرات*** في إطار ***مراحل*** النضج الخمس: *البدء والتكوين والتأسيس والاستراتيجية والديناميكية*. وتصف هذه المؤشرات الخطوات والإجراءات التي يجب اتخاذها لتحقيق أو الحفاظ على مرحلة معينة من النضج في التسلسل الهرمي لجانب/عامل/بُعد ما. ويجب إثبات كل مؤشر لكي يُظهر بلد ما نضجه المقدّر في إطار جانب/ عامل معيّن؛ وإذا كان الأمر خلاف ذلك، لا يمكن اعتبار أن البلد قد أحرز تقدماً لكي ينظر في المرحلة التالية.

المنهجية - ما هو نوع التقييم المستخدم؟	يعد نشر نموذج نضج قدرات الأمن السيبراني للدول عملية متعددة الخطوات ومتعددة أصحاب المصلحة، وتتكون من ثلاث مراحل رئيسية: 1) تحديد سياق البحوث المكتبية التي أجراها فريق التنفيذ. 2) مناقشات الأفرقة المتخصصة المعدَلة داخل بلد ما على مدى ثلاثة إلى أربعة أيام مع أصحاب المصلحة الرئيسيين، مثل الأوساط الأكاديمية، والعدالة الجنائية، وجهات إنفاذ القانون، وموظفي تكنولوجيا المعلومات وممثلي كيانات القطاع العام، وأصحاب البنية التحتية الحيوية، وواضعي السياسات، وموظفي تكنولوجيا المعلومات من الحكومة والقطاع الخاص (بما في ذلك المؤسسات المالية)، وشركات الاتصالات، والقطاع المصرفي، والمجتمع المدني والشركاء الدوليين. 3) تقرير مفصل لنموذج نضج قدرات الأمن السيبراني للدول يصف سياق الأمن السيبراني داخل بلد ما، ويلخص النتائج لكل عامل وجانب من نموذج النضج، ويحدد مراحل نضج قدرات الأمن السيبراني، ويقدم توصيات تمكّن البلد من تعزيز قدرته في مجال الأمن السيبراني. وخضع التقرير لاستعراض نظراء من اللجنة التقنية للمركز العالمي لقدرات الأمن السيبراني، وقُدّم إلى الحكومة للتعليق عليه. للحصول على مزيد التفاصيل، يرجى زيارة العنوان التالي: https://gcscc.ox.ac.uk/cmm-review-process
أسلوب جمع البيانات الأولي	• أفرقة متخصصة معدَلة (جمع البيانات الأولية الرئيسية) • استبيانات ودراسات استقصائية (دراسات إقليمية لمنظمة الدول الأمريكية) • مقابلات (اختيارية للحصول على أدلة إضافية)
هل لديكم جمع بيانات ثانوية؟	نعم (كجزء من البحوث المكتبية قبل/ بعد قيام الأفرقة المتخصصة المعنية بنموذج نضج قدرات الأمن السيبراني للدول بعملها). • معلومات من مصادر مفتوحة • وثائق غير منشورة • وثائق وسجلات • استبيانات ودراسات استقصائية
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	• كل مناقشة من مناقشات الأفرقة المتخصصة المعدَلة المعنية بنموذج نضج قدرات الأمن السيبراني للدول تتعلق ببُعد واحد أو أكثر، مما يسمح بجمع الأدلة فيما يتعلق بكل بُعد مرتين على الأقل. ويتيح ذلك أيضاً إمكانية التثليث وجمع إجابات مختلفة على السؤال نفسه من مختلف أصحاب المصلحة. • تُسجل جلسات الأفرقة المتخصصة المعدَلة المعنية بنموذج نضج قدرات الأمن السيبراني للدول بموافقة مسبقة، وتستخدم بعض الجهات المنفذة نصوصاً مجهولة المصدر للجلسات من أجل تحليل الردود على الأسئلة على نطاق مجموعة بيانات الاستعراض. • تؤكد البحوث المكتبية الأدلة المقدمة من الأفرقة المتخصصة المعدَلة المعنية بنموذج نضج قدرات الأمن السيبراني للدول. • يخضع التقرير لاستعراض نظراء من اللجنة التقنية للمركز العالمي لقدرات الأمن السيبراني، ويقدّم إلى الحكومة للتعليق عليه. • تستخدم بعض الجهات المنفذة أداة ترميز المجال المنظم (SFC) التي تسمح لهم بإدخال وترميز الإجابات المستمدة من البحوث المكتبية والأفرقة المتخصصة المعدّلة المعنية بنموذج نضج قدرات الأمن السيبراني للدول، مما يمكّنها من التحقق من صحة المؤشرات في كل مرحلة من مراحل عملية الاستعراض. وتتطور الأساليب مع إدخال أداة ترميز المجال المنظم التي تشهد على الدافع المستمر لتحسين منهجيات استعراض نموذج نضج قدرات الأمن السيبراني للدول.
ما هي المخرجات الرئيسية للتقييم؟	يُقدّم تقرير قائم على الأدلة إلى الحكومة.

نسق عرض مخرجات التقييم	• تقرير مكتوب بما في ذلك التوصيات (PDF) • عرض ملخص تنفيذي للجهة المستضيفة (اختياري) • ورشة عمل للتحقق من الصحة مع الجهة المستضيفة وأصحاب المصلحة • أداة التصور (منظمة الدول الأمريكية https://www.cybersecurityobservatory.org)
هل يمكن نشر مخرجات التقييم؟	نعم. تُقدِّر الحكومة عرض و/ أو نشر التقرير أو أي جزء منه.
إذا كانت الإجابة بنعم، فكيف يمكن تقييم التقارير السابقة؟	يمكن العثور على جميع تقييمات نموذج نضج قدرات الأمن السيبراني للدول، بما في ذلك روابط التقارير المنشورة، على المواقع الإلكترونية التالية: • https://gcscc.ox.ac.uk/cmm-reviews • https://cybilportal.org/tools/portal-of-cybersecurity-capacity-maturity-model-cmm- review-reports/ (للحصول على تفاصيل بشأن حالة التقرير، يرجى الاطلاع على بوابة "Cybil" الإلكترونية من خلال البحث "نموذج نضج قدرات الأمن السيبراني للدول + اسم البلد")
ما الدليل على التأثير؟	توصّل تقييم مستقل لعيّنة من عمليات نشر نموذج نضج قدرات الأمن السيبراني للدول، أُجري في فبراير 2020 إلى أن: • استعراض نموذج نضج قدرات الأمن السيبراني للدول عزز الوعي بالأمن السيبراني وبناء القدرات. • استعراض نموذج نضج قدرات الأمن السيبراني للدول ساهم في زيادة التعاون داخل الحكومة. • بلداناً استشهدت بنموذج نضج قدرات الأمن السيبراني للدول كأساس لتطوير استراتيجياتها وسياساتها (مثل مقدونيا الشمالية وليتوانيا وجورجيا). • استعراض نموذج نضج قدرات الأمن السيبراني للدول عزز المصداقية الداخلية لبرنامج الأمن السيبراني داخل الحكومات. • استعراض نموذج نضج قدرات الأمن السيبراني للدول ساعد في تحديد الأدوار والمسؤوليات داخل الحكومات. وزاد استعراض نموذج من تمويل بناء القدرات في مجال الأمن السيبراني. • استعراض نموذج نضج قدرات الأمن السيبراني للدول ساعد في تمكين إقامة شبكات والتعاون مع قطاع الأعمال والمجتمع بشكل أوسع. واستُكمِل نموذج نضج قدرات الأمن السيبراني للدول أكثر من 120 مرة، ونُشِرت عملياته في أكثر من 85 بلداً، واستُخدم للعمل مع الحكومات الوطنية في جميع مناطق العالم. ويشمل ذلك: • دراستان إقليميتان (2016 و2020) أجرتهما منظمة الدول الأمريكية • أكثر من 25 استعراضاً بالتعاون مع البنك الدولي والوكالة الكورية للإنترنت والأمن (KISA) بشأن المرحلة الأولى والمرحلة الثانية من برامج قدرات الأمن السيبراني العالمية وكجزء من استعراضات نموذج نضج قدرات الأمن السيبراني للدول للكومنولث، ومحفظة برنامج والجماعة الاقتصادية لدول إفريقيا الغربية (ECOWAS) • فريق الاستجابة لحالات الطوارئ الحاسوبية (CERT) وتقييم القدرات في منطقة المحيط الهادئ مع الاتحاد ومجموعة الاتصالات لآسيا والمحيط الهادئ (APT) ومركز معلومات الشبكات لآسيا والمحيط الهادئ (APNIC) وشركاء آخرين • بناء القدرات في مجال الأمن السيبراني في منطقة الكومنولث مع منظمة الكومنولث للاتصالات. واستُخدمت بيانات مستمدة من استعراضات نموذج نضج قدرات الأمن السيبراني للدول لأغراض الأوراق الأكاديمية التالية: • Creese, S. وReisdorf, B. C. وBada, M. وShillair, R. وRoberts, T. وDutton, W. H (2019). "قدرة الأمن السيبراني للأمم"، صفحات من 165 إلى 179 في Graham, M. and Dutton, W. H. (محرران)، *المجتمع والإنترنت: كيف تغير شبكات المعلومات والاتصالات حياتنا*، الطبعة الثانية. أكسفورد: مطبعة جامعة أكسفورد.

	• Dutton, W. H. وCreese, S. وShillair, R. وBada, M (2019). "قدرة الأمن السيبراني: هل هي مهمة؟". *مجلة سياسة المعلومات*، 9: 280-306. doi:10.5325/jinfopoli.9.2019.0280 • Creese, S. وDutton, W. H. وEsteve-González, P. وShillair, R (2021). "بناء قدرات الأمن السيبراني: الفوائد عبر الوطنية والانقسامات الدولية". ورقة ستُقدّم في مؤتمر البحوث المعني بسياسات الاتصالات والمعلومات والإنترنت، واشنطن العاصمة، فبراير 2021. متاح على SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658350
ما هي فوائد إجراء تقييم ما؟	إن الهدف من استعراض نموذج نضج قدرات الأمن السيبراني للدول، جمع البيانات بشأن مشهد قدرة الأمن السيبراني لبلد ما، وتحديد أي مرحلة تم الوصول إليها من المراحل الخمس لنضج الأمن السيبراني عبر أبعاد نموذج النضج. وتُستخدم البيانات لإصدار تقرير قائم على الأدلة يُقدم إلى الحكومة مع توصيات من أجل: • قياس مدى نضج قدرات الأمن السيبراني لبلد ما؛ • تفصيل مجموعة عملية من الإجراءات من أجل الحدّ من فجوات النضج في قدرات الأمن السيبراني وإزالتها؛ • تحديد أولويات الاستثمار وبناء القدرات في المستقبل؛ • بناء حالات أعمال للاستثمار وما يقابلها من تحسينات متوقعة في أداء الأمن السيبراني الوطني.
هل لديكم عملية حساب للترجيحات؟	كلا
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	نعم - تقدير النضج وليس الترتيب. يتكون نموذج نضج قدرات الأمن السيبراني للدول من خمس مراحل من النضج تتراوح من *مرحلة البدء* إلى *المرحلة الديناميكية*. وتتضمن مرحلة البدء نهجاً مخصصاً للقدرة، في حين أن المرحلة الديناميكية تمثل نهجاً استراتيجياً وقدرةً على التكيف مع اعتبارات متغيرة تتعلق بالبيئة. إن التواجد في مرحلة معينة يعني أن الدولة في وضع محدد من حيث النضج المتعلق بقدرة الأمن السيبراني. ويقترح نموذج نضج قدرات الأمن السيبراني للدول الأدلة التي ستكون مطلوبةً لتحديد مرحلة معينة من النضج لعامل/ جانب ما. وتحقيقاً للوصول إلى مستوى نضج ما في أي بُعد من أبعاد نموذج نضج قدرات الأمن السيبراني للدول، يجب استيفاء جميع المؤشرات الخاصة بعامل/ جانب ما من ذلك البُعد. وعليه، يشير نموذج نضج قدرات الأمن السيبراني للدول بشكل مباشر إلى المجالات التي تتطلب مزيداً من التطوير للوصول إلى المرحلة التالية من النضج والبيانات المطلوبة لإثبات مثل ذلك المستوى من نضج القدرات.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• ما هي قدرات الأمن السيبراني الحالية في بلد ما؟ • ما هي فجوات الأمن السيبراني الحالية في بلد ما؟ • ما هي حالة تنفيذ الاستراتيجية والسياسة؟ • من هي الجهات الفاعلة المشمولة وما هي الأدوار والمسؤوليات؟ • ما هي الخطوات التي يمكن أن يتخذها بلد ما ليصبح أكثر أماناً في مجال الأمن السيبراني؟
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	البدء/ الجرد والتحليل/ المراقبة والتقييم
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	بما أن الأفرقة المتخصصة المعدّلة المعنية بنموذج نضج قدرات الأمن السيبراني للدول تجمع مجموعة كبيرة من أصحاب المصلحة على المستوى الوطني بالإضافة إلى الشركاء الدوليين في مكان واحد (حيثما أمكن ذلك)، فإن استعراضات نموذج النضج تتسم بوضع مثالي من حيث التنسيق مع الأنشطة الأخرى، أي قبله وبعده وبالتوازي معه. ويسمح نسق الفريق المتخصص المعدّل المعني بنموذج النضج أيضاً بجمع المدخلات أثناء الجلسة لإجراء تقييمات أخرى، عند الاقتضاء.
ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات	تعد استعراضات القدرات السيبرانية، إلى جانب استعراضات القدرات الوطنية للاستجابة للحوادث وتقييمات المخاطر الوطنية، النشاط الأول في قائمة المنتدى العالمي للخبرة السيبرانية فيما يتعلق بعملية الاستراتيجية الوطنية وجزءاً من مرحلة البدء. ويعد استعراض نموذج نضج قدرات الأمن السيبراني للدول، بفضل نهجه المتمثل في أصحاب المصلحة المتعددين وشموليته ونهجه الشفاف، أمراً

السيبرانية (GFCE)؟	مثالياً للجمع بين مختلف أصحاب المصلحة في بلد ما، والممولين وجهات التنفيذ، ولتوفير أساس مشترك يتم على أساسه للتخطيط لنشاط بناء القدرات السيبرانية وتنفيذها.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	دراسات حالة لنموذج نضج قدرات الأمن السيبراني للدول: شمال مقدونيا وغانا وساموا وجورجيا والتقارير الإقليمية لمنظمة الدول الأمريكية: https://gcscc.ox.ac.uk/case-studies دراسة حالة السنغال: الاجتماع السنوي للمنتدى العالمي للخبرة السيبرانية في سنغافورة، *"الاستراتيجيات الوطنية. مقابلات ما وراء الستار"*: https://thegfce.org/national-strategies-interviews-behind-the-cover البنك الدولي: البرنامج العالمي لقدرات الأمن السيبراني. الدروس المستخلصة والتوصيات من أجل تعزيز البرنامج: https://cybilportal.org/publications/global-cybersecurity-capacity-program-lessons- learned-and-recommendations-towards-strengthening-the-program/ الأمن السيبراني في دول المحيط الهادئ الجزرية: https://t.co/smxYhtrqBz?amp=1
ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	إن معظم الجهات المنفذة مؤسسات بحثية حصلت على موافقة أخلاقية من مجالس البحث الخاصة بها لجمع البيانات من أجل إجراء هذا التقييم. ويخضع كل تقرير من تقارير نموذج نضج قدرات الأمن السيبراني للدول لاستعراض نظراء من اللجنة التقنية للمركز العالمي لقدرات الأمن السيبراني التي تتألف من كبار الأكاديميين وخبراء في مجال الأمن السيبراني.
ترجى إضافة أي معلومات إضافية	كيف تُفيد استعراضات نموذج نضج قدرات الأمن السيبراني للدول البحوث في مجال بناء القدرات السيبرانية: https://gcscc.ox.ac.uk/our-approach تقرير منظمة الدول الأمريكية/ مصرف التنمية للبلدان الأمريكية لعام 2020 بشأن الأمن السيبراني: المخاطر والتقدم والمضي قدماً في أمريكا اللاتينية ومنطقة البحر الكاريبي: https://publications.iadb.org/en/2020-cybersecurity-report- risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean تقرير منظمة الدول الأمريكية/ مصرف التنمية للبلدان الأمريكية لعام 2020 بشأن الأمن السيبراني: هل نحن جاهزون في أمريكا اللاتينية ومنطقة البحر الكاريبي؟: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean المنتدى العالمي للخبرة السيبرانية - تقييم القدرات الوطنية للأمن السيبراني باستخدام نموذج النضج: https://thegfce.org/wp-content/uploads/2020/04/Assessnationalcybersecuritycapacityusingamaturitymodel.pdf مبادرة المنتدى العالمي للخبرة السيبرانية: إحراز تقدم في مجال الأمن السيبراني في السنغال وغرب إفريقيا: https://cybilportal.org/projects/progressing-cybersecurity-in-senegal-and-west-africa-gfce-initiative/ مبادرة المنتدى العالمي للخبرة السيبرانية: تقييم وتنمية قدرات الأمن السيبراني: https://cybilportal.org/projects/assessing-and-developing-cybersecurity-capability-gfce-initiative/

إطار وضع الاستراتيجيات السيبرانية وتنفيذها (CSDI)

شركة MITRE

يشمل *إطار وضع الاستراتيجيات السيبرانية وتنفيذها* (CSDI) لدى شركة MITRE نموذجاً رباعي المراحل: (1) فهم السياق الوطني للمخاطر/الفرص السيبرانية؛ (2) تقييم القدرات الحالية عبر ثمانية مجالات قدرات رئيسية فضلاً عن الأسس الاستراتيجية ("القدرة على بناء القدرات")؛ (3) وضع وتحديد أولويات الأهداف والاستثمارات الاستراتيجية استناداً إلى الفجوات المقدرة؛ (4) وضع خرائط طريق للتنفيذ من أجل الاستدامة على المدى الطويل.

نظرة عامة

تاريخ آخر تحديث للأداة	سبتمبر 2020
ما اسم أداة التقييم؟	إطار وضع الاستراتيجيات السيبرانية وتنفيذها (CSDI)
ما اسم المنظمة التي تحتفظ بالأداة؟	شركة MITRE
من هم منفذو التقييمات؟	شركة MITRE
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	https://cybilportal.org/tools/national-cyber-strategy-development-implementation-framework/
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	Gary Bundy: gbundy@mitre.org Cynthia Wright: cawright@mitre.org Johanna Vazzana: jvazzana@mitre.org
التغطية الجغرافية	إقليمية أو وطنية أو تنظيمية
من الذي يستطيع استخدام الأداة؟	أي شخص
ما هي المَحاور أو المواضيع المشمولة؟	فيما يلي المجالات الثمانية التي جرى تقييمها: 1) القانون المدني والتنظيم والمساءلة 2) السياسة العامة والمعايير 3) تعبئة الموارد عن علم بالمخاطر 4) عمليات الصمود 5) الاستجابة للحوادث 6) منع الجريمة السيبرانية ومقاضاة مرتكبيها 7) تنمية القوى العاملة السيبرانية 8) الوعي العام/الثقافة العامة بشأن الأمن السيبراني. وفي كل مجال من هذه المجالات، يُنظر إلى انخراط أصحاب المصلحة المتعددين والشراكات بينهم على أنها عوامل تمكينية رئيسية، وتركز نُهُج التنفيذ الرامية لتطوير القوى العاملة بوجه خاص على إقامة شراكات فعّالة بين القطاعين العام والخاص. وتُدرج الأسس الاستراتيجية أيضاً في التقييمات، وأهم هذه العوامل هو التزام القادة وانخراط أصحاب المصلحة.

ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☐ تدابير وأعراف بناء الثقة ☐ الدبلوماسية السيبرانية ☒ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☐ التقاط الحوادث وتحليلاتها ☐ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/أو الوطنية
نوع المؤشرات	المؤشرات هي مؤشرات نوعية تركز في المقام الأول على آليات وسياسات وعمليات وتعبئة موارد. وهي عموماً ليست تقنية في طبيعتها على وجه التحديد (أي أنها لا تركز على معماريات شبكة معينة أو على اختبار نظام عملي).
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	ما هو عدد المؤشرات المستخدمة وكيفية تطبيقها؟ ويُستخدم أكثر من 100 مؤشر، مجمَّعةً ضمن مجالات القدرات المناسبة.
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	التحليل القائم على البحوث والاستطلاعات/المقابلات التي يجريها أصحاب المصلحة.
أسلوب جمع البيانات الأولي	• معلومات المصادر المفتوحة • المقابلات • الاستبيانات والاستطلاعات • الوثائق والسجلات
هل لديكم جمع بيانات ثانوية؟	ورش عمل لأصحاب المصلحة

ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	• استعراض الجودة الداخلية • تُدار الاستبيانات عبر أوسع مجموعة ممكنة من أصحاب المصلحة لتوسيع دائرة الأفكار/إقرار صحتها • استطلاع يُسنِد الدرجات آلياً
ما هي المخرجات الرئيسية للتقييم؟	نتائج الجمع بين البحوث المفتوحة المصادر، وتحليل التهديدات/الفرص، والتقييم المدار ومقابلات المتابعة، لإنتاج "مخطط رادراي" بديهي مصمَم لتسهيل تحقيق الهدف العليم بالمخاطر وتحديد أولويات الاستثمار في مجالات القدرات الثمانية، إلى جانب تقرير مفصل يتضمن توصيات حسب الأولوية.
نسق عرض مخرجات التقييم	• تقرير • أداة العرض المرئي
هل يمكن نشر مخرجات التقييم؟	نعم، بموافقة الكيان الطالب
كيف يمكن النفاذ إلى التقارير السابقة؟	بناءً على طلب من الحكومة/المنظمة التي جرى تقييمها.
ما الدليل على التأثير؟	في كل بلد تربطه علاقة مستمرة مع شركة MITRE، أجرت الحكومة و/أو المنظمات المقيّمة تغييرات في الأهداف الاستراتيجية وهياكل/آليات الإدارة وعمليات التنسيق التشغيلي، واتصالات وعمليات الاستجابة للحوادث، ونُهج تطوير القوى العاملة و/أو محاور برنامج الوعي العام التي تبين الأولويات المحددة من خلال هذا التعامل.
ما هي فوائد إجراء تقييم ما؟	تكتسب البلدان و/أو المنظمات و/أو كيانات المساعدة المقيَّمة أفكاراً عميقة بشأن سياق مخاطرها/فرصها الاستراتيجية ومحركات قدراتها واحتياجاتها وثغراتها في شكل يسهِّل أحد الجوانب الرئيسية للاستثمار في القدرات: أي تحديد الأولويات. ومن خلال وضع استراتيجية متابعة وتنفيذ ورش عمل، فهي تحدد أدوار ومسؤوليات أصحاب المصلحة الرئيسية؛ وممارسات الإدارة الفضلى؛ وفرص الشراكة؛ ونُهج تعبئة الموارد؛ والفجوات وأوجه الغموض التشريعية والسياساتية؛ والمتطلبات التأسيسية (المسبقة)، التي تتأطر جميعها في سياق ما تنفرد به من مشهد التهديدات واحتياجات تنمية القدرات. بالإضافة إلى ذلك، ونظراً لأن التقييم يركز على نهج الحكومة بأكملها أو نهج المنظمة بأكملها، تُجرى ورش عمل باستخدام أدوات تفكير ومشاركة مثبتة من حيث التصميم، فهو يعزز مشاركة أصحاب المصلحة وقبولهم وهو أمر ضروري للتنفيذ الفعّال.
هل لديكم عملية حساب للترجيحات؟	يتساوى "ترجيح" مجالات القدرات في التقييم. إلا أن مجالات القدرات مختلفة ستكتسي أهمية أكبر من غيرها لبلدان/منظمات معينة حسب السياق الاستراتيجي والقدرات الحالية والموارد البشرية/المالية. ويهدف هذا النهج تحديداً إلى تحديد المجالات التي ينبغي أن تكون "مرجحة" بدرجة أكبر لكل كيان مقيَّم على أساس المخاطر/الاحتياجات التي ينفرد بها.
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	يجري إعداد المخطط الراداري (أداة مخرجات واحدة بالإضافة إلى تحليل مفصل وتقرير التوصيات) على مكيال من أربع نقاط. ولكنه ليس نموذج النضج: إذ يصار إلى تقييم فجوات القدرات في سياق حالات البلاد/المنظمة النهائية المطلوبة بدلاً من مجموعة موضوعية من المعايير القياسية. ويساعد هذا النهج على ضمان امتناع البلدان/المنظمات عن "ملاحقة" مقاييس أقل أهمية بالنسبة لسياق التهديدات الاستراتيجية لديها، ويسمح لجهات التنفيذ بالمساعدة على تصميم استراتيجيات الاستثمار وفقاً للاحتياجات الأقرب صلة بالأهداف الاقتصادية والأمنية.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• ما هو مشهد التهديدات السيبرانية/الفرص لدينا؟ • في ضوء هذا المشهد، ما هي أهدافنا فيما يتعلق ببناء وتأمين تكنولوجيا المعلومات والاتصالات/القدرات والخدمات الرقمية؟ • من هي الجهات صاحبة المصلحة في هذا المضمار، وما هي أدوارها؟ • ما هي فجوات القدرات فيما يتعلق بغاياتنا الاستراتيجية؟ • من بين تلك الفجوات، أين ينبغي لنا تحديد أولويات جهودنا؟ • ما هي الأهداف التي يمكن أن تساعد في تحقيق غاياتنا ذات الأولوية؟ • "كيف يمكننا" تصميم مبادرات لتحقيقها؟" • من بين المبادرات المختلفة التي يمكن أن نتبعها، أي منها تحقق أكبر عائد على الاستثمار من حيث التأثير والجدوى؟ • ما هي الموارد التي يمكن أن تفعل فعلها في هذا الصدد؟ • من هم شركاؤنا المحتملون في اتباع مبادرات مختارة؟ • كيف نضع خارطة طريق للتنفيذ وننفذها؟ • كيف يمكننا أن نزيد من مشاركة أصحاب المصلحة ومن الدعم العام؟
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	التمهيد/ التقدير والتحليل/ وضع الاستراتيجية/ التنفيذ
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	بتقديم منظور يشمل كامل الحكومة/المنظمة ويستند إلى مشهد محدد للتهديدات/الفرص، يقدم هذا النهج إطاراً مشتركاً لأصحاب المصلحة لتحديد مواردهم وأولوياتها وتحقيق الأهداف المشتركة. ومن خلال تمييز الثغرات في القدرات حسب مجالات القدرات الرئيسية، فهو يساعد الكيانات على الحفاظ على التركيز على المجالات الأوثق صلة بها، مع الاستمرار في تقديم الرؤية الواضحة في مجالات أخرى قد تسنح فيها فرص بناء القدرات، مثل موارد برنامج المساعدة التي يمكنها إنماء القدرات دون تحويل الموارد الداخلية الشحيحة عن مجراها. وأخيراً، لأن هذا النهج محدد ضمن إطار أصحاب المصلحة المتعددين، فإنه يسهل التركيز على الاتصالات وتبادل المعلومات والعمليات الشفافة التي تكفل كون أصحاب المصلحة والشركاء على بينة من الأولويات العليا والأنشطة الجارية (ومتقبلين لها).
ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية (GFCE)؟	إنه يوضح مجالات الحاجة ذات الأولوية، وجهات الاتصال المناسبة لدى أصحاب المصلحة، والبرامج الأخرى الجارية/المتاحة والموارد البشرية/المالية المتاحة.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	أجريت جميع التقييمات حتى الآن للبلدان/المنظمات بناءً على طلبها أو بطلب من وزارة الخارجية الأمريكية. ولم يُنشر أي منها، على الرغم من أن حكومات بوتسوانا وغانا وأوكرانيا وإكوادور أعربت علناً عن تقديرها في خطابات عامة و/أو نشرات وسائل التواصل الاجتماعي و/أو اجتماعات القمة بين الحكومات. ولعل التزكية الكبرى تتمثل في أن الوكالات الفيدرالية الأمريكية والبلدان الشريكة ما زالت تطلب هذا الإطار، وتثق في توصياتنا بشأن المساعدة وتتصرف وفقها، وأن عدد البلدان التي نتعامل معها مباشرةً قد ازداد من ثلاثة إلى أكثر من عشرين بلداً في السنوات الأربع التي استعملنا خلالها هذا الإطار، ويسعى كل بلد بنشاط إلى الحصول على مشورتنا ومساعدتنا المستمرة. وعلى المستوى الإقليمي، يبلغ عدد البلدان التي نتعامل معها أكثر من 90 بلداً وما فتئ يتزايد مع تقديم طلبات جديدة ناشئة عن كل تعامل للحصول على مساعدة محددة.

ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	شركة MITRE هي منظمة بحث وتطوير ممولة فيدرالياً ذات متطلبات صارمة للتحكم في الجودة الداخلية وميثاق عام يلتزم صراحة بتقديم خدمة محايدة خالية من تضارب المصالح دعماً للمصلحة العامة.
ترجى إضافة أي معلومات إضافية	وُضع هذا الإطار تحت رعاية وزارة الخارجية الأمريكية بمكتب المنسق المعني بالقضايا السيبرانية، وجاء تحسينه من خلال تعاملات ثنائية وإقليمية موجهة من وزارة الخارجية. واستخدام هذا التقييم خارج الالتزامات الموجهة من وزارة الخارجية الأمريكية لا يعني بالضرورة دعم حكومة الولايات المتحدة أو أنه يتماشى مع سياساتها؛ ولكن ترد ضمناً في نموذجنا وتوصياتنا قيم الولايات المتحدة التي تشمل حرية المعلومات والالتزام بشبكة إنترنت حرة ومفتوحة وبحكم القانون وحقوق الإنسان.

الرقم القياسي العالمي للأمن السيبراني (GCI)

الاتحاد الدولي للاتصالات (ITU)

يدعم *الرقم القياسي العالمي للأمن السيبراني* (GCI) 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. 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، يصار إلى إعداده والموافقة عليه من خلال عملية تشاورية في إطار المسألة 3/2 (بشأن "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني") الموكلة إلى لجنة الدراسات 2 لقطاع تنمية الاتصالات. ويُدار الاستطلاع عبر منصة إلكترونية تُجمع من خلالها الأدلة الداعمة.

ويقيس التكرار الرابع لاستبيان الرقم القياسي العالمي للأمن السيبراني لعامي 2019-2020، 20 مؤشراً عاماً من خلال 82 سؤالاً. وتجسد المؤشرات العشرون الركائز الخمس للبرنامج العالمي للأمن السيبراني (GCA)، *القانونية والتقنية والتنظيمية والمطورة للقدرات والتعاونية*. وقد قدم مكتب تنمية الاتصالات بالاتحاد (BDT) استبيان الإصدار الرابع من الرقم القياسي العالمي للأمن السيبراني والوثائق ذات الصلة المتعلقة بالرقم القياسي العالمي للأمن السيبراني إلى لجنة الدراسات 2 لقطاع تنمية الاتصالات في أكتوبر 2019، قبل إطلاق الاستطلاع. وفي مارس 2020، قدم مكتب تنمية الاتصالات تقريراً إلى لجنة الدراسات 2 بشأن حالة الردود على الاستبيان وأطلع الأعضاء على الخطوات المقبلة في عملية تحليل البيانات وأشار إلى أن إعداد الترجيح سيكتمل من خلال إشراك فريق من الخبراء يصار إلى تشكيله عبر عملية تشاور مفتوحة مع الدول الأعضاء في الاتحاد وأعضاء القطاع والشركاء في مكتب تنمية الاتصالات. وفي أكتوبر 2020، قدم فريق الخبراء المعني بتحديد الترجيح توصيات الترجيح بشأن مؤشرات الإصدار الرابع من الرقم القياسي العالمي للأمن السيبراني والمؤشرات الفرعية والمؤشرات دون الفرعية، واقترح إدخال تعديلات على استبيان الرقم القياسي العالمي للأمن السيبراني في عمليات التكرار المستقبلية. ويتواصل التحقق من الردود على الاستبيان، من أجل الإقرار النهائي بصحتها من جانب البلدان المقدِّمة. ويُتوقع أن يُنشر التقرير النهائي في عام 2021.

نظرة عامة

تاريخ آخر تحديث للأداة	آخر تحديث لأداة التاريخ جرى آخر تحديث للمنشور في مارس 2019. ونحن في طور جمع البيانات واستكمال التحقق من البيانات المقدمة من أجل تقرير الإصدار الرابع من الرقم القياسي العالمي للأمن السيبراني.
ما اسم أداة التقييم؟	الرقم القياسي العالمي للأمن السيبراني (GCI)
ما اسم المنظمة التي تحتفظ بالأداة؟	الاتحاد الدولي للاتصالات (ITU)
من هم منفذو التقييمات؟	الاتحاد الدولي للاتصالات (ITU)
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	• الموقع الإلكتروني للاتحاد الدولي للاتصالات: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx • بوابة Cybil الإلكترونية: https://cybilportal.org/projects/itu-global-cybersecurity-index-gci- programme/
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	فريق الرقم القياسي العالمي للأمن السيبراني (GCI): gci@itu.int
التغطية الجغرافية	عالمية
من الذي يستطيع استخدام الأداة؟	• الدول الأعضاء: الوزارات / الوكالات • وكالات الأمن السيبراني/واضعو السياسات • الهيئات الأكاديمية • خبراء الأمن السيبراني • أي أفراد مهتمين وقد تلزم العضوية في الاتحاد للهيئات الأكاديمية والمنظمات التي ترغب في التشارك بالتعاون بشأن الرقم القياسي العالمي للأمن السيبراني.

ما هي المَحاور أو المواضيع المشمولة؟	تتضمن محاور الرقم القياسي العالمي للأمن السيبراني (GCI) ما يلي: **التدابير القانونية:** • القانون الأساسي بشأن الجريمة السيبرانية • لائحة الأمن السيبراني **التدابير التقنية:** • الأفرقة الوطنية/الحكومية المعنية بالاستجابة للحوادث (CERT/CIRT/CSRIT) • الأفرقة القطاعية المعنية بالاستجابة للحوادث (CERT/CIRT/CSRIT) • الإطار الوطني لتنفيذ معايير الأمن السيبراني • حماية الأطفال على شبكة الإنترنت (COP) **التدابير التنظيمية:** • الاستراتيجيات الوطنية للأمن السيبراني (NCS) • الوكالات المسؤولة/الوطنية • مقاييس الأمن السيبراني **تدابير بناء القدرات:** • حملات توعية العموم • تدريب للمهنيين في مجال الأمن السيبراني • البرامج التعليمية والمناهج الأكاديمية الوطنية • برامج البحث والتطوير في مجال الأمن السيبراني • صناعة الأمن السيبراني الوطنية • آليات الحوافز الحكومية لدعم تنمية الأمن السيبراني **تدابير التعاون:** • الاتفاقات الثنائية • المشاركة في الآليات (المنتديات) الدولية • - اتفاقات متعددة الأطراف • الشراكات بين القطاعين العام والخاص • الشراكات بين الوكالات. وللاطلاع على وصف كامل لكل تدبير، يرجى الرجوع إلى التقارير المنشورة في العنوان التالي: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☒ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☒ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☒ التقاط الحوادث وتحليلاتها ☒ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات

	الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/أو الوطنية
نوع المؤشرات	جمع بيانات الرقم القياسي العالمي للأمن السيبراني هو جمع نوعي يستعمل نظام اثنيني لتقييم وجود أو غياب نشاط أو دائرة أو تدبير على وجه التحديد.

كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	لا يتبع الرقم القياسي العالمي للأمن السيبراني مجموعة من المؤشرات مرتبة مسبقاً. وفي كل عملية تكرار يعدَّل الاستبيان ويراجَع مع مراعاة الملاحظات التقييمية الواردة من مسؤولي الاتصال والأعضاء في البلدان. ولذلك قد يتناقص عدد المؤشرات أو يزداد، ولا يوجد عدد ثابت من المؤشرات لكل موضوع محوري. على سبيل المثال، انظر الجدول أدناه الذي يورد تفاصيل عدد المؤشرات في كل تكرار حتى الآن. **GCIv1**: 17 مؤشراً تتضمن 17 سؤالاً رئيسياً **GCIv2**: 25 مؤشراً تتضمن 157 سؤالاً **GCIv3**: 25 مؤشراً تتضمن 50 سؤالاً رئيسياً **GCIv4**: 20 مؤشراً تتضمن 82 سؤالاً رئيسياً
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	يستعمل الرقم القياسي العالمي للأمن السيبراني الأسلوبين الأولي والثانوي للتقييم. ويجمع فريق الرقم القياسي العالمي للأمن السيبراني بيانات للبلدان التي لا تشارك ويُطلعها على النتائج للموافقة عليها، ويتحقق أيضاً من الردود المقدمة من جهات الاتصال التابعة للدول الأعضاء بالاتحاد ويقر بصحتها.
أسلوب جمع البيانات الأولي	• معلومات المصادر المفتوحة • الوثائق غير المنشورة • الاستبيانات والاستطلاعات • الوثائق والسجلات
هل لديكم جمع بيانات ثانوية؟	نعم. ويجرى جمع البيانات الثانوية للبلدان التي تستجيب لاستبيان الرقم القياسي العالمي للأمن السيبراني من خلال الخطوات التالية: • يقوم الاتحاد بالتحقق فيحدد الردود الناقصة والوثائق والروابط الداعمة باستخدام معلومات مفتوحة المصدر ووثائق غير منشورة واستبيانات واستطلاعات ووثائق وسجلات متاحة للعموم. • وترسَل الردود المتحقَق منها إلى مسؤول الاتصال في البلد الذي يحسِّن من دقة الردود عند الضرورة. • ويقر الاتحاد بصحة التعديلات النهائية من مسؤول الاتصال في البلد، ويعيد الوثيقة مرة أخرى إلى كل مسؤول اتصال للموافقة النهائية عليها. • وتُستخدم لاحقاً الردود الاستبيانية المتحقَق منها لأغراض التحليل والتقييم والتصنيف.
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	لمسؤولي الاتصال بشأن الرقم القياسي العالمي للأمن السيبراني الذين تعينهم الوزارات عادةً خلفية/خبرة في مجال الأمن السيبراني والعمل في مناصب ذات صلة بالأمن السيبراني ضمن مختلف الوزارات. وبالإضافة إلى ذلك، ترد الروابط والوثائق المطلوبة والمتحقَق منها من المواقع الإلكترونية العمومية الرسمية للحكومات وفي بعض الأحيان من الوثائق الرسمية المكتومة. ويمكننا اللجوء إلى مدققين متمرسين من المجالات ذات الصلة بالإنترنت فيُتطلب منهم تنفيذ عملية التحقق أكثر من مرة بشأن كل بلد ومعاودة تداولها مع البلدان إلى حين الحصول على التأكيد النهائي لضمان الدقة.
ما هي المخرجات الرئيسية للتقييم؟	وفي كل تكرار، يُنشر التقرير النهائي والنتائج.
نسق عرض مخرجات التقييم	تقرير
هل يمكن نشر مخرجات التقييم؟	نعم. يمكن نشر المخرجات. والرقم القياسي العالمي للأمن السيبراني مادة مفتوحة لزيادة الوعي على الصعيد العالمي. ويمكن الاطلاع على جميع التقارير السابقة عبر الرابط الإلكتروني: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
كيف يمكن النفاذ إلى التقارير السابقة؟	يمكن النفاذ إلى التقارير السابقة وتنزيلها عبر الرابط الإلكتروني التالي: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ما الدليل على التأثير؟	تبين المشاركة المتزايدة للدول الأعضاء في الرقم القياسي العالمي للأمن السيبراني (GCI) الاهتمام المتزايد باستمرار بالرقم القياسي: **(2015) GCIv1** 105 بلدان **(2017) GCIv2** 134 بلداً **(2018) GCIv3** 155 بلداً **(2020-2019) GCIv4** 163 بلداً حالياً وتطلب بلدان عديدة من الاتحاد الدولي للاتصالات أن يدعمها في تطوير وضع الأمن السيبراني لديها، من قبيل الدعم في وضع الاستراتيجيات الوطنية وتحسينها وفي إنشاء أفرقة مواجهة الطوارئ الحاسوبية (CERT) وفي أنشطة بناء القدرات، في جملة أمور أخرى. وقد تمكنت البلدان ذات الدرجات المنخفضة والمتوسطة (استناداً إلى مديات الدرجات، التي ظلت ثابتة على مر الوقت) من تلقي تدخلات هادفة تؤدي إلى انخفاض مطرد في عدد هذه البلدان.
ما هي فوائد إجراء تقييم ما؟	تساعد التقييمات في تحديد الثغرات في تطوير الأمن السيبراني ضمن الأمم والمناطق، فضلاً عن إذكاء الوعي بشأن الأمن السيبراني في جميع أنحاء العالم. ويساعد هذا التقييم أيضاً على تحديد أحوج البلدان إلى الدعم في تحسين وضع الأمن السيبراني لديها. 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 السليمة وبناء ثقافة عالمية للأمن السيبراني.
هل لديكم عملية حساب للترجيحات؟	نعم. ويقوم أعضاء فريق الخبراء المعني بالرقم القياسي العالمي للأمن السيبراني (GCI) بتقييم ترجيح المؤشرات في إطار الرقم القياسي GCI استناداً إلى أهمية المؤشرات ضمن الركائز الخمس للبرنامج العالمي للأمن السيبراني (GCA)؛ والصلة بالأهداف الرئيسية للرقم القياسي GCI وإطاره المفاهيمي، وتيسر البيانات وجودتها. ويقدم فريق الخبراء توصيات غير متحيزة بعد اجتماع فريق الخبراء المعني بتحديد الترجيح الذي يُعقد في كل تكرار للرقم القياسي GCI.
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	نعم. وتُحسب متوسطات ترجيحات المؤشرات من كل خبير للحصول على الترجيح النهائي لكل مؤشر. ومن خلال دالة مطبَّقة، يتلقى البلد الذي رد بالإيجاب على السؤال وأقرنه بإثبات موثق درجة كاملة عن المؤشر، في حين يتلقى البلد الذي ليس لديه دليل أو الذي يجيب بالنفي درجة صفرية عن ذلك المؤشر. وتُقيَّس الدرجات الإجمالية وتُصنف.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• ما هي الاتجاهات والأنماط العالمية الحالية في سياسة الأمن السيبراني؟ • كيف يمكن للدول الأعضاء تحديد مواطن القوة والضعف لديها في تدابير الأمن السيبراني؟ • ما هي مستويات التزام البلدان بالأمن السيبراني، وما هي البلدان التي تقدم أفضل الممارسات في مجال الأمن السيبراني؟
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	التمهيد/ التقدير والتحليل/ وضع الاستراتيجية/التنفيذ/المراقبة والتقييم
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	يساعد تقييم الرقم القياسي العالمي للأمن السيبراني (GCI) على تحديد مكامن القوة والضعف النسبية في التزامات الدول الأعضاء المتعلقة بالأمن السيبراني، وإعلام الدول الأعضاء بالمجالات التي قد تحتاج فيها لدعم إضافي في بناء القدرات، أو المجالات التي يمكنها فيها أن تقدم الدعم للآخرين. فعلى سبيل المثال، يمكن للاتحاد، من خلال تقييم الرقم القياسي العالمي للأمن السيبراني، تحديد الاحتياجات التعليمية في مجال الأمن السيبراني في الأنظمة التعليمية للأعضاء.

السنة	مرتفع	متوسط	منخفض
2019-2018	54	53	87
2017-2016	30	60	104
2015-2014	19	52	122

ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	تطلب بلدان عديدة كل عام المساعدة في إعداد أفرقة الاستجابة للطوارئ الحاسوبية (CERT) والاستراتيجيات الوطنية للأمن السيبراني نتيجةً لتقييم الرقم القياسي العالمي للأمن السيبراني وما يسنده من درجات ومرتبات. وعلى سبيل المثال: أطلقت **بنن** استراتيجية للأمن السيبراني نتيجة لزيادة الوعي من خلال الرقم القياسي العالمي للأمن السيبراني https://news.itu.int/benin-launches-a-new-national- cybersecurity-strategy/ واعتمدت **جمهورية الكونغو** تشريع الأمن السيبراني، قانون الجريمة السيبرانية: https://postetelecom.gouv.cg/le-senat-adopte-a-lunanimite-la-creation-de-lagence-nationale-de-securite-des-systemes-dinformation/ وفي عام 2018، تبين التقدم المحرز في التزامات الأمن السيبراني، على النحو المبلغ عنه إلى تقييمات الرقم القياسي العالمي للأمن السيبراني (GCI)، على النحو التالي: • في بنن وإستونيا وبولندا وزمبابوي وزامبيا ومصر وجنوب إفريقيا وإسواتيني، بوضع قوانين بشأن الجريمة السيبرانية؛ • في أوغندا، بصياغة تشريعاتها المتعلقة بحماية البيانات/الخصوصيات؛ • في أستراليا وبوتسوانا وكندا والجمهورية التشيكية والدانمارك واليابان والأردن وهولندا وإسبانيا وساموا وسنغافورة ولكسمبرغ، عند تحديث الاستراتيجية الوطنية للأمن السيبراني؛ • في الكاميرون وملاوي وتنزانيا وزمبابوي، بصياغة الاستراتيجية الوطنية للأمن السيبراني. تغطية وسائط الإعلام للرقم القياسي العالمي للأمن السيبراني https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx
ما هي الآليات التي تضمن استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	• يقوم فريقنا بإثبات صحة المساهمات المقدمة إلى الرقم القياسي العالمي للأمن السيبراني (GCI) بشكل مستقل • ويقدم فريق مستقل من الخبراء مدخلات بشأن ترجيحات المؤشرات ضمن النموذج، بحيث لا يتمكن خبير بمفرده من تغيير الترجيح كثيراً.

إطار تقييم القدرات الوطنية (NCAF)

وكالة الاتحاد الأوروبي المعنية بالأمن السيبراني (ENISA)

يتمثل الهدف الرئيسي *لإطار تقييم القدرات الوطنية* (NCAF) في إنشاء أداة للتقييم الذاتي لدعم الدول الأعضاء في الاتحاد الأوروبي في قياس مستوى نضج قدراتها في مجال الأمن السيبراني. ولتحقيق هذا الهدف، استخدمت وكالة الاتحاد الأوروبي المعنية بالأمن السيبراني (ENISA) الأهداف الاستراتيجية للاستراتيجيات الوطنية بشأن الأمن السيبراني لدى الدول الأعضاء في الاتحاد الأوروبي كنقطة انطلاق. وبما أن قدرات الأمن السيبراني هي الأدوات الرئيسية التي تستعملها البلدان لتحقيق أهداف الاستراتيجية الوطنية للأمن السيبراني (NCSS)، يضم إطار تقييم الأمن السيبراني أسئلة على خمسة مستويات من النضج، مع مراعاة 17 هدفاً استراتيجياً مدرجاً في معظم استراتيجيات الأمن السيبراني الوطنية الأوروبية. ويقدم الإطار رؤية بسيطة تمثل مدى نضج الأمن السيبراني لدى دولة عضو على ثلاثة مستويات مختلفة هي: مستوى هدف معين، ومستوى مجموعة أهداف، ومستوى إجمالي.

نظرة عامة

تاريخ آخر تحديث للأداة	2 ديسمبر 2020
ما اسم أداة التقييم؟	إطار تقييم القدرات الوطنية (NCAF)
ما اسم المنظمة التي تحتفظ بالأداة؟	وكالة الاتحاد الأوروبي المعنية بالأمن السيبراني (ENISA)
من هم منفذو التقييمات؟	الدول الأعضاء في الاتحاد الأوروبي
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework وسيجري تطوير إطار تقييم القدرات الوطنية (NCAF) ليصبح أداة إلكترونية على شبكة الإنترنت في عام 2021.
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	وكالة الاتحاد الأوروبي المعنية بالأمن السيبراني (ENISA)
التغطية الجغرافية	الاتحاد الأوروبي/عالمية
من الذي يستطيع استخدام الأداة؟	الجمهور المستهدف من إطار تقييم القدرات الوطنية (NCAF) هو واضعو السياسات والخبراء والمسؤولون الحكوميون الذين يتولون مسؤولية تصميم وتنفيذ وتقييم الاستراتيجيات الوطنية للأمن السيبراني، وعلى نطاق أوسع، قدرات الأمن السيبراني. وبالإضافة إلى ذلك، يمكن أن تكون النتائج الرسمية الواردة في الوثيقة المنشورة ذات قيمة لخبراء سياسات الأمن السيبراني والباحثين على المستوى الوطني أو الأوروبي.
ما هي المَحاور أو المواضيع المشمولة؟	ما هي المواضيع أو المواضيع المشمولة؟ ويغطي النموذج المفاهيمي لإطار التقييم الذاتي 17 هدفاً استراتيجياً مستمداً من الاستراتيجية الوطنية للأمن السيبراني (NCSS) لدى الدول الأعضاء في الاتحاد الأوروبي وهو منظم حول أربع مجموعات رئيسية. وتغطي كل واحدة من هذه المجموعات مجالاً محورياً رئيسياً لبناء قدرات الأمن السيبراني وتتضمن أهدافاً مختلفة. ثم يقيَّم كل هدف بحسب الأسئلة على مختلف مستويات النضج. وتغطي المجموعات المواضيع التالية: **(I) إدارة الأمن السيبراني ومعاييره** 1 وضع خطة وطنية للطوارئ السيبرانية 2 وضع تدابير أمنية أساسية 3 تأمين الهوية الرقمية وبناء الثقة في الخدمات العامة الرقمية وتنظر هذه المجموعة في جوانب التخطيط كي تتأهب الدولة العضو ضد الهجمات السيبرانية، وفي معايير لحماية الدول الأعضاء والهوية الرقمية.

	(II) بناء القدرات والوعي 4 تنظيم تمارين الأمن السيبراني 5 إنشاء قدرة على الاستجابة للحوادث 6 إذكاء وعي المستعملين 7 تقوية البرامج التدريبية والتعليمية 8 تعزيز البحث والتطوير 9 تقديم حوافز للقطاع الخاص للاستثمار في التدابير الأمنية 10 تحسين الأمن السيبراني في سلسلة التوريد وتقيِّم هذه المجموعة قدرة الدول الأعضاء على إذكاء الوعي بمخاطر الأمن السيبراني وتهديداته وكيفية التصدي لها. وبالإضافة إلى ذلك، يقيس هذا البعد قدرة البلاد على الاستمرار في بناء قدرات الأمن السيبراني وزيادة المعارف والمهارات في مجال الأمن السيبراني. **(III) الجانب القانوني والتنظيمي** 11 حماية البنية التحتية الحرجة للمعلومات، ومشغلي الخدمات الأساسية (OES) ومقدمي الخدمات الرقمية (DSP) 12 التصدي للجريمة السيبرانية 13 إنشاء آليات للإبلاغ عن الحوادث 14 تعزيز الخصوصيات وحماية البيانات وتقيس هذه المجموعة قدرة الدول الأعضاء على وضع الصكوك القانونية والتنظيمية اللازمة للتصدي للجريمة السيبرانية ومعالجة المتطلبات القانونية مثل الإبلاغ عن الحوادث ومسائل الخصوصية وحماية البنية التحتية الحرجة للمعلومات (CIIP). **(IV) التعاون** 15 إقامة شراكات بين القطاعين العام والخاص 16 إضفاء طابع مؤسسي على التعاون بين الوكالات العامة 17 المشاركة في التعاون الدولي وتقيِّم هذه المجموعة التعاون وتبادل المعلومات بين مجموعات أصحاب المصلحة المختلفة على المستويين الوطني والدولي.
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☒ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☐ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☒ التقاط الحوادث وتحليلاتها ☒ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني

	☒ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/أو الوطنية
نوع المؤشرات	يتضمن الإطار مؤشرات نوعية مبنية على مستويين، هما المستوى الاستراتيجي والمستوى التشغيلي. وبالنسبة لكل هدف أدرج في إطار التقييم الذاتي، هناك سلسلة من المؤشرات الموزعة بين مستويات النضج الخمسة. ويستند كل مؤشر إلى سؤال ثنائي (نعم/لا). وقد يكون المؤشر مطلوباً أو غير مطلوب.
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	يقدم هذا النموذج درجة على أساس قيمة معلمتين هما، ***مستوى النضج***، و***نسبة التغطية***. ويمكن حساب كل من هاتين المعلمتين على مستويات مختلفة: '1' لكل هدف، أو '2' لكل مجموعة أهداف أو '3' إجمالاً. بالإضافة إلى ذلك، من أجل التكيف مع خصائص تنفرد بها كل من الدول الأعضاء في الاتحاد الأوروبي مع السماح أيضاً بلمحة عامة متسقة، تحسب الدرجة انطلاقاً من عينتين مختلفتين على مستوى المجموعة والمستوى الإجمالي: • **الدرجات العامة**: عينة كاملة تشمل جميع الأهداف المدرجة ضمن المجموعة أو ضمن الإطار العام (من 1 إلى 17) • **الدرجات المحددة**: عينة محددة لا تشمل إلا الأهداف التي اختارتها الدولة العضو (تقابل عادةً الأهداف الواردة في الاستراتيجية الوطنية للأمن السيبراني الخاصة بكل بلد) ضمن المجموعة أو ضمن الإطار العام. ويعرض جدول لكل مجموعة، مجموعة من المؤشرات الشاملة في شكل أسئلة تمثل مستوى معيناً من النضج. وهذا الاستبيان هو الأداة الرئيسية للتقييم الذاتي. ولكل هدف، هناك مجموعتان من المؤشرات تجب الإشارة إليهما: • مجموعة من الأسئلة عن نضج الاستراتيجية (9 أسئلة عامة)، مرتبة من 'أ' إلى 'ج' لكل مستوى من مستويات النضج، ومكررة لكل هدف؛ ومجموعة من الأسئلة عن القدرات في مجال الأمن السيبراني (319 سؤالاً بشأن قدرات الأمن السيبراني)، مرقمة من 1 إلى 10 لكل مستوى من مستويات النضج، وهي تخص المجال المشمول بالهدف.
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	**مستويات النضج**: مكيال نضج خماسي المستويات **النعوت**: تستند إلى الأبعاد الأربعة/المجموعات الأربع التي تغطي مجالات بناء قدرات الأمن السيبراني **أسلوب التقييم**: أسلوب التقييم الذاتي **عرض النتائج**: عرض النتائج على مستويات مختلفة من التفاصيل.
أسلوب جمع البيانات الأولي	• توقع أنشطة تنسيق لجمع البيانات ودمجها. • تحديد هيئة مركزية تتولى مسؤولية استكمال التقييم الذاتي على المستوى الوطني. • استعمال عملية التقييم كطريقة لتناقل مواضيع الأمن السيبراني والتواصل بشأنها. • استعمال الاستراتيجية الوطنية للأمن السيبراني (NCSS) بوصفها مجالاً لاختيار الأهداف الخاضعة للتقييم. وعندما يتطور نطاق الاستراتيجية الوطنية للأمن السيبراني، ضمان اتساق تفسير الدرجة مع تطور هذه الاستراتيجية. ودورة حياة الاستراتيجية الوطنية للأمن السيبراني (NCSS) هي عملية تستغرق عدة سنوات.

هل لديكم جمع بيانات ثانوية؟	عند ملء استبيان التقييم الذاتي، يوضع في الاعتبار أن الهدف الأساسي هو دعم الدول الأعضاء في بناء القدرات في مجال الأمن السيبراني.
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	ينبغي للدولة العضو/البلد في الاتحاد الأوروبي الذي يجري التقييم أن يضمن الدقة للاستفادة من نتائج هذا الإطار.
ما هي المخرجات الرئيسية للتقييم؟	تُقدَّم نتائج التقييم على ثلاثة مستويات مختلفة هي: مستوى هدف معين، ومستوى مجموعة أهداف، ومستوى إجمالي. ويصار إلى تقييم البلد وتلقي نتيجة عامة نهائية تأخذ في الاعتبار جميع أهداف كل مجموعة، ونتيجة محددة نهائية لا تأخذ في الاعتبار إلا الأهداف المختارة التي يرغب البلد في تقييمها. وبالإضافة إلى ذلك، يقدم إطار تقييم القدرات الوطنية (NCAF) أيضاً نسبة التغطية. وتُحسب نسبة التغطية على أنها **النسبة** بين **العدد الإجمالي للأسئلة** المندرجة ضمن الهدف و**عدد الأسئلة التي يرد الجواب عليها بالإيجاب**. ويعبَّر عن نسبة التغطية كنسبة مئوية.
نسق عرض مخرجات التقييم	تقرير عرض مرئي عبر الأداة الإلكترونية على شبكة الإنترنت (عمل مستقبلي للمعهد الأوروبي لمعايير الاتصالات)
هل يمكن نشر مخرجات التقييم؟	لا تُنشر نتائج التقييم إلا إذا قررت الدولة العضو القيام بذلك بمبادرة منها.
كيف يمكن النفاذ إلى التقارير السابقة؟	تستطيع الدولة العضو تتبع تقدمها بمرور الوقت استناداً إلى عمليات إعادة التقييم.
ما الدليل على التأثير؟	ما هي الأدلة الموجودة على ذلك؟ إجمالاً، شاركت نحو 20 دولة عضواً في وضع هذا الإطار وشاركت جميع الدول الأعضاء تقريباً في ورشة عمل إقرار الصحة حيث عُرض الإطار ونوقش باستفاضة. وبعبارة أدق، ينبغي للإطار أن يمكّن الدول الأعضاء من: • إجراء تقييم لقدرات الأمن السيبراني الوطنية الخاصة بها؛ • إذكاء الوعي بمستوى نضج البلاد؛ • تحديد مجالات التحسين؛ • بناء قدرات الأمن السيبراني.
ما هي فوائد إجراء تقييم ما؟	إطار تقييم القدرات الوطنية (NCAF) هو أداة يمكن أن تساعد البلدان على التالي: • تقديم معلومات مفيدة لوضع استراتيجية طويلة الأجل (مثل الممارسات السليمة والمبادئ التوجيهية)؛ • تحديد العناصر الناقصة في الاستراتيجية الوطنية للأمن السيبراني (NCSS)؛ • مواصلة بناء قدرات الأمن السيبراني؛ • دعم المساءلة عن الإجراءات السياساتية؛ • الحصول على مصداقية إزاء الشركاء العامين والدوليين؛ • دعم التوعية وتعزيز الصورة العامة كمنظمة شفافة؛ • توقع الإشكالات الكامنة في المستقبل؛ • تحديد الدروس المستفادة وأفضل الممارسات؛ • تقديم خط أساس بشأن قدرات الأمن السيبراني في الاتحاد الأوروبي لتسهيل المناقشات؛ • تقييم القدرات الوطنية المتعلقة بالأمن السيبراني.
هل لديكم عملية حساب للترجيحات؟	يمكن للدولة العضو في الاتحاد الأوروبي أن تعرض نتائج التقييم بعرض مستوى النضج لقدرات الأمن السيبراني في البلاد أو لمجموعة من الأهداف أو حتى لهدف واحد. ولجميع الأهداف المقيَّمة نفس الصلة بإطار التقييم، ومن ثم فهي تتمتع بنفس الأهمية. وينطبق ذلك أيضاً على المؤشرات المنشورة ضمن الإطار.
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	يهدف إطار تقييم القدرات الوطنية (NCAF) إلى قياس قدرات الدول الأعضاء في مجال الأمن السيبراني فيما يتعلق بالأهداف السبعة عشرة. بيد أن الدولة العضو تستطيع اختيار الأهداف التي تريد تقييمها وأن تحصر تقييمها في مجموعة فرعية من الأهداف البالغ عددها 17 هدفاً.

الرقم القياسي الوطني للأمن السيبراني (NCSI)

أكاديمية الحوكمة الإلكترونية (eGA)

إن *الرقم القياسي الوطني للأمن السيبراني* (NCSI) هو رقم قياسي عالمي يقيس تأهب البلدان لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية. وهو أيضاً قاعدة بيانات تحتوي على مواد أدلة متاحة للعموم وأداة لبناء القدرات الوطنية في مجال الأمن السيبراني..

ويركز الرقم القياسي الوطني للأمن السيبراني على جوانب قابلة للقياس في الأمن السيبراني تنفذها الحكومة المركزية:

1 **التشريعات السارية** - القوانين واللوائح والأوامر وغيرها

2 **الوحدات المنشأة** - منظمات ودوائر قائمة وما إلى ذلك.

3 **أنساق التعاون** - اللجان وأفرقة العمل وما إلى ذلك

4 **النتائج** - السياسات والتمارين والتكنولوجيات والمواقع الإلكترونية والبرامج، وما إلى ذلك.

ومنذ عام 2016، جرى تقييم 160 بلداً باستخدام الرقم القياسي الوطني للأمن السيبراني (NCSI). ويشكل جمع البيانات واستعراضها ونشرها عملية مستمرة في الرقم القياسي الوطني للأمن السيبراني. ولا ينشر الرقم القياسي الوطني للأمن السيبراني تكرارات سنوية. وعند تقديم دليل جديد، يصار إلى تقييمه فإذا كان ذا أساس، تجري التغييرات اللازمة في قائمة الترتيب على الفور. وقد وُضعت منهجية الرقم القياسي الوطني للأمن السيبراني في عام 2016 وجرى تحديثها في عام 2018. ويجري حالياً استعراض المنهجية وسيُنشر التكرار الجديد في موعد أقصاه عام 2022.

نظرة عامة

تاريخ آخر تحديث للأداة	يجري تحديث المدخلات القطرية الواردة في الرقم القياسي الوطني للأمن السيبراني (NCSI) باستمرار، مما يعني أن الرقم القياسي الوطني للأمن السيبراني نفسه قيد التحديث باستمرار.
ما اسم أداة التقييم؟	الرقم القياسي الوطني للأمن السيبراني (NCSI)
ما اسم المنظمة التي تحتفظ بالأداة؟	أكاديمية الحوكمة الإلكترونية (eGA)
من هم منفذو التقييمات؟	• أكاديمية الحوكمة الإلكترونية • الكيانات والمؤسسات ذات الصلة بالأمن السيبراني في البلدان ذات الترتيب المصنَّف
يرجى تقديم روابط إلكترونية إلى الأداة وأي معلومات إضافية	بوابة Cybil الإلكترونية: https://cybilportal.org/projects/national-cybersecurity-index/
بمن ينبغي الاتصال لمناقشة ترتيب التقييم؟	السيدة Epp Maaten: epp.maaten@ega.ee السيد Radu Serrano: radu.serrano@ega.ee السيدة Merle Maigre: merle.maigre@ega.ee الفريق المعني بالرقم القياسي الوطني للأمن السيبراني: ncsi@ega.ee
التغطية الجغرافية	عالمية
من الذي يستطيع استخدام الأداة؟	• الوزارات/الوكالات القُطرية • وكالات الأمن السيبراني/صانعو القرار • الهيئات الأكاديمية • خبراء الأمن السيبراني • أي شخص مهتم وللتعاون في جمع البيانات القُطرية عن الرقم القياسي الوطني للأمن السيبراني، ما عليكم إلا إلى التواصل مع الفريق المعني بالرقم القياسي الوطني للأمن السيبراني.

ما هي المَحاور أو المواضيع المشمولة؟	**1 وضع سياسات الأمن السيبراني:** 1.1 وحدة سياسة الأمن السيبراني 2.1 نسق تنسيق سياسة الأمن السيبراني 3.1 استراتيجية الأمن السيبراني 4.1 خطة تنفيذ استراتيجية الأمن السيبراني **2 تحليل التهديدات السيبرانية والمعلومات عنها:** 1.2 وحدة تحليل التهديدات السيبرانية 2.2 تُنشر تقارير عن التهديدات السيبرانية العامة سنوياً 3.2 موقع إلكتروني خاص بالسلامة السيبرانية والأمن السيبراني **3 التعليم والتنمية المهنية:** 1.3 كفاءات السلامة السيبرانية في التعليم الابتدائي أو الثانوي 2.3 برنامج الأمن السيبراني على مستوى البكالوريوس 3.3 برنامج الأمن السيبراني على مستوى الماجستير 4.3 برنامج الأمن السيبراني على مستوى الدكتوراه 5.3 الرابطة المهنية للأمن السيبراني. **4 مساهمة في الأمن السيبراني العالمي:** 1.4 الاتفاقية بشأن الجريمة السيبرانية 2.4 تمثيل أنساق التعاون الدولي 3.4 المنظمة الدولية للأمن السيبراني التي تستضيفها البلاد 4.4 بناء قدرات الأمن السيبراني للبلدان الأخرى **5 حماية الخدمات الرقمية:** 1.5 مسؤولية مقدمي الخدمات الرقمية عن الأمن السيبراني 2.5 معيار الأمن السيبراني للقطاع العام 3.5 سلطة إشرافية مختصة **6 حماية الخدمات الأساسية:** 1.6 تحديد مشغلي الخدمات الأساسية 2.6 متطلبات الأمن السيبراني لمشغلي الخدمات الأساسية 3.6 سلطة إشرافية مختصة 4.6 المراقبة المنتظمة للتدابير الأمنية **7 خدمات التعرف الإلكتروني والثقة:** 1.7 معرف هوية ثابت فريد 2.7 متطلبات أنظمة التجفير 3.7 تعرف الهوية الإلكتروني 4.7 التوقيع الإلكتروني 5.7 الختم الزمني 6.7 خدمة الإيصال المسجَّل الإلكترونية 7.7 سلطة إشرافية مختصة **8 حماية البيانات الشخصية:** 1.8 تشريعات حماية البيانات الشخصية 2.8 سلطة حماية البيانات الشخصية **9 الاستجابة للحوادث السيبرانية:** 1.9 وحدة الاستجابة للحوادث السيبرانية 2.9 مسؤولية الإبلاغ 3.9 جهة اتصال واحدة للتنسيق الدولي **10 إدارة الأزمات السيبرانية:** 1.10 خطة إدارة الأزمات السيبرانية 2.10 تمرين إدارة الأزمات السيبرانية على المستوى الوطني

	3.10 المشاركة في تمارين الأزمات السيبرانية الدولية 4.10 الدعم التشغيلي للمتطوعين في الأزمات السيبرانية **11 مكافحة الجريمة السيبرانية:** 1.11 تجريم الجرائم السيبرانية 2.11 وحدة الجريمة السيبرانية 3.11 وحدة الأدلة الجنائية الرقمية 4.11 جهة اتصال على مدار الساعة طوال أيام الأسبوع بشأن الجريمة السيبرانية الدولية **12 العمليات السيبرانية العسكرية:** 1.12 وحدة العمليات السيبرانية 2.12 تمرين العمليات السيبرانية 3.12 المشاركة في التمارين السيبرانية الدولية
ما هي المحاور أو المواضيع التي يتناولها المنتدى العالمي للخبرات السيبرانية (GFCE)؟	السياسات والاستراتيجيات ☒ الاستراتيجيات ☒ التقييمات ☐ تدابير وأعراف بناء الثقة ☒ الدبلوماسية السيبرانية ☐ القانون الدولي في الفضاء السيبراني إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP) ☒ الاستجابة لحوادث الأمن الحاسوبي الوطنية ☒ التقاط الحوادث وتحليلاتها ☒ تمارين الأمن السيبراني ☒ حماية البنى التحتية الحرجة للمعلومات الجريمة السيبرانية ☒ الأُطر القانونية/قانون الجريمة السيبرانية ☒ إنفاذ القوانين في الفضاء السيبراني ☐ التدريب على التعامل مع الجريمة السيبرانية ☒ منع الجريمة السيبرانية الثقافة والمهارات ☒ الوعي بالأمن السيبراني ☒ التعليم والتدريب ☒ تنمية القوى العاملة المعايير ☒ المعايير الدولية و/أو الوطنية
نوع المؤشرات	إن جمع البيانات الرقم القياسي الوطني للأمن السيبراني (NCSI) هو جمع بيانات نوعي يستعمل نظام قيم لتقييم وجود تشريع قانوني محدد و/أو وحدة متخصصة و/أو نسق تعاون رسمي و/أو نتيجة.
كم عدد المؤشرات المستخدمة وكيف يصار إلى تطبيقها؟	هناك ما مجموعه 46 مؤشراً (معروضة في شكل المحاور والمواضيع سالفة الذكر). وتوزَّع المؤشرات نفسها على 12 قدرة. ولكل مؤشر قيمة تبين الأهمية النسبية للمؤشر في الرقم القياسي، ومعيار يشرح نوع البيانات التي يمكن تقديمها كدليل. وللحصول على قيمة إيجابية لأي معيار، يجب تقديم مواد الأدلة كبيانات. وإذا استوفت البيانات المقدمة

	جميع جوانب المعيار، فإنها تُقبل كمواد أدلة كافية.
المنهجية - أي نوع من أنواع التقييم يُستعمل؟	يصار إلى إدخال كل بلد وتحديثه في الرقم القياسي الوطني للأمن السيبراني (NCSI) على أساس كل حالة على حدة. وبمجرد دخول/تحديث بلد ما، سيقوم الرقم القياسي بعرضه في ترتيب مقارن عالمي.
أسلوب جمع البيانات الأولي	• معلومات المصادر المفتوحة • الوثائق والسجلات • التشريعات والوثائق الرسمية الأخرى • مواقع إلكترونية رسمية
هل لديكم جمع بيانات ثانوية؟	نعم. والرقم القياسي الوطني للأمن السيبراني (NCSI) ليس رقماً ساكناً، لذا فإن جمع البيانات مستمر على مدار العام. • معلومات المصادر المفتوحة • الوثائق والسجلات • التشريعات والوثائق الرسمية الأخرى • مواقع إلكترونية رسمية
ما هي الآليات المُعتمَدة لضمان دقة البيانات التي جُمعت؟	يجب أن تكون جميع مواد الأدلة معلومات علنية ومتاحة للعموم. ولا يمكن إلا للبيانات الرسمية أن تُعتبر مواد أدلة. وتتمثل الأدلة/الإحالات المقبولة في التشريعات القانونية والوثائق الرسمية والمواقع الإلكترونية الرسمية. وعندما يكتمل جمع البيانات، يستعرض المعلومات المقدمة خبيران على الأقل من خبراء الرقم القياسي الوطني للأمن السيبراني. وبعد التفتيش، تنشر مجموعة البيانات على الموقع الإلكتروني للرقم القياسي الوطني للأمن السيبراني (NCSI).
ما هي المخرجات الرئيسية للتقييم؟	• معلومات محدّثة على الصفحات الإلكترونية عن البلدان (بالنسبة للبلدان القائمة في الرقم القياسي الوطني للأمن السيبراني) • صفحات إلكترونية عن البلدان (بالنسبة للبلدان التي لم تُدرَج بعد في الرقم القياسي الوطني للأمن السيبراني) • تصنيف الترتيب وفق الرقم القياسي الوطني للأمن السيبراني (الذي يحدّث كل مرة يجري فيها تحديث الصفحة الإلكترونية لبلد ما)
نسق عرض مخرجات التقييم	• على موقع إلكتروني • أداة العرض المرئي (مع إمكانية مقارنة مجموعات البيانات السابقة أو الحالية لبلد واحد أو بين البلدان) • إمكانية تنزيل الصفحة الإلكترونية لبلد ما بنسق PDF
هل يمكن نشر مخرجات التقييم؟	نعم، دائماً
كيف يمكن النفاذ إلى التقارير السابقة؟	بالنسبة لأي صفحة إلكترونية لبلد معين، يُظهر الرقم القياسي الوطني للأمن السيبراني حالة تحديث معلومات البلد. وتقدم هذه الصفحة عادة أحدث المعلومات المتاحة. ويمكن للزائر الاطلاع على معلومات بشأن التحديث السابق عن طريق اختيار تاريخ تحديث محدد من قائمة منسدلة تُعرف بإيعاز *"اختيار الإصدار" ("Choose a version").*
ما الدليل على التأثير؟	• يبرهن تزايد مشاركة البلدان في الرقم القياسي الوطني للأمن السيبراني على تزايد الاهتمام باستمرار بالرقم القياسي. وقد طلبت فرادى البلدان تقييمات فردية مفصلة منفصلة استناداً إلى الرقم القياسي الوطني للأمن السيبراني، للتأكد من الحالة الراهنة لأمنها السيبراني الوطني وتحسينه. • واستخدم الباحثون الأكاديميون هذه الأداة للعمل على دراسات حالة فردية أو متعددة.
ما هي فوائد إجراء تقييم ما؟	يمكن للبلدان تحديد مستوى استعدادها لمنع التهديدات السيبرانية. ومن خلال السماح بقابلية المقارنة بين البلدان وفرز الدرجات إلى مؤشرات، ويدعم الرقم القياسي الوطني للأمن السيبراني نهجاً عابر للحدود الوطنية وتعاونياً إزاء الأمن السيبراني، تُتبادل فيه أفضل الممارسات بين بلدان متعددة.
هل لديكم عملية	كلا

حساب للترجيحات؟	
هل تعتمدون آلية لإسناد الدرجات و/أو المراتب في تقييمكم؟	نعم - بالنسبة إلى المؤشرات، وبالنسبة إلى درجة الرقم القياسي الوطني للأمن السيبراني (القُطرية)، وبالنسبة إلى مستوى التنمية الرقمية (DDL)، وبالنسبة إلى الفارق (بين درجة الرقم القياسي الوطني للأمن السيبراني ودرجة مستوى التنمية الرقمية). • ولكل رقم قياسي قيمة تبين الأهمية النسبية للمؤشر في الرقم القياسي. وتعطى القيم من فريق الخبراء وفقاً للاعتبارات التالية: نقطة واحدة - لتشريع قانوني ينظم مجالاً محدداً نقطتان إلى ثلاث نقاط - لوحدة متخصصة نقطتان - لنسق رسمي للتعاون نقطة واحدة إلى ثلاث نقاط - نتيجة/منتَج • ويبين تقييم الرقم القياسي الوطني للأمن السيبراني النسبة المئوية التي يحصل عليها البلد من القيمة القصوى للمؤشرات. وتبلغ الدرجة القصوى للرقم القياسي الوطني للأمن السيبراني 100 (100 في المائة) على الدوام بغض النظر عن إضافة أو إزالة المؤشرات. • وبالإضافة إلى درجة الرقم القياسي الوطني للأمن السيبراني، يبين جدول الرقم القياسي أيضاً مستوى التنمية الرقمية (DDL). ويُحسب مستوى التنمية الرقمية وفقاً للرقم القياسي لتنمية تكنولوجيا المعلومات والاتصالات (IDI) والرقم القياسي لجاهزية الشبكة (NRI). ويمثل مستوى التنمية الرقمية النسبة المئوية المتوسطة التي نالها البلد من القيمة القصوى لكلا الرقمين القياسيين. ويبين الفارق العلاقة بين درجة الرقم القياسي الوطني للأمن السيبراني ومستوى التنمية الرقمية. وتَظهر نتيجة إيجابية إذا واكب تطور الأمن السيبراني في البلد تطوره الرقمي أو سبقه. وتُظهر نتيجة سلبية تقدم المجتمع الرقمي للبلد على أمنه السيبراني الوطني.

التفاصيل

ما هي الأسئلة الرئيسية التي يمكن أن تساعد الأداة في الإجابة عليها؟	• كيف أعد بلدي لمواجهة هجوم/تهديد سيبراني؟ • ما الذي ينقص بلدي للوقاية من التهديدات السيبرانية؟ • ما هي المؤسسات المناسبة لهذه المهمة؟ • كيف يمكننا مواصلة تحسين تأهبنا لمواجهة التهديدات السيبرانية المتغيرة؟ • ما هي بعض الممارسات الفضلى في العالم التي يمكننا تكييفها لأغراضنا و/أو تنفيذها؟
في أي مرحلة من دورة حياة الاستراتيجية ينبغي إجراء التقييم؟	يمكن أن يحدث التقييم (تحليل البلد) في أي مرحلة من دورة حياة الاستراتيجية كي يواكب الرقم القياسي الوطني للأمن السيبراني أحدث المعلومات قدر الإمكان. ولكن يوصى لفرادى البلدان بمرحلة (مراحل) "التمهيد" و"التقدير والتحليل" أو "المراقبة والتقييم".
كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟	كيف يساعد التقييم في مواءمة الأنشطة الأخرى؟ يساعد الرقم القياسي الوطني للأمن السيبراني على التعرف على مواطن القوة والضعف النسبيين في مستوى تأهب البلد لدرء التهديدات السيبرانية، ويحدد بالتالي أين يمكن أن يلزم دعم إضافي في مجال بناء القدرات، أو المجالات التي يمكنه فيها أن يقدم الدعم للآخرين. وكذلك تقدم الصفحات الإلكترونية القُطرية في الرقم القياسي الوطني للأمن السيبراني أفضل الممارسات على الصعيد الوطني التي يمكن للبلدان الأخرى تكييفها/تنفيذها بمساعدة أو بدون مساعدة من جهات مانحة. أو منظمات دولية وما إلى ذلك.
ما الدور الذي يقوم به التقييم في عملية إقامة صلة الوصل مع المنتدى العالمي للخبرات السيبرانية (GFCE)؟	بما أن الرقم القياسي الوطني للأمن السيبراني يعرض معلومات متاحة للعموم تتاح للممولين والمنفذين رؤية مواطن القوة والضعف النسبية في بلد ما. وبالتالي، فقد يتواصلون مع هذه البلدان لاقتراح بناء القدرات السيبرانية أو أنشطة وتحسينات مماثلة، حيثما تدعو الحاجة إليها.
ما هي دراسات الحالة أو التزكيات المتاحة فيما يتعلق بفوائد الأداة؟	استعراض الحالة: سلامة وأمن الفضاء السيبراني والديمقراطية الإلكترونية في بلدان الشراكة الشرقية (2017) بواسطة أكاديمية الحوكمة الإلكترونية
ما هي الآليات التي تضمن	يتأكد فريقنا من صحة المساهمات الواردة من البلدان المساهمة إلى الرقم القياسي الوطني للأمن

استقلالية ونزاهة وحياد النتائج التي تتوصلون إليها؟	السيبراني على نحو مستقل.
ترجى إضافة أي معلومات إضافية	**كتيب إرشادي:** • الأمن السيبراني الوطني في الممارسة العملية (2020) صادر عن أكاديمية الحوكمة الإلكترونية **مدونة إلكترونية صوتية/مقال:** • ماذا ينبغي للحكومات أن تفعل لتأمين الفضاء السيبراني الوطني لديها؟ (2020) من أكاديمية الحوكمة الإلكترونية • الرقم القياسي الوطني للأمن السيبراني - ما مدى استعداد بلدكم للتصدي لهجوم سيبراني؟ (2020) من أكاديمية الحوكمة الإلكترونية • ما هي النظافة السيبرانية؟ (2020) من أكاديمية الحوكمة الإلكترونية **مقال:** • 160 بلداً في الرقم القياسي الوطني للأمن السيبراني (العوائق والدروس المستفادة والوقائع المثيرة للاهتمام (2020) من أكاديمية الحوكمة الإلكترونية.

نظرة عامة على الأدوات

	أداة بناء القدرات لمكافحة الجريمة السيبرانية	نضج الأمن السيبراني في منطقة آسيا والمحيط الهادئ	CRI	CMM	CSDI	GCI	NCAF	NCSI
السياسات والاستراتيجيات								
الاستراتيجيات	●	●	●	●	●	●	●	●
التقييمات	●	●	●	●	●	●	●	●
تدابير وأعراف بناء الثقة		●	●	●		●	●	
الدبلوماسية السيبرانية		●	●	●		●	●	●
القانون الدولي في الفضاء السيبراني	●	●	●					
إدارة الحوادث وحماية البنية التحتية الحرجة للمعلومات (CIIP)								
الاستجابة لحوادث الأمن الحاسوبي الوطنية	●	●	●	●	●	●	●	●
التقاط الحوادث وتحليلها			●	●		●	●	●
تمارين الأمن السيبراني			●	●		●	●	●
حماية البنى التحتية الحرجة للمعلومات	●	●	●	●	●	●	●	●
الجريمة السيبرانية								
الأطر القانونية/قانون الجريمة السيبرانية	●	●	●	●	●	●	●	●
إنفاذ القوانين في الفضاء السيبراني.	●	●	●	●	●	●	●	●
التدريب في مجال الجريمة السيبرانية	●		●	●	●	●	●	
منع الجريمة السيبرانية	●		●	●	●	●	●	●
الثقافة والمهارات								
الوعي بالأمن السيبراني	●	●	●	●	●	●	●	●
التعليم والتدريب	●	●	●	●	●	●	●	●
تنمية القوى العاملة	●	●	●	●	●	●	●	●
المعايير								
المعايير الدولية أو الوطنية			●	●	●	●	●	●