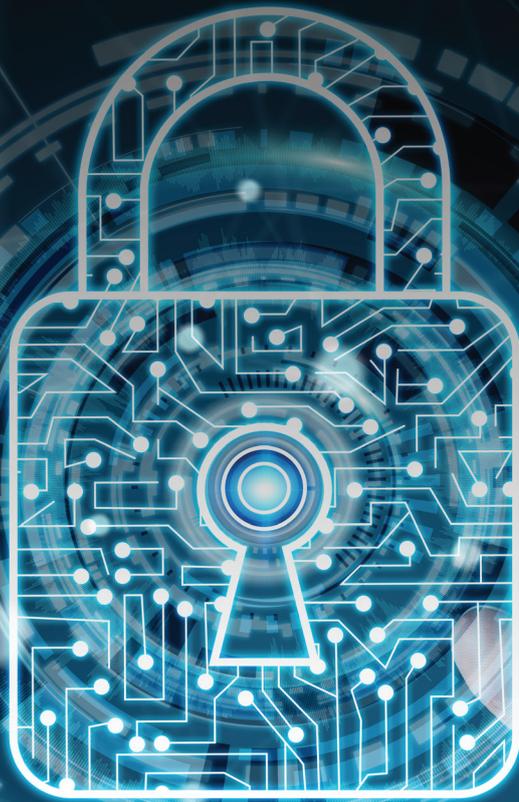


الرقم القياسي العالمي للأمن السيبراني

لعام 2020



الرقم القياسي العالمي للأمن السيبراني لعام 2020

قياس الالتزام بالأمن السيبراني



شكر وعرفان

الرقم القياسي العالمي للأمن السيبراني (GCI) هو مبادرة للاتحاد الدولي للاتصالات (ITU)، وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT)، تم تشكيلها وتحسينها من خلال عمل مجموعة متنوعة من الخبراء والمساهمين في البلدان والمنظمات الدولية الأخرى. ويود الاتحاد أن يعرب عن تقديره وشكره لجميع الشركاء والمساهمين على عملهم الجاد والتزامهم بتقديم الدعم لهذه المبادرة، والأهم من ذلك، المساعدة في تعزيز فهمنا الجماعي لالتزامات الأمن السيبراني.

ويود الاتحاد أن يسلم الضوء بوجه خاص على المساهمات الواردة من خلال لجنة الدراسات 2 لقطاع تنمية الاتصالات، وفريق التشاور لإدارة مكتب تنمية الاتصالات (BDT)، وعملهما المتعلق بإدخال تغييرات على الاستبيان الخاص بالرقم القياسي. ويود الفريق المعني بالأمن السيبراني في مكتب تنمية الاتصالات أن يشكر أعضاء الاتحاد على ترشيحاتهم للخبراء لتقديم المشورة في عملية الترجيح. ويود في المنهجية مزيد من المعلومات بشأن عملية الترجيح ومشاركة الخبراء. وقدمت مساهمات الخبراء التالية أسماؤهم من أعضاء الاتحاد دعماً قيماً في تحديد القيم الترجيحية:

السيد عبد العزيز الزرعوني (هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA)، الإمارات العربية المتحدة)، والبروفيسور ماركو جيرك (معهد أبحاث الجرائم السيبرانية، ألمانيا)، والسيدة ميليسا هاثاواي (معهد بوتوماك (Potomac) للدراسات السياسية، الولايات المتحدة الأمريكية)، والسيدة فانيسا كوبيتي كرافو (ANATEL، البرازيل)، والسيد سكوت جيمس شاكلفورد (جامعة إنديانا، برنامج الأمن السيبراني وإدارة الإنترنت، الولايات المتحدة الأمريكية)، والسيد غيريك غونكاليس (ANSSI، بنن)، والمهندس إمانويل ثيكيسو (هيئة تنظيم الاتصالات في بوتسوانا (BOCRA)، بوتسوانا)، والسيد دلاميني (وزارة تكنولوجيا المعلومات والاتصالات، إسواتيني)، والسيد فيليمون جوهانس (وزارة تكنولوجيا المعلومات والاتصالات، ناميبيا)، والسيد بالاكيم أسيه (Cyber Defense Africa S.A.S، توغو)، والسيد نوا ج. ساماتيبيلي (هيئة تكنولوجيا المعلومات والاتصالات في زامبيا (ZICTA)، زامبيا)، والسيد غونزالو دياز دي فالديس أولافاريتا (شيلي)، والسيدة جيسيكا ماتشادو ألفاريز (إدارة كوبا، كوبا)، والمهندسة راكيل بينيا (فنزويلا)، وميترو جاكوبو بيلو خويأ (الحرس الوطني لأمانة الأمن وحماية المواطنين، المكسيك)، والسيد رينزو زيغارا (وزارة النقل والاتصالات، بيرو)، والسيد جونيور ماكتاير (اتحاد الاتصالات الكاريبي (CTU)، ترينيداد وتوباغو)، والسيد فرناندو هيرنانديز، هيئة تنظيم الاتصالات في أوروغواي، أوروغواي)، والسيدة آن-راشيل إنيه (المكتب الأمريكي لتسجيل أرقام الإنترنت (ARIN)، الولايات المتحدة الأمريكية)، والسيد محمد عوده سلمان (الأردن)، والسيدة ندى خاطر (وزارة الاقتصاد الرقمي والريادة، الأردن)، والسيد يوسف أحمد بهيجي (وزارة المواصلات والاتصالات، مملكة البحرين)، والسيدة عزيزة الراشدي (وزارة النقل والاتصالات وتقنية المعلومات، عُمان)، والسيد عبد الرحمن الحسن (الهيئة الوطنية للأمن السيبراني (NCA)، المملكة العربية السعودية)، والمهندس محمد علوي (وزارة الاتصالات وتكنولوجيا المعلومات، دولة فلسطين)، والسيد خليلي أورهمان كيبزوي (سلطة إصدار الشهادات الجذرية (ARCA)، أفغانستان)، والسيد نصرت الله غافوري (سلطة إصدار الشهادات الجذرية (ARCA)، أفغانستان)، والسيدة شو مينغ (وزارة المعلومات والتكنولوجيا، الفريق الوطني للاستجابة لطوارئ الشبكة الحاسوبية، الصين)، والسيدة وان شينشين (وزارة المعلومات والتكنولوجيا، الفريق الوطني للاستجابة لطوارئ الشبكة الحاسوبية، الصين)، والسيدة كاثرين م. سوبهياداس (إدارة الاتصالات، فيجي)، وبوان ليانا شوهايمان (وزارة الاتصالات والوسائط المتعددة، ماليزيا)، والسيد بوان نور الدين هاني حسين (وزارة الاتصالات والوسائط المتعددة، ماليزيا)، والسيد يان نونغ سو (المركز الوطني للأمن السيبراني، إدارة تكنولوجيا المعلومات والأمن السيبراني، ميانمار)، والسيد جاكرا بونغ شافونغ، وزارة الاقتصاد والمجتمع الرقمي، تايلاند)، والسيد آن أوليغوفيتش خوبايف (دائرة أمن المعلومات، روسيا)، والسيد أندريه سيرجيفيتش جيفوف (دائرة أمن المعلومات، روسيا)، والسيد إغيز توراغانبايف (اللجنة الحكومية لتكنولوجيا المعلومات والاتصالات في قيرغيزستان، جمهورية قيرغيزستان)، والسيد محمدان أليمكولوف (اللجنة الحكومية لتكنولوجيا المعلومات والاتصالات في قيرغيزستان، جمهورية قيرغيزستان)، والسيد فلاديمير يوريفيتش شورين (دائرة أمن المعلومات في خدمة الأمن في المؤسسة الجمهورية الموحدة، بيلاروس)، والسيد نستوراس شولياراس (الأمانة العامة لوزارة الاتصالات والبريد للإدارة الرقمية، اليونان)، والسيدة إيغليه فاسيلياوسكايت (وزارة الدفاع الوطني في جمهورية ليتوانيا، ليتوانيا)، والسيد تاداس شاكوناس (وزارة الدفاع الوطني في جمهورية ليتوانيا، ليتوانيا)، والسيدة رادوجا (صربيا)، والسيد ماتييه سالميك (المركز الوطني للأمن السيبراني SK-CERT، سلوفاكيا)، والسيد راتيسلاف جانوتا (المركز الوطني للأمن السيبراني SK-CERT، سلوفاكيا)، والسيد إيدان مورشلاند (المملكة المتحدة)، والسيد ميغيل بينتو (BitSight، الولايات المتحدة الأمريكية)، والسيد نونيل بانتجواتي (إندونيسيا)، والسيدة إنتان راهايو (إندونيسيا)، والسيد ماما كيرييه جونغا (فريق الاستجابة للحوادث الأمنية الحاسوبية في غامبيا (gmCSIRT)، غامبيا)، والسيدة بانثال غوفو (كينيا)، والسيدة سونام شوكي (دائرة تكنولوجيا المعلومات والاتصالات، بوتان)، والسيد عقيل طه سعدون (أمانة تكنولوجيا المعلومات والاتصالات، العراق)، والسيد ثائر كاظم علي (CERTIraq، العراق).

ويود فريق الأمن السيبراني التابع للاتحاد أن يتوجه بالشكر إلى جهات الاتصال المعنية بالرقم القياسي العالمي للأمن السيبراني التي قامت بجمع البيانات من مختلف بلدانها بشأن التزامات الأمن السيبراني. وما كان لهذا التقرير أن يرى النور بدون جهات الاتصال القطرية المعنية بالرقم القياسي.

والفريق ممتن للعديد من الزملاء والمتدربين في الاتحاد الذين قدموا الدعم لإعداد هذا التقرير. ويعتذر الفريق لأي فرد أو منظمة أسقطت سهواً من هذه القائمة ويعرب عن امتنانه لكل من ساهم في الرقم القياس العالمي للأمن السيبراني. ويرجى الاتصال بفريق الأمن السيبراني التابع للاتحاد من خلال عنوان البريد الإلكتروني التالي gci@itu.int فيما يخص أي تعليقات أو استفسارات تتعلق بهذا المنشور. © الاتحاد الدولي للاتصالات (ITU)، 2021. جميع حقوق النشر محفوظة. لا يجوز استنساخ أي جزء من هذا المنشور بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

إخلاء مسؤولية

التسميات المستخدمة في هذا المنشور وطريقة عرض المواد فيه لا تعني بأي حال من الأحوال التعبير عن أي رأي من جانب الاتحاد الدولي للاتصالات فيما يتعلق بالوضع القانوني لأي من البلدان أو الأقاليم أو المدن أو المناطق أو لسلطاتها، أو فيما يتعلق بتعيين حدودها أو تخومها. والإشارة إلى شركات محددة أو منتجات صناعية معينة لا تعني أن الاتحاد الدولي للاتصالات يدعمها أو يوصي بها تفضيلاً لها على غيرها من الشركات والمنتجات المماثلة لها التي لم يشر إليها. عدا ما يتعلق بالخطأ والسهو، يشار إلى المنتجات المسجلة الملكية بالأحرف الأولية من أسمائها بالإنكليزية.

اتخذ الاتحاد الدولي للاتصالات جميع الاحتياطات المعقولة للتحقق من المعلومات الواردة في هذا المنشور. ومع ذلك، توزع المواد المنشورة دون أي ضمان من أي نوع، سواء كان صريحاً أو ضمناً. وتقع مسؤولية تفسير المواد واستعمالها على عاتق القارئ. والآراء والنتائج والاستنتاجات المعرب عنها في هذا المنشور لا تعبر بالضرورة عن وجهات نظر الاتحاد الدولي للاتصالات أو أعضائه.

:ISBN

978-92-61-33926-5 (نسخة إلكترونية)

978-92-61-33936-4 (نسخة EPUB)

978-92-61-33946-3 (نسخة Mobi)



أصبحت الحاجة إلى فضاء سيبراني آمن ومأمون أكثر أهمية من ذي قبل، خاصة وأنا نعتمد جميعاً على "شرايين الحياة الرقمية" بشكل متزايد. وكان أحد أكبر التحديات التي طرحتها جائحة كوفيد-19 إيجاد طرق للتواصل بشكل مفيد مع بعضنا البعض، بالرغم من عدم اليقين والقلق والتغيير. وحتى قبل تفشي الجائحة، كان الأمن السيبراني ضرورياً للحفاظ على سلامتنا على الإنترنت حتى تتمكن من القيام بالمهام اليومية الحاسمة.

ولقد ألهمتني قدرة الناس على التكيف مع هذه البيئة غير المؤكدة واستخدامهم للتكنولوجيا لإيجاد حلول مبتكرة. وواجهت العديد من المنظمات، بما في ذلك الاتحاد الدولي للاتصالات، تحديات جديدة ناجمة عن العمل عن بُعد. ويرتبط الأمن السيبراني بشكل أساسي بالعمل عن بُعد، بدءاً من إدارة المشاركين في المكالمات الفيديوية إلى التأكد من تقاسم الوثائق بأمان. ولذلك، واصل الاتحاد العمل مع البلدان لتحقيق المزيد من الكفاءة والفعالية وإحداث الأثر في المجالات التي تشتد فيها الحاجة إلى خدماتنا.

وعندما أطلق الرقم القياسي العالمي للأمن السيبراني لأول مرة في 2015، لم يكن بوسع سوى عدد قليل من الناس تصور الوضع الذي نجد فيه أنفسنا حالياً. ومن شأن هذه الصيغة الأخيرة للرقم القياسي أن يساعد في تعزيز المزيد من الإجراءات الرامية إلى تأمين الأنظمة الإيكولوجية الرقمية اللازمة للتعافي والنمو، من خلال قياس أنواع التزامات الأمن السيبراني التي تعهدت بها البلدان ومدى انتشارها.

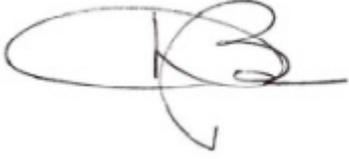
وتكشف عملية إعداد هذه الصيغة أن العديد من البلدان تحرز تقدماً في التزاماتها بالاستجابة لتحديات الأمن السيبراني، على الرغم من الجهات الفاعلة التي استفادت من رغبتنا في الحصول على المعلومات، ومخاوفنا بشأن الوباء، والتحول إلى العمل من المنزل والتعلم عن بُعد، والاعتماد على أنظمة الرعاية الصحية، وأكثر من ذلك.

ويبين تقرير الرقم القياسي العالمي للأمن السيبراني أن العديد من البلدان سنت تشريعات ولوائح جديدة بشأن الأمن السيبراني لمعالجة مجالات مثل الخصوصية والنفوذ غير المصرح به والسلامة على الإنترنت. ويؤكد أيضاً الحاجة إلى وضع استراتيجيات وآليات لتنمية القدرات ومساعدة الحكومات والشركات على الاستعداد بشكل أفضل للمخاطر السيبرانية المتزايدة والتخفيف من أثارها. وأكثر من نصف بلدان العالم لديها الآن فريق استجابة للحوادث الحاسوبية (CIRT) وما يقرب ثلثي البلدان لديها شكل من أشكال الاستراتيجيات الوطنية للأمن السيبراني التي توجه وضعها العام في مجال الأمن السيبراني.

ويكشف الرقم القياسي العالمي للأمن السيبراني أن الأمن السيبراني قضية إنمائية حقاً وأن هناك حاجة ملحة لمعالجة فجوة القدرات السيبرانية المتزايدة بين البلدان المتقدمة والبلدان النامية من خلال تعزيز المعارف والارتقاء بالمهارات وبناء الكفاءات. ونحن بحاجة إلى سد هذه الفجوة من خلال بحث جذورها وتنمية القدرات من حيث البنية التحتية الرقمية والمهارات الرقمية والموارد في العالم النامي.

وآمل أن يظل الرقم القياسي العالمي للأمن السيبراني أداة مفيدة لتنمية قدرات الحكومات وواضعي السياسات وخبراء الأمن السيبراني والهيئات الأكاديمية في تحديد مجالات التحسين وتبسيط الضوء على أفضل الممارسات لتعزيز الأمن السيبراني على الصعيد الوطني.

وأود أن أشكر البلدان على مشاركتها ومساهمتها القيمة في هذا الجهد، ولا سيما مشاركتها أثناء وضع هذه الصيغة وجمع البيانات والتحقق منها. كما أود أن أشكر جميع المشاركين في عملية لجان الدراسات على دعمهم وتوجيههم. وأدعو جميع الدول الأعضاء في الاتحاد إلى الاستمرار في موافاتنا بمعلومات محدّثة عما تُحرزه من تقدم في تنفيذ التزاماتها في مجال الأمن السيبراني، ليتسنى لنا تبادل الاطلاع على الخبرات والأبحاث والحلول تبادلاً فَعَّالاً من أجل تهيئة فضاء سيبراني يثق به الجميع.



دورين بوغدان-مارتن
مديرة مكتب تنمية الاتصالات بالاتحاد

ملخص تنفيذي

أطلق الاتحاد الدولي للاتصالات (ITU) الرقم القياسي العالمي للأمن السيبراني (GCI) لأول مرة في 2015 لقياس الالتزامات التي قطعتها 193 دولة عضواً في الاتحاد ودولة فلسطين¹. في مجال الأمن السيبراني لمساعدتهما في تحديد مجالات التحسين وتشجيع البلدان على اتخاذ الإجراءات اللازمة، من خلال إذكاء الوعي بحالة الأمن السيبراني في جميع أرجاء العالم. ومع تطور مخاطر الأمن السيبراني وأولوياته وموارده، تكيف الرقم القياسي أيضاً لإعطاء لمحة أدق عن تدابير الأمن السيبراني التي تتخذها البلدان.

ويهدف هذا التقرير إلى فهم أفضل لالتزامات البلدان تجاه الأمن السيبراني، وتحديد الفجوات، وتشجيع دمج الممارسات الجيدة، وتوفير رؤى مفيدة للبلدان لتحسين أوضاع الأمن السيبراني لديها.

وأفادت البلدان باستخدام الرقم القياسي لتيسير ما يلي:

- المناقشات من خلال المنتديات المنشأة رسمياً والتي تمكن من إجراء تقييمات ذاتية وتنسيق أفضل؛
 - جمع الرؤى حول المبادرات الوطنية الشاملة والموارد المستخدمة لإدارة الأمن السيبراني على المستوى الوطني؛
 - المقارنة مع الممارسات الجيدة والشركاء والجيران الإقليميين؛
 - زيادة الوعي بين مختلف أصحاب المصلحة بشأن احتياجات التنسيق على المستوى الوطني.
- تبيّن نتائج الرقم القياسي تحسناً وتعزيزاً شامليين لجميع الركائز الخمس لبرنامج الأمن السيبراني، بيد أن الفجوات الإقليمية في القدرات السيبرانية لا تزال قائمة. وأبرز التقرير الممارسات التوضيحية التي تتبعها البلدان.

البلدان التي خضعت للقياس	سنة التجميع	جهات الاتصال من البلدان	الاستبيانات المقدمة	متوسط نمو النتيجة الإجمالية منذ 2018
194	2020	169	150	9,5%



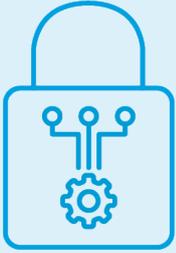
يقابل الرقم القياسي 82 سؤالاً عن التزامات الدول الأعضاء في مجال الأمن السيبراني من خلال خمس ركائز:

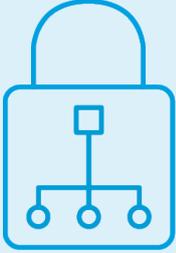
- التدابير القانونية؛
- التدابير التقنية؛
- التدابير التنظيمية؛
- تدابير تنمية القدرات؛
- التدابير التعاونية.

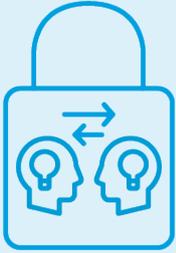
يبين الجدول أدناه الالتزامات العالمية بمؤشرات محددة لكل ركيزة.

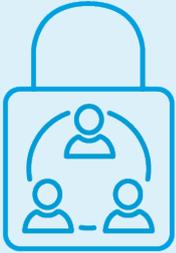
¹ تشارك دولة فلسطين في أعمال الاتحاد الدولي للاتصالات بموجب القرار 99 (المراجع في دي، 2018) الصادر عن مؤتمر المندوبين المفوضين.

التدابير القانونية		قياس القوانين واللوائح المتعلقة بالجريمة السيبرانية والأمن السيبراني	
167	بلداً لديها شكل من أشكال تشريعات الأمن السيبراني		
133	لائحة بشأن حماية البيانات		
97	لائحة بشأن البنية التحتية الحيوية		

التدابير التقنية		قياس تنفيذ القدرات التقنية من خلال الوكالات الوطنية والقطاعية	
131	فريقاً من الأفرقة الوطنية للحوادث الحاسوبية النشطة		
104	أفرقة مشاركة في فريق إقليمي للاستجابة للحوادث الحاسوبية		
101	آلية إبلاغ عن حماية الأطفال عبر الإنترنت		

التدابير التنظيمية		قياس الاستراتيجيات والمنظمات الوطنية التي تنفذ الأمن السيبراني	
127	استراتيجية وطنية للأمن السيبراني		
136	وكالة للأمن السيبراني		
86	استراتيجية ومبادرة بشأن حماية الأطفال على الإنترنت تم الإبلاغ عنها		

تنمية القدرات		قياس حملات التوعية، والتدريب والتعليم والحوافز لتنمية القدرات في مجال الأمن السيبراني	
142	بلداً يقوم بمبادرات التوعية السيبرانية		
94	بلداً لديه برامج خاصة بالبحث والتطوير في مجال الأمن السيبراني		
98	بلداً يبلغ عن وجود صناعات وطنية في مجال الأمن السيبراني		

التعاون		قياس الشراكات بين الوكالات والشركات والبلدان	
166	بلداً منخرطاً في شراكات بين القطاعين العام والخاص في مجال الأمن السيبراني		
90	بلداً لديه اتفاقات ثنائية بشأن الأمن السيبراني		
112	بلداً لديه اتفاقات متعددة الأطراف بشأن الأمن السيبراني		

تغييرات في الرقم القياسي العالمي للأمن السيبراني تؤثر على النتائج

- تستند هذه الطبعة من الرقم القياسي العالمي للأمن السيبراني إلى البيانات المبلغ عنها من الدول الأعضاء بمستوى مشاركة قياسي، من 105 ردود في صيغة الفترة 2013-2014 إلى 150 استبياناً في 2020.
- تم تحديث الاستبيان الخاص بالرقم القياسي. وأعيد تحديد الأسئلة أو إضافتها أو إزالتها في كل من الركائز الخمس (القانونية والتقنية والتنظيمية وتنمية القدرات والتدابير التعاونية) للتعبير عن التغييرات في المخاوف والجهود المتعلقة بالأمن السيبراني. والتغييرات التي أدخلت على الاستبيان لها تأثير على النتائج، حيث تشكل أحد العوامل في درجات البلدان وترتيبها.
- تختلف عملية الترجيح عن الصيغ السابقة، ما يبرز التغييرات بشكل جزئي في هيكل الأسئلة فضلاً عن إضافة أسئلة وحذف أخرى.
- استندت ترجيحات المؤشرات إلى توصيات الخبراء. وعيّن أعضاء الاتحاد خبراء لتقديم المشورة في عملية الترجيح لتخصيص القيم الترجيحية للمؤشرات على أساس الأهمية النسبية للأمن السيبراني. ويمكن أن تؤثر الاختلافات في تخصيص القيم الترجيحية على درجات البلدان وترتيباتها.
- وأعد قسم لتقديم مزيد من المعلومات عن بناء استبيان الرقم القياسي وتكوينه والتغييرات الأخيرة التي أدخلت عليه (الملحق A).
- العديد من البلدان، وخاصة أعلى البلدان أداءً، متقاربة بشكل متزايد من حيث الدرجات، وهذا هو السبب في ضرورة تفسير الرتب الفردية بعناية.
- رفضت بعض البلدان التحقق من البيانات المجمعة أو المشاركة في هذه الطبعة من الرقم القياسي العالمي للأمن السيبراني. وينبغي ألا تعتبر البيانات المتعلقة بهذه البلدان (التي تحمل علامة *) بيانات معتمدة رسمياً من أي ممثل عن ذلك البلد. وبما أن هذه البيانات جمعت من خلال البحث عبر الإنترنت، كان من الضروري أن تُفسر العناصر الناقصة على أنه لم يتم العثور عليها بدلاً من كونها غير موجودة.
- وبالإضافة إلى ذلك، ربما أثرت مشاركة البلدان إيجاباً على النتائج في بعض الحالات، حيث إنه كلما زادت مساهمة بلد ما في الاستبيان، زاد احتمال الحصول على ردود إيجابية.
- وهناك العديد من المجالات التي تتفوق فيها البلدان، والمجالات التي يوجد فيها مجال لتعزيز الجهود، وينبغي عدم تشجيع البلدان على التركيز على التصنيفات.
- وبالنسبة إلى البلدان التي لم تقدم ردوداً على الاستبيان، أجريت بحوث مكتبية من خلال المعلومات المتاحة للجمهور في المواقع الإلكترونية الرسمية وغيرها من الموارد. وبالنسبة إلى البلدان التي أجريت بحوث مكتبية بشأنها، قد لا تعبر البيانات المجمعة بدقة عن وضع الأمن السيبراني في البلاد. ولا يحتوي الرقم القياسي على بيانات تقديرية.

جدول المحتويات

ii	شكر وعرفان
iv	تمهيد
vi	ملخص تنفيذي
x	قائمة بالجدول والأشكال
1	الرقم القياسي العالمي للأمن السيبراني: الخلفية والسياق
2	المواضيع الرئيسية
2	التدابير القانونية: التخطيط للتدخلات المستقبلية
2.2	التدابير التقنية: زيادة نشر أفرقة الاستجابة للحوادث الحاسوبية (CIRT)/أفرقة مواجهة الطوارئ الحاسوبية (CERT)
3.2	التدابير التنظيمية: مواءمة الاستراتيجية
4.2	تدابير تنمية القدرات: تنمية القدرات في مجال الأمن السيبراني
5.2	التدابير التعاونية: معالجة إجراءات الأمن السيبراني الجماعية
6.2	حماية الأطفال على الإنترنت
7.2	خلاصة
3	نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتبات
1.3	الدرجات والمرتبات العالمية للبلدان
2.3	الدرجات والمرتبات الإقليمية للبلدان
4	الرقم القياسي العالمي للأمن السيبراني: الموجزات القطرية
32	منطقة إفريقيا
54	منطقة الأمريكتين
72	منطقة الدول العربية
83	منطقة آسيا والمحيط الهادئ
102	منطقة كومنولث الدول المستقلة
107	أوروبا
130	مسرد المصطلحات
131	الملحق A: المنهجية
137	الملحق B: الرقم القياسي العالمي للأمن السيبراني (الطبعة الرابعة)

قائمة بالجدول والأشكال

الجدول

- الجدول 1: عدد البلدان التي لديها استراتيجية وطنية للأمن السيبراني وفريق CIRT.....10
- الجدول 2: البلدان المشاركة في شراكات دولية و/أو محلية بين القطاعين العام والخاص21
- الجدول 3: نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتببات.....24
- الجدول 4: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة إفريقيا.....27
- الجدول 5: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة الأمريكتين.....28
- الجدول 6: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة الدول العربية.....29
- الجدول 7: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة آسيا-المحيط الهادئ.....29
- الجدول 8: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة كومونولث الدول المستقلة.....30
- الجدول 9: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة أوروبا.....30
- الجدول A1: المشاركة في الرقم القياسي العالمي للأمن السيبراني وسنوات جمع البيانات.....131
- الجدول A2: وصف ركائز الرقم القياسي العالمي للأمن السيبراني لعام 2020.....132
- الجدول B1: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير القانونية.....137
- الجدول B2: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التقنية.....141
- الجدول B3: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التنظيمية.....144
- الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات.....146
- الجدول B5: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التعاونية.....150

الأشكال

- الشكل 1: البلدان التي لديها تشريعات لحماية البيانات.....2
- الشكل 2: البلدان التي اتخذت تدابير الإخطار بالخرق.....3
- الشكل 3: البلدان التي لديها تشريعات بشأن سرقة المعلومات الشخصية.....3
- الشكل 4: تشريعات بشأن سرقة الهوية وحماية البيانات والخصوصية، على مستوى النفاذ إلى الإنترنت (النسبة المئوية للسكان).....4
- الشكل 5: تشريعات بشأن النفاذ غير القانوني.....4
- الشكل 6: البلدان التي لديها تشريعات بشأن التحرش عبر الإنترنت.....5
- الشكل 7: عدد البلدان التي لديها أفرقة وطنية للاستجابة للحوادث الحاسوبية.....6
- الشكل 8: عدد أفرقة CIRT الخاصة بقطاع معيّن.....7
- الشكل 9: البلدان التي تعالج قضايا البنية التحتية الحيوية والقدرة على الصمود.....9
- الشكل 10: مستعملو الإنترنت (حسب التغطية بفريق استجابة للحوادث الحاسوبية واستراتيجية وطنية للأمن السيبراني).....9
- الشكل 11: حجم السكان غير الموصولين (حسب التغطية بفريق استجابة للحوادث الحاسوبية واستراتيجية وطنية للأمن السيبراني).....10
- الشكل 12: تقييم دورة الحياة كجزء من الاستراتيجية الوطنية للأمن السيبراني.....11
- الشكل 13: عمليات مراجعة الأمن السيبراني التي تجري على الصعيد الوطني.....11
- الشكل 14: مقاييس لتقييم المخاطر المرتبطة بالفضاء السيبراني على الصعيد الوطني.....12

- الشكل 15: الرقم القياسي العالمي للأمن السيبراني وغير الموصولين 13
- الشكل 16: أهداف التنمية المستدامة (8، 9، 10) 13
- الشكل 17: درجة حملات التوعية العامة بالأمن السيبراني (لكل بلد مقارنة مع انتشار الإنترنت) 14
- الشكل 18: عدد البلدان التي لديها حملات توعية بشأن الأمن السيبراني تستهدف الشركات الصغيرة والمتوسطة والقطاع الخاص والوكالات الحكومية 15
- الشكل 19: عدد البلدان التي لديها برامج تعليمية/دورات تدريب محددة من أجل المهنيين العاملين في مجال الأمن السيبراني 16
- الشكل 20: عدد البلدان التي تنفذ دورات في مجال الأمن السيبراني في المناهج الأكاديمية الوطنية (حسب مرحلة التعليم) 17
- الشكل 21: عدد البلدان التي لديها آلية تحفيزية لتنمية القدرات في مجال الأمن السيبراني 18
- الشكل 22: البلدان المشاركة في اتفاقات ثنائية بشأن الأمن السيبراني 19
- الشكل 23: البلدان التي لديها اتفاق ثنائي بشأن الأمن السيبراني (حسب المواضيع المشمولة) 19
- الشكل 24: عدد البلدان المشاركة في اتفاقات الأمن السيبراني المتعددة الأطراف (الموقعة والمصدق عليها) 20
- الشكل 25: المشاركة في الأنشطة الدولية 20
- الشكل 26: تقارير من سلسلة الاتحاد الخاصة بحماية الأطفال على الإنترنت 21
- الشكل 27: البلدان التي لديها استراتيجية لحماية الأطفال على الإنترنت 22

1 الرقم القياسي العالمي للأمن السيبراني: الخلفية والسياق

تأتي الصيغة الرابعة للرقم القياسي العالمي للأمن السيبراني (GCI) في وقت مختلف تماماً عن سابقه. وعندما أُطلق البرنامج العالمي للأمن السيبراني لأول مرة في 2007، كان أول هاتف iPhone على بعد شهر واحد من إصداره ولم يكن فيسبوك مفتوحاً إلا للمستعملين من خارج الجامعات في الولايات المتحدة لمدة عام فقط. وكان هناك مليار شخص موصولين بالإنترنت وكانت هناك مخاوف من تجاوز كمية البيانات المستحثة البالغة 255 إكسابايت التخزين المتاح¹ واليوم، أعادت الهواتف الذكية تشكيل الحياة اليومية، وأصبحت وسائل التواصل الاجتماعي جزءاً لا يتجزأ من مجال المجتمع الأوسع. وفي الوقت الحالي، هناك 3,5 مليار شخص موصولين بالإنترنت ويقدر العالم الرقمي بنحو 44 زيتابايت، مع انعدام خطر التخزين غير المتاح بفضل الحوسبة السحابية² وبالإضافة إلى ذلك، أثر انتشار تكنولوجيا المعلومات والاتصالات على النظام الإيكولوجي الوطني الأوسع مما بث الحياة في إمكانيات تنظيمية جديدة مثل خدمات الحكومة الإلكترونية والنماذج الاقتصادية والإنتاجية الجديدة مثل الصناعة 4.0 والاقتصاد الرقمي الأوسع.

وتتأثر جميع البلدان إلى حد ما بالفجوة الرقمية، وينبغي أن يحظى الأمن السيبراني بأولوية عالية كعامل تمكين رئيسي للاقتصاد والمجتمع والحكومة التي تعتمد على الأنظمة الرقمية.

وقد أثرت جائحة كوفيد-19 تأثيراً شديداً على كيفية عمل المجتمعات. ومع بدء انتشار الجائحة في أبريل 2020، أشارت شركة Akamai إلى زيادة حركة الإنترنت بنسبة 30 في المائة³ وتؤدي التكنولوجيا دوراً رئيسياً في الحفاظ على توصيل الناس، من العمل عن بُعد إلى التعلم عن بُعد ولكي يحقق العصر الرقمي إمكاناته، يجب أن يكون الفضاء السيبراني الموثوق والأمن عنصراً أساسياً. وبعد مرور عام على إعلان منظمة الصحة العالمية عن أن كوفيد-19- جائحة وتطوير أنظمة إدارة ولقاحات جديدة، يستمر اعتمادنا على التكنولوجيات الرقمية في النمو. وبما أن العالم يوصل غير الموصولين، يجب ضمان فضاء سيبراني آمن وجدير بالثقة.

وثمة اعتراف متزايد بخطر الأمن السيبراني⁴ وقد ولدت الجائحة المستمرة انعدام الثقة، لا سيما عبر الإنترنت. وتشكل البيانات المجمعة في إطار الرقم القياسي بداية محادثة أوسع بشأن الأمن السيبراني، يكتسي السياق المحلي والملاحظات حولها بأهمية حاسمة في رسم الطريق إلى الأمام.

وللمساعدة في إنشاء فضاء سيبراني موثوق وآمن في أعقاب الجائحة، يمكن أن يكون الرقم القياسي بمثابة نقطة انطلاق لفهم تأثير الجائحة على جهود الأمن السيبراني وكيفية عمل البلدان بشأن معالجة الأمن السيبراني والثقة. فعلى سبيل المثال، أبلغت بعض البلدان عن تأخر إقرار القوانين ودخولها حيز النفاذ، وتنفيذ أفرقة الاستجابة للحوادث الحاسوبية أو تحسينها، ووضع استراتيجيات الأمن السيبراني الوطنية أو تنفيذها، وتنفيذ جهود تنمية القدرات. وحتى الاتفاقات التعاونية لم تعد تستفيد من التفاعل والتعاون مع الأفراد.

ونظراً لاستمرار تغير العالم، من المهم أن تقوم الحكومات بتقييم السياسات والممارسات القائمة فيما يتعلق بالأمن السيبراني. ومع تطور الأمن السيبراني وتكيفه، تطورت كذلك طريقة قياسه. وقد تم تحديث الأسئلة الواردة في الرقم القياسي بشأن دور أفرقة الاستجابة للحوادث الحاسوبية، والاتفاقات التعاونية، والأطر التنظيمية، والوعي العام. وعلى الرغم من أن هذه التغييرات تجعل الرقم القياسي أقل قابلية للمقارنة مع مرور الوقت، تجسد هذه الصيغة الالتزامات الحالية للبلدان بدقة أكبر.

¹ http://core.xsomo.com.jm/images/web/File/white%20papers/Expanding_Digital_Universe_IDC_WhitePaper_Q22507.pdf

² <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>

³ <https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html>

⁴ <http://reports.weforum.org/global-risks-report-2020/executive-summary/>

2 المواضيع الرئيسية

1.2 التدابير القانونية: التخطيط للتدخلات المستقبلية

العديد من التحديات اليوم تضعف الثقة في الإنترنت وتمنع المجتمع الرقمي من العمل بكامل إمكاناته. فعلى سبيل المثال، تُقدر الخسائر العالمية التي تعزى إلى الجرائم السيبرانية من ترليون دولار أمريكي في 2020⁵ إلى 6 تريليون دولار أمريكي في 2021⁶. ووضع إطار قانوني وتنظيمي لحماية المجتمع وتعزيز بيئة رقمية آمنة ومأمونة أمر أساسي في هذا الشأن وينبغي أن يتم في بداية أي جهود وطنية في مجال الأمن السيبراني.

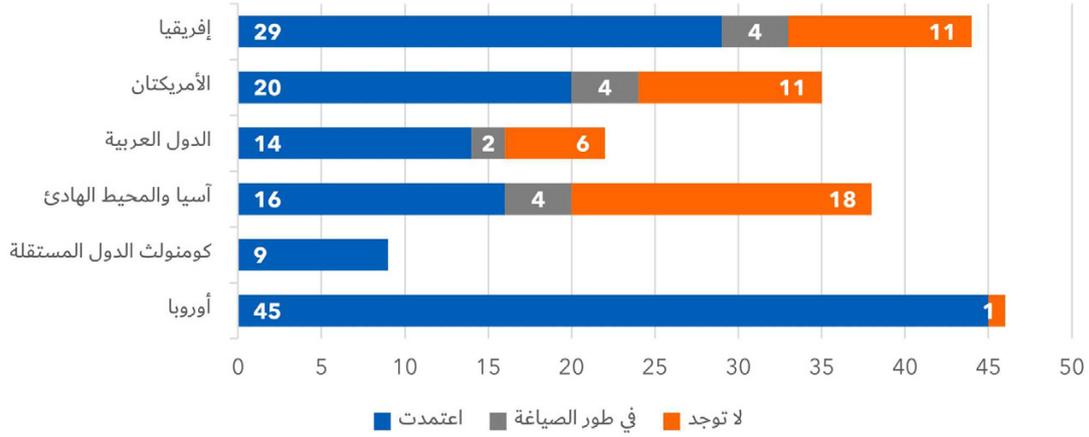
وتشمل الأطر القانونية والتنظيمية وضع تشريعات تحدد ما يشكل الأنشطة غير المشروعة في الفضاء السيبراني، بالإضافة إلى تعريف الأدوات الإجرائية اللازمة للتحقيق والمقاضاة وإنفاذ هذه التشريعات؛ وإنشاء خطوط أساسية للأمن السيبراني وآليات للامتثال من أجل مجموعة من أصحاب المصلحة الوطنيين؛ ووضع إجراءات لضمان الاتساق مع الالتزامات الدولية.

وتقيّم الطبعة الرابعة من الرقم القياسي العالمي للأمن السيبراني تدخلات الأمن السيبراني ضمن الإطار القانوني لبلد ما من خلال قياس وجود:

- المتطلبات الأساسية التي يجب على أصحاب المصلحة في القطاعين العام والخاص الالتزام بها؛
- الصكوك القانونية التي تحظر الأعمال الضارة.

حماية البيانات

الشكل 1: البلدان التي لديها تشريعات لحماية البيانات



المصدر: الاتحاد الدولي للاتصالات

وقد تتخذ تشريعات حماية البيانات شكل تنظيم يمكن أن يجبر مثلاً منظمة على الكشف عن خرق الأمن السيبراني أو وضع متطلبات مراجعة سنوياً.

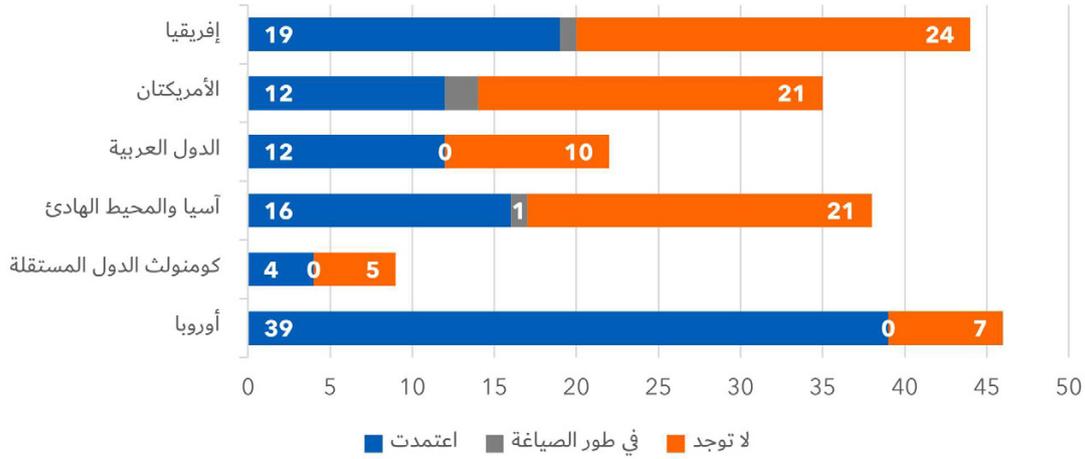
وظاهرياً، قد يلاحظ المدافعون عن الخصوصية أن عدداً كبيراً من البلدان التي لديها بالفعل لوائح لحماية البيانات والخصوصية قد عملت على تحديثها. وبالإضافة إلى ذلك، وقع 133 بلداً على لوائح حماية البيانات والخصوصية لتصبح قانوناً، وهناك 15 بلداً في طور الصياغة، و46 بلداً ليست لديها لوائح. وقامت بلدان كثيرة لديها لوائح معمول بها بتحديث تشريعاتها لتجسيد الاتفاقات والقواعد الجديدة.

ومنذ الصيغة الأخيرة، قام مزيد من البلدان بتنفيذ تدابير تتطلب الإخطار بالخرق. وفي هذه الطبعة، أدخلت 102 من البلدان متطلبات الإخطار بخرق البيانات والإبلاغ عن الحوادث في التشريعات والسياسات.

⁵ <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>

⁶ <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

الشكل 2: البلدان التي اتخذت تدابير الإخطار بالخرق



المصدر: الاتحاد الدولي للاتصالات

سرقة الهوية والبيانات على الإنترنت

على الرغم من أن البلدان اتخذت إجراءات بشأن النفاذ غير القانوني، لا تزال التشريعات المتعلقة بسرقة البيانات والهوية على الإنترنت تفتقر إلى الاهتمام، غير أن حماية الهوية على الإنترنت مهمة للغاية خاصة مع التحول الحالي إلى البيئة الرقمية. وقد تحول سكان العالم إلى استخدام الإنترنت من خلال وسائل التواصل الاجتماعي وممارسات العمل التي تحتاج إلى قدر كبير من الأمن لأن الهوية المسروقة يمكن أن تعرض الحياة اليومية للخطر على المستويين الخاص والمهني.

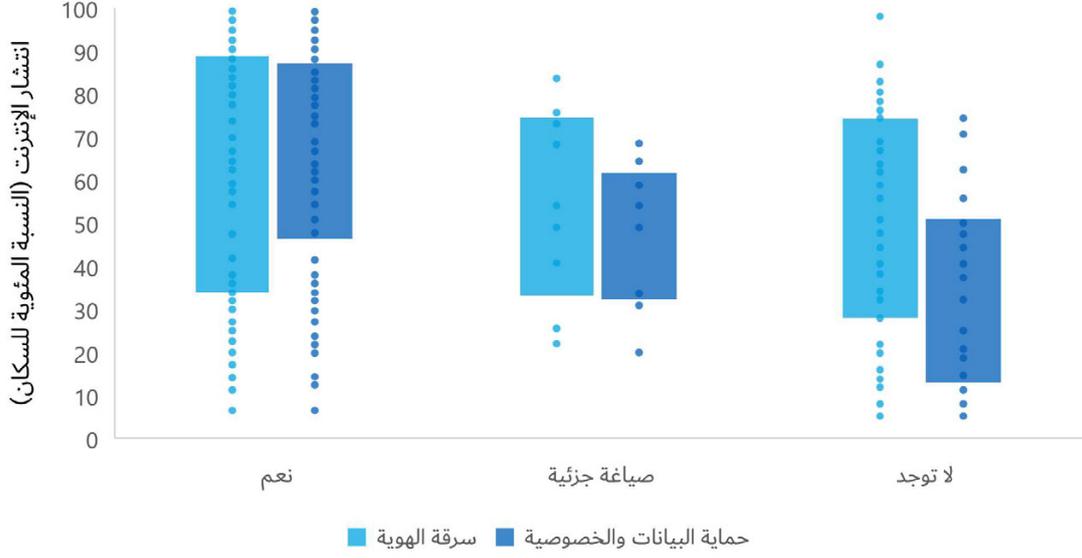
الشكل 3: البلدان التي لديها تشريعات بشأن سرقة المعلومات الشخصية



المصدر: الاتحاد الدولي للاتصالات

وكما يتضح من الشكل 4، عند النظر إلى متوسط معدل انتشار الإنترنت، من الأرجح أن يكون للبلدان ذات معدل انتشار الإنترنت المرتفع قوانين أو لوائح بشأن حماية البيانات على الإنترنت بالمقارنة مع البلدان ذات معدل انتشار الإنترنت المنخفض. وعلى النقيض من ذلك، من الأرجح وجود لوائح لحماية البيانات والخصوصية في البلدان التي تنتشر فيها الإنترنت بدرجة عالية. وتبرز هذه الاتجاهات جزئياً، الظروف الاقتصادية والتنموية الشاملة واستراتيجيات الرقمنة الحكومية. وجدير بالإشارة إلى أن بعض البلدان قد استعدت لزيادة انتشار الإنترنت من خلال وضع تشريعات استباقية تتعلق بسرقة الهوية وحماية البيانات والخصوصية.

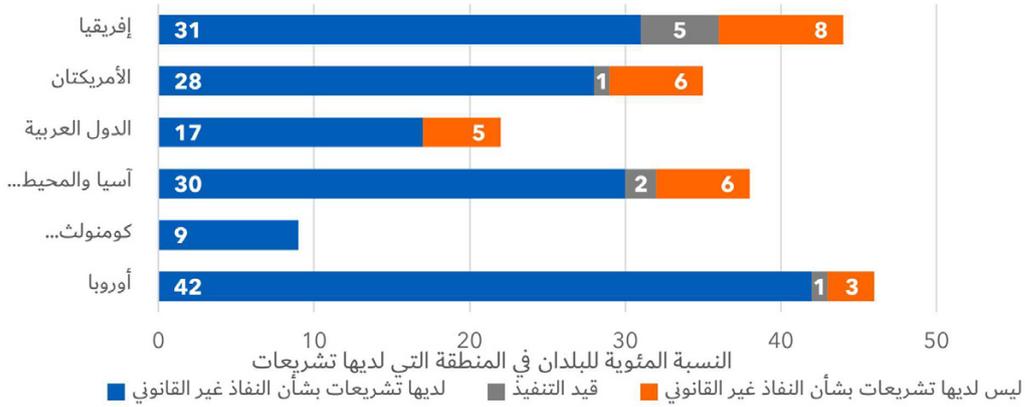
الشكل 4: تشريعات بشأن سرقة الهوية وحماية البيانات والخصوصية، على مستوى النفاذ إلى الإنترنت (النسبة المئوية للسكان)



المصدر: الاتحاد الدولي للاتصالات/قاعدة بيانات مؤشرات تكنولوجيا المعلومات والاتصالات

كما هو مبين في الشكل 5، فإن معظم البلدان لديها تشريعات بشأن النفاذ غير القانوني، مع القليل من الاختلافات المهمة بين المناطق.

الشكل 5: تشريعات بشأن النفاذ غير القانوني



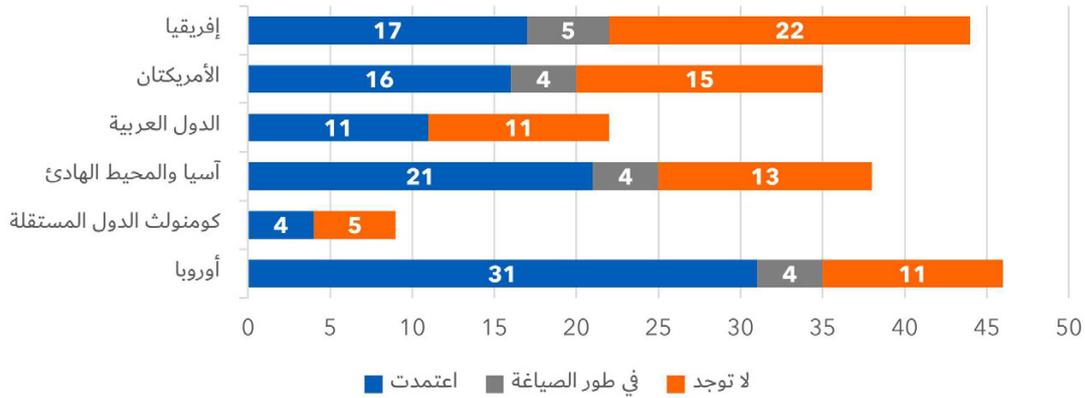
المصدر: الاتحاد الدولي للاتصالات/قاعدة بيانات مؤشرات تكنولوجيا المعلومات والاتصالات

السلوك المعادي للمجتمع عبر الإنترنت

يشكل السلوك المعادي للمجتمع على الإنترنت تحدياً مستمراً تعمل البلدان على زيادة دعمه من الناحية التشريعية. ويقيس الرقم القياسي العالمي جانبيين: التحرش عبر الإنترنت، والعنصرية وكرهية الأجانب على الإنترنت.

ولا يزال التحرش عبر الإنترنت يمثل مشكلة مستمرة: في الولايات المتحدة في 2020، "عانى 41% من الأمريكيين شخصياً من شكل من أشكال التحرش عبر الإنترنت".⁷ وتعرضت امرأة واحدة على الأقل من كل 10 نساء في الاتحاد الأوروبي للتحرش عبر الإنترنت.⁸ وفي إحدى الدراسات الاستقصائية التي أجريت بشأن البالغين في 32 بلداً، أبلغ واحد من كل خمسة بالغين عن تعرضه لخطاب يحض على الكراهية عبر الإنترنت.⁹

الشكل 6: البلدان التي لديها تشريعات بشأن التحرش عبر الإنترنت



المصدر: الاتحاد الدولي للاتصالات/قاعدة بيانات مؤشرات تكنولوجيا المعلومات والاتصالات

وعلى الصعيد العالمي، اعتمد 100 بلد تشريعات تجرم حالات التحرش وإساءة المعاملة عبر الإنترنت، و17 بلداً يصد صياغة هذه التدابير وتنفيذها، و77 بلداً ليس لديها تشريعات بشأن هذا الموضوع. بيد أن ما يشكل إساءة المعاملة غالباً ما يكون غير محدد بشكل جيد.

وتواجه الجهود الرامية إلى التصدي للعنصرية وكراهية الأجانب على الإنترنت حواجز حول الوضوح، ولكن هناك عدد كبير من البلدان التي هي بصد وضع شكل من أشكال التشريعات في هذا الاتجاه. وتقوم عدة بلدان بتوسيع أو تكييف القوانين غير المتصلة بالإنترنت بشأن العنصرية وكراهية الأجانب مع السياق الإلكتروني. وتختلف عتبة ما يشكل جريمة اختلافاً كبيراً حيث إن ما قد يكون قانونياً في بلد ما يمكن أن يشكل جريمة يعاقب عليها القانون في بلد آخر. غير أن بعض البلدان قررت كتابة أحكام خاصة بالسلوك العنصري على الإنترنت.

2.2 التدابير التقنية: زيادة نشر أفرقة الاستجابة للحوادث الحاسوبية (CIRT)/أفرقة مواجهة الطوارئ الحاسوبية (CERT)

من الضروري على الصعيد الوطني وضع آليات، وهيكل مؤسسية، فعالة للتعامل مع التهديدات والحوادث السيبرانية على نحو موثوق. وتمكن أفرقة الاستجابة للحوادث الحاسوبية (CIRT) أو أفرقة مواجهة الطوارئ الحاسوبية (CERT)، البلدان من الاستجابة للحوادث على الصعيد الوطني باستخدام نقطة اتصال مركزية وتشجيع اتخاذ إجراءات سريعة ومنهجية، وتمكين البلدان من التعلم من الخبرات وبناء القدرة على الصمود في مجال الأمن السيبراني.

وغالباً ما يتم تطوير وتنفيذ الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وفقاً للتشريعات والسياسات الوطنية. ويمكن أن تكون هذه الأفرقة جزءاً من مؤسسة حكومية أو تحت مظلة وزارة معينة أو كيان آخر. وعندما تفتقر البلدان إلى الوقت أو المعرفة أو الموارد اللازمة لإنشاء فريق CIRT وطني، تُسند بعض مسؤوليات الفريق إلى طرف ثالث.

⁷ <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>

⁸ https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf

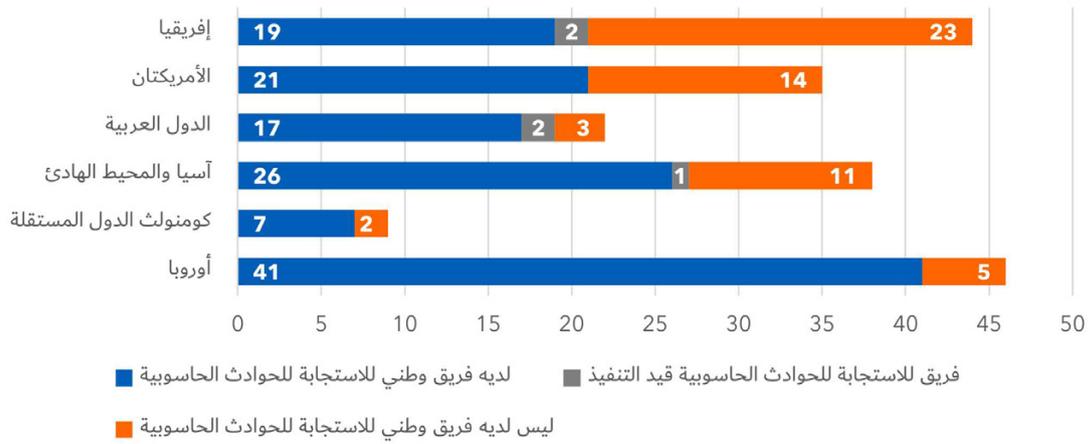
⁹ https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1

يجري إنشاء أفرقة جديدة للاستجابة للحوادث الحاسوبية

في نهاية عام 2020، أنشأ 131 بلداً أفرقة وطنية للاستجابة للحوادث الحاسوبية، بما في ذلك 10 أفرقة CIRT تم إنشاؤها منذ إصدار الرقم القياسي العالمي للأمن السيبراني لعام 2018. ويجري حالياً إنشاء أربعة أفرقة CIRT وطنية.

وعلى الرغم من إحراز العديد من البلدان التقدم في تنفيذ الأفرقة CIRT، يواجه العديد منها، ولا سيما أقل البلدان نمواً (LDC)، عقبات كبيرة تحول دون إنشاء هذه الأفرقة. ويمكن أن يعوق نقص الموارد والمعرفة التكنولوجية والنظام الإيكولوجي للأمن السيبراني، والبحث والتطوير، وتحديد الأولويات، والإرادة السياسية الجهود المبذولة في مجال التدابير التقنية للتصدي لتحديات الأمن السيبراني.

الشكل 7: عدد البلدان التي لديها أفرقة وطنية للاستجابة للحوادث الحاسوبية



المصدر: الاتحاد الدولي للاتصالات

على الرغم من أن منطقة إفريقيا لا تصدر المجال التقني، أنشئت ستة أفرقة CIRT إضافية منذ إصدار الرقم القياسي العالمي للأمن السيبراني لعام 2018، وتقدمت المنطقة من 13 إلى 19 بلداً لديها فريق CIRT وطني. ويوجد في منطقة الأمريكتين 21 فريقاً من أفرقة الاستجابة للحوادث الحاسوبية، وفي منطقة الدول العربية هناك 17 بلداً لديه فريق CIRT وطني. غير أنه لا توجد أفرقة CIRT وطنية في بلدين فقط في منطقة كومونولث الدول المستقلة وفي ستة بلدان في منطقة أوروبا.

ويتيح الرقم القياسي أيضاً تتبع أنشطة أفرقة الاستجابة للحوادث الحاسوبية. ومن بين 131 فريقاً من أفرقة الاستجابة للحوادث الحاسوبية المنفذة، شارك 11 فريقاً في جميع الأنشطة التالية:

- إذكاء الوعي بالأمن السيبراني وحماية الأطفال على الإنترنت من خلال تقديم نصائح وأدلة وكتيبات ودورات تدريبية ومقاطع فيديو؛
- تقديم نصائح بشأن الأمن السيبراني إلى المتخصصين في مجال تكنولوجيا المعلومات؛
- إجراء تدريبات سيبرانية خلال العامين الماضيين؛
- التواصل مع الأفرقة CIRT الإقليمية والمنتدى العالمي لأفرقة الاستجابة لحوادث وأمن المعلومات (FIRST)¹⁰؛
- الاعتماد من قبل مقدم موثوق¹¹ أو شهادة أخرى معترف بها.

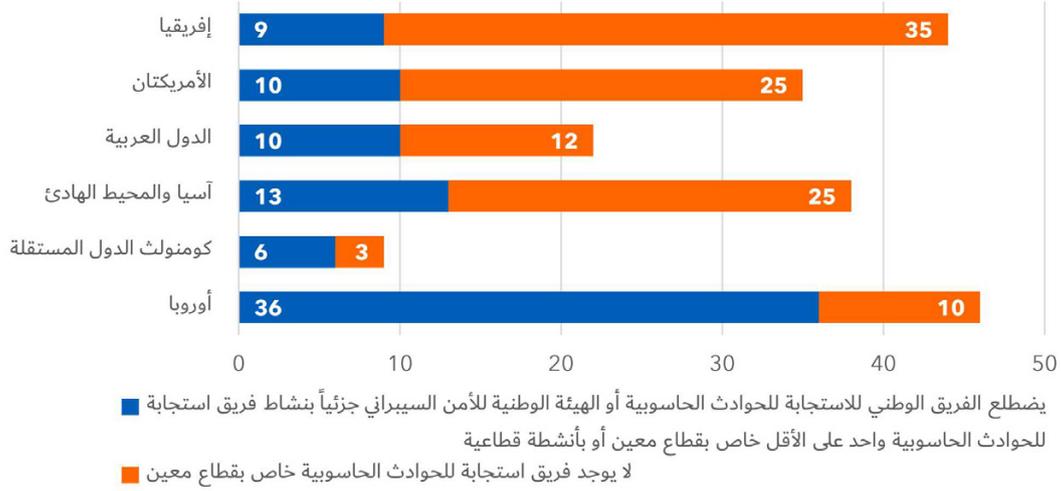
وفي حين تعالج الأفرقة CIRT الوطنية قضايا على المستوى الوطني، تعالج الأفرقة CIRT الخاصة بالقطاعات احتياجات الأمن السيبراني المتعلقة بقطاع معين مثل الصحة والنقل والاتصالات والمرافق العامة. وتخدم أنواع أخرى من هذه الأفرقة الشركات متعددة الجنسيات أو الشركات الكبيرة، والجامعات الخاصة، وغيرها، وهذه الأنواع الأخرى من الأفرقة CIRT لم يتم تتبعها في هذا التقرير بشأن الرقم القياسي العالمي للأمن السيبراني.

¹⁰ www.first.org

¹¹ www.trusted-introducer.org/

الشكل 8: عدد أفرقة CIRT الخاصة بقطاع معيّن

بلدان لديها فريق CIRT واحد على الأقل خاص بقطاع معين، حسب المنطقة



المصدر: الاتحاد الدولي للاتصالات

كما هو مبين في الشكل 8، لا يوجد لدى ثلثي البلدان أفرقة CIRT خاصة بقطاعات محددة. ومن بين 76 بلداً لديها فريق CIRT خاص بقطاع معيّن، يقوم 37 بلداً بحملات توعية، وتدريبات سيبرانية، وتبادل المعلومات المتعلقة بالحوادث والتهديدات علناً أو سراً مع المجتمع المحلي.

3.2 التدابير التنظيمية: موازنة الاستراتيجية

تدرس التدابير التنظيمية آليات الإدارة والتنسيق داخل البلدان المعنية بالأمن السيبراني. وتشمل التدابير التنظيمية ضمان استدامة الأمن السيبراني على أعلى مستوى من السلطة التنفيذية وإسناد الأدوار والمسؤوليات ذات الصلة لمختلف الكيانات الوطنية وجعلها مسؤولة عن وضع الأمن السيبراني الوطني.

ولا توجد دائماً تدابير تنظيمية في البلدان التي تتمتع ببنية تحتية قوية للاتصالات. وإن مقارنة استقصاء الحكومة الإلكترونية للأمم المتحدة لعام 2020 في عقد العمل بشأن الرقم القياسي للبنية التحتية للاتصالات لأغراض التنمية المستدامة، وهو جزء من الرقم القياسي للتأهب للحكومة الإلكترونية¹² مقابل النتائج الإجمالية للتدابير التنظيمية، تُظهر أنه رغم وجود اتجاه ضعيف، هناك بلدان كثيرة تحقق حالياً نتائج جيدة في مجال تدابير البنية التحتية للاتصالات، ولكنها لا تملك التدابير التنظيمية اللازمة لمعالجة قضايا الأمن السيبراني.

ويمكن أن يسهم الافتقار إلى تدابير تنظيمية كافية في انعدام المسؤوليات والمساءلة الواضحة في إدارة الأمن السيبراني على الصعيد الوطني، ويمكن أن يحول دون التنسيق الفعال داخل الحكومات وبين القطاعات.

أهمية الاستراتيجيات الوطنية الحديثة للأمن السيبراني

غالباً ما تشكل الاستراتيجية الوطنية للأمن السيبراني (NCS) حجر الزاوية الرئيسي للتدابير التنظيمية على مستوى الأمن السيبراني الوطني. ووفقاً لدليل الاتحاد بشأن تطوير استراتيجية وطنية للأمن السيبراني، فإن الاستراتيجية الوطنية للأمن السيبراني بمثابة إطار عمل أو استراتيجية شاملة يجب تطويرها وتنفيذها وتفعيلها في إطار نهج متعدد أصحاب المصلحة يعالج الإجراءات المنسقة من أجل الوقاية والاستعداد والاستجابة والتعافي من الحوادث من جانب السلطات الحكومية والقطاع الخاص والمجتمع المدني.¹³

¹² <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>

¹³ <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx>

وتزايد عدد البلدان التي تضع استراتيجيات وطنية للأمن السيبراني من أجل إدارة الأمن السيبراني بطريقة أكثر تنظيماً. ويمكن لهذه الاستراتيجية أن تقدم عدة فوائد، بما في ذلك البلدان التي تجمع بين أصحاب المصلحة المعنيين، وتوضح الأولويات الوطنية وتخطط لتنمية القدرات في مجال الأمن السيبراني.

وبما أن الرقم القياسي العالمي للأمن السيبراني بلغ مرحلة النضج، يجري التركيز بشكل أكبر على البلدان التي تشارك في تحديثات منتظمة لاستراتيجياتها الوطنية بشأن الأمن السيبراني، لضمان تكيفها مع الحقائق المتطورة. وفي الواقع، فإن وجود استراتيجية وطنية للأمن السيبراني بمثابة خطوة أولى إيجابية لوضع الأمن السيبراني في البلدان، ولكن، يتعين إجراء مراجعات بشكل منتظم وفقاً للتغيرات في التهديدات والأولويات في مجال الأمن السيبراني. وعادة ما تعتمد البلدان، عند تحديث استراتيجيتها وطنية، إطاراً زمنياً يتراوح بين 4 و5 سنوات. وقد اختارت بعض البلدان أطراً زمنية أطول تمتد لعقد من الزمن أو أكثر.

ومع امتلاك 127 بلداً استراتيجية وطنية بشأن الأمن السيبراني، سواء كانت حالية أو مضي عليها أكثر من خمس سنوات، أو في طور الصياغة، أظهر 60 بلداً التقدم في وضع أهداف أكثر وضوحاً من خلال مراجعة وتطوير استراتيجيات جديدة للأمن السيبراني أو عن طريق تحديث خطة عملها.

حماية البنية التحتية الحيوية/القدرة على الصمود على الصعيد الوطني

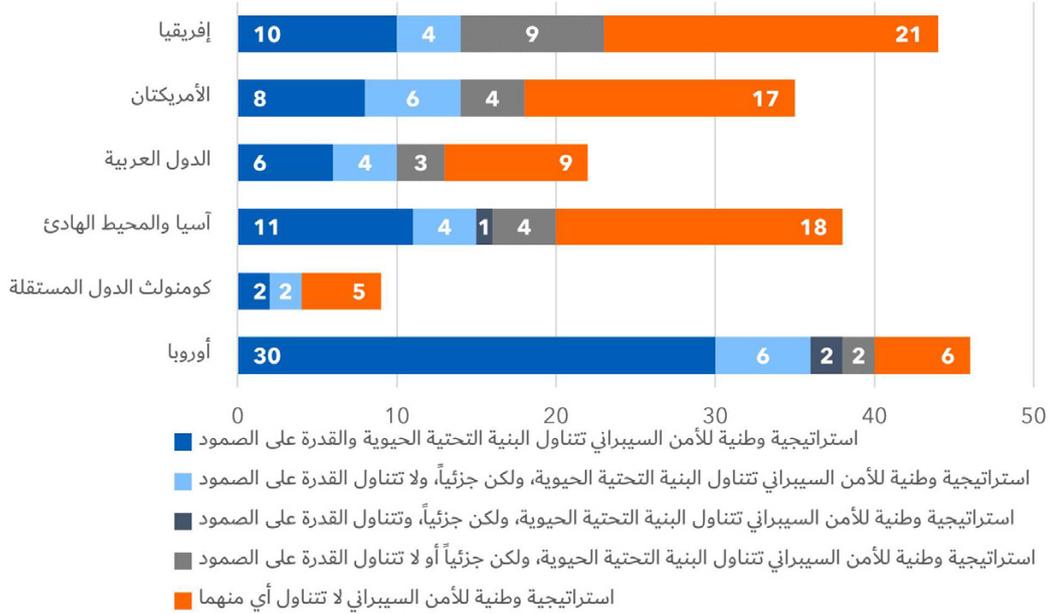
من الجوانب الهامة في العملية الإنمائية لاستراتيجية وطنية للأمن السيبراني وجود مجموعة واضحة من الأهداف المتعلقة بحماية البنية التحتية الحيوية. ويشكل ضمان استمرارية العمليات على الصعيد الوطني تحدياً مستمراً بالنسبة للبلدان. وما زالت البنية التحتية الحيوية، مثل الشبكات الكهربائية ومحطات تنقية المياه وأنظمة النقل تواجه مخاطر في مجال الأمن السيبراني. وإن العواقب المحتملة لحادث يؤثر على البنية التحتية الحيوية مرتفعة، وينبغي أن تؤدي الاستراتيجية إلى مزيد من الاهتمام بجهود إدارة المخاطر التي تهدف إلى تقليل احتمالية وتصعيد الأحداث بالغة العواقب.

ومن المتوقع أن يرتفع الإنفاق على الأمن السيبراني للبنية التحتية الحيوية إلى 9 مليارات دولار أمريكي خلال العام المقبل ليصل إلى 105,99 مليار دولار أمريكي في 2021.¹⁴ ومع تحول البنية التحتية الحيوية، مثلها مثل باقي القوى العاملة، إلى ظروف العمل القائم على التباعد الاجتماعي، فقد احتاجت إلى موازنة سطح الهجوم المتزايد. وأشارت مؤسسة ABI للبحوث أن الاستثمار في الأمن السيبراني يختلف اختلافاً كبيراً اعتماداً على الإقليم والقطاع والتوصيلية، مع أعلى مستوى من الإنفاق في مجالات الدفاع والخدمات المالية وتكنولوجيا المعلومات والاتصالات، ولكنه متأخر في القطاعات الصناعية.¹⁵

<https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/> ¹⁴

<https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/> ¹⁵

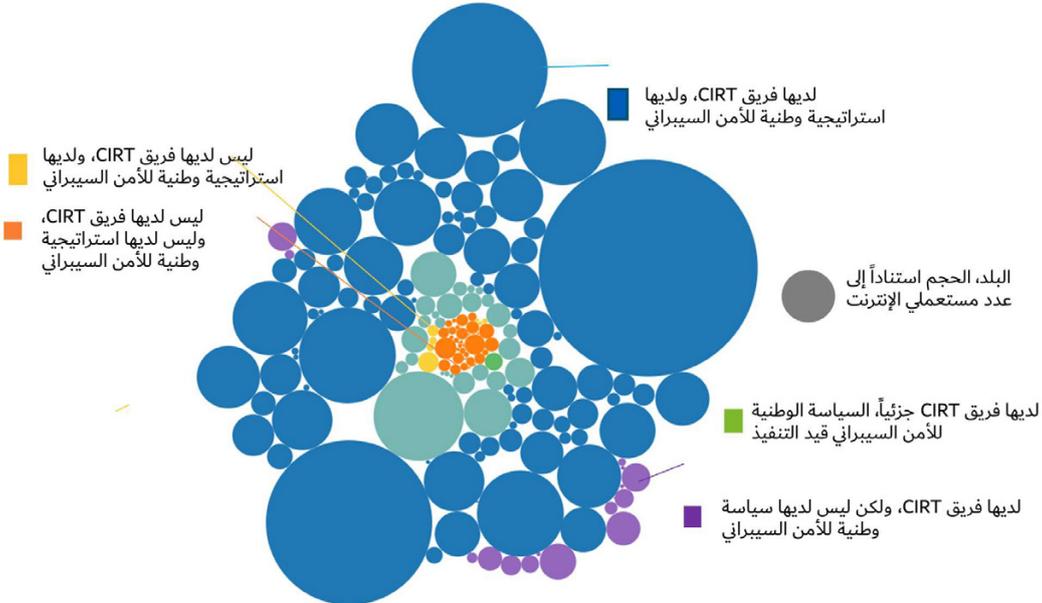
الشكل 9: البلدان التي تعالج قضايا البنية التحتية الحيوية والقدرة على الصمود



المصدر: الاتحاد الدولي للاتصالات

تحديد أولوية الأمن السيبراني كجزء من البنية التحتية الحيوية والقدرة على الصمود لا ينعكس في التزامات الميزانية فحسب، بل وأيضاً في استراتيجيات الأمن السيبراني الوطنية. وتتناول الاستراتيجيات الوطنية للأمن السيبراني في كثير من الأحيان البنية التحتية الحيوية و/أو القدرة على الصمود في مجال الأمن السيبراني. ومع ذلك، لا تتناول عدة بلدان أي منهما.

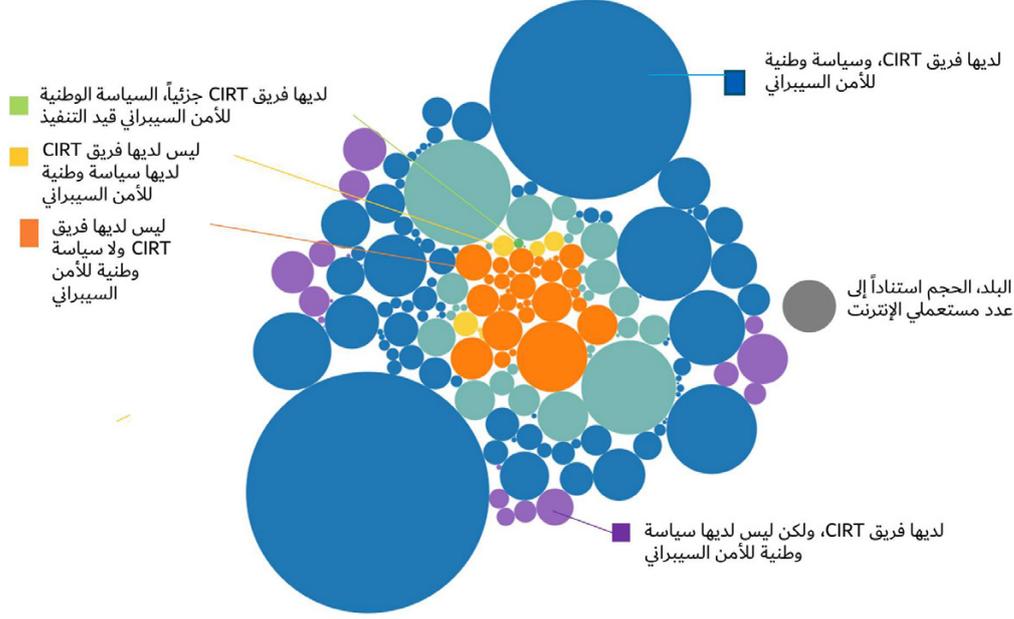
الشكل 10: مستعملو الإنترنت (حسب التغطية بفريق استجابة للحوادث الحاسوبية واستراتيجية وطنية للأمن السيبراني)



المصدر: الرقم القياسي العالمي للأمن السيبراني، الاتحاد الدولي للاتصالات/مؤشرات تكنولوجيا المعلومات والاتصالات

عند النظر إلى البلدان في العالم من حيث عدد مستعملي الإنترنت، يوجد أكثر من 95 في المائة من مستعملي الإنترنت في بلدان لديها استراتيجية وطنية للأمن السيبراني وفريق CIRT وطني على السواء.

الشكل 11: حجم السكان غير الموصولين (حسب التغطية بفريق استجابة للحوادث الحاسوبية واستراتيجية وطنية للأمن السيبراني)



المصدر: الرقم القياسي العالمي للأمن السيبراني، الاتحاد الدولي للاتصالات/ مؤشرات تكنولوجيا المعلومات والاتصالات

ومع ذلك، غالباً ما تفتقر البلدان الأقل توصيلاً إلى سياسة وطنية للأمن السيبراني و/أو فريق وطني للاستجابة للحوادث الحاسوبية. ويعيش 9 في المائة من السكان غير الموصولين في بلدان لا توجد فيها أفرقة للاستجابة للحوادث الحاسوبية أو استراتيجية وطنية للأمن السيبراني، في حين أن نسبة 15 في المائة إضافية تعيش في بلدان لا توجد فيها استراتيجية، ولكن مع وجود فريق وطني CIRT. وأكثر من نصف أقل البلدان نمواً تفتقر إلى فريق CIRT، و60 في المائة لا توجد فيها عملية لوضع استراتيجية وطنية للأمن السيبراني أو لم يتم الشروع فيها بعد.

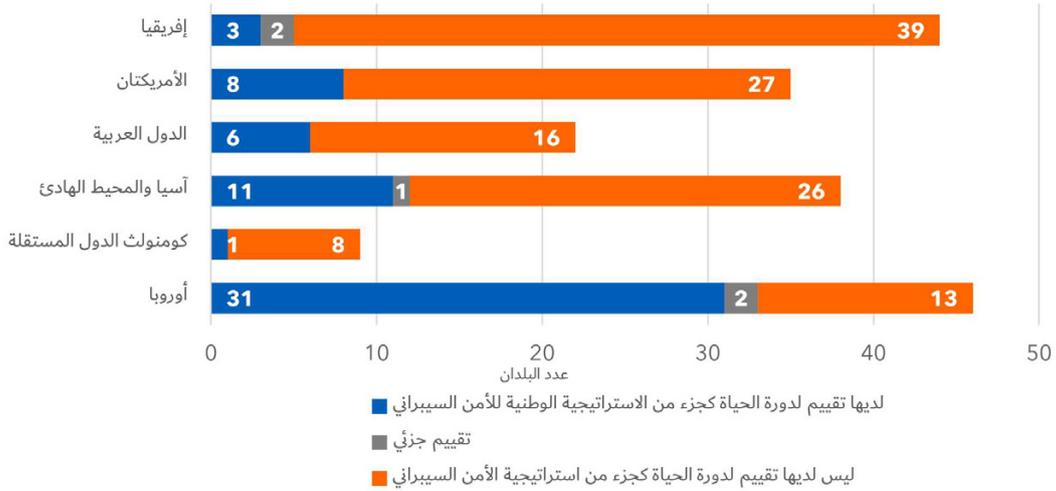
الجدول 1: عدد البلدان التي لديها استراتيجية وطنية للأمن السيبراني وفريق CIRT

فريق CIRT وطني	لديها استراتيجية وطنية للأمن السيبراني	استراتيجية وطنية للأمن السيبراني جارية أو أقل من 5 أعوام	بدون استراتيجية وطنية للأمن السيبراني
فريق CIRT وطني	90 بلداً	29	18
لا يوجد فريق CIRT وطني	7	1	49

المصدر: الاتحاد الدولي للاتصالات

البدان التي لا تملك استراتيجية وطنية أقل احتمالاً أن يكون لديها فريق CIRT. ولا غرابة في أن يكون 49 بلداً بدون فريق CIRT ولا استراتيجية وطنية للأمن السيبراني، بين 63 بلداً بدون فريق CIRT، و67 بلداً بدون استراتيجية وطنية للأمن السيبراني.

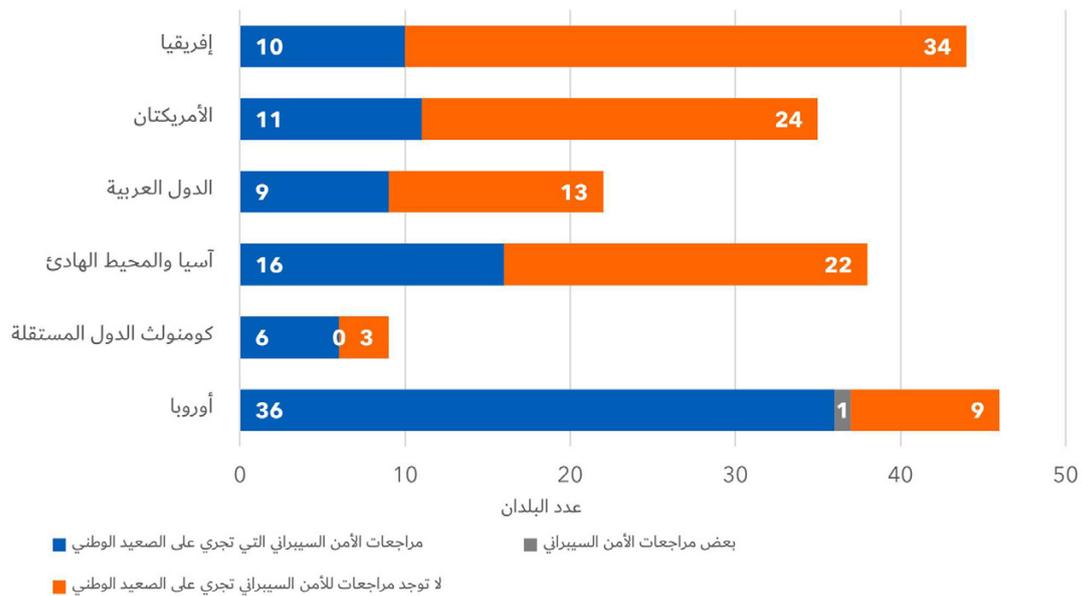
الشكل 12: تقييم دورة الحياة كجزء من الاستراتيجية الوطنية للأمن السيبراني



المصدر: الاتحاد الدولي للاتصالات

ووجود استراتيجية وطنية للأمن السيبراني خطوة أولى إيجابية بالنسبة لوضع الأمن السيبراني، ولكن هناك حاجة إلى إجراء تحديثات ومراجعات منتظمة. ولا تقوم العديد من البلدان التي لديها استراتيجية وطنية للأمن السيبراني بالمراجعة وإعادة التكييف بشكل منتظم في ضوء التغيرات في التهديدات والأولويات في مجال الأمن السيبراني. ومن بين 98 بلداً لديها استراتيجية وطنية محدثة للأمن السيبراني، لا يقوم سوى 60 بلداً بإدراج تقييمات دورة الحياة كجزء من استراتيجيته.

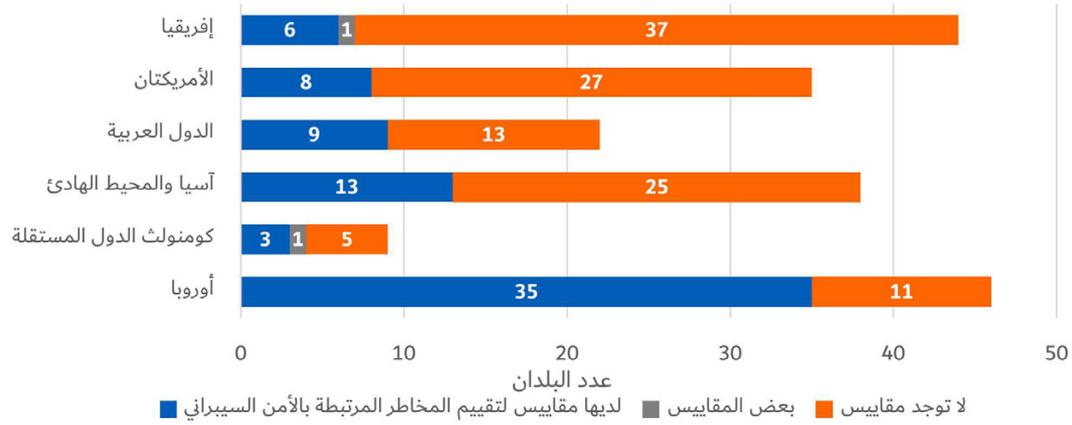
الشكل 13: عمليات مراجعة الأمن السيبراني التي تجري على الصعيد الوطني



المصدر: الاتحاد الدولي للاتصالات

مراجعات الأمن السيبراني التي تجري على الصعيد الوطني (الشكل 13) أكثر شيوعاً من عمليات تقييم دورة الحياة. ولم يُقِيم تواتر هذه المراجعات كجزء من هذه الصيغة للرقم القياسي.

الشكل 14: مقاييس لتقييم المخاطر المرتبطة بالفضاء السيبراني على الصعيد الوطني



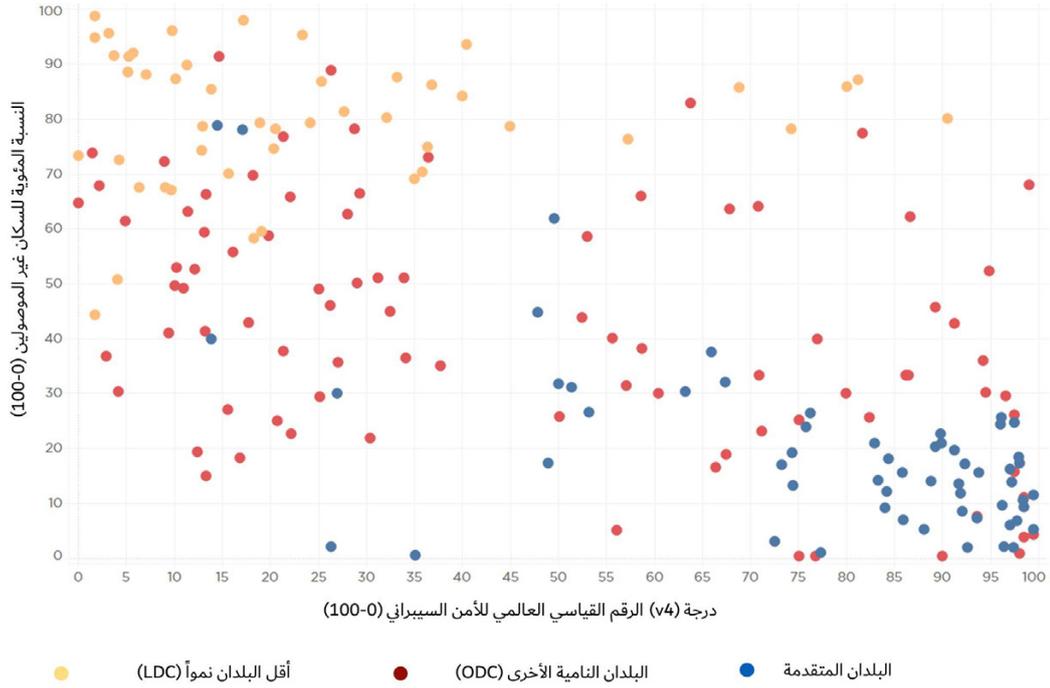
المصدر: الاتحاد الدولي للاتصالات

وبالمثل، لا تملك معظم البلدان مقاييس لتقييم المخاطر المرتبطة بالفضاء السيبراني على الصعيد الوطني. ويمكن أن يزيد الافتقار إلى هذه المقاييس من صعوبة تقييم البلدان للمخاطر الحالية، وتحديد أولويات التدخلات المتعلقة بالأمن السيبراني، وتتبع التقدم المحرز.

4.2 تدابير تنمية القدرات: تنمية القدرات في مجال الأمن السيبراني

تشير تقديرات المنتدى الاقتصادي العالمي إلى أن "ما يقرب من مليون شخص يستعملون الإنترنت لأول مرة كل يوم، وثلثي سكان العالم يمتلكون جهازاً متنقلاً"¹⁶ وفي حين أن مزايا التكنولوجيا الرقمية تجلب فوائد اقتصادية ومجتمعية هائلة، يمكن للمخاطر السيبرانية أن تعادل فوائد الرقمنة. وإن تأمين المجال السيبراني من خلال أنشطة تنمية القدرات في مجال الأمن السيبراني أمر أساسي إذ يساهم في الحد من قضايا مثل الفجوة الرقمية والمخاطر السيبرانية.

الشكل 15: الرقم القياسي العالمي للأمن السيبراني وغير الموصولين



المصدر: الرقم القياسي العالمي للأمن السيبراني، المؤشرات العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات للاتحاد

كما يتضح من الشكل 15، فالبلدان التي تميل إلى تحقيق نتائج أقل في الرقم القياسي العالمي للأمن السيبراني هي أكثر احتمالاً أن تكون من أقل البلدان نمواً وأن توجد بها نسبة مئوية عالية من السكان غير الموصولين. وإذا بدأ هؤلاء الناس بالتوصيل على نحو متزايد، يحتاجون إلى الدعم لتنمية القدرات في مجال الأمن السيبراني للاستجابة بشكل أفضل للتهديدات. بيد أنه من الأرجح أن تواجه عدة بلدان، وخاصة أقل البلدان نمواً، تحديات تتعلق بالموارد لسد الفجوة في قدراتها السيبرانية، بما في ذلك نقص المعرفة المؤسسية والقيود على السياسات ونقص المهارات وغيرها لحماية أنظمتها في مجال تكنولوجيا المعلومات والاتصالات، سواء فعلياً أو افتراضياً.

وتشكل عدة بلدان من بين أقل البلدان نمواً حالات استثنائية مثل بنغلاديش وبنن ورواندا وتنزانيا، التي أظهرت التزامات قوية في مجال الأمن السيبراني. وعلى وجه الخصوص، أبلغت هذه البلدان جميعها عن وجود صناعة وطنية للأمن السيبراني، وهي سمة رئيسية لتدابير تنمية القدرات.

الشكل 16: أهداف التنمية المستدامة (8، 9، 10)



المصدر: الأمم المتحدة (<https://sdgs.un.org/goals>)

لتعزيز العمل اللائق والنمو الاقتصادي، وبناء بنى تحتية قادرة على الصمود، وتحفيز التصنيع الشامل والمستدام، وتشجيع الابتكار، والحد من أوجه عدم المساواة داخل البلدان وفيما بينها، من الضروري تنمية القدرات في مجال الأمن السيبراني لتعزيز العمليات والمهارات والموارد والبحوث والتطورات الرامية إلى تعزيز القدرات الوطنية. وتعزز قدرات الأمن السيبراني أيضاً تطوير القدرات الجماعية وتيسير التعاون الدولي والشراكات للتصدي بفعالية للتحديات المتصلة بالأمن السيبراني.

ويمكن أن تسهم أدوات وتدابير تنمية القدرات في إدارة المخاطر المتصلة بالأمن السيبراني وحماية المواطنين والبنية التحتية والأعمال التجارية وبناء مجتمعات سيبرانية أقوى.

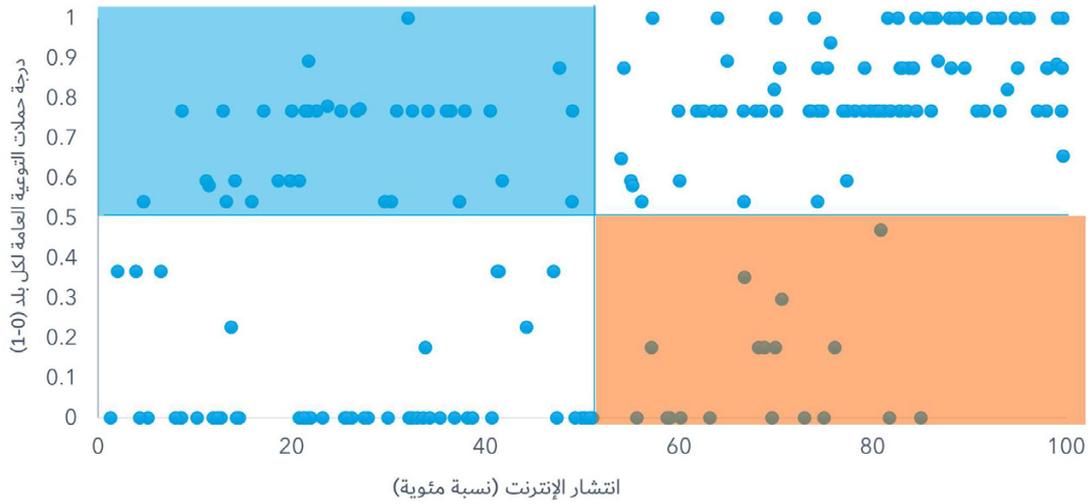
إذكاء الوعي العام بالأمن السيبراني

إذكاء الوعي بالأمن السيبراني على نحو فعال أمر ضروري للحفاظ على يقظة المواطنين والشركات والحكومات والشباب والمنظمات. ومع التحول الحالي إلى الخدمات الرقمية، يتعين على الحكومات أن تتأكد من أن جميع المستعملين على علم بالمخاطر التي يواجهونها أثناء تنفيذ الأنشطة الرقمية.

وعند المقارنة بين حملات التوعية العامة بالأمن السيبراني وانتشار الإنترنت، تنقسم البلدان إلى أربع مجموعات رئيسية:

- 1 انتشار منخفض للإنترنت/تعزيز الوعي بالأمن السيبراني (الإطار الأزرق في الشكل 17): هذه البلدان مهيأة بشكل أفضل لتوصيل غير الموصولين وتزويد الناس بالوعي اللازم عبر الإنترنت.
- 2 انتشار منخفض للإنترنت/عدم تعزيز الوعي بالأمن السيبراني: لم توصل هذه البلدان بعد غير الموصولين، ولا تتاح موارد التوعية للناس في مجال الأمن السيبراني.
- 3 انتشار مرتفع للإنترنت/تعزيز الوعي بالأمن السيبراني: هذه البلدان موصولة رقمياً وتشارك في أنشطة التوعية بالأمن السيبراني للمساعدة في تعزيز السلوك الآمن على الإنترنت.
- 4 انتشار مرتفع للإنترنت/عدم تعزيز الوعي بالأمن السيبراني (الإطار البرتقالي في الشكل 17): هذه البلدان موصولة رقمياً، ولكن قد لا يكون سكانها على علم بالمخاطر السيبرانية.

الشكل 17: درجة حملات التوعية العامة بالأمن السيبراني (لكل بلد مقارنة مع انتشار الإنترنت)



المصدر: الاتحاد الدولي للاتصالات

حملات التوعية العامة بشأن الأشخاص ذوي الإعاقة وكبار السن

بقدر ما تجلب الإنترنت والعالم الرقمي فرصاً غير مسبوقه، لا يُراعى في كثير من الأحيان الأشخاص ذوو الإعاقة وكبار السن عند اتخاذ القرارات التشغيلية وخيارات التكنولوجيا. وهناك ما يقدر بنحو 752 مليون شخص تتراوح أعمارهم بين 65 عاماً وما فوق في عام 2021.¹⁷ وبمقارنة هذا العدد بعدد البلدان التي تقوم بحملات توعية تركز على الأشخاص ذوي الإعاقة وكبار السن، تبدو النتيجة منخفضة بشكل ملحوظ. ومن بين 194 بلداً، لم يكن هناك سوى 18 في المائة من البلدان التي تقوم بإذكاء الوعي بشأن الأشخاص ذوي الإعاقة وقامت 25 في المائة منها بحملات من أجل كبار السن. والعدد القليل من البلدان المنخرطة في رفع مستوى الوعي فيما يخص هاتين

¹⁷ <https://population.un.org/wpp/DataQuery/>

الفئتين المحددتين من السكان مثير للقلق لأن ذلك يولد فجوات وثغرات رقمية كبيرة نظراً لحد الأشخاص ذوي الإعاقة وكبار السن على استخدام الخدمات الرقمية، مثل تطبيقات تتبع المخالطين لحالات كوفيد-19.

زيادة التركيز على الوعي السيبراني في الشركات الصغيرة والمتوسطة (SME) والقطاع الخاص والحكومات

تحولت العمليات التجارية إلى النسق الإلكتروني بشكل أكبر خلال جائحة كوفيد-19، مما أدى إلى زيادة الطلب على ممارسات الأمن السيبراني في القطاع الخاص. وكثيراً ما تمثل الشركات الصغيرة والمتوسطة الحجم الأكثر شيوعاً للأعمال داخل البلد، حيث تشكل المؤسسات الصغيرة والمتوسطة 90 في المائة من الشركات وتنبع 50 في المائة من العمالة من هذه المؤسسات، وتسهم المشاريع الصغيرة والمتوسطة الرسمية بنسبة تصل إلى 40 في المائة في الناتج المحلي الإجمالي في الاقتصادات الناشئة¹⁸ مما يولد الحاجة إلى أنشطة التوعية بالأمن السيبراني بالنسبة للشركات الصغيرة والمتوسطة.

الشكل 18: عدد البلدان التي لديها حملات توعية بشأن الأمن السيبراني تستهدف الشركات الصغيرة والمتوسطة والقطاع الخاص والوكالات الحكومية



المصدر: الاتحاد الدولي للاتصالات

وتظهر نتائج الرقم القياسي أن حوالي 60 في المائة من البلدان تشارك أو شاركت خلال العامين الماضيين في زيادة الوعي السيبراني بين الشركات الصغيرة والمتوسطة أو شركات القطاع الخاص أو الوكالات الحكومية مقابل 38 في المائة من البلدان التي لم تُبلِّغ عن أي حملات للأمن السيبراني. وقد شاركت هذه البلدان من خلال إبلاغ الفئة المستهدفة بخطوط الأساس للسلامة والأمن السيبراني عبر الإنترنت، أو عن طريق توفير الموارد من خلال الفريق الوطني، أو إتاحة أدوات لتأمين الشبكات. و2 في المائة من البلدان في مرحلة مبكرة من تطوير حملات تستهدف الشركات الصغيرة والمتوسطة وشركات القطاع الخاص والوكالات الحكومية

الحكومات تدرك الحاجة إلى برامج تعليمية خاصة بقطاع معين وتدريب المهنيين في مجال الأمن السيبراني

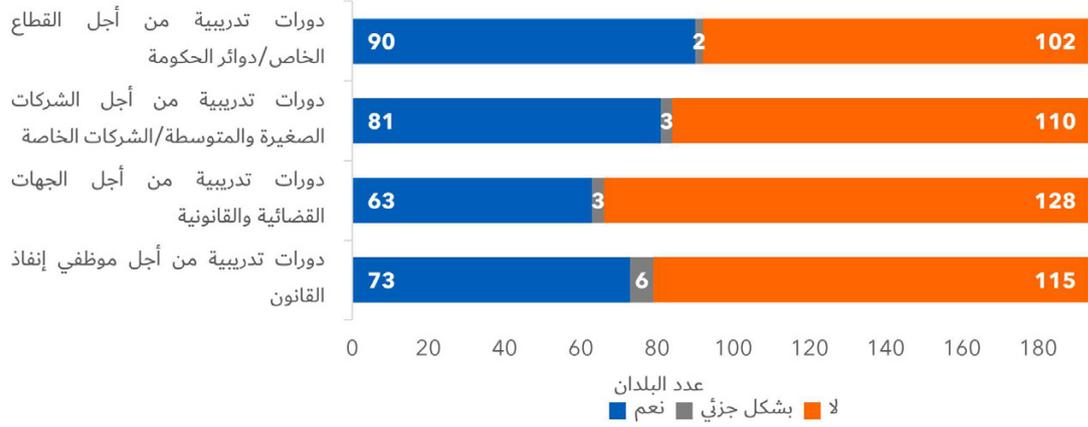
من المهم بشكل متزايد توفير برامج تدريبية لتلبية مختلف احتياجات القطاعات. ويتوقع محللو الأمن السيبراني أنه سيكون هناك من 3,5 مليون¹⁹ إلى 4 ملايين²⁰ وظيفة شاغرة في مجال الأمن السيبراني على مستوى العالم في 2021. ورغم هذه الفجوة المتوقعة، لم يقم عدد كبير من البلدان بتطوير تدريب خاص بقطاع معين، ويفتقر أكثر من 50 في المائة من البلدان إلى برامج مصممة خصيصاً لقطاعات أو مهن محددة مثل إنفاذ القانون والأطراف الفاعلة القانونية والشركات الصغيرة والمتوسطة والشركات الخاصة والمسؤولين الحكوميين.

¹⁸ <https://www.worldbank.org/en/topic/sme/finance>

¹⁹ <https://cybersecurityventures.com/jobs/>

²⁰ تقرير أبحاث ESG: استقصاء عن العمل الرقمي لعام 2019 (esg-global.com)

الشكل 19: عدد البلدان التي لديها برامج تعليمية/دورات تدريب محددة من أجل المهنيين العاملين في مجال الأمن السيبراني



المصدر: الاتحاد الدولي للاتصالات

كما هو مبين في الشكل 19، أفادت نسبة 46 في المائة (90 بلداً) من البلدان بتقديم تدريب خاص بالقطاع الوطني في مجال الأمن السيبراني لموظفي القطاع العام والمسؤولين الحكوميين، وتوفر نسبة 41 في المائة (81 بلداً) تدريبات في مجال تنمية القدرات بشأن قضايا الأمن السيبراني للمهنيين العاملين في مجال تكنولوجيا المعلومات، بما في ذلك الشركات الصغيرة والمتوسطة والقطاع الخاص، وتوفر نسبة 37 في المائة (73 بلداً) تدريبات لموظفي إنفاذ القانون، فيما تكفل نسبة 32 في المائة (63 بلداً) من البلدان عدم تخلف الجهات القضائية وغيرها من الجهات القانونية عن الركب في ضمان القدرة على الصمود والأمن.

وأفادت البلدان بأنها تقدم هذا التدريب في مجال الأمن السيبراني من خلال أفرقتها الوطنية للاستجابة للحوادث الحاسوبية ومراكز الأمن السيبراني الوطنية والدورات التدريبية التي اعتمدها أو أفرقتها الحكومات والتي تقدمها مؤسسات إقليمية ودولية أخرى. وأيدت بعض البلدان التي تسعى إلى زيادة عدد المهنيين في مجال الأمن السيبراني، ولكنها غير قادرة على توفير التدريب الوطني، التدريب الدولي الذي تقدمه هيئات إصدار شهادات في مجال الأمن السيبراني مثل SANS²¹ وISC وICSPA²² وISACA²³.

دورات الأمن السيبراني من أجل التعليم الابتدائي والثانوي أصبحت أكثر انتشاراً

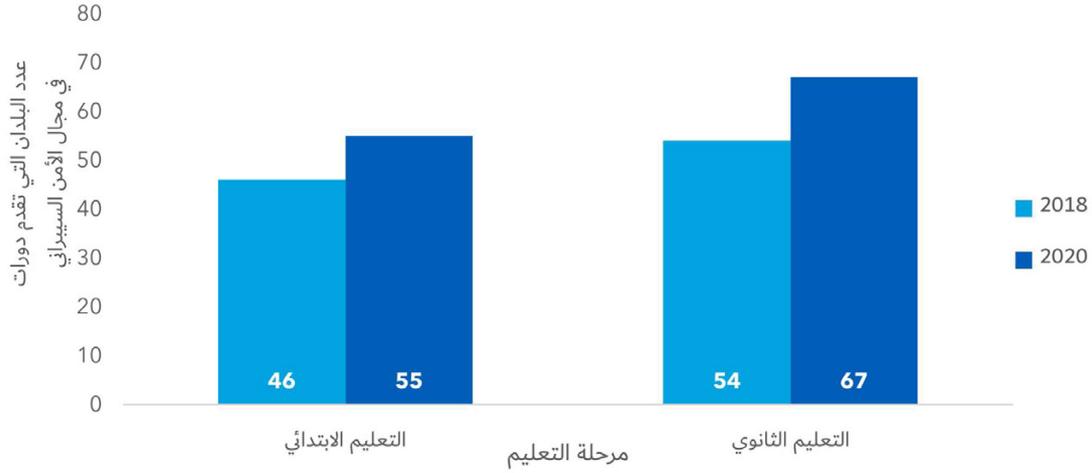
مع تحول الدول إلى توفير التعليم عبر الإنترنت، تُقدم دورات السلامة والأمن السيبراني ليس فقط في التعليم العالي، بل وأيضاً في المدارس الابتدائية والثانوية.

²¹ <https://www.sans.org/>

²² <https://icspa.org/about-us/>

²³ <https://www.isaca.org/>

الشكل 20: عدد البلدان التي تنفذ دورات في مجال الأمن السيبراني في المناهج الأكاديمية الوطنية (حسب مرحلة التعليم)



المصدر: الاتحاد الدولي للاتصالات

كما يتضح من الشكل 20، تقوم البلدان بدمج المزيد من دورات الأمن السيبراني في المناهج التعليمية الوطنية منذ إنشاء الرقم القياسي العالمي للأمن السيبراني في 2018. وتقدم خمسة في المائة من البلدان، من 46 إلى 55، دورات تمهيدية بشأن الحفاظ على سلامة الأطفال على الإنترنت في التعليم الابتدائي وتوفر 7 في المائة من البلدان، من 54 إلى 67، موارد في المناهج الدراسية الثانوية للطلاب المهتمين بممارسة الأمن السيبراني كمهنة لبدء التعلم في هذا المجال في سن مبكرة.

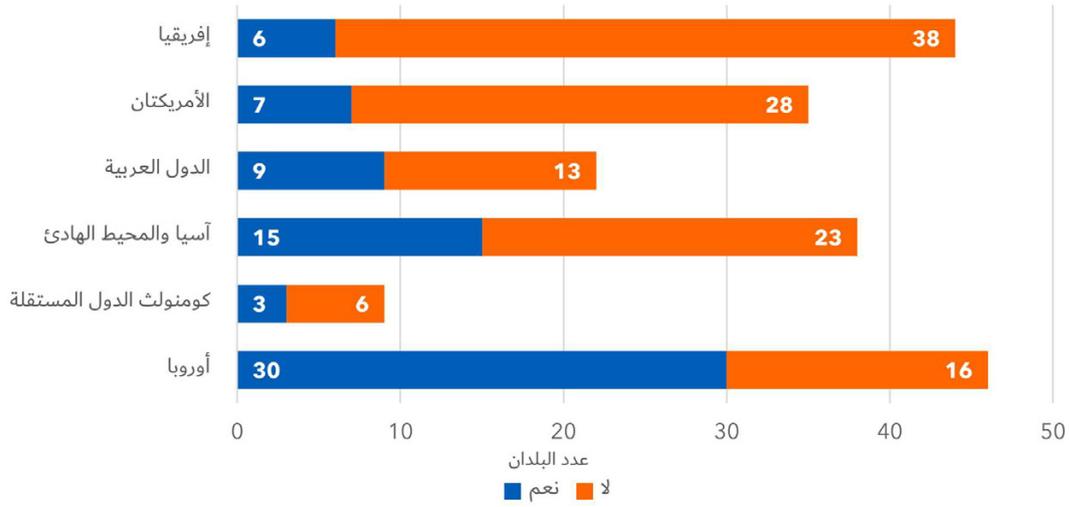
الحوافز الحكومية لتطوير الأمن السيبراني متأخرة

يجب أن يكون تعزيز الأمن السيبراني على الصعيد الوطني مصحوباً بتعزيز ثقافة الأمن السيبراني، وتشجيع تحول المواقف بين قادة الأعمال بالابتعاد عن الأمن السيبراني كمشكلة متصلة بتكنولوجيا المعلومات، إلى نظرة أكثر شمولية تقدر دور الأمن السيبراني في تحسين كفاءة وأداء الأعمال بشكل عام. وأسبقية الأمن السيبراني بين المنظمات عملية تتطلب توافر بنية تحتية وآليات لتشجيع اعتماد الأمن السيبراني. وتنعكس البلدان التي تعزز تطوير الأمن السيبراني في القطاع الخاص وتشجع تطوير الشركات ذات الصلة بالأمن السيبراني في إدماج الحوافز في إطار الأمن السيبراني الخاص بها.

ويمكن أن تشجع البلدان اعتماد الأمن السيبراني في القطاع الخاص من خلال آليات الحوافز، مثل الحوافز الضريبية القائمة على معايير الأمن السيبراني، أو الإعفاءات الضريبية، أو إدراج معايير الأمن السيبراني كعقود جزئية. وهذا من شأنه أن يشجع الأطراف الفاعلة في القطاع الخاص على إيلاء الأولوية للأمن السيبراني ضمن الهياكل والعمليات التشغيلية، وبالتالي تحسين وضع الأمن السيبراني في بلد ما على المدى القصير والمتوسط والطويل.

غير أن هذه الطبعة من الرقم القياسي تبين أن 124 بلداً لم تقدم أي حوافز بشأن الأمن السيبراني، مما يبرز ضرورة اعتماد الدول الأعضاء هذه الحوافز لتسريع إجراءات الأمن السيبراني.

الشكل 21: عدد البلدان التي لديها آلية تحفيزية لتنمية القدرات في مجال الأمن السيبراني



المصدر: الاتحاد الدولي للاتصالات

5.2 التدابير التعاونية: معالجة إجراءات الأمن السيبراني الجماعية

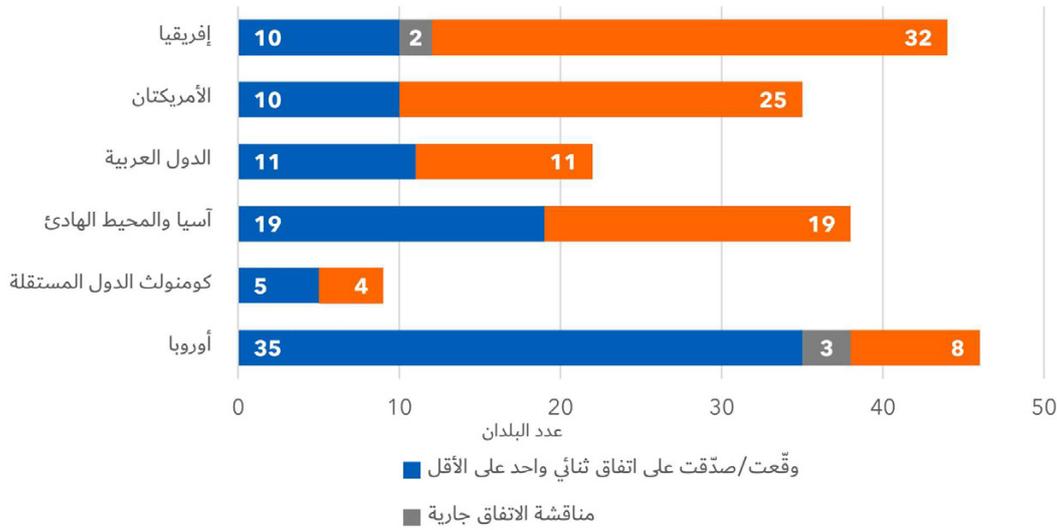
يتزايد تجرّد التهديدات الأمنية السيبرانية من أي حدود،²⁴ ويظل التعاون أداة أساسية لمواجهة تحديات الأمن السيبراني. ولا يزال الأمن السيبراني قضية عابرة للحدود الوطنية نظراً لزيادة التوصيل البيئي والبنى التحتية المترابطة. ولا يمكن لصاحب مصلحة واحد أن يضمن أمن النظام الإيكولوجي السيبراني العالمي أو إدارته، ويحتاج إلى تعاون وطني وإقليمي ودولي لتوسيع نطاقه وأثره. وفي إطار ركيزة التعاون هذه، أتاح الاستبيان تعداد البلدان التي لديها اتفاقية ثنائية ومتعددة الأطراف، والبلدان المنخرطة في شراكات بين الوكالات وبين القطاعين العام والخاص. وتشمل الأهداف النموذجية للتعاون في مجال الأمن السيبراني تنسيق تدابير الحد الأدنى من الأمن، وتبادل المعلومات والممارسات الجيدة، وتدوين قواعد السلوك.

الاتفاقيات الثنائية والمتعددة الأطراف

تكتسي الاتفاقيات الثنائية والمتعددة الأطراف أهمية حاسمة في تقنين القواعد والسلوكيات وتعزيز التعاون الدولي بشأن الأمن السيبراني.

<https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019> ²⁴

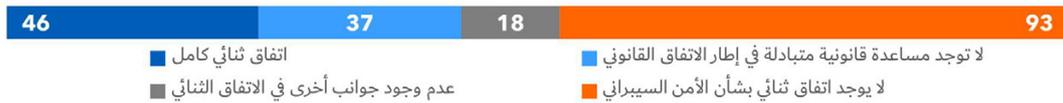
الشكل 22: البلدان المشاركة في اتفاقات ثنائية بشأن الأمن السيبراني



المصدر: الاتحاد الدولي للاتصالات

وتظهر البيانات المستخلصة أن 90 بلداً لديها اتفاق ثنائي في مجال الأمن السيبراني. وبالنسبة إلى الاتفاقات المتابعة في سياق الرقم القياسي، تبرم البلدان اتفاقات بشأن الأمن السيبراني في مجال تنمية القدرات. وفي بعض الحالات، يتعلق الاتفاق بتبادل المعلومات فقط، حيث لا يشكل الأمن السيبراني دائماً البند الأساسي في الاتفاق، بل يُدرج كجزء من مواضيع أخرى. وبالنسبة إلى 37 بلداً، تشمل اتفاقاتها الثنائية تبادل المعلومات وتدابير تنمية القدرات على السواء، ولكنها لا تتناول المساعدة القانونية المتبادلة.

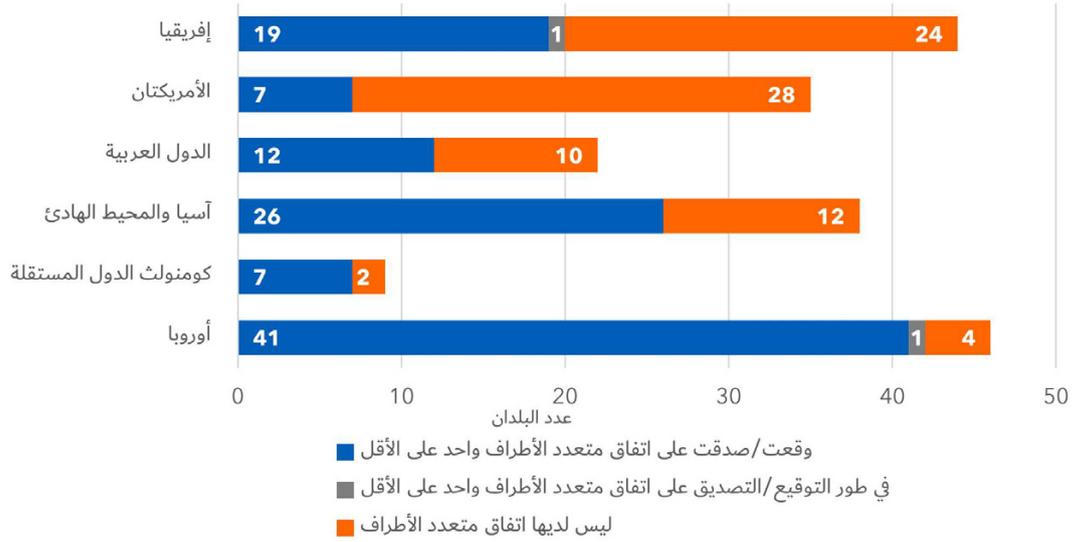
الشكل 23: البلدان التي لديها اتفاق ثنائي بشأن الأمن السيبراني (حسب المواضيع المشمولة)



المصدر: الاتحاد الدولي للاتصالات

ونظراً إلى مشكلة العمل الجماعي التي ينطوي عليها الأمن السيبراني، عملت بعض البلدان على ضمان التوقيع ليس فقط على الاتفاقات الثنائية، بل وأيضاً على الاتفاقات المتعددة الأطراف. وبالنسبة لعملية إعداد هذه الصيغة للرقم القياسي العالمي للأمن السيبراني، شملت الاتفاقات المتعددة الأطراف الاتفاقات المبرمة بين ثلاثة أطراف أو أكثر، بما فيها الحكومات والمنظمات الإقليمية، باستثناء الاتفاقيات الدولية، مثل اتفاقية بودابست بشأن الجريمة السيبرانية.

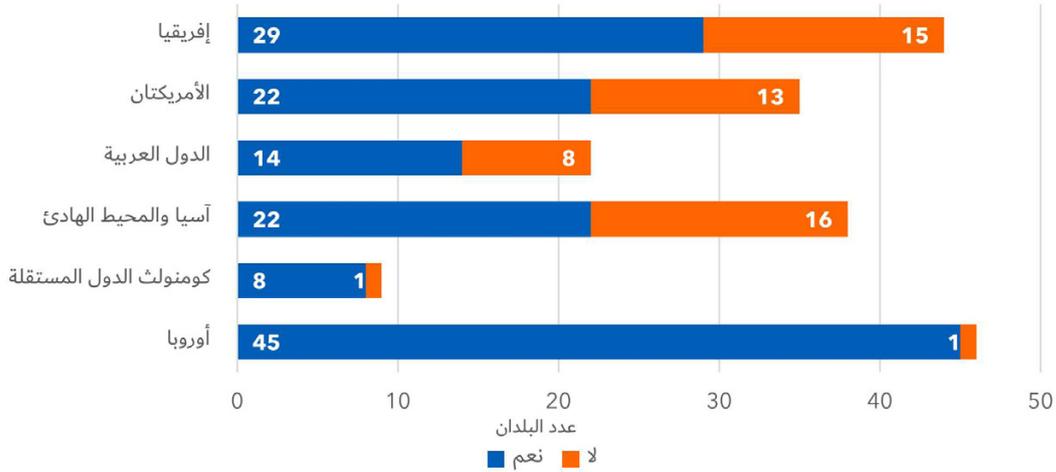
الشكل 24: عدد البلدان المشاركة في اتفاقات الأمن السيبراني المتعددة الأطراف (الموقعة والمصدق عليها)



المصدر: الاتحاد الدولي للاتصالات

من المرجح أن تبرم البلدان اتفاقاً متعدد الأطراف بدلاً من اتفاق ثنائي، حيث وُقِع ما يقرب من 57 في المائة من البلدان على اتفاق متعدد الأطراف، مقارنة بنسبة 46 في المائة من البلدان التي وقّعت على اتفاق ثنائي. وبالإضافة إلى ذلك، وقّعت بلدان عديدة (99 بلداً) أو صدقت على اتفاق متعدد الأطراف بشأن تبادل المعلومات وتمتية القدرات.

الشكل 25: المشاركة في الأنشطة الدولية



المصدر: الاتحاد الدولي للاتصالات

إلى جانب التعاون الرسمي بين بلدين أو أكثر، تتيح المشاركة في الأنشطة الدولية للبلدان فرصاً لفهم الممارسات الجيدة والنهج الجديدة للتصدي لتهديدات الأمن السيبراني. وعلى مدى العامين الماضيين، شارك 140 بلداً في أنشطة دولية مع بلدان أخرى مثل المؤتمرات وورش العمل والشراكات والاتفاقيات بشأن الأمن السيبراني.

الشراكات بين القطاعين العام والخاص

إلى جانب التعاون مع بلدان أخرى، تتعاون البلدان مع جهات فاعلة من القطاع الخاص. وتعد الشراكات بين القطاعين العام والخاص (PPP) بالغة الأهمية لجهود الأمن السيبراني، بدءاً من تبادل المعلومات الاستخباراتية القابلة للتنفيذ، وتبادل الممارسات الجيدة، إلى الإبلاغ عن احتياجات وأولويات البحث والتطوير. ويعرض الجدول 2 عدد البلدان المشاركة في الشراكات بين القطاعين العام والخاص على الصعيدين الدولي و/أو المحلي.

الجدول 2: البلدان المشاركة في شركات دولية و/أو محلية بين القطاعين العام والخاص

عدم وجود شركات دولية بين القطاعين العام والخاص	شركات دولية بين القطاعين العام والخاص في طور التنفيذ	شركات دولية بين القطاعين العام والخاص	
14	0	62	شركات محلية بين القطاعين العام والخاص
0	0	1	شركات محلية بين القطاعين العام والخاص في طور التنفيذ
104	1	12	عدم وجود شركات محلية بين القطاعين العام والخاص

المصدر: الاتحاد الدولي للاتصالات

بغية الانخراط في النظام الإيكولوجي الأوسع للأمن السيبراني، نظمت بعض البلدان مؤتمرات وورش عمل، في حين تعاقبت بلدان أخرى مع شركات من القطاع الخاص لإعداد دورات تدريبية من أجل القطاع العام. وأبلغ عدد متزايد من البلدان عن تطوير مجتمعات للعلوم والتكنولوجيات لتعزيز أنظمتها الإيكولوجية للأمن السيبراني. ويمكن أن تكون هذه المنصات بمثابة موقع للقطاعين العام والخاص من أجل الاجتماع وتقديم التدريب وتنظيم ورش عمل ومساعدة الشركات الناشئة واستضافة المسابقات. والهدف من هذا النوع من المبادرات المشتركة بين القطاعات تطوير نظام إيكولوجي للأمن السيبراني وتبادل المعارف والكفاءات بين مختلف أصحاب المصلحة، والباحثين والطلاب وخبراء الأمن السيبراني والشركات الناشئة والمؤسسات الحكومية والشركات الأجنبية. وتُظهر البيانات المجمعة أن ما يقرب من نصف البلدان لديها شراكة من نوع واحد على الأقل، حيث يشارك 86 بلداً أو سيشارك قريباً، إما في شراكة دولية أو محلية بين القطاعين العام والخاص، مع انخراط 60 بلداً منها في شركات محلية ودولية على السواء.

6.2 حماية الأطفال على الإنترنت

الشكل 26: تقارير من سلسلة الاتحاد الخاصة بحماية الأطفال على الإنترنت



المصدر: الاتحاد الدولي للاتصالات

كما أشير في المبادئ التوجيهية بشأن حماية الأطفال على الإنترنت، تمثل حماية الأطفال على الإنترنت تحدياً عالمياً يتطلب نهجاً عالمياً.²⁵ وجاءت المبادئ التوجيهية في وقت كان فيه التعلم عن بُعد يعني استخدام الأطفال للإنترنت أكثر من أي وقت مضى، وتعرضهم بشكل أكبر للمخاطر خلال جائحة كوفيد-19. وعلى عكس الأجيال

السابقة التي انساقَت إلى التعلُّم عن بُعد عن طريق الراديو بسبب الأوبئة،²⁶ أتاحت التكنولوجيات الرقمية تجارب تعليمية تفاعلية ثنائية الاتجاه لا تعزز توصيل الطلاب بمواد التعلُّم فحسب، بل وأيضاً ببعضهم البعض.

وأعدت المبادئ التوجيهية للاتحاد بشأن حماية الأطفال على الإنترنت لمساعدة الأطفال والآباء والمعلمين في إدارة المخاطر عبر الإنترنت، مع الاستفادة أيضاً من إمكانيات التكنولوجيا الرقمية وتعزيز مهاراتهم الرقمية. وبالإضافة إلى ذلك، تقدم المبادئ التوجيهية أيضاً توصيات إلى واضعي السياسات لتسريع وضع واعتماد استراتيجية وخطط عمل وطنية سليمة لحماية الأطفال على الإنترنت، فضلاً عن تعزيز مشاركة القطاع الخاص في وضع هذه السياسات.

وفي هذا الصدد، تتيح المسائل المتعلقة بحماية الأطفال على الإنترنت قياس مدى استعداد البلدان للجيل الرقمي من خلال عدة بنود مثل القوانين القائمة لحماية الأطفال على الإنترنت، وآلية الإبلاغ عن القضايا على الإنترنت، وحملات التوعية والمناهج الدراسية فضلاً عن البلدان التي وضعت واتبعت استراتيجية لحماية الأطفال على الإنترنت.

الشكل 27: البلدان التي لديها استراتيجية لحماية الأطفال على الإنترنت



المصدر: الاتحاد الدولي للاتصالات

ووفقاً للاستبيان، أفاد 86 بلداً من أصل 194 بلداً باتخاذ تدابير لحماية الأطفال على الإنترنت. غير أن البيانات المجمعة تشير إلى أن 13 في المائة من البلدان لديها استراتيجية مستقلة مكرسة لحماية الأطفال على الإنترنت. ومن ناحية أخرى، لدى 30 في المائة من البلدان مبادرات لحماية الأطفال على الإنترنت مدمجة في استراتيجيات أو تشريعات أو مبادرات أوسع نطاقاً بشأن الجريمة السيبرانية.

وتبين النتائج كذلك أن أداء منطقة أوروبا جيد في المسائل المتعلقة بحماية الأطفال على الإنترنت، حيث نفذت 89 في المائة من البلدان القوانين المتعلقة بحماية الأطفال على الإنترنت تنفيذاً تاماً. وبالإضافة إلى ذلك، سُجِّلت 101 آلية للإبلاغ على الصعيد العالمي، بما في ذلك الخطوط الساخنة والمواقع الإلكترونية وعناوين البريد الإلكتروني ووسائل التواصل الاجتماعي، بل ذهب 81 من البلدان إلى أبعد من ذلك، من خلال تقاسم استراتيجياتها بشأن حماية الأطفال على الإنترنت ومبادراتها الأوسع نطاقاً.

7.2 خلاصة

إن الأمن السيبراني والسلوكيات والممارسات دائمة التطور. وسواء تعلق الأمر بحالة طوارئ صحية عالمية، أو تغير المناخ، أو ارتفاع نسبة الشيخوخة بين السكان، أو تحديات مستقبلية أخرى، توفر التكنولوجيات الرقمية أداة محفزة للمساعدة في دفع العالم إلى الأمام. وعندما تصل أهداف التنمية المستدامة (SDG) إلى مرحلة النضج في 2030، من المتوقع أن يكون 90 في المائة من سكان العالم المتوقعين، أو 7,5 مليار شخص، موصولين بالإنترنت.²⁷ مع ما يقدر بنحو 24,1 مليار²⁸ إلى 125 مليار²⁹ جهاز من أجهزة إنترنت الأشياء الموصولة. وإذا كان للجهود المبذولة في سبيل تحقيق أهداف التنمية المستدامة أن تستمر، فستكون هناك حاجة إلى الأمن السيبراني لضمان حلول رقمية آمنة وموثوقة وجديرة بالثقة.

ومن الدروس المستفادة من جائحة كوفيد-19- ضرورة معالجة مشاكل العمل الجماعي مثل الصحة أو الأمن السيبراني باتباع نهج شامل ومتعدد التخصصات. وسوف تتطلب معالجة جميع ركائز الرقم القياسي - القانونية والتقنية والتنظيمية وتنمية القدرات والتدابير التعاونية - توصيل الناس ببعضهم البعض وإرساء الثقة. وقد

²⁶ <https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/>

²⁷ <https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/>

²⁸ <https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030-generating-1-5-trillion-annual-revenue-301061873.html>

²⁹ https://cdn.ihs.com/www/pdf/loT_ebook.pdf

يتعين على البلدان، إلى جانب العمل معاً، أن تدعم دولاً أخرى أقل قدرة على التصدي لتحديات الأمن السيبراني، مثل أقل البلدان نمواً والدول الجزرية الصغيرة النامية والبلدان النامية غير الساحلية.

وللمضي قدماً في هذا المضمار، يتعين على البلدان معالجة مواطن القوة ومواطن الضعف لديها في مجال الأمن السيبراني والاستفادة من مزاياها التنافسية لتعزيز القدرات السيبرانية والصحة العامة. ويمكن أن يساعد الرقم القياسي العالمي للأمن السيبراني البلدان على الشروع في هذه العملية. ولمواصلة ذلك، قد تحتاج البلدان إلى النظر فيما يلي:

- التقييمات المنتظمة لالتزاماتها في مجال الأمن السيبراني، بما في ذلك المقاييس ذات المغزى؛
- مواصلة تطوير الأفرقة CIRT الوطنية ومواصلة إنشاء أفرقة CIRT خاصة بالقطاعات؛
- رصد وتحديث الاستراتيجيات الوطنية للأمن السيبراني من خلال خطط تنفيذ واضحة؛
- الشمول والتنوع ضمن القوة العاملة في مجال الأمن السيبراني، لا سيما الفئات الممثلة تمثيلاً ناقصاً مثل النساء والشباب؛
- المشاركة المنتظمة في الأنشطة الدولية لتبادل الممارسات الجيدة ودراسات الحالة وتحسين القدرة على التأهب والاستجابة؛
- تحسين قدرات الأمن السيبراني لدى الشركات المتناهية الصغر والصغيرة والمتوسطة (MSME)؛
- المشاركة المنتظمة لجميع أصحاب المصلحة المعنيين في الأمن السيبراني، بما في ذلك القطاع الخاص والهيئات الأكاديمية والمجتمع المدني.

3 نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتببات

1.3 الدرجات والمرتببات العالمية للبلدان

يعرض الجدول التالي الدرجة والمرتببة لكل بلد شارك في الاستبيان.

المرتبة	الدرجة	اسم البلد
18	96,6	البرازيل
19	96,25	بلجيكا
20	96,13	إيطاليا
21	96,04	عُمان
22	95,78	فنلندا
23	95,48	مصر
24	94,88	إندونيسيا
25	94,59	فيتنام
26	94,55	السويد
27	94,5	قطر
28	93,98	اليونان
29	93,89	النمسا
30	93,86	بولندا
31	93,15	كازاخستان
32	92,6	الدنمارك
33	92,53	الصين
33	92,53	كرواتيا
34	92,36	سلوفاكيا
35	91,28	هنغاريا
36	90,93	إسرائيل**
37	90,58	تنزانيا
38	89,92	مقدونيا الشمالية
39	89,8	صربيا
40	89,31	أذربيجان
41	88,82	قبرص
42	86,97	سويسرا**

الجدول 3: نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتببات

المرتبة	الدرجة	اسم البلد
1	100	الولايات المتحدة الأمريكية**
2	99,54	المملكة المتحدة
2	99,54	المملكة العربية السعودية
3	99,48	إستونيا
4	98,52	جمهورية كوريا
4	98,52	سنغافورة
4	98,52	إسبانيا
5	98,06	الاتحاد الروسي
5	98,06	الإمارات العربية المتحدة
5	98,06	ماليزيا
6	97,93	ليتوانيا
7	97,82	اليابان
8	97,67	كندا**
9	97,6	فرنسا
10	97,5	الهند
11	97,49	تركيا
12	97,47	أستراليا
13	97,41	لكسمبرغ
13	97,41	ألمانيا
14	97,32	البرتغال
15	97,28	لاتفيا
16	97,05	هولندا**
17	96,89	النرويج**
17	96,89	موريشيوس

الرقم القياسي العالمي للأمن السيبراني لعام 2020

الجدول 3: نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتبات (تابع)

المرتبة	الدرجة	اسم البلد
73	68,88	زامبيا
74	68,83	شيلي
75	67,82	كوت ديفوار
76	67,45	كوستاريكا
77	67,38	بلغاريا
78	65,93	أوكرانيا
79	64,88	باكستان
80	64,32	ألبانيا
81	63,72	كولومبيا
82	58,76	كوبا
83	58,65	سري لانكا
84	57,09	باراغواي
85	56,07	بروني دار السلام
86	55,67	بيرو
87	53,23	الجبل الأسود
88	53,06	بوتسوانا
89	50,57	بيلاروس
90	50,47	أرمينيا**
91	50,12	الأرجنتين
92	49,64	قيرغيزستان
93	45,63	كاميرون
94	44,99	جمهورية نيبال
95	40,44	تشاد
96	39,98	بوركينافاسو**
97	36,83	ملاوي
98	36,49	زمبابوي
99	36,41	ميانمار
100	35,85	السنگال
101	35,15	ليختنشتاين**
102	35,03	السودان
103	34,11	بنما

المرتبة	الدرجة	اسم البلد
43	86,69	غانا
44	86,5	تايلاند
45	86,23	تونس
46	85,86	أيرلندا
47	84,76	نيجيريا
48	84,04	نيوزيلندا**
49	83,65	مالطة
50	82,41	المغرب
51	81,7	كينيا
52	81,68	المكسيك
53	81,27	بنغلاديش
54	81,07	جمهورية إيران الإسلامية
55	81,06	جورجيا
56	80,06	بنن
57	79,95	رواندا
58	79,81	أيسلندا
59	78,46	جنوب إفريقيا**
60	77,86	البحرين
61	77	فلبين
62	76,29	رومانيا
63	75,78	مولدوفا
64	75,15	أوروغواي
65	75,07	الكويت
66	75,05	الجمهورية الدومينيكية
67	74,93	سلوفينيا
68	74,37	الجمهورية التشيكية
69	72,57	موناكو
70	71,11	أوزبكستان
71	70,96	الأردن
72	69,98	أوغندا

الجدول 3: نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتبات (تابع)

المرتبة	الدرجة	اسم البلد
134	18,34	بوتان
135	18,23	إسواتيني
136	17,74	كابو فيردي
137	17,25	الصومال
138	17,1	طاجيكستان**
139	16,89	بربادوس
140	16,14	دولة بوليفيا المتعددة القوميات
141	15,64	سان تومي وبرينسيبي
142	15,62	أنتيغوا وبربودا
143	14,72	جمهورية الكونغو**
144	14,48	تركمانستان**
145	13,84	كيريباتي
146	13,83	سان مارينو
147	13,37	البهاما
148	13,3	السلفادور**
149	13,23	سيشيل**
150	13,13	غواتيمالا
151	12,99	أنغولا
152	12,88	فانواتو
153	12,44	سانت كيتس ونيفيس**
154	12,18	سانت فنسنت وغرينادين**
155	11,47	ناميبيا
156	11,38	النيجر
157	11,36	غابون
158	10,96	سانت لوسيا**
159	10,29	بليز
160	10,14	مالي**
161	9,85	غينيا بيساو
162	9,72	ليبيريا
163	9,41	غرينادا
164	9,08	ليسوتو

المرتبة	الدرجة	اسم البلد
104	33,95	الجزائر
105	33,19	توغو
106	32,53	جامايكا**
107	32,12	غامبيا
108	31,2	سورينام
109	30,44	لبنان**
110	29,44	البوسنة والهرسك
111	29,33	ساموا
112	29,08	فيجي
113	28,78	ليبيا
114	28,11	غيانا
115	27,74	إثيوبيا
116	27,06	فنزويلا
117	26,38	أندورا**
118	26,33	بابوا غينيا الجديدة**
119	26,3	إكوادور
120	26,2	منغوليا
121	25,31	سيراليون
122	25,18	دولة فلسطين
123	24,18	موزامبيق
124	23,33	مدغشقر**
125	22,18	ترينيداد وتوباغو
126	22,14	الجمهورية العربية السورية**
127	21,42	ناورو**
128	20,95	تونغا**
129	20,71	العراق**
130	20,53	غينيا**
131	20,34	جمهورية لاو الديمقراطية الشعبية
132	19,12	كمبوديا**
133	18,94	موريتانيا

الرقم القياسي العالمي للأمن السيبراني لعام 2020

المرتبة	الدرجة	اسم البلد
176	3,24	جمهورية إفريقيا الوسطى**
177	2,95	ملديف**
178	2,2	هندوراس**
179	1,73	جيبوتي
179	1,73	بوروندي
179	1,73	إريتريا**
180	1,46	غينيا الاستوائية**
181	1,35	جمهورية كوريا الشعبية الديمقراطية**
182	0	ميكرونيزيا*
182	0	الفايكان*
182	0	اليمن*

* لم تُجمع أي بيانات

** لا يوجد رد على الاستبيان

الجدول 3: نتائج الرقم القياسي العالمي للأمن السيبراني: الدرجات والمرتبات (تابع)

المرتبة	الدرجة	اسم البلد
165	9	نيكاراغوا**
166	7,08	جزر سليمان
167	6,4	هايتي
168	5,78	توفالو**
169	5,75	جنوب السودان**
170	5,3	جمهورية الكونغو الديمقراطية
171	5,2	أفغانستان
172	4,9	جزر مارشال**
173	4,26	تيمور-ليشتي**
174	4,2	دومينيكا
175	3,72	جزر القمر**

2.3 الدرجات والمرتبات الإقليمية للبلدان

الجدول 4: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة إفريقيا

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
13	45,63	كاميرون
14	40,44	تشاد
15	39,98	بوركينافاسو**
16	36,83	ملاوي
17	36,49	زيمبابوي
18	35,85	السنغال
19	33,19	توغو
20	32,12	غامبيا
21	27,74	إثيوبيا
22	25,31	سيراليون
23	24,18	موزامبيق
24	23,33	مدغشقر
25	20,53	غينيا**
26	18,23	إسواتيني

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	96,89	موريشيوس
2	90,58	تنزانيا
3	86,69	غانا
4	84,76	نيجيريا
5	81,7	كينيا
6	80,06	بنن
7	79,95	رواندا
8	78,46	جنوب إفريقيا**
9	69,98	أوغندا
10	68,88	زامبيا
11	67,82	كوت ديفوار
12	53,06	بوتسوانا

الجدول 4: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة إفريقيا (تابع)

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
7	68,83	شيلي
8	67,45	كوستاريكا
9	63,72	كولومبيا
10	58,76	كوبا
11	57,09	باراغواي
12	55,67	بيرو
13	50,12	الأرجنتين
14	34,11	بنما
15	32,53	جامايكا**
16	31,2	سورينام
17	28,11	غيانا
18	27,06	فنزويلا
19	26,3	إكوادور
20	22,18	ترينيداد وتوباغو
21	16,89	بربادوس
22	16,14	دولة بوليفيا المتعددة القوميات
23	15,62	أنتيغوا وبربودا
24	13,37	البهاما
25	13,3	السلفادور**
26	13,13	غواتيمالا
27	12,44	سانت كيتس ونيفيس
28	12,18	سانت فنسنت وغرينادين**
29	10,96	سانت لوسيا**
30	10,29	بليز
31	9,41	غرينادا
32	9	نيكاراغوا
33	6,4	هايتي
34	4,2	دومينيكا
35	2,2	هندوراس**

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
27	17,74	كابو فيردي
28	15,64	سان تومي وبرينسيبي
29	14,72	جمهورية الكونغو**
30	13,23	سيشيل**
31	12,99	أنغولا
32	11,47	ناميبيا
33	11,36	النيجر
34	11,38	غابون
35	10,14	مالي**
36	9,85	غينيا بيساو
37	9,72	ليبيريا
38	9,08	ليسوتو
39	5,75	جنوب السودان**
40	5,3	جمهورية الكونغو الديمقراطية
41	3,24	جمهورية إفريقيا الوسطى**
42	1,73	بوروندي
42	1,73	إريتريا**
43	1,46	غينيا الاستوائية**

* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

الجدول 5: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة الأمريكتين

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	100	الولايات المتحدة الأمريكية**
2	97,67	كندا**
3	96,6	البرازيل
4	81,68	المكسيك
5	75,15	أوروغواي
6	75,07	الجمهورية الدومينيكية

* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

الجدول 6: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة الدول العربية

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
2	98,06	ماليزيا
3	97,82	اليابان
4	97,49	الهند
5	97,47	أستراليا
6	94,88	إندونيسيا
7	94,55	فيتنام
8	92,53	الصين
9	86,5	تايوان
10	84,04	نيوزيلندا**
11	81,27	بنغلاديش
12	81,06	جمهورية إيران الإسلامية
13	77	فلبين
14	64,88	باكستان
15	58,65	سري لانكا
16	56,07	بروني دار السلام
17	44,99	جمهورية نيبال
18	36,41	ميانمار
19	29,33	ساموا
20	29,08	فيجي
21	26,33	بابوا غينيا الجديدة**
22	26,2	منغوليا
23	21,42	ناورو**
24	20,95	تونغا**
25	20,34	جمهورية لاو الديمقراطية الشعبية
26	19,12	كمبوديا**
27	18,34	بوتان
28	13,84	كيريباتي
29	12,88	فانواتو
30	7,08	جزر سليمان
31	5,78	توفالو**
32	5,2	أفغانستان

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	99,54	المملكة العربية السعودية
2	98,06	الإمارات العربية المتحدة
3	96,04	عُمان
4	95,48	مصر
5	94,5	قطر
6	86,23	تونس
7	82,41	المغرب
8	77,86	البحرين
9	75,05	الكويت
10	70,96	الأردن
11	35,03	السودان
12	33,95	الجزائر
13	30,44	لبنان**
14	28,78	ليبيا
15	25,18	دولة فلسطين
16	22,14	الجمهورية العربية السورية**
17	20,71	العراق**
18	18,94	موريتانيا
19	17,25	الصومال
20	3,72	جزر القمر**
21	1,73	جيبوتي
22	0	اليمن*

* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

الجدول 7: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة آسيا-المحيط الهادئ

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	98,52	جمهورية كوريا
1	98,52	سنغافورة

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
4	97,93	ليتوانيا
5	97,6	فرنسا
6	97,5	تركيا
7	97,41	لكسمبرغ
7	97,41	ألمانيا
8	97,32	البرتغال
9	97,28	لاتفيا
10	97,05	هولندا**
11	96,89	النرويج**
12	96,25	بلجيكا
13	96,13	إيطاليا
14	95,78	فنلندا
15	94,59	السويد
16	93,98	اليونان
17	93,89	النمسا
18	93,86	بولندا
19	92,6	الدنمارك
20	92,53	كرواتيا
21	92,36	سلوفاكيا
22	91,28	هنغاريا
23	90,93	إسرائيل**
24	89,92	جمهورية مقدونيا الشمالية
25	89,8	صربيا
26	88,82	قبرص
27	86,97	سويسرا**
28	85,86	أيرلندا
29	83,65	مالطة
30	81,07	جورجيا
31	79,81	أيسلندا
32	76,29	رومانيا
33	75,78	مولدوفا

الجدول 7: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة آسيا-المحيط الهادئ (تابع)

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
33	4,9	جزر مارشال**
34	4,26	تيمور-ليشتي**
35	2,95	ملديف**
36	1,35	جمهورية كوريا الشعبية الديمقراطية**
37	0	ميكرونيزيا*

* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

الجدول 8: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة كومنولث الدول المستقلة

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	98,06	الاتحاد الروسي
2	93,15	كازاخستان
3	89,31	أذربيجان
4	71,11	أوزبكستان
5	50,57	بيلاروس
6	50,47	أرمينيا**
7	49,64	قيرغيزستان
8	17,1	طاجيكستان**
9	14,48	تركمستان**

* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

الجدول 9: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة أوروبا

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
1	99,54	المملكة المتحدة
2	99,48	إستونيا
3	98,52	إسبانيا

الجدول 9: نتائج الرقم القياسي العالمي للأمن السيبراني: منطقة أوروبا (تابع)

المرتبة الإقليمية	الدرجة الإجمالية	اسم البلد
34	74,93	سلوفينيا
35	74,37	الجمهورية التشيكية
36	72,57	موناكو
37	67,38	بلغاريا
39	65,93	أوكرانيا
40	64,32	ألبانيا
41	53,23	الجيل الأسود
42	35,15	ليختنشتاين**
43	29,44	البوسنة والهرسك
44	26,38	أندورا**
45	13,83	سان مارينو
46	0	الفاتيكان*

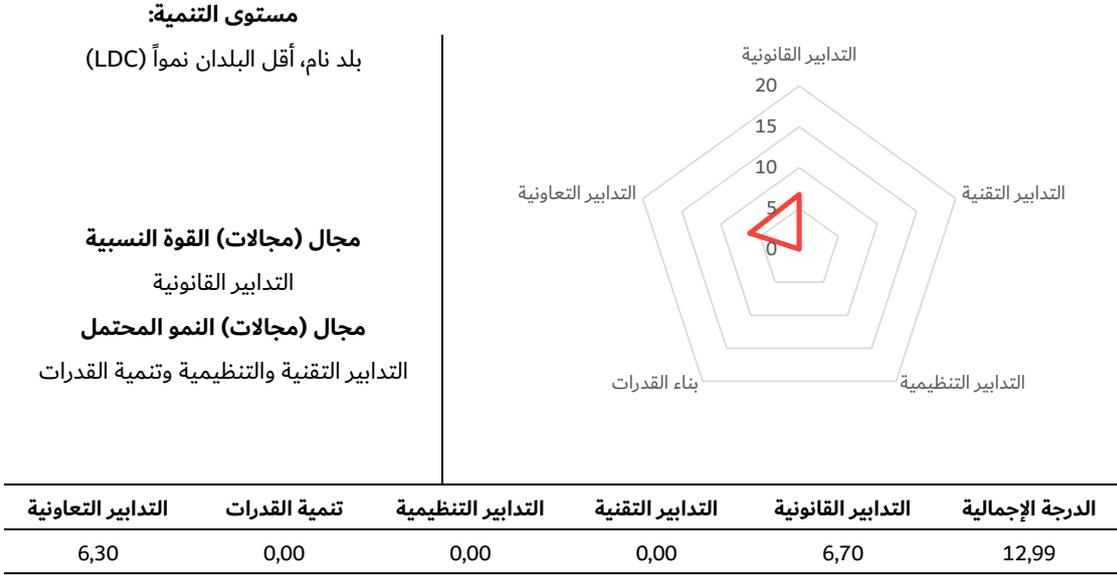
* لا توجد بيانات

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

4 الرقم القياسي العالمي للأمن السيبراني: الموجزات القطرية

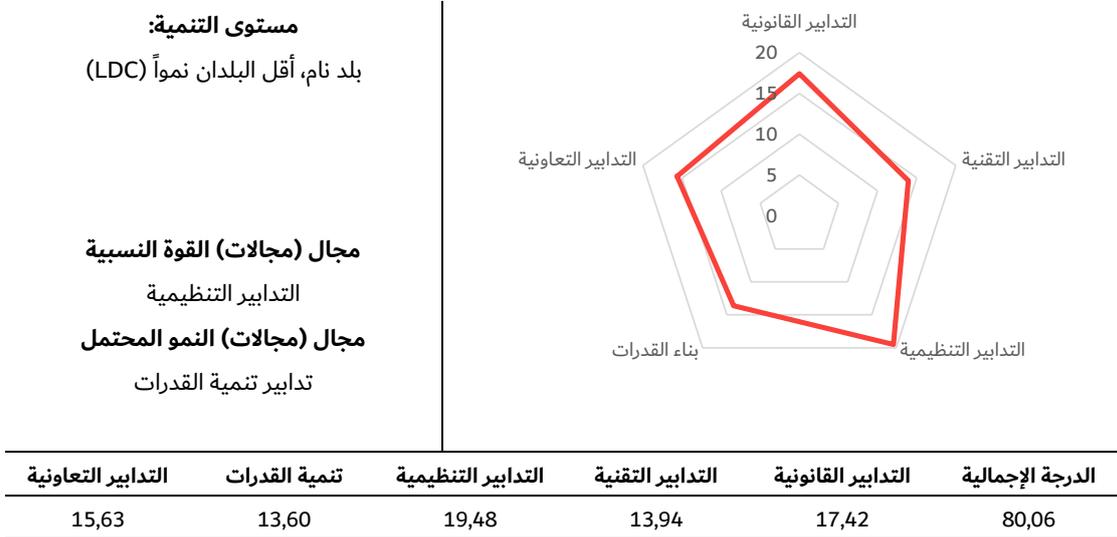
منطقة إفريقيا

جمهورية أنغولا



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بنين

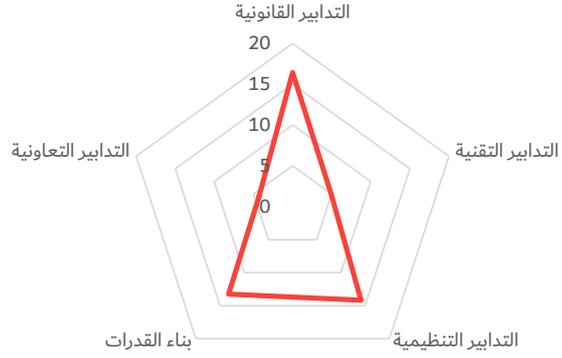


المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بوتسوانا

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التعاونية والتقنية



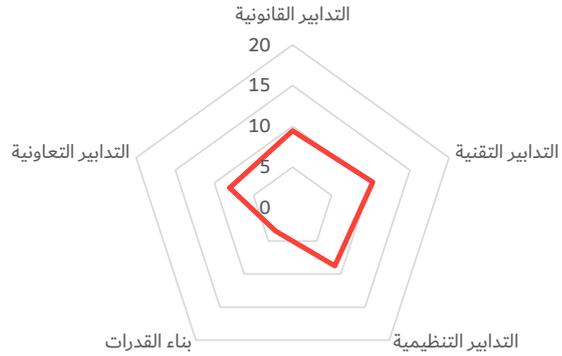
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
53,06	16,44	4,95	14,16	13,23	4,26

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

بوركينافاسو**

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التقنية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
39,98	9,47	10,25	8,75	3,47	8,04

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بروندي

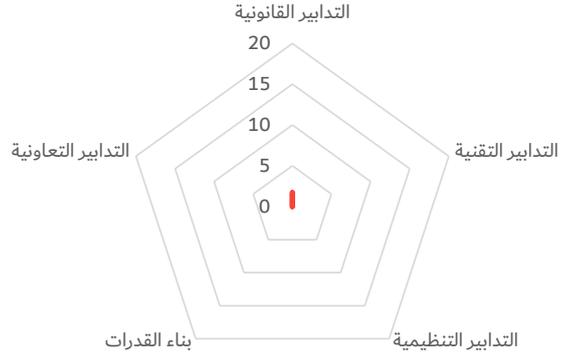
مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	0,00	0,00	1,73	1,73

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كابو فيردي

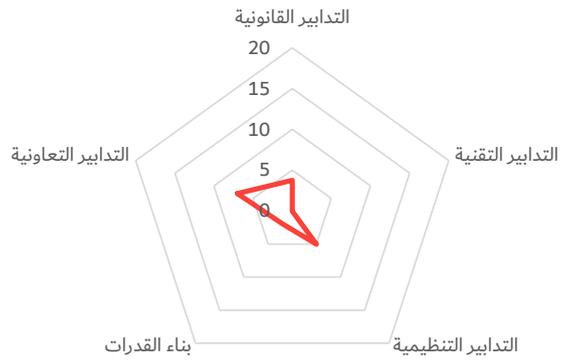
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
7,00	1,96	5,00	0,00	3,77	17,74

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الكاميرون

مستوى التنمية:

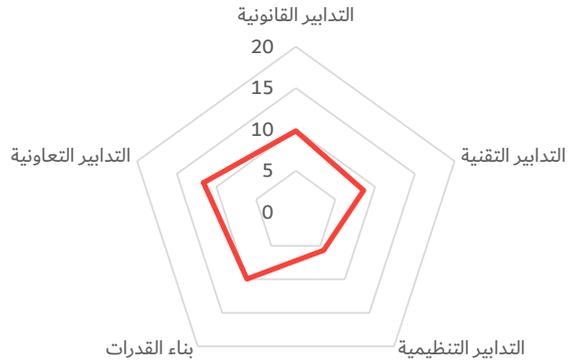
بلد نام

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
45,63	9,84	8,54	5,67	9,95	11,63

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية إفريقيا الوسطى**

مستوى التنمية:

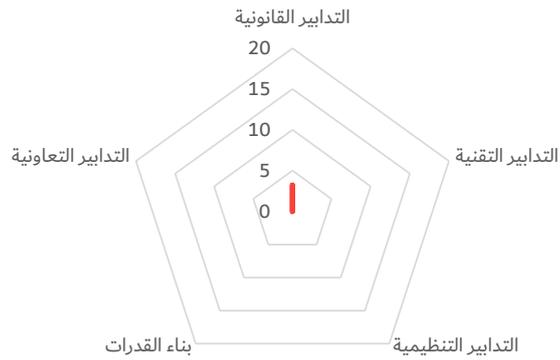
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية
وتدابير تنمية القدرات والتدابير التعاونية



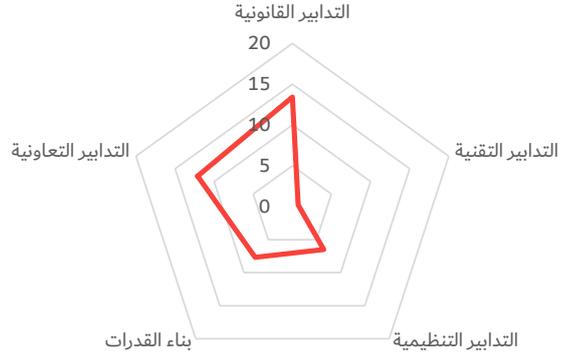
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
3,24	3,24	0,00	0,00	0,00	0,00

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية تشاد

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



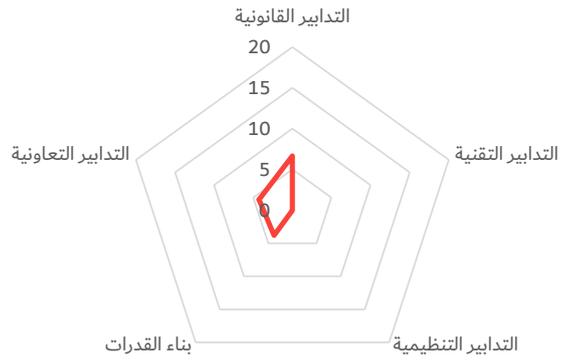
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
12,11	7,67	6,50	0,73	13,43	40,44

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الكونغو**

مستوى التنمية:
بلد نام

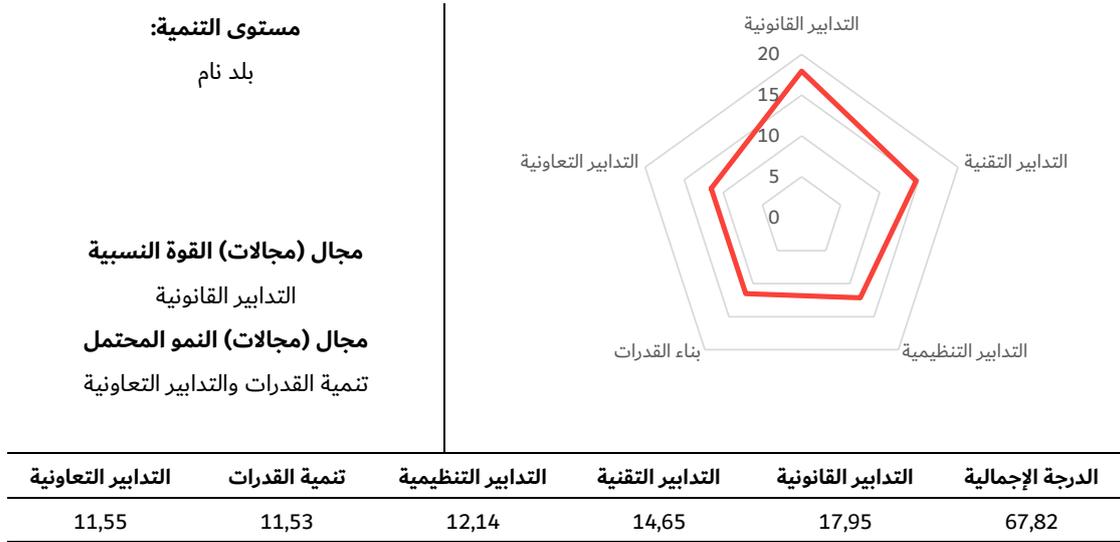
مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	3,80	0,00	0,00	6,66	14,72

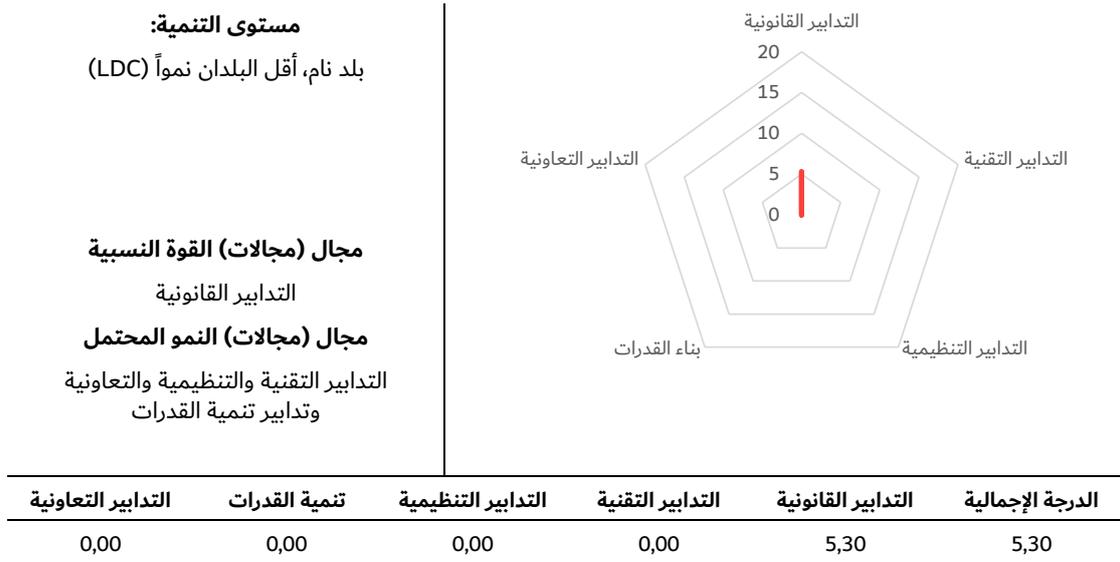
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كوت ديفوار



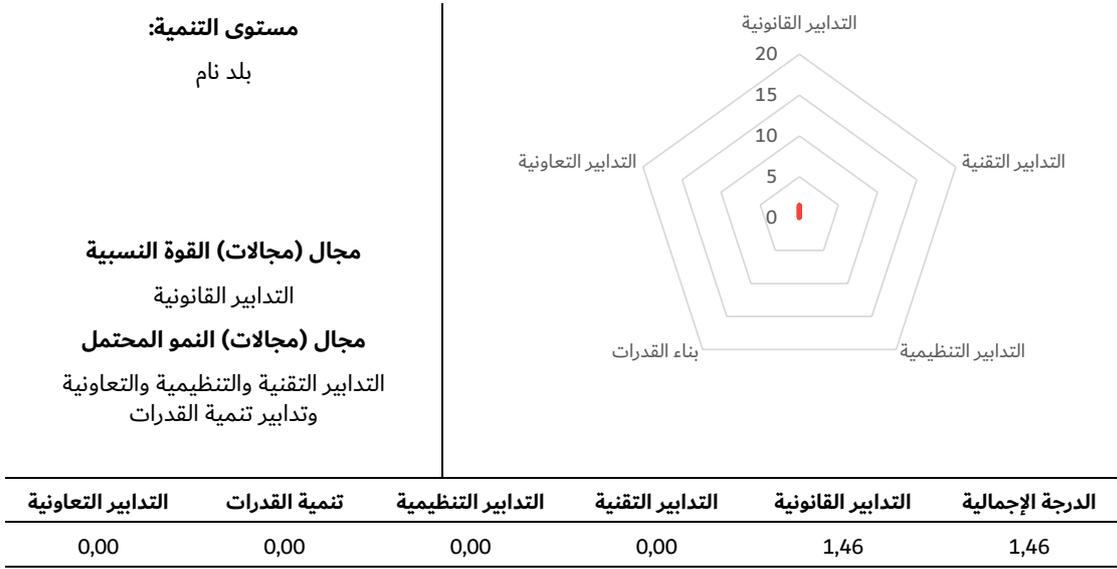
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الكونغو الديمقراطية



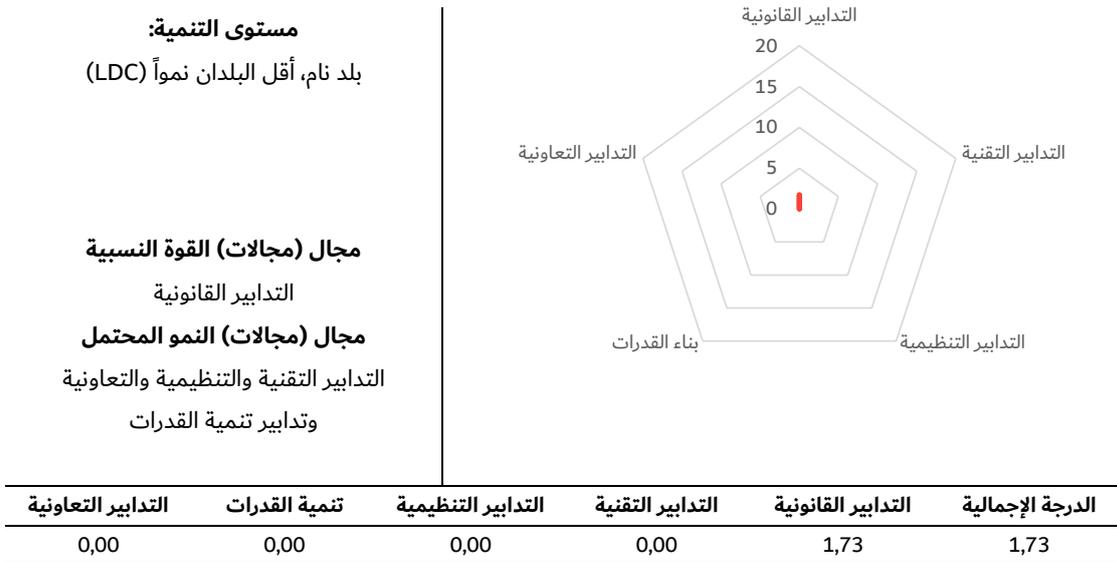
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية غينيا الاستوائية**



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

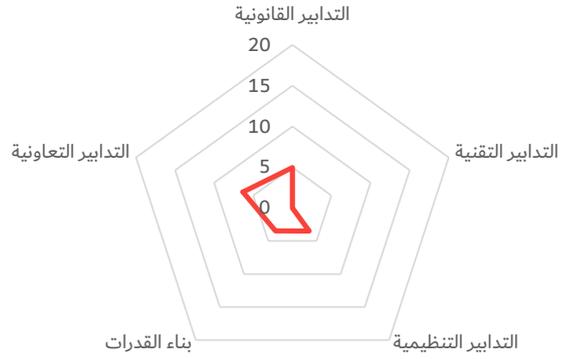
إريتريا**



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التعاونية
مجال (مجالات) النمو المحتمل
التدابير التقنية

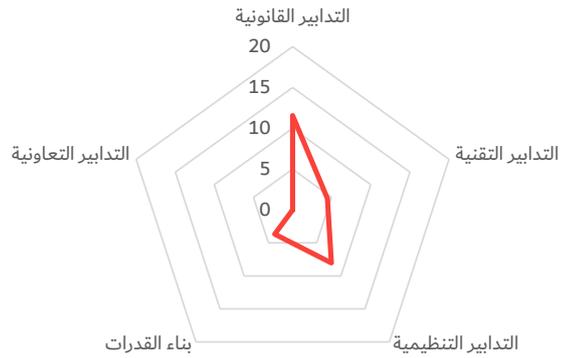


الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
18,23	4,96	0,00	3,49	3,47	6,31

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

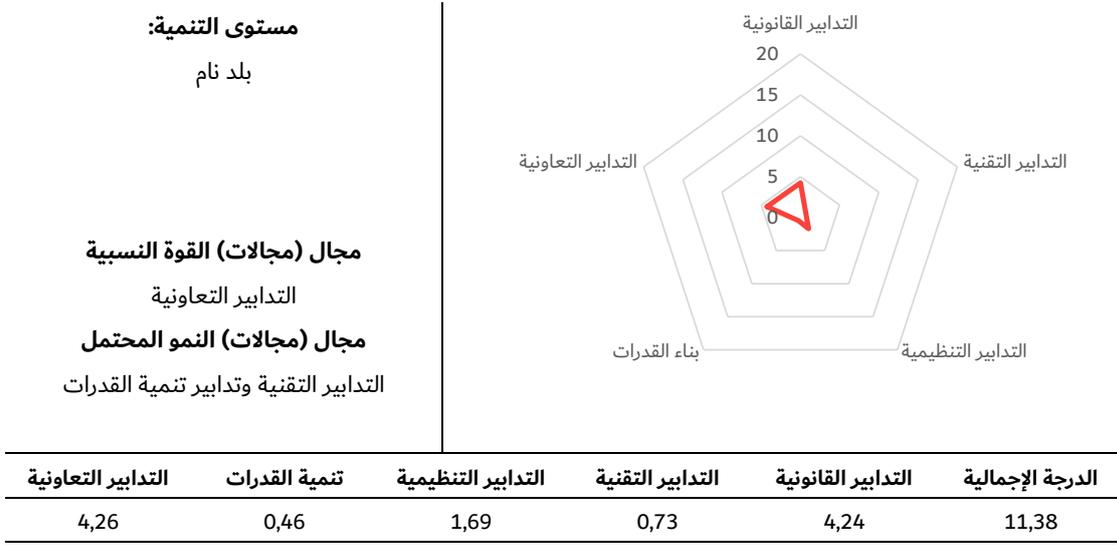
مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
27,74	11,56	4,46	8,03	3,69	0,00

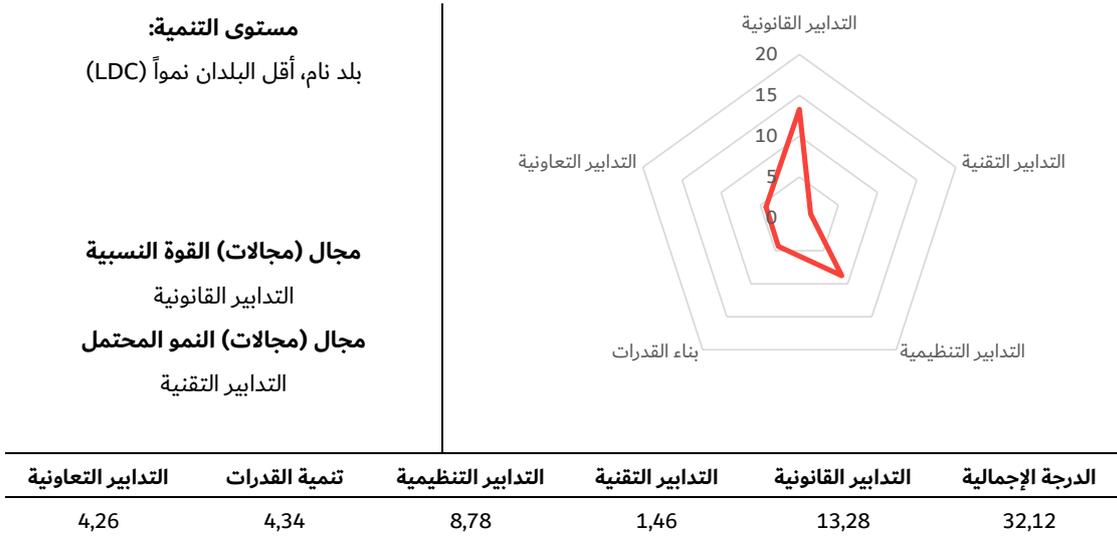
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الجمهورية الغابونية



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية غامبيا



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

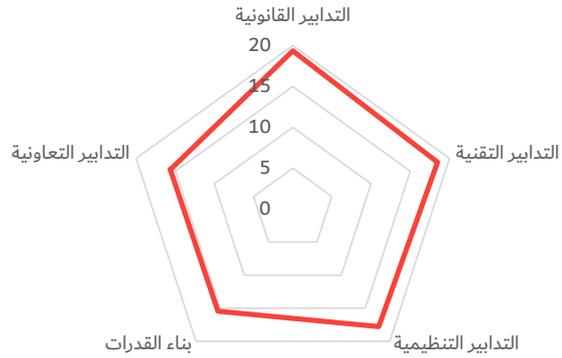
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية

مجال (مجالات) النمو المحتمل

تنمية القدرات والتدابير التعاونية



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
86,69	19,35	18,48	17,78	15,44	15,63

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية غينيا **

مستوى التنمية:

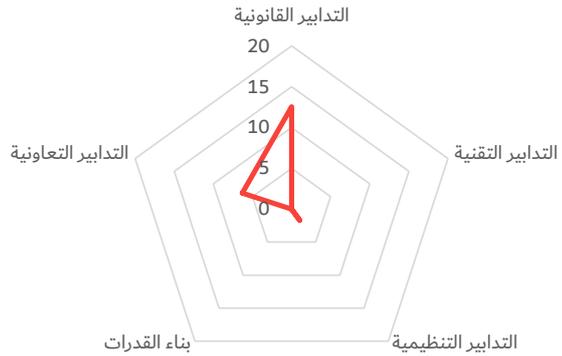
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية وتدابير تنمية القدرات



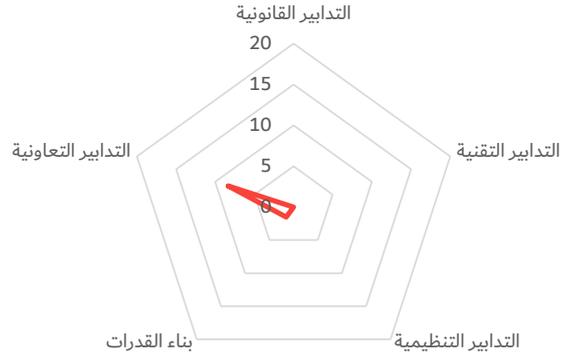
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
20,53	12,54	0,00	1,69	0,00	6,30

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية غينيا-بيساو

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير التعاونية
مجال (مجالات) النمو المحتمل
التدابير القانونية والتقنية والتنظيمية



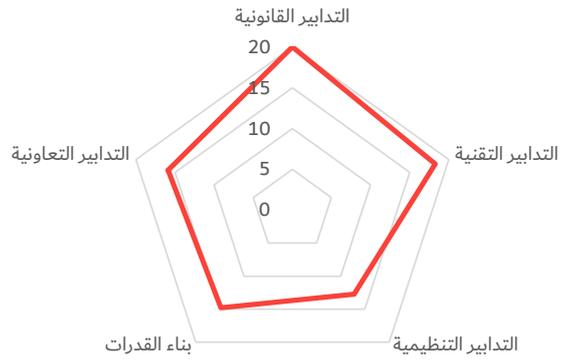
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
0,00	0,00	0,00	1,52	8,33	9,85

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كينيا

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



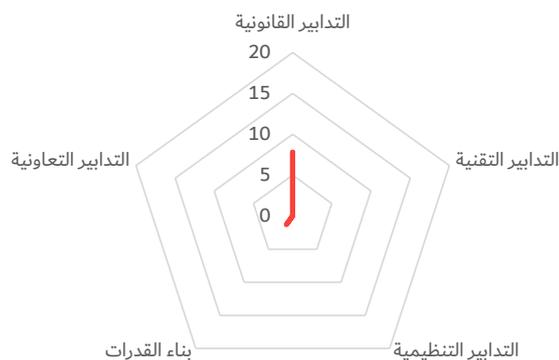
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	18,27	12,75	14,79	15,89	81,70

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة ليسوتو

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
7,82	0,00	0,00	1,26	0,00	9,08

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية ليبيريا

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التقنية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
2,31	4,11	0,00	1,26	2,04	9,72

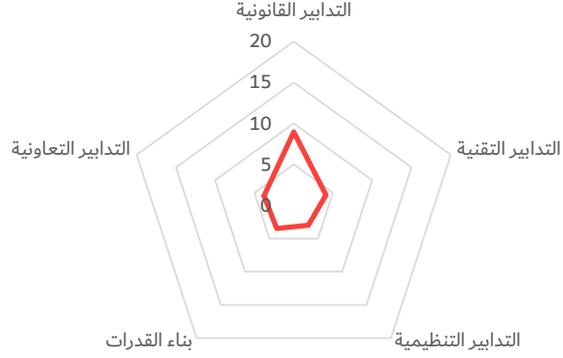
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية مدغشقر**

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير القانونية

مجال (مجالات) النمو المحتمل
التدابير التنظيمية والتعاونية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
3,78	3,47	3,00	4,11	8,96	23,33

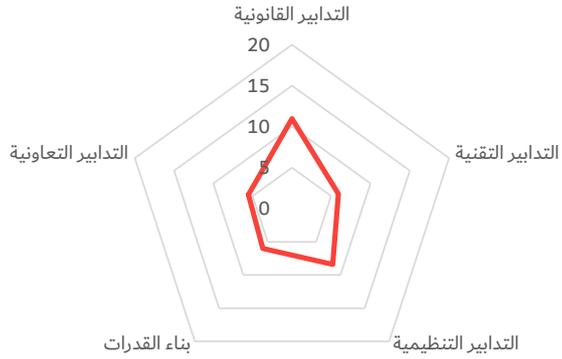
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

ملاوي

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتنظيمية

مجال (مجالات) النمو المحتمل
التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
5,54	6,00	8,40	5,92	10,98	36,83

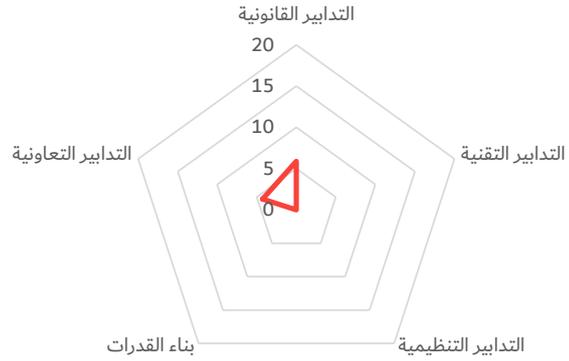
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية مالي

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية

مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية وتدابير تنمية
القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	0,00	0,00	0,00	5,89	10,14

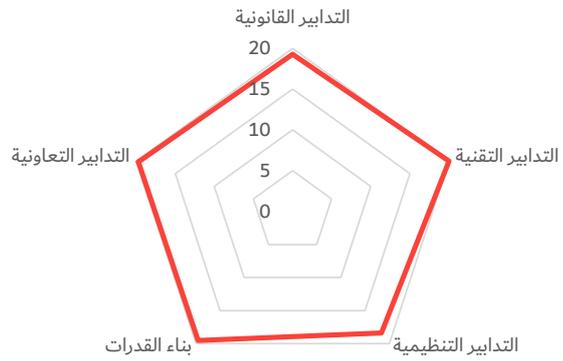
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية موريشيوس

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير التقنية والتعاونية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل
التدابير التنظيمية



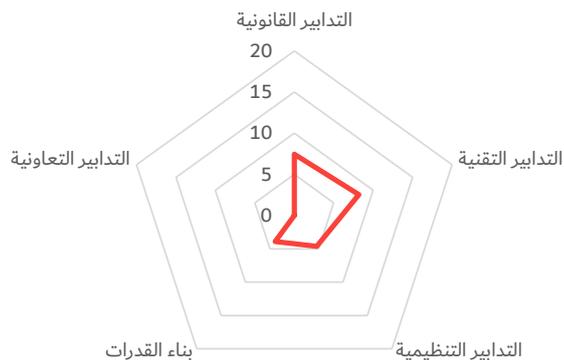
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,70	19,54	18,38	20,00	19,27	96,89

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية موزامبيق

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التقنية والقانونية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



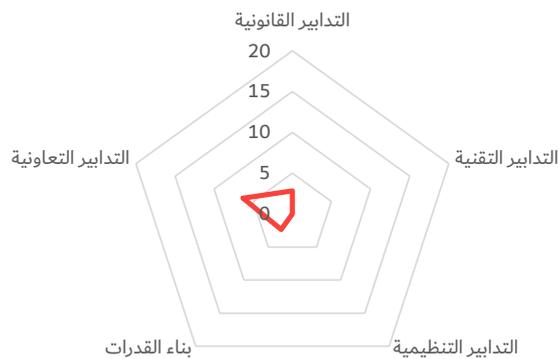
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
7,46	8,19	4,62	3,92	0,00	24,181

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية ناميبيا

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير التعاونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية



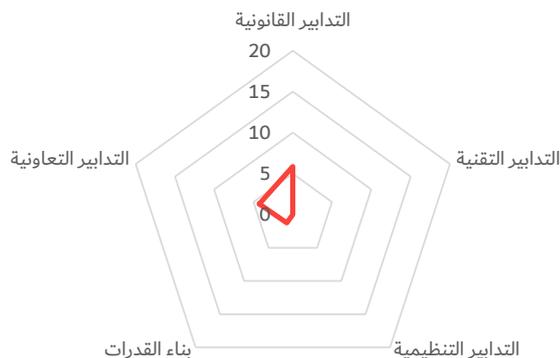
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
2,84	0,00	0,00	2,34	6,30	11,47

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية النيجر

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية



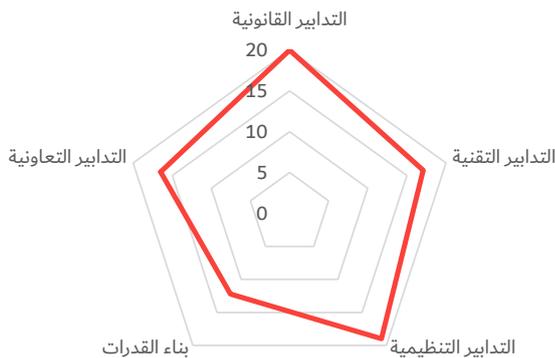
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
11,36	5,87	0,00	0,00	1,23	4,26

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية نيجيريا الاتحادية

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



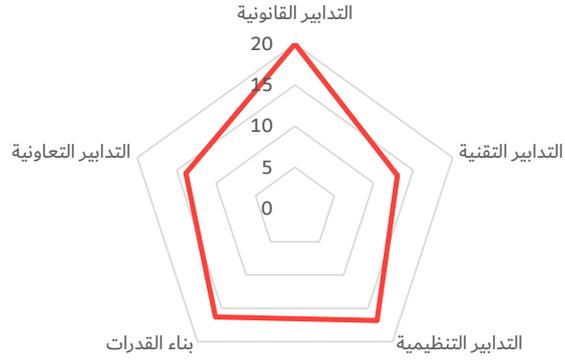
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
84,76	20,00	17,09	18,98	12,21	16,48

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية رواندا

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



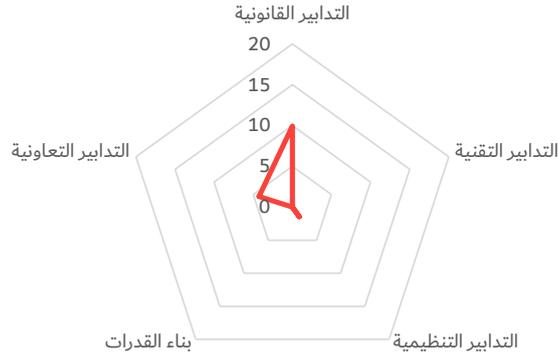
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
13,82	16,30	16,83	13,00	20,00	79,95

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سان تومي وبرينسيبي الديمقراطية

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية وتدابير تنمية القدرات



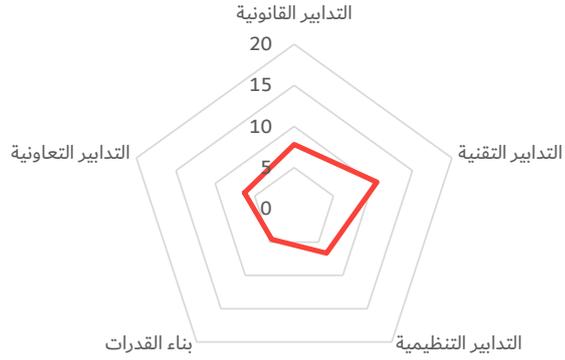
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	0,00	1,44	0,00	9,94	15,64

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية السنغال

مستوى التنمية:
بلد نام، أقل البلدان النامية (LDC)

مجال (مجالات) القوة النسبية
التدابير التقنية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



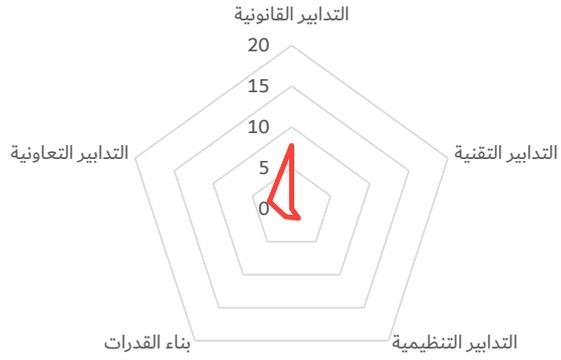
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
6,30	4,58	6,66	10,50	7,82	35,85

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سيشيل**

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية

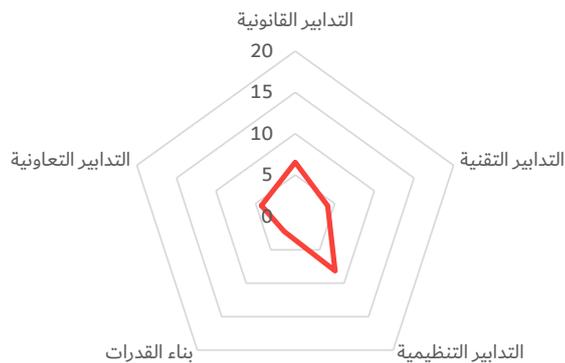


التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
2,83	1,23	1,44	0,00	7,73	13,23

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التنظيمية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



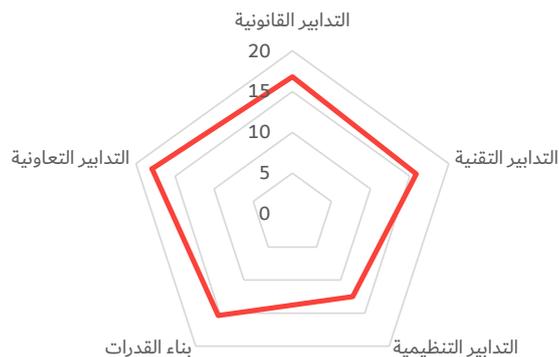
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
6,54	4,11	8,16	2,24	4,26	25,31

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

جمهورية جنوب إفريقيا**

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير التعاونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
16,82	15,85	12,50	15,37	17,93	78,46

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

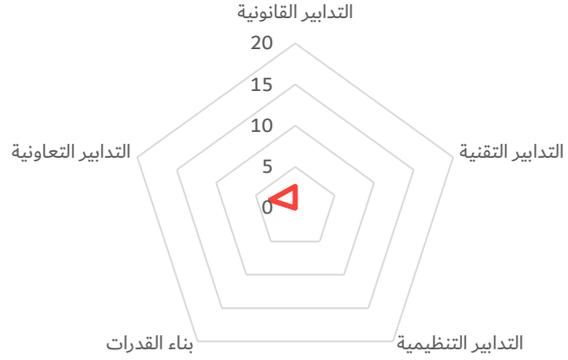
الرقم القياسي العالمي للأمن السيبراني لعام 2020

جمهورية جنوب السودان**

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التعاونية

مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية وتدابير تنمية
القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
3,12	0,00	0,00	0,00	2,63	5,75

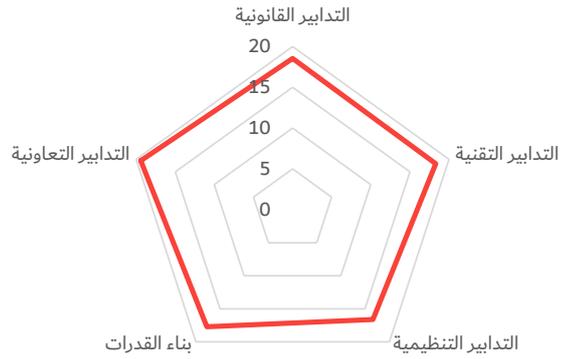
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية تنزانيا المتحدة

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التعاونية

مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	17,72	16,60	18,31	18,54	90,58

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية توغو

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
5,49	0,00	3,61	4,90	19,19	33,19

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية أوغندا

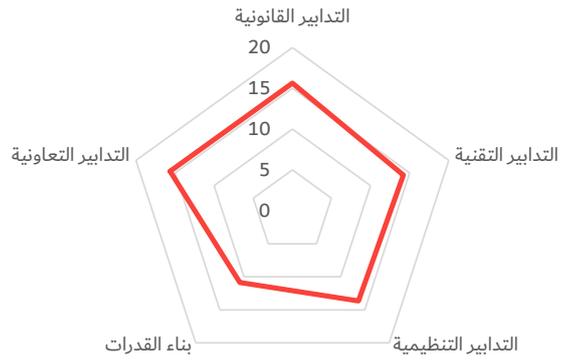
مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,63	10,87	13,65	14,19	15,64	69,98

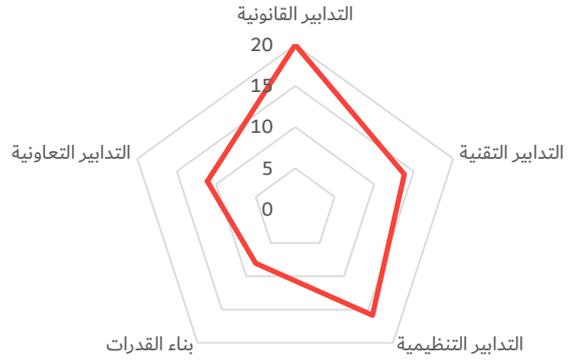
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الرقم القياسي العالمي للأمن السيبراني لعام 2020

جمهورية زامبيا

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



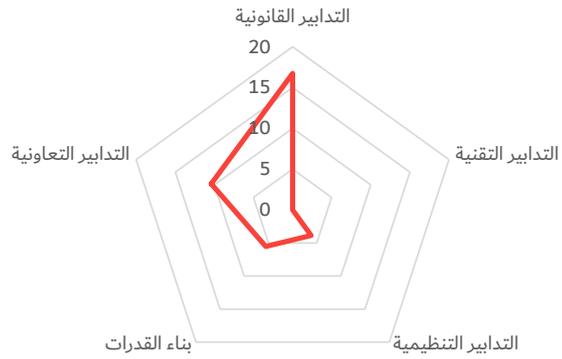
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
11,12	8,07	15,86	13,82	20,00	68,88

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية زيمبابوي

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
10,40	5,52	3,84	0,00	16,73	36,49

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

منطقة الأمريكتين

أنتيغوا وبربودا

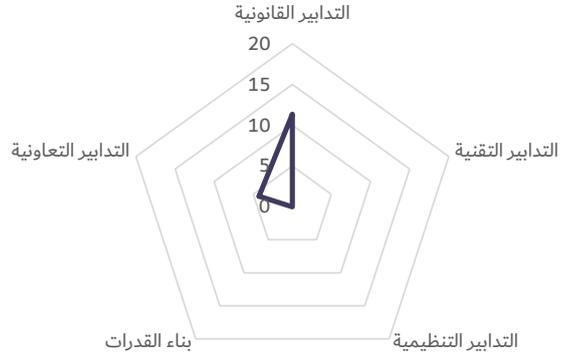
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
11,36	0,00	0,00	0,00	4,26	15,62

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الأرجنتين

مستوى التنمية:

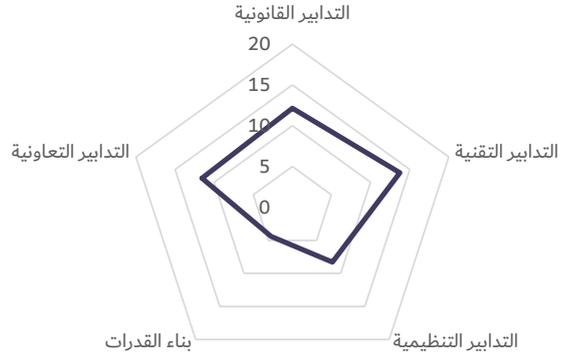
بلد نام

مجال (مجالات) القوة النسبية

التدابير التقنية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
12,15	13,75	8,29	4,38	11,55	50,12

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

كومنولث البهاما

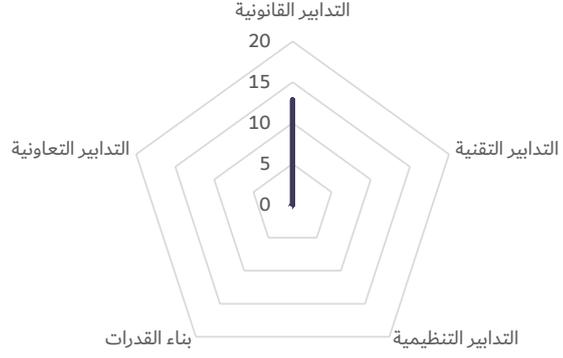
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية
وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
12,85	0,00	0,00	0,52	0,00	13,37

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

بربادوس

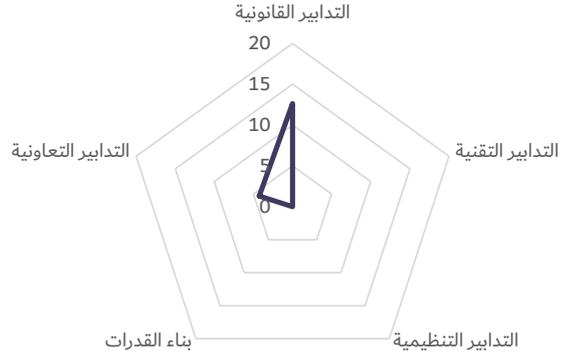
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية
وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
12,63	0,00	0,00	0,00	4,26	16,89

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
5,77	0,00	3,01	1,52	0,00	10,29

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة بوليفيا المتعددة القوميات

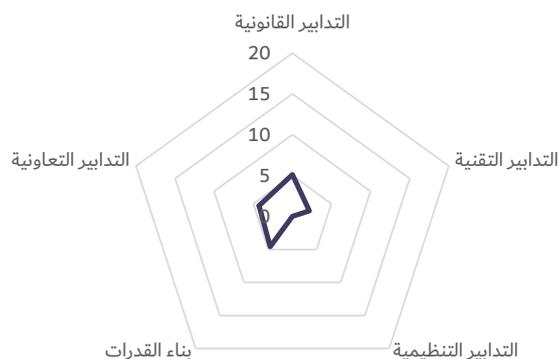
مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
5,13	2,18	0,00	4,58	4,26	16,14

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية البرازيل الاتحادية

مستوى التنمية:

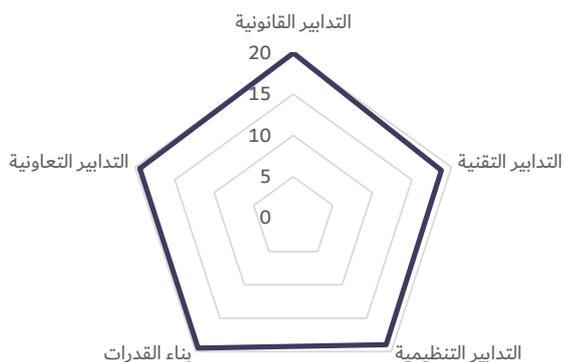
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	19,48	18,98	18,73	20,00	96,60

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

كندا**

مستوى التنمية:

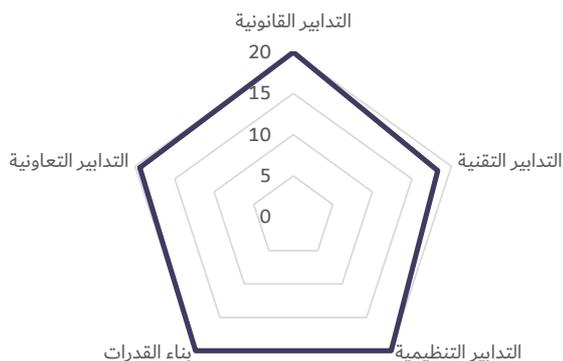
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتنظيمية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	20,00	20,00	18,27	20,00	97,67

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

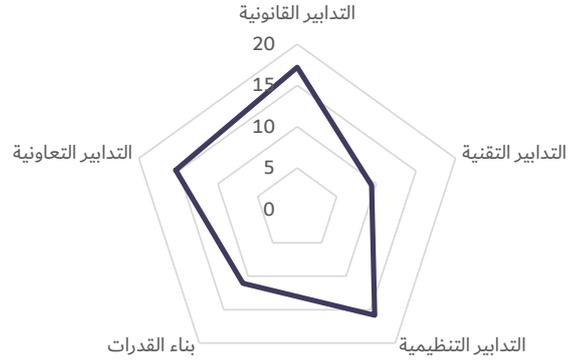
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,33	11,07	15,84	9,39	17,20	68,83

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

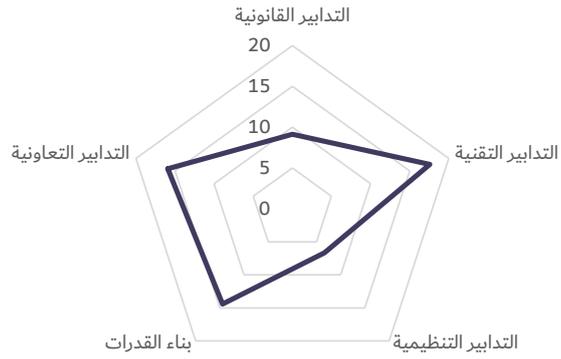
بلد نام

مجال (مجالات) القوة النسبية

التدابير التقنية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,93	14,42	6,67	17,58	9,14	63,72

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

كوستاريكا

مستوى التنمية:

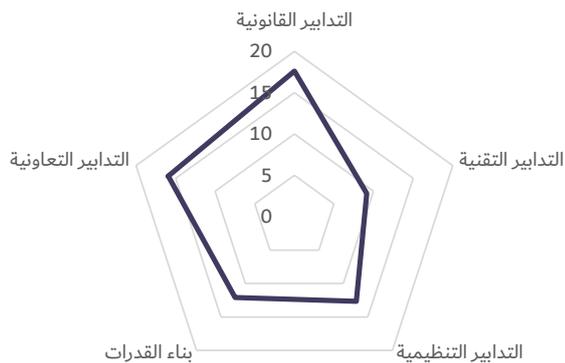
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,93	12,11	12,66	9,14	17,62	67,45

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

كوبا

مستوى التنمية:

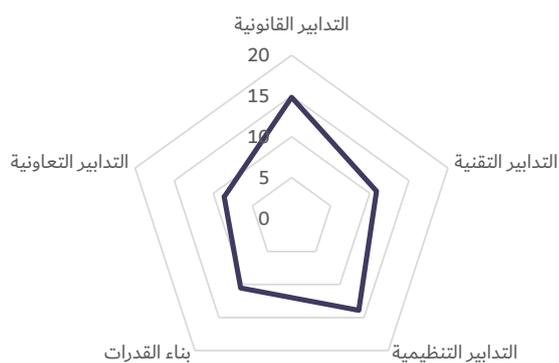
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
8,61	10,52	13,91	10,87	14,85	58,76

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

كومنولث دومينيكا

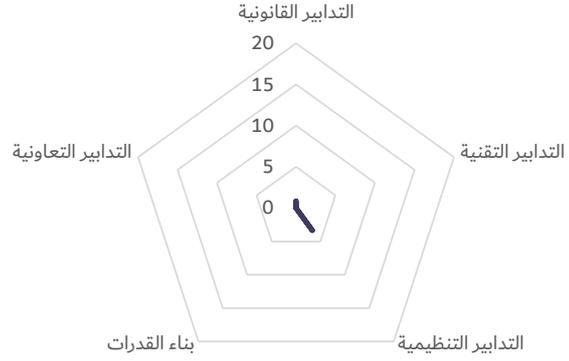
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتعاونية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	3,35	0,00	0,85	4,20

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الجمهورية الدومينيكية

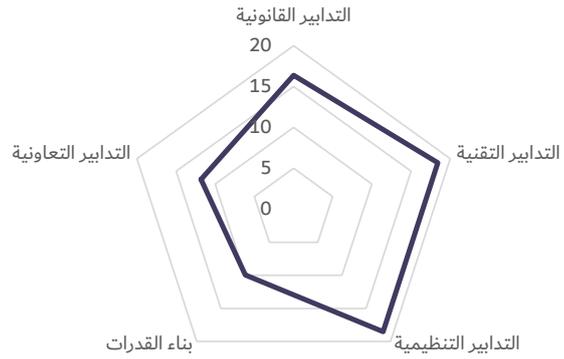
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
11,81	9,94	18,52	18,42	16,38	75,07

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

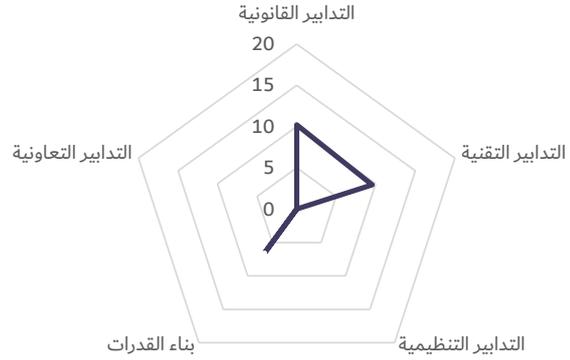
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية والتعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	6,53	0,00	9,55	10,22	26,30

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

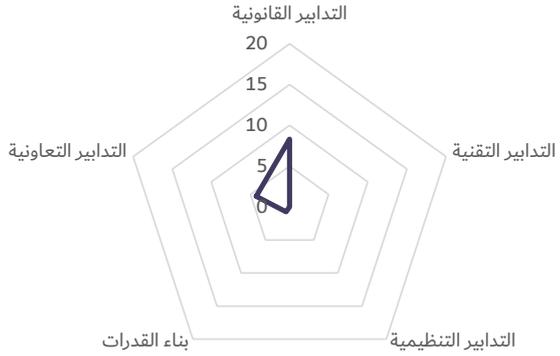
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	0,72	0,00	0,00	8,32	13,30

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

غرينادا

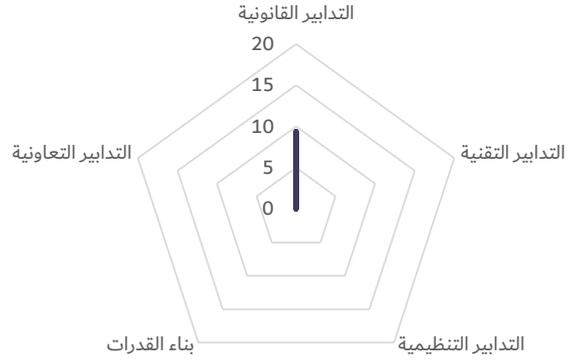
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	0,00	0,00	9,41	9,41

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية غواتيمالا

مستوى التنمية:

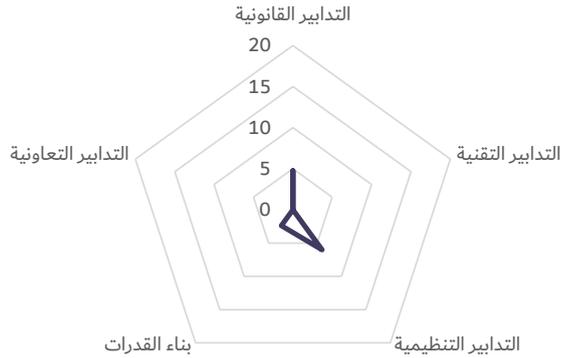
بلد نام

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتعاونية

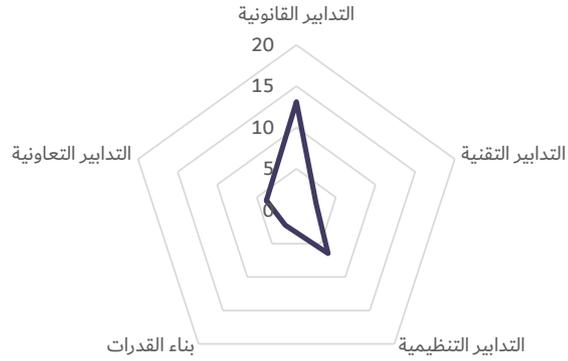


التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	2,36	6,01	0,00	4,76	13,13

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات

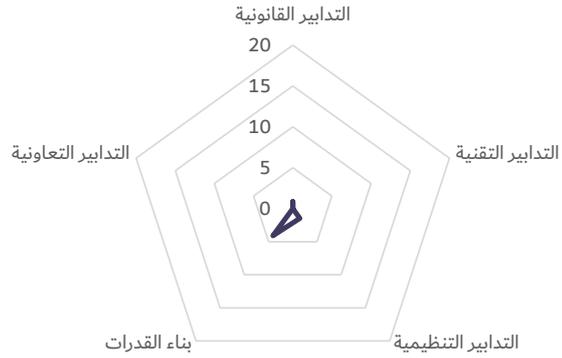


التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
3,78	2,24	6,47	2,50	13,12	28,11

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
تدابير تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	4,09	1,46	0,00	0,85	6,40

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية هندوراس**

مستوى التنمية:

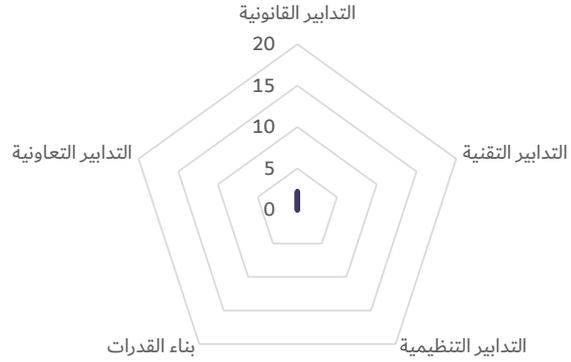
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	0,00	0,00	2,20	2,20

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جامايكا**

مستوى التنمية:

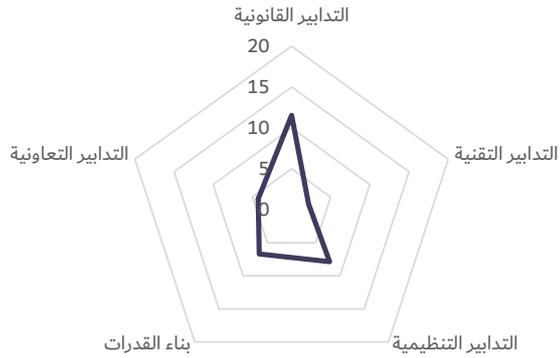
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

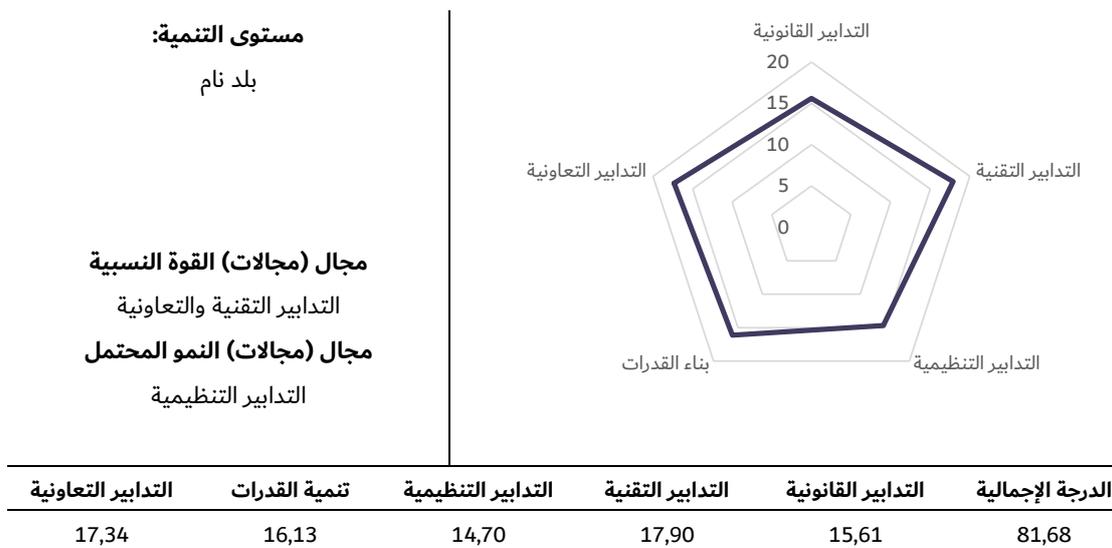
مجال (مجالات) النمو المحتمل

التدابير التقنية

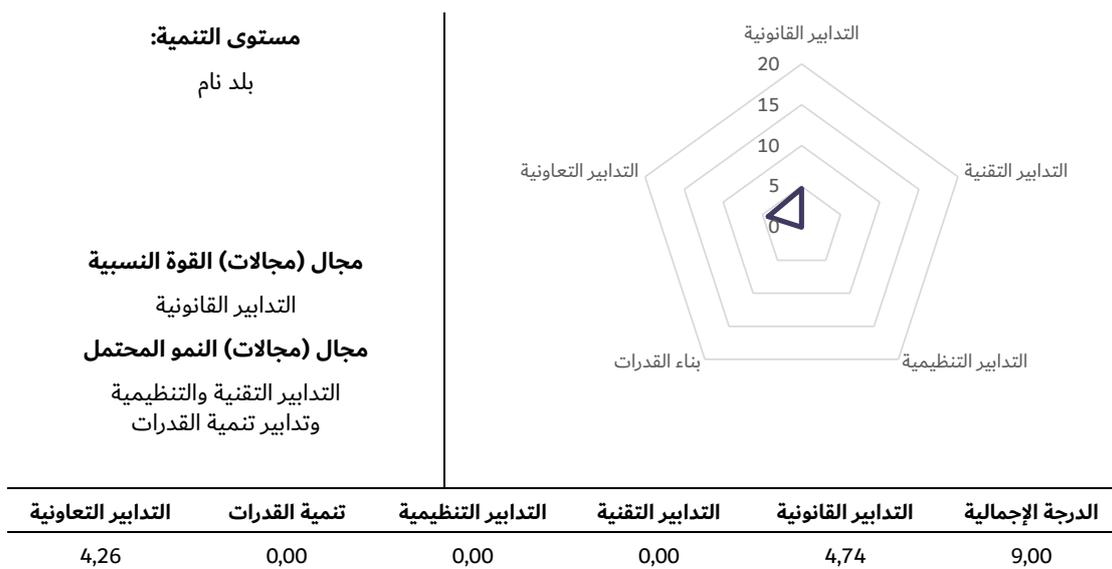


التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	6,68	7,87	2,18	11,54	32,53

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بنما

مستوى التنمية:

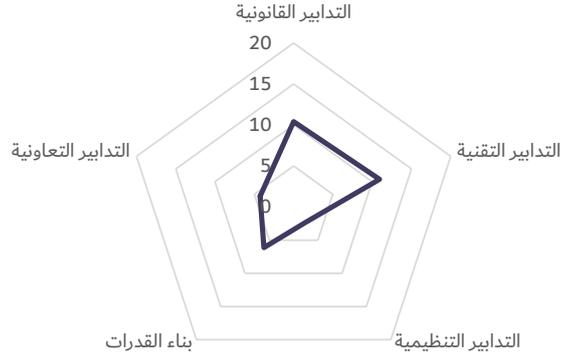
بلد نام

مجال (مجالات) القوة النسبية

التدابير التقنية والقانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	6,12	2,37	10,94	10,41	34,11

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية باراغواي

مستوى التنمية:

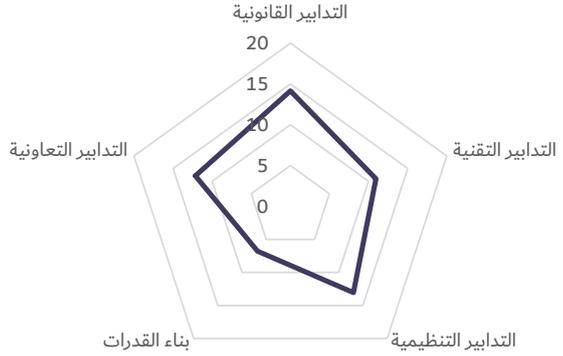
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

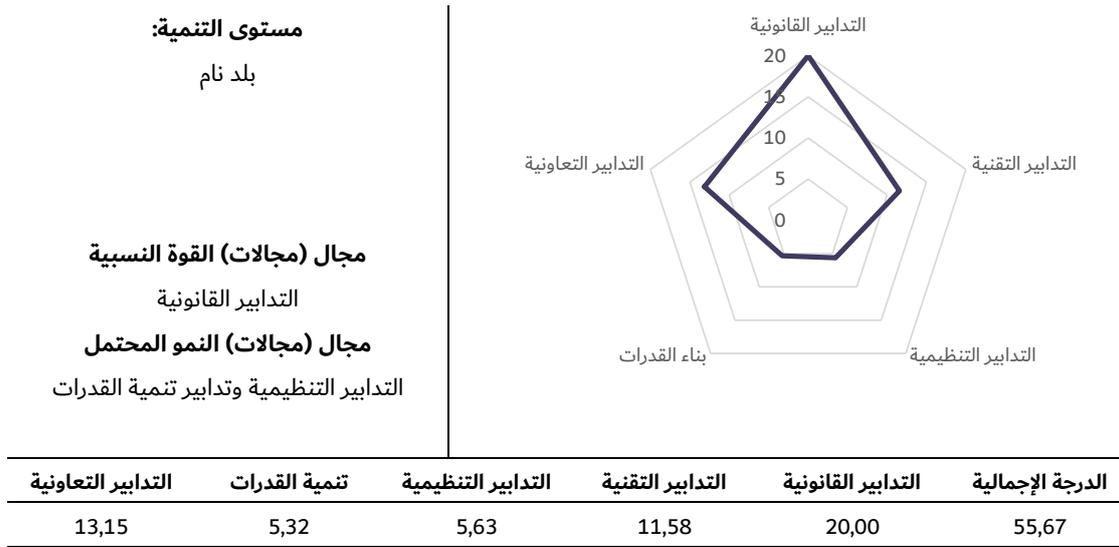
مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



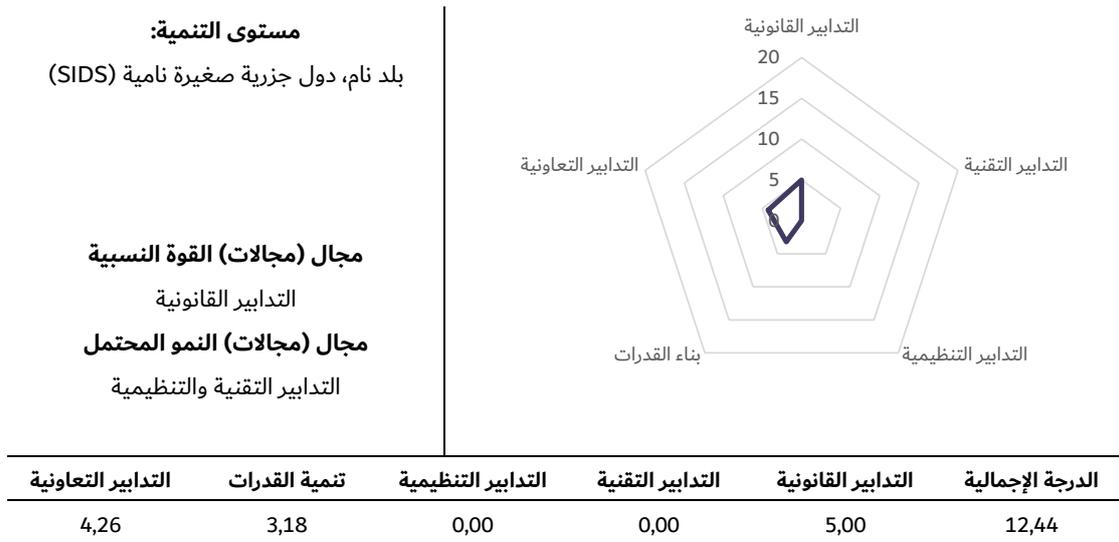
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
12,14	6,79	13,06	10,94	14,15	57,09

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

اتحاد سانت كيتس ونيفيس



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

سانت لوسيا**

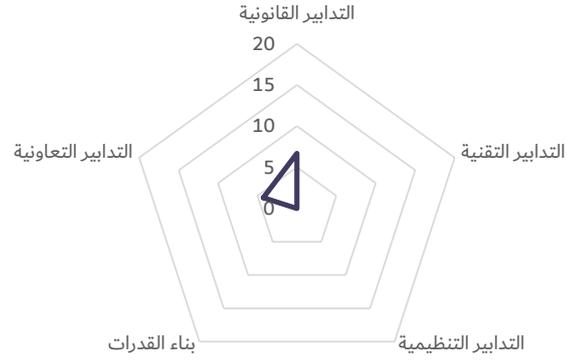
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
6,70	0,00	0,00	0,00	4,26	10,96

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

سانت فنسنت وجرينادين**

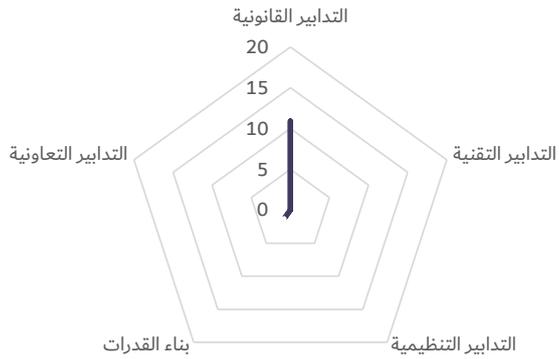
مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية



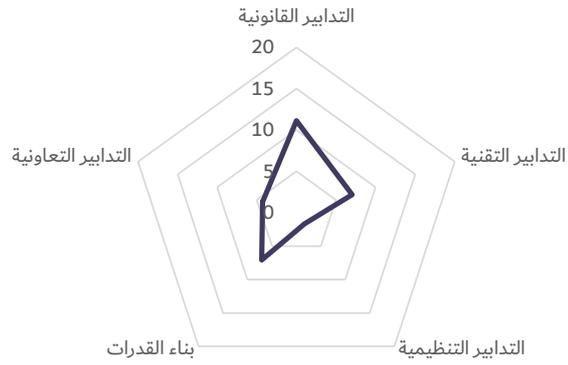
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
10,95	0,00	0,00	1,23	0,00	12,18

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سورينام

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



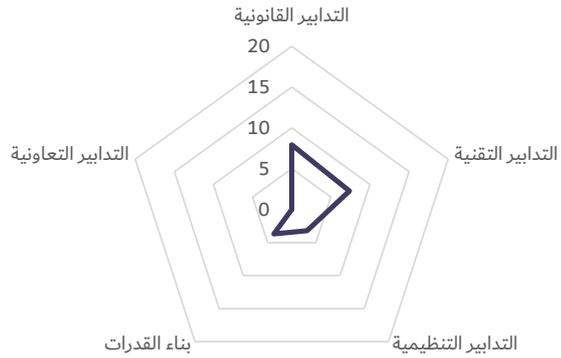
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	7,08	1,69	7,04	11,13	31,20

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

ترينيداد وتوباغو

مستوى التنمية:
بلد نام، دول جزرية صغيرة نامية (SIDS)

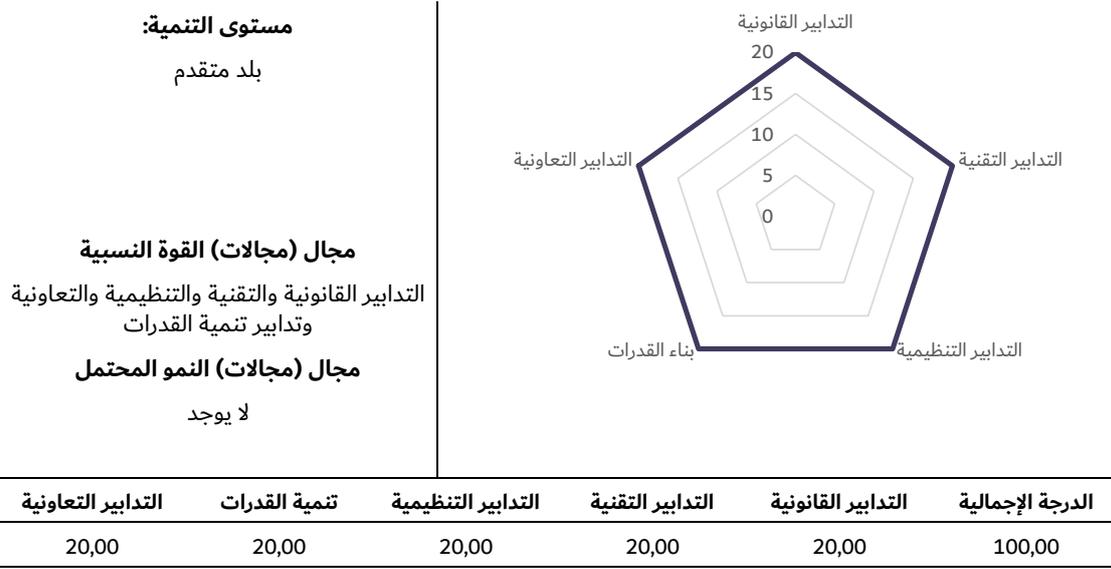
مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	3,69	3,18	7,38	7,94	22,18

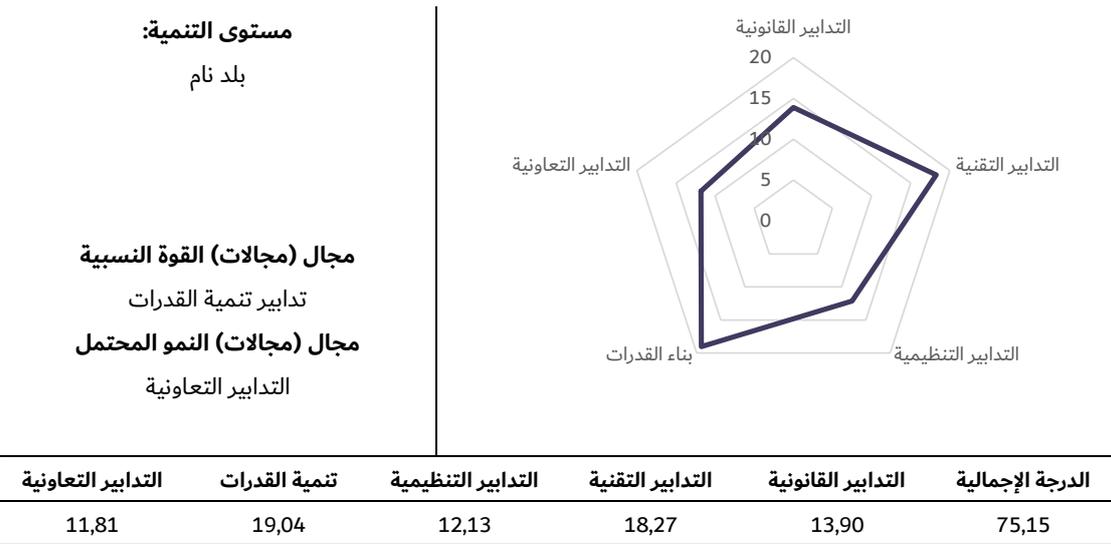
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الولايات المتحدة**



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية أوروغواي الشرقية



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية فنزويلا البوليفارية

مستوى التنمية:

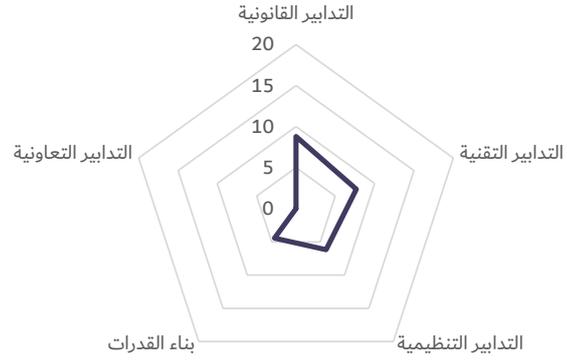
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	4,41	6,17	7,67	8,80	27,06

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

منطقة الدول العربية

الجمهورية الجزائرية الديمقراطية الشعبية

مستوى التنمية:

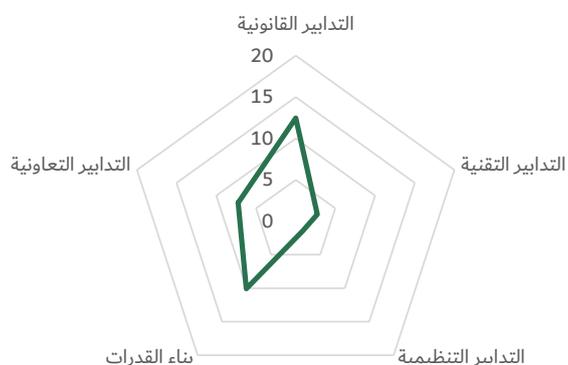
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
7,25	10,07	1,44	2,73	12,46	33,95

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة البحرين

مستوى التنمية:

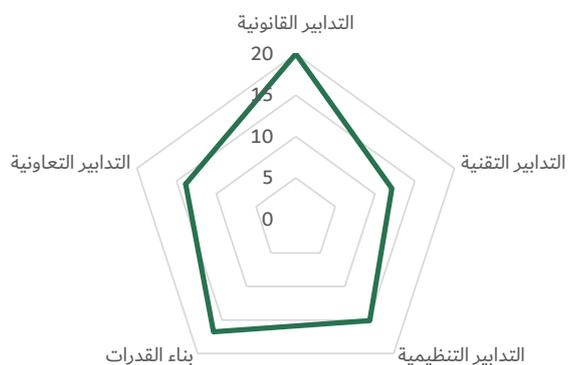
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
13,86	16,77	15,11	12,12	20,00	77,86

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

اتحاد جزر القمر**

مستوى التنمية:

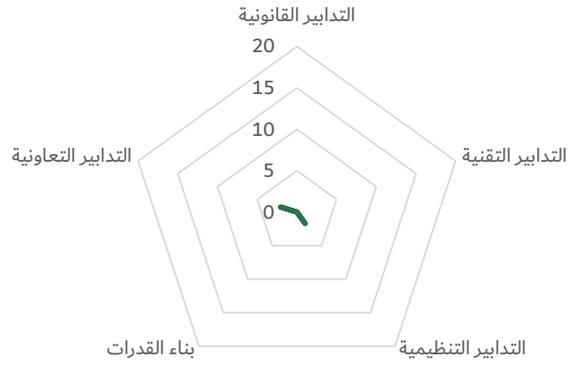
بلد نام، أقل البلدان نمواً (LDC)،
دول جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير القانونية والتقنية وتدابير تنمية
القدرات



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
3,72	0,00	0,00	1,69	0,00	2,04

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية جيبوتي

مستوى التنمية:

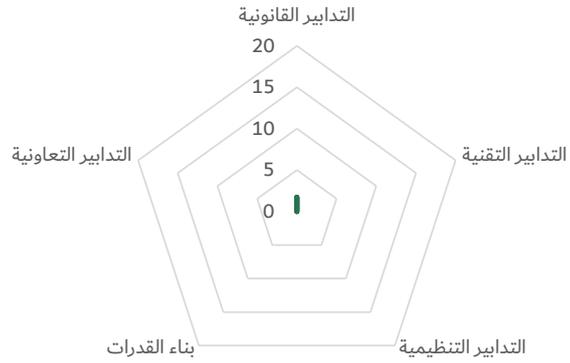
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية والتعاونية
وتدابير تنمية القدرات



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
1,73	1,73	0,00	0,00	0,00	0,00

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية مصر العربية

مستوى التنمية:

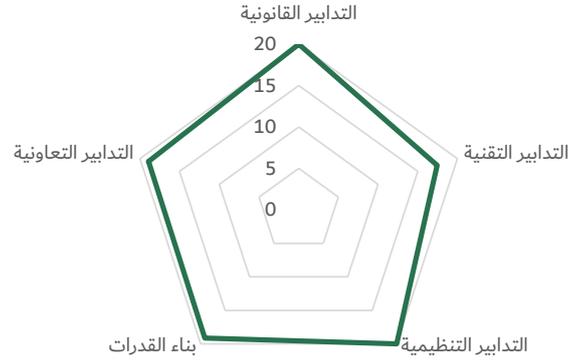
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية والتنظيمية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
18,91	19,12	20,00	17,45	20,00	95,48

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية العراق **

مستوى التنمية:

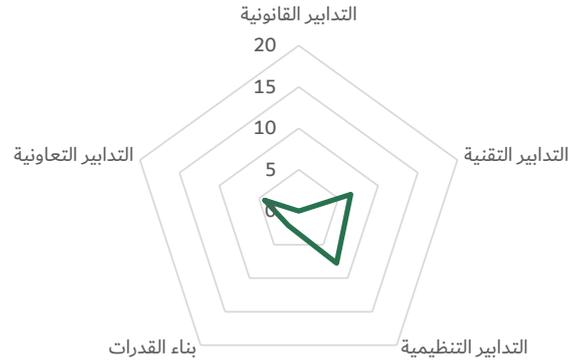
بلد نام

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

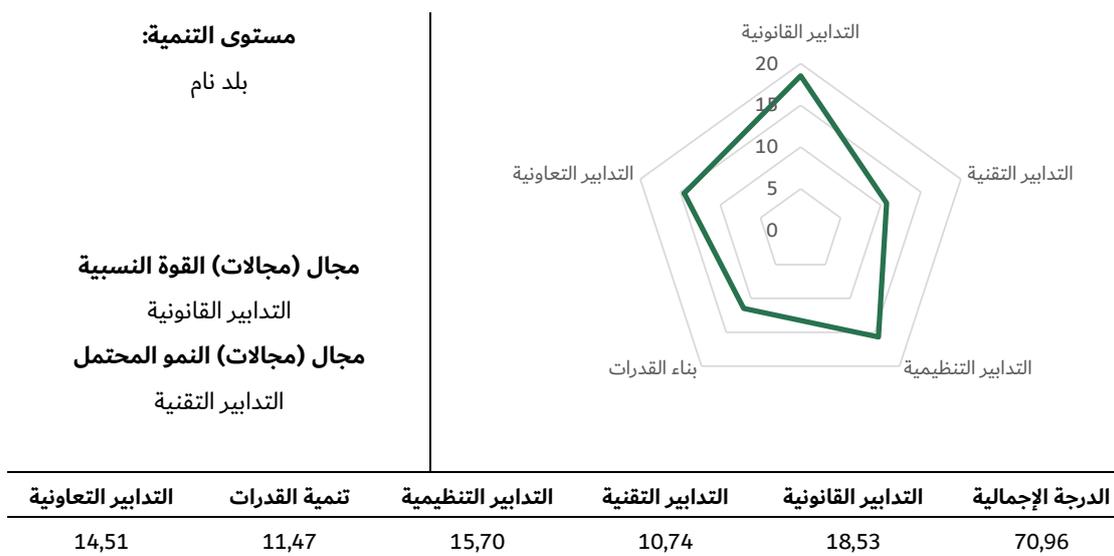
التدابير القانونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	2,14	7,75	6,56	0,00	20,71

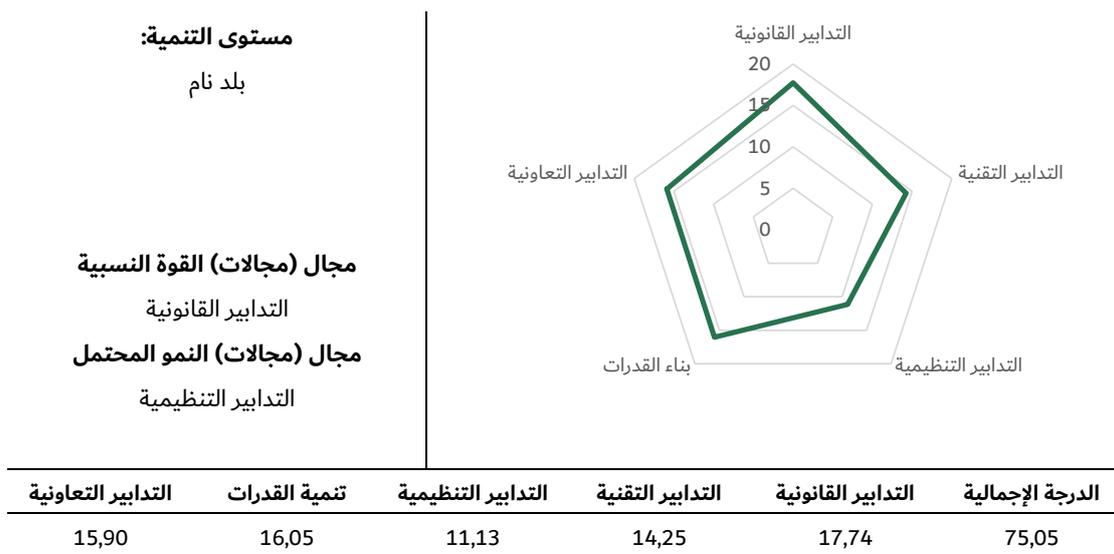
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

المملكة الأردنية الهاشمية



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة الكويت



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

لبنان**

مستوى التنمية:

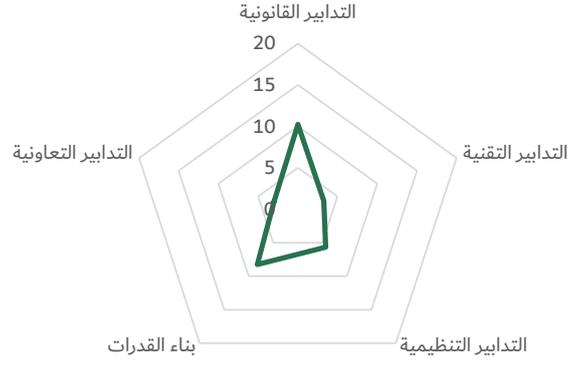
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
2,99	8,26	5,69	3,27	10,24	30,44

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة ليبيا

مستوى التنمية:

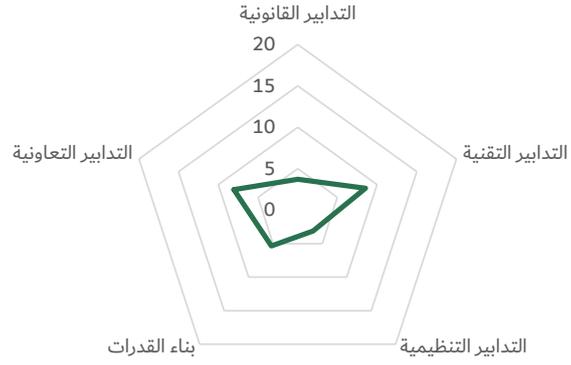
بلد نام

مجال (مجالات) القوة النسبية

التدابير التقنية والتعاونية

مجال (مجالات) النمو المحتمل

التدابير القانونية والتنظيمية



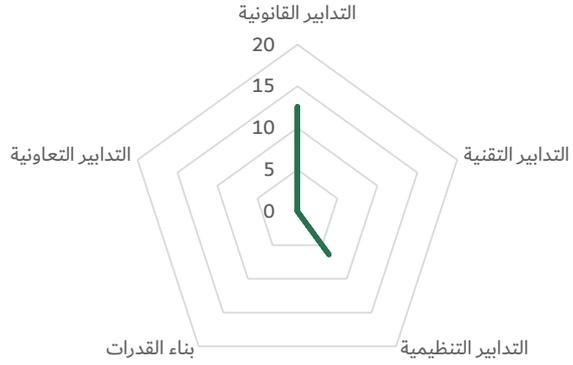
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
8,04	5,34	3,13	8,54	3,73	28,78

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية موريتانيا الإسلامية

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية وتدابير تنمية القدرات



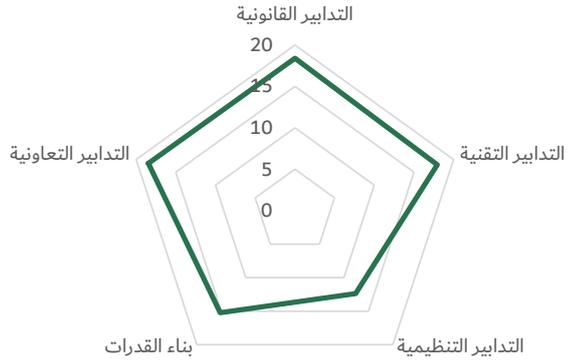
الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
18,94	12,55	0,00	6,39	0,00	0,00

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة المغرب

مستوى التنمية:
بلد نام

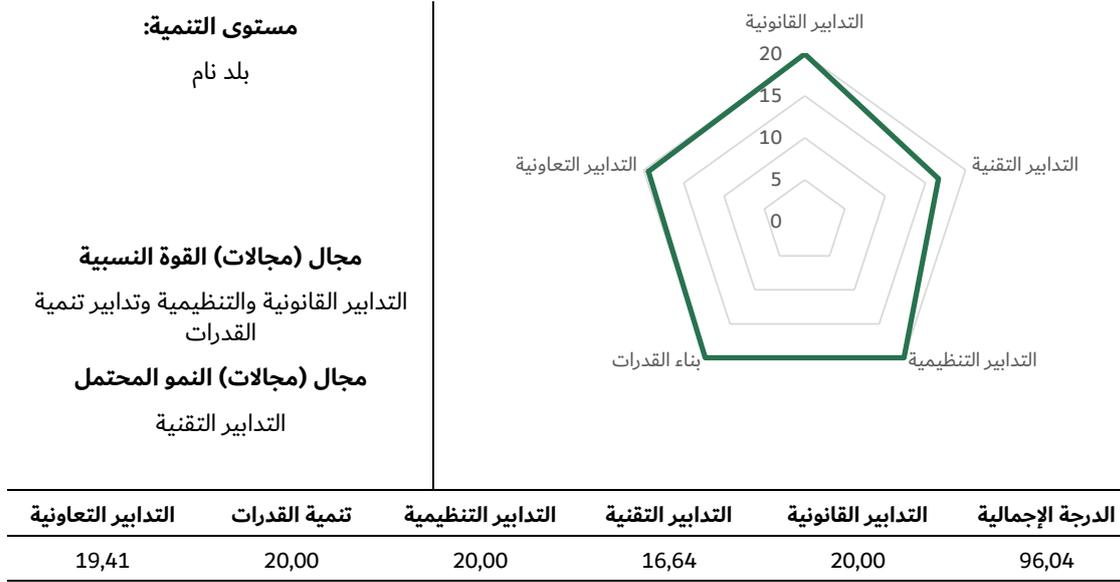
مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
82,41	18,40	17,94	12,37	15,24	18,46

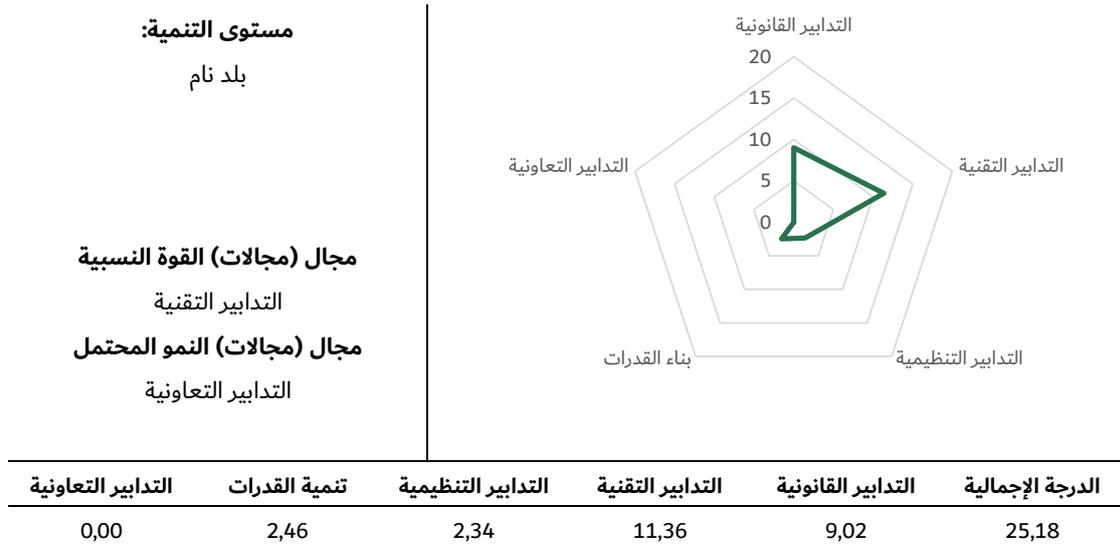
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

سلطنة عُمان



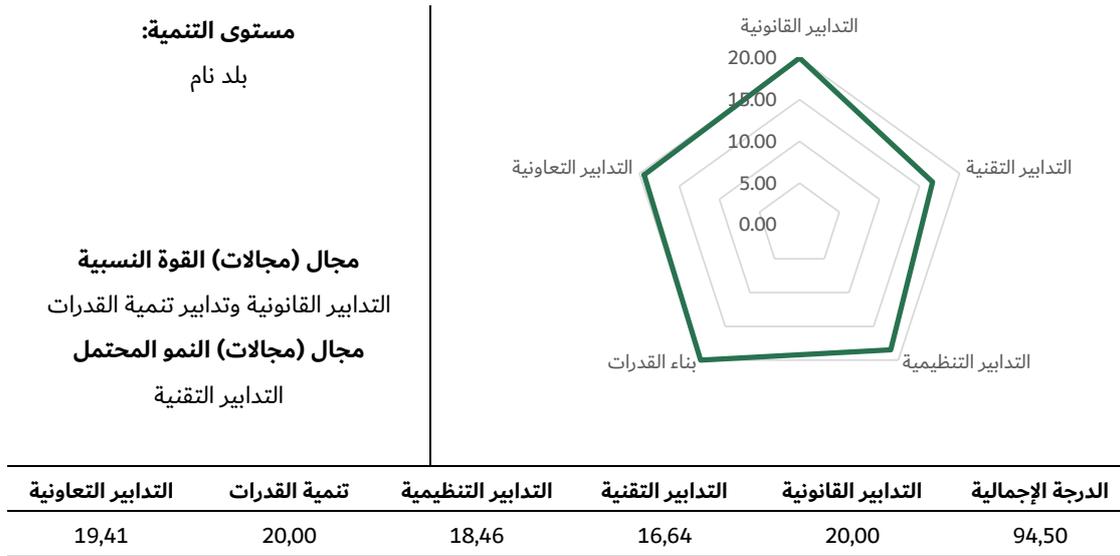
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة فلسطين



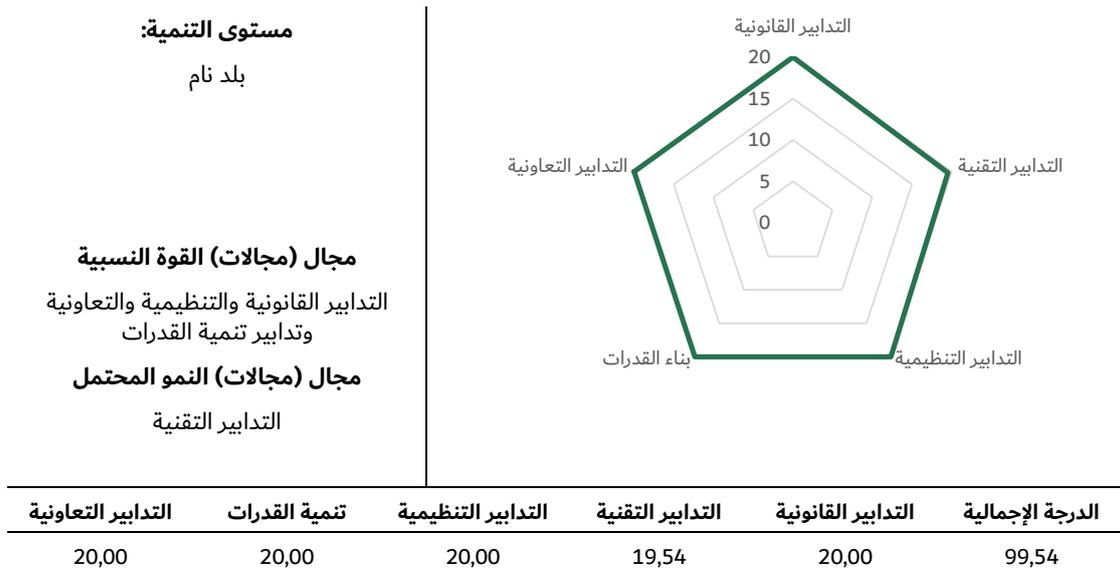
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة قطر



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

المملكة العربية السعودية

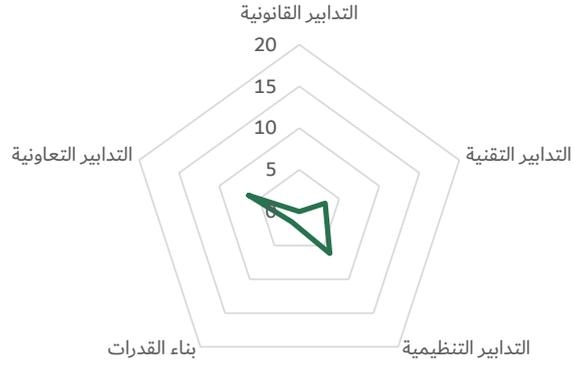


المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الصومال الاتحادية

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التنظيمية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير القانونية



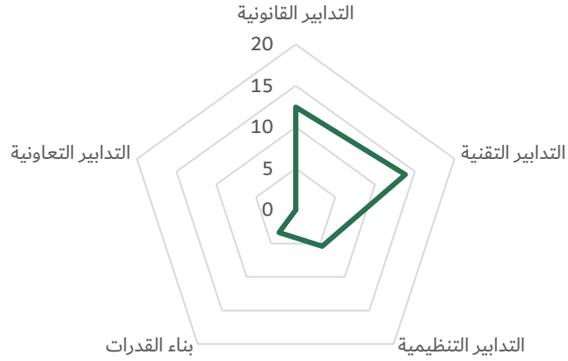
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
6,31	1,52	6,17	3,25	0,00	17,25

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية السودان

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
التدابير التقنية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	3,38	5,41	13,81	12,43	35,03

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الجمهورية العربية السورية**

مستوى التنمية:

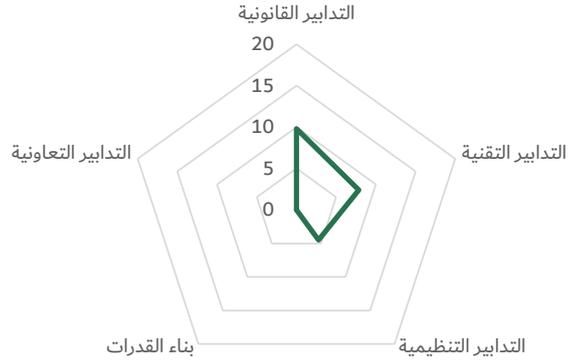
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

تنمية القدرات والتدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	4,49	7,85	9,80	22,14

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

تونس

مستوى التنمية:

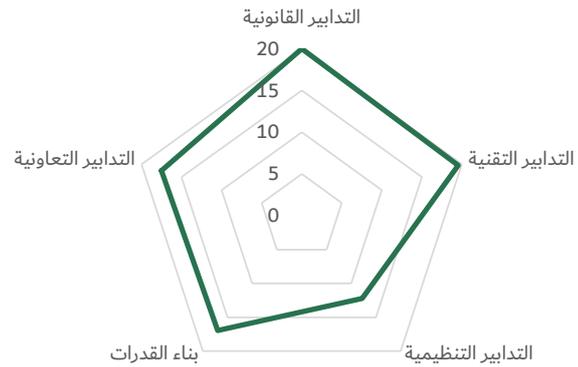
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية

مجال (مجالات) النمو المحتمل

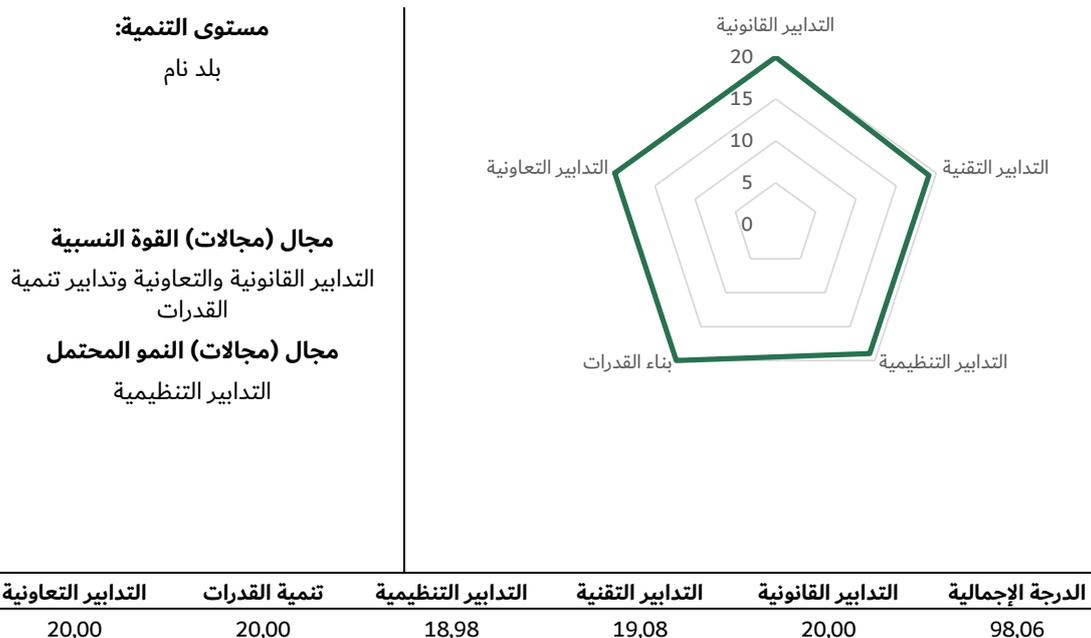
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
17,52	16,96	12,21	19,54	20,00	86,23

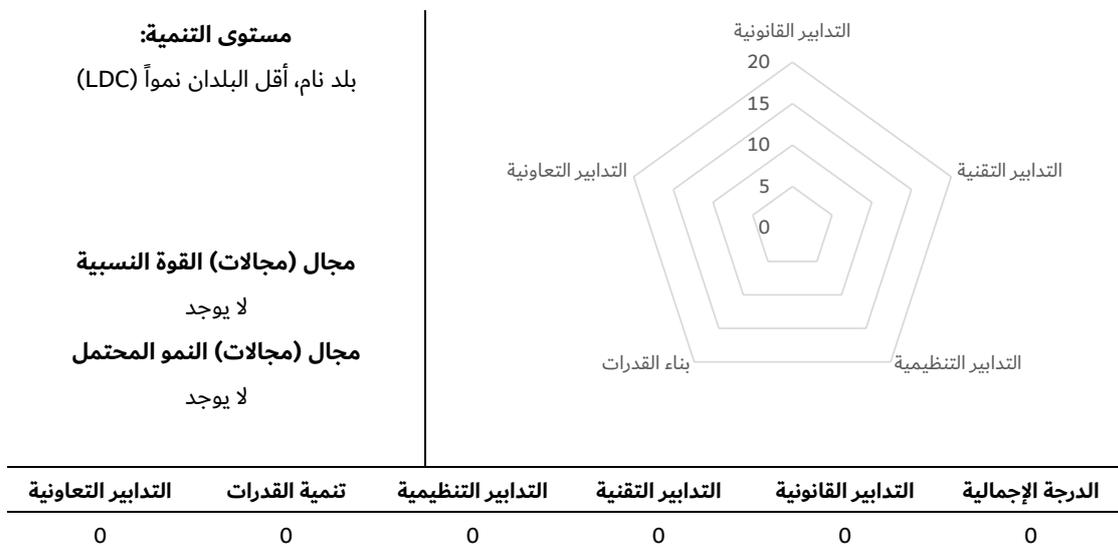
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الإمارات العربية المتحدة



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية اليمن*



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

منطقة آسيا والمحيط الهادئ

أفغانستان

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التنظيمية
مجال (مجالات) النمو المحتمل
تنمية القدرات والتدابير التعاونية



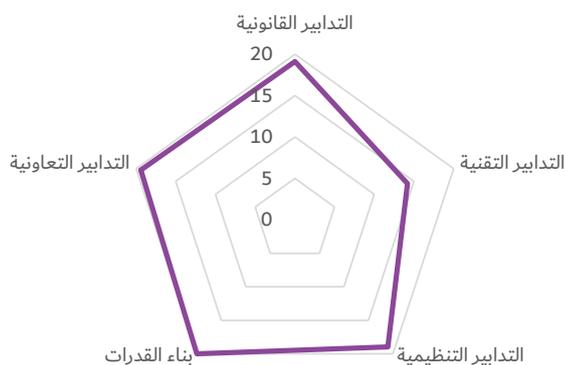
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
0,40	1,46	3,35	0,00	0,00	5,20

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

أستراليا

مستوى التنمية:
بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية وتدابير تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



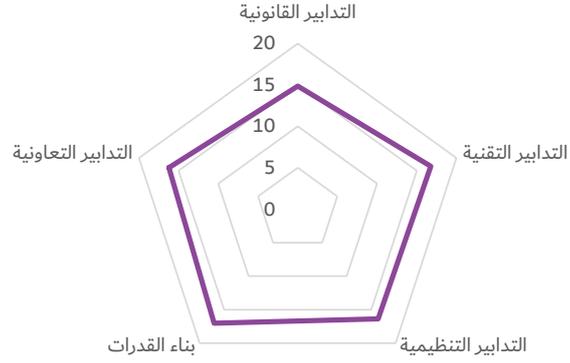
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,08	18,98	20,00	19,41	97,47

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بنغلاديش الشعبية

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية
تنمية القدرات والتدابير التقنية
مجال (مجالات) النمو المحتمل
التدابير القانونية



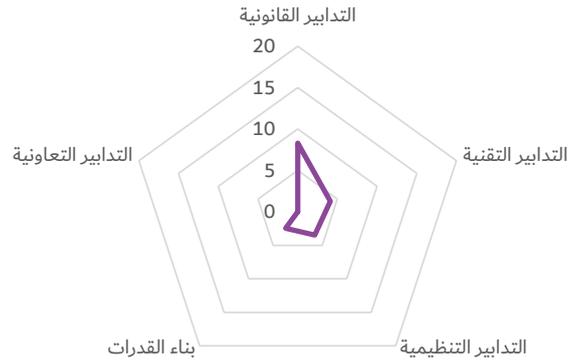
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
14,86	16,77	16,39	17,03	16,22	81,27

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة بوتان

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
8,30	4,12	3,47	2,45	0,00	18,34

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

بروني دار السلام

مستوى التنمية:

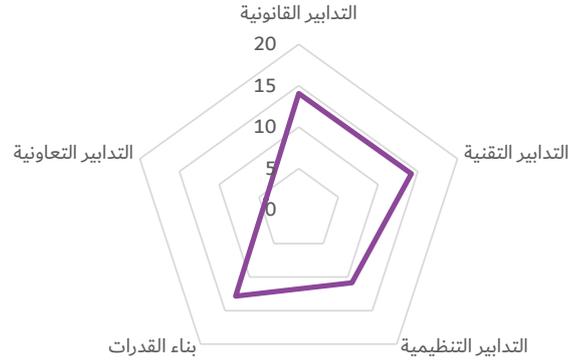
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,12	12,85	10,84	14,19	14,06	56,07

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة كمبوديا**

مستوى التنمية:

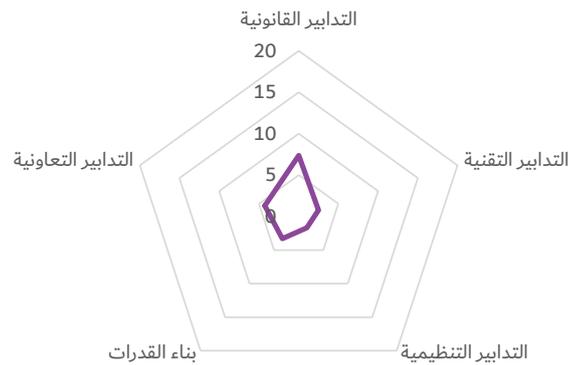
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

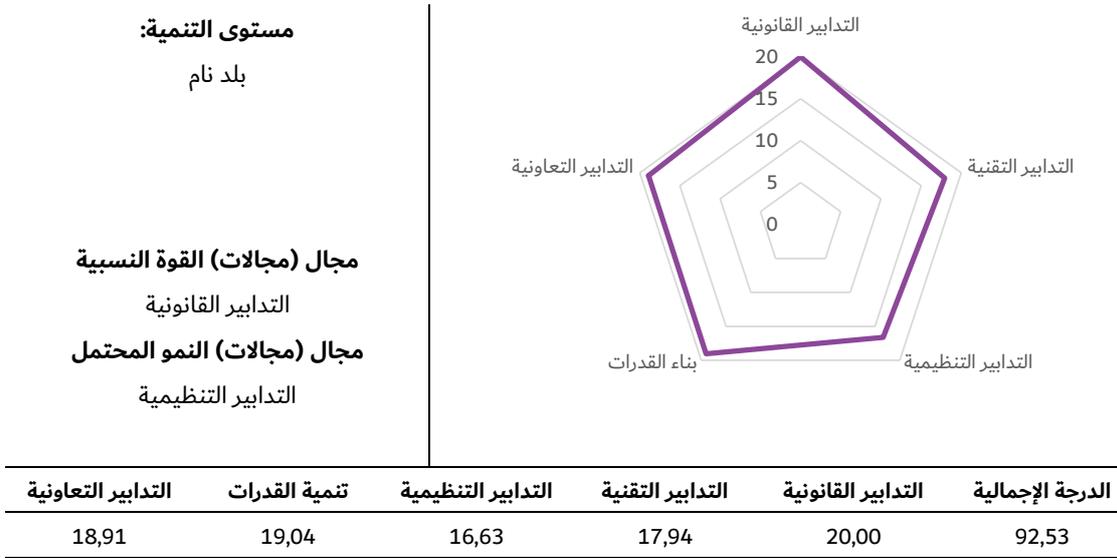
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	3,29	1,69	2,50	7,38	19,12

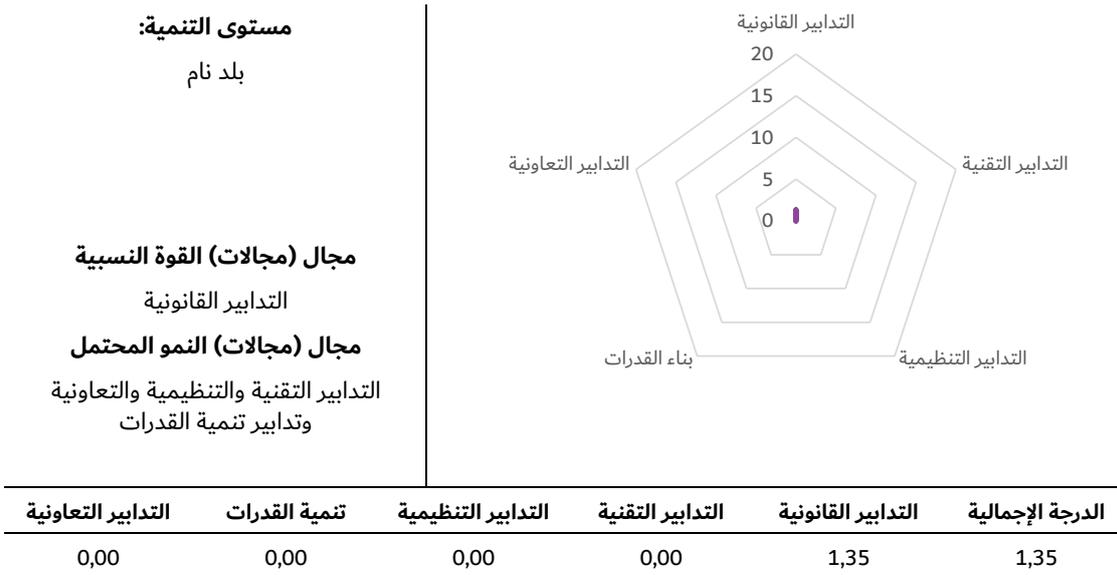
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الصين الشعبية



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كوريا الديمقراطية الشعبية **

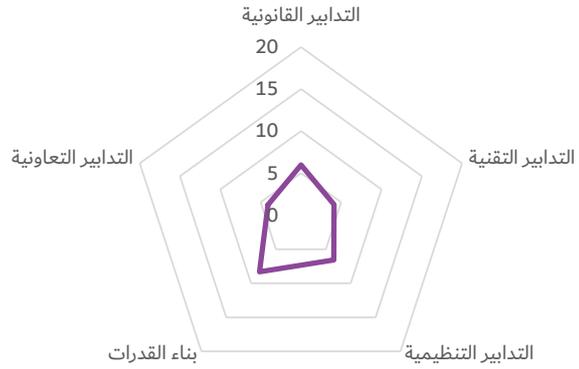


المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية فيجي

مستوى التنمية:
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية



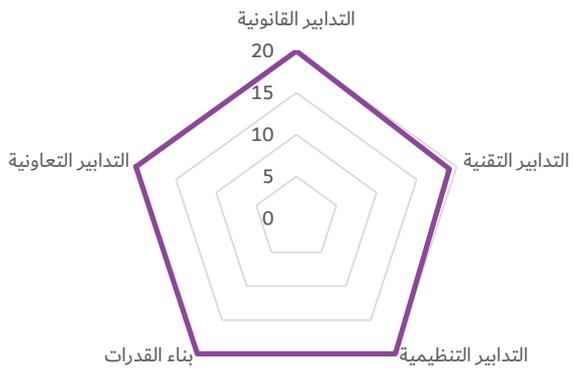
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
5,99	4,11	6,59	8,31	4,07	29,08

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الهند

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
وتدابير تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,08	18,41	20,00	20,00	97,49

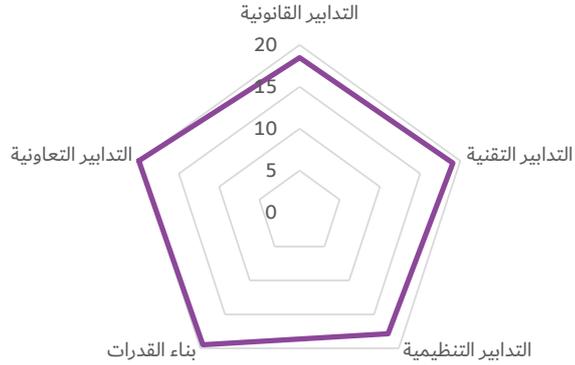
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية إندونيسيا

مستوى التنمية:

بلد نام

مجالات (مجالات) القوة النسبية
التدابير التعاونية وتدابير تنمية القدرات
مجالات (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	19,48	17,84	19,08	18,48	94,88

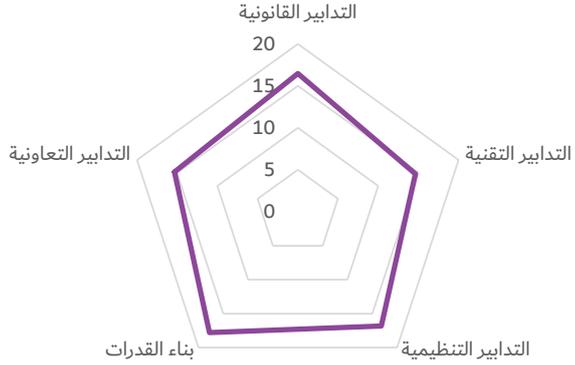
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية إيران الإسلامية

مستوى التنمية:

بلد نام

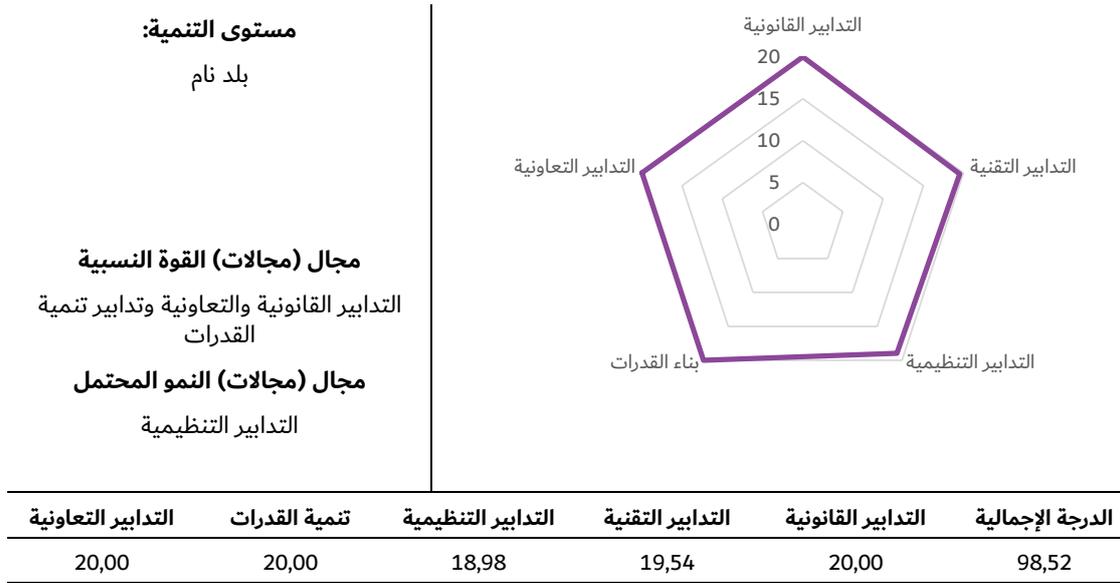
مجالات (مجالات) القوة النسبية
تدابير تنمية القدرات والتدابير التنظيمية
مجالات (مجالات) النمو المحتمل
التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,33	17,80	16,82	14,63	16,48	81,06

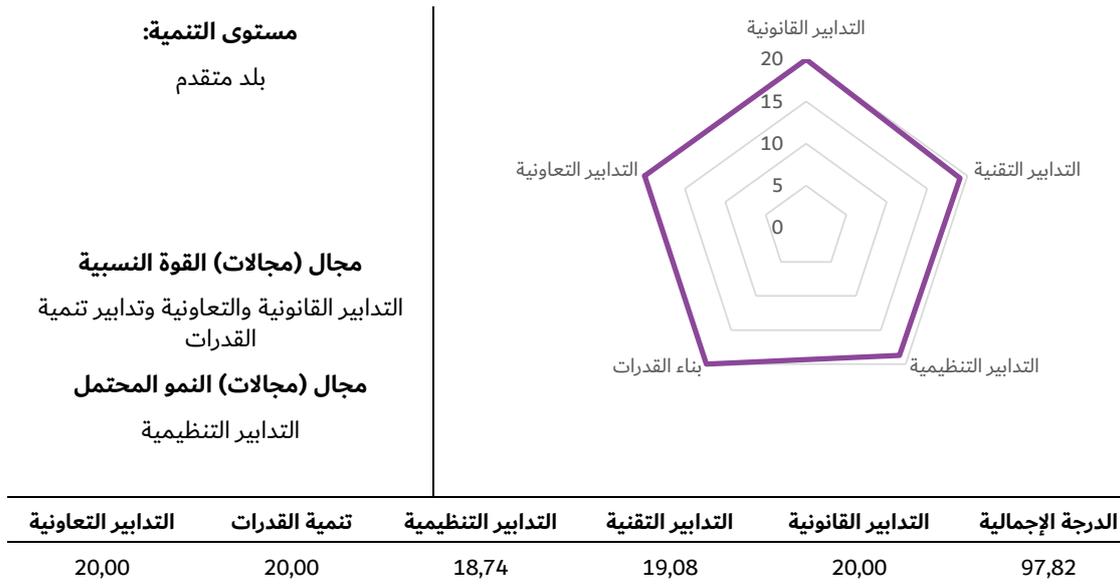
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كوريا



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

اليابان



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كيريباتي

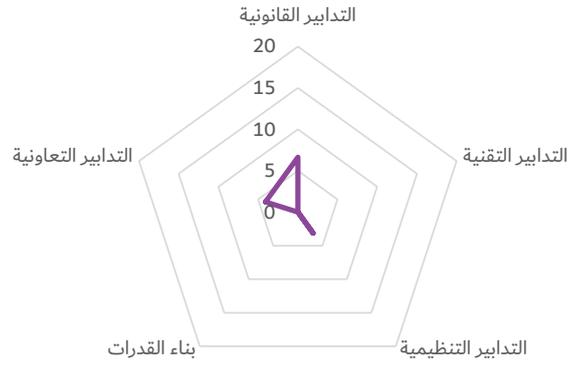
مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
6,64	0,00	3,13	0,00	4,07	13,84

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية لاو الديمقراطية الشعبية

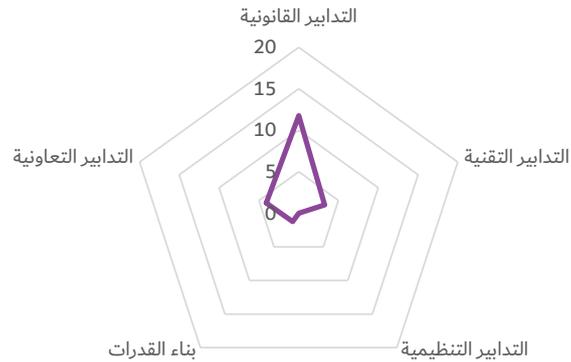
مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
11,77	3,27	0,00	1,23	4,07	20,34

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

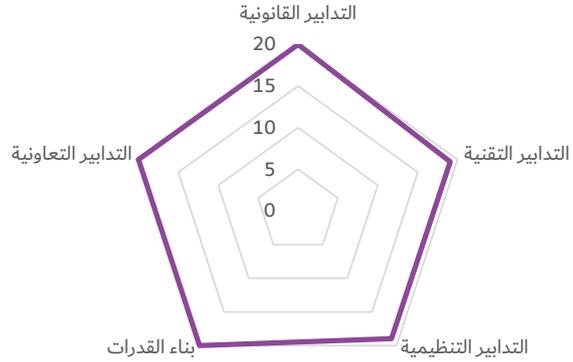
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية والتعاونية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	20,00	18,98	19,08	20,00	98,06

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية ملديف **

مستوى التنمية:

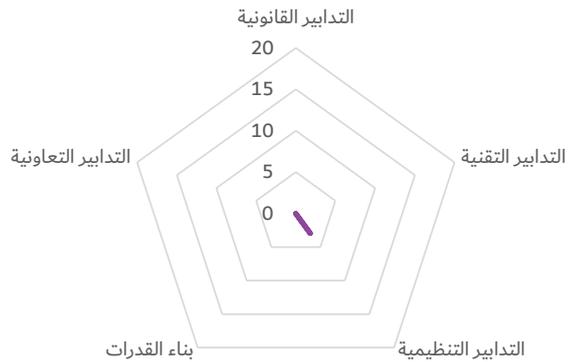
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

التدابير القانونية والتقنية والتعاونية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	0,00	2,95	0,00	0,00	2,95

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية جزر مارشال**

مستوى التنمية:

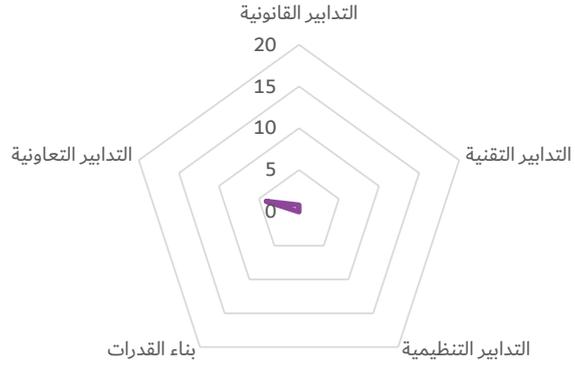
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
0,83	0,00	0,00	0,00	4,07	4,90

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

ولايات ميكرونيزيا الموحدة*

مستوى التنمية:

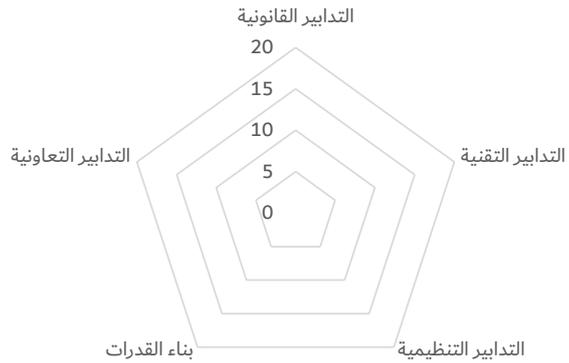
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

لا يوجد

مجال (مجالات) النمو المحتمل

لا يوجد



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
0	0	0	0	0	0

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

منغوليا

مستوى التنمية:

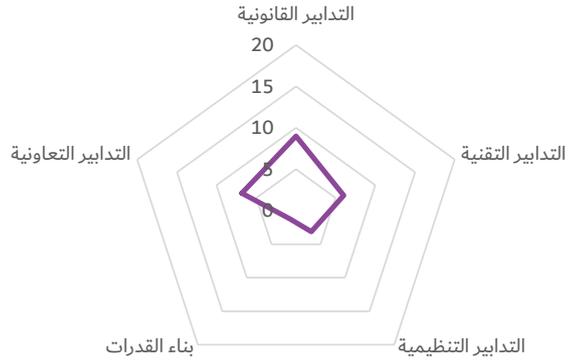
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
9,00	6,02	3,13	1,23	6,82	26,20

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

اتحاد ميانمار

مستوى التنمية:

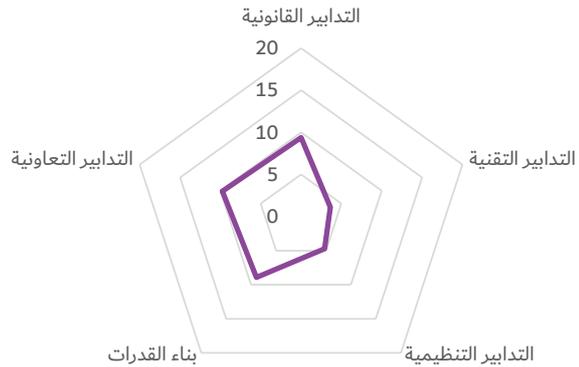
بلد نام، أقل البلدان نمواً (LDC)

مجال (مجالات) القوة النسبية

التدابير التعاونية والقانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
9,39	3,64	4,71	8,92	9,75	36,41

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية ناورو**

مستوى التنمية:

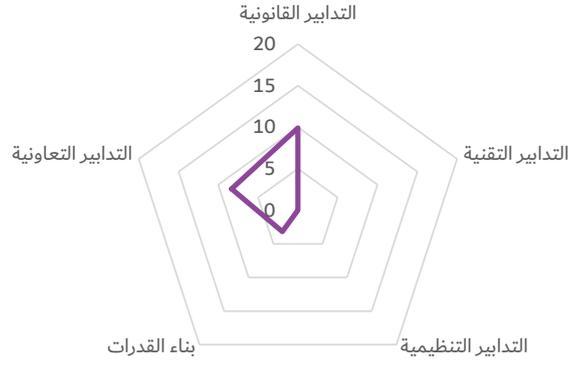
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
9,91	0,00	0,00	3,18	8,33	21,42

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية نيبال الديمقراطية الاتحادية**

مستوى التنمية:

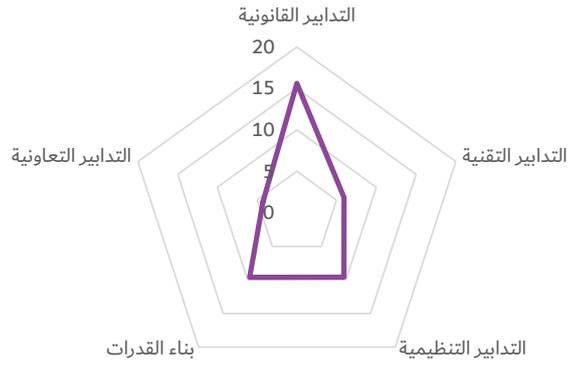
بلد نام، أقل البلدان نمواً (LDC)
بلد غير ساحلي

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
15,61	5,94	9,58	9,60	4,26	44,99

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

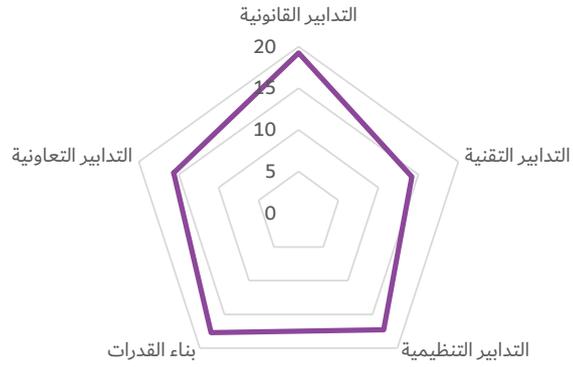
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تممية القدرات	التدابير التعاونية	الدرجة الإجمالية
19,24	14,19	17,27	17,71	15,63	84,04

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية باكستان الإسلامية

مستوى التنمية:

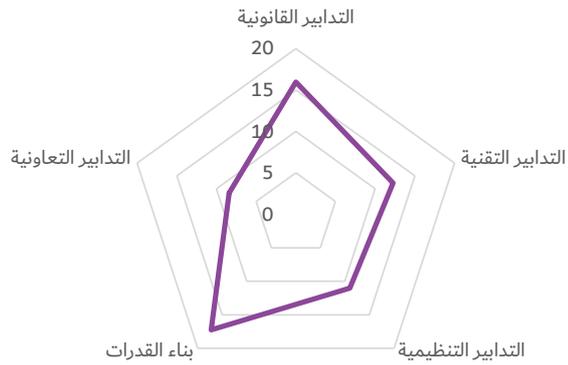
بلد نام

مجال (مجالات) القوة النسبية

تدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تممية القدرات	التدابير التعاونية	الدرجة الإجمالية
15,97	8,38	11,01	17,25	12,26	64,88

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

بابوا غينيا الجديدة**

مستوى التنمية:

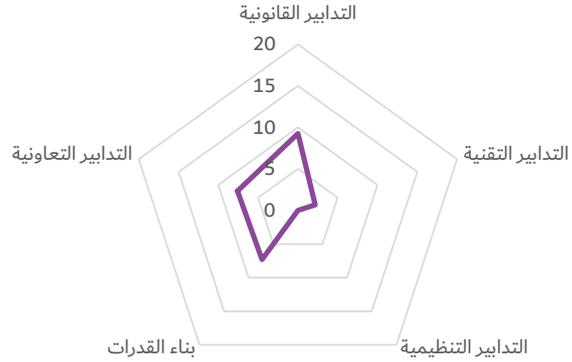
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجالات (مجالات) القوة النسبية

التدابير القانونية

مجالات (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
9,26	2,18	0,00	7,30	7,59	26,33

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية الفلبين

مستوى التنمية:

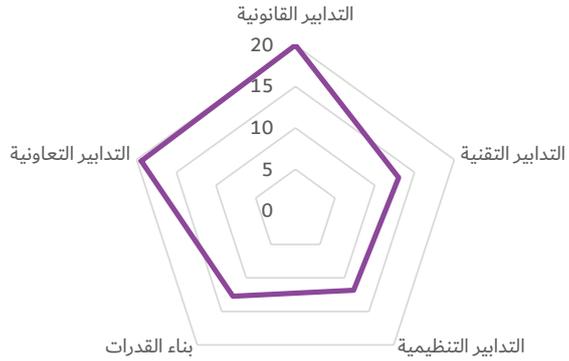
بلد نام

مجالات (مجالات) القوة النسبية

التدابير القانونية والتعاونية

مجالات (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	13,00	11,85	12,74	19,41	77,00

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

دولة ساموا المستقلة

مستوى التنمية:

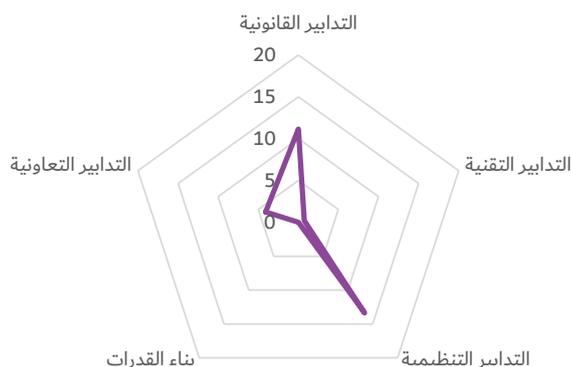
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

تنمية القدرات والتدابير التقنية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
11,15	0,73	13,37	0,00	4,07	29,33

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سنغافورة

مستوى التنمية:

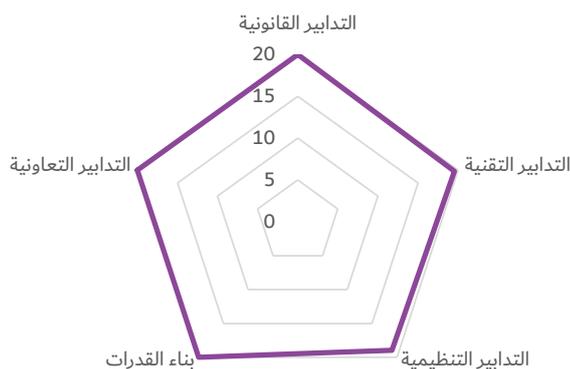
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير القانونية والتعاونية وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



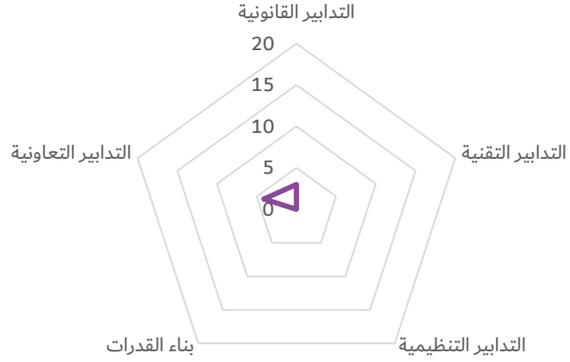
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,54	18,98	20,00	20,00	98,52

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير التعاونية والقانونية

مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,07	0,00	0,00	0,00	3,00	7,08

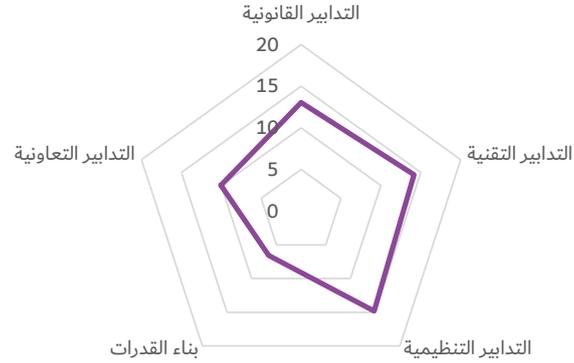
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سري لانكا الاشتراكية الديمقراطية

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير التنظيمية والتقنية

مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
10,04	6,58	14,82	14,15	13,05	58,65

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

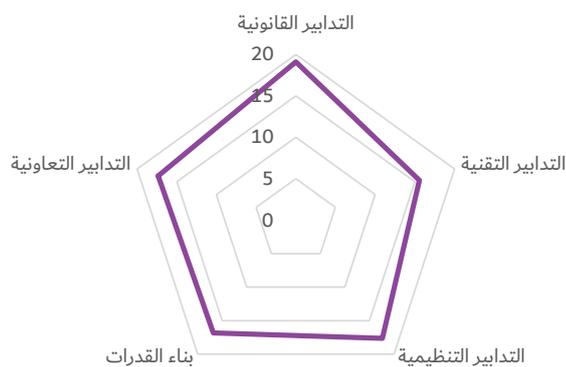
بلد نام

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
17,34	16,84	17,64	15,57	19,11	86,50

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية تيمور ليشتي الديمقراطية**

مستوى التنمية:

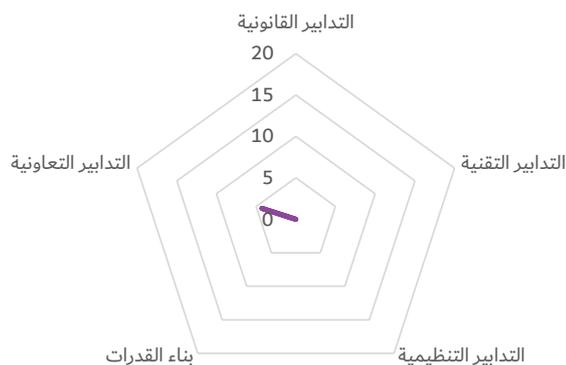
بلد نام، أقل البلدان نمواً (LDC)،
دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير القانونية والتقنية والتنظيمية
وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	0,00	0,00	0,00	0,00	4,26

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة تونغا**

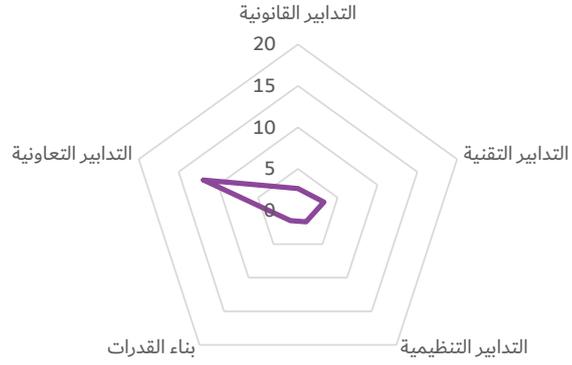
مستوى التنمية:
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
11,85	1,52	1,69	3,27	2,63	20,95

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

توفالو**

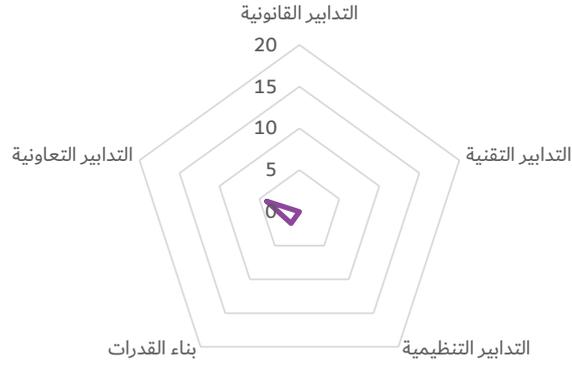
مستوى التنمية:
بلد نام، أقل البلدان نمواً (LDC)،
دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير القانونية والتقنية والتنظيمية



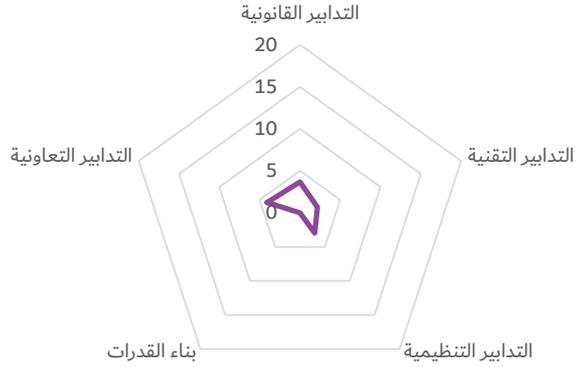
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,07	1,71	0,00	0,00	0,00	5,78

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية فانواتو

مستوى التنمية:
بلد نام، دولة جزرية صغيرة نامية (SIDS)

مجال (مجالات) القوة النسبية
التدابير التعاونية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



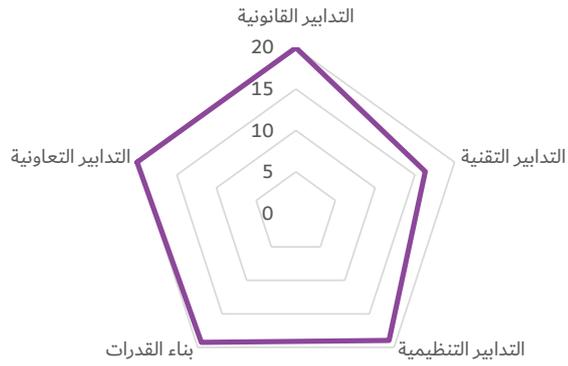
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,07	0,00	2,95	2,18	3,69	12,88

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية فيتنام الاشتراكية

مستوى التنمية:
بلد نام

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	19,26	18,98	16,31	20,00	94,55

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

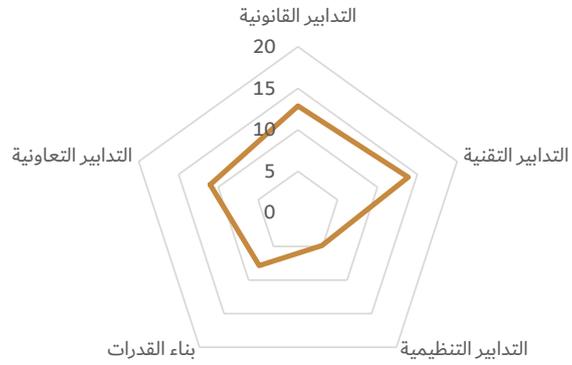
* لا توجد بيانات

منطقة كومنولث الدول المستقلة

جمهورية أرمينيا **

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التقنية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



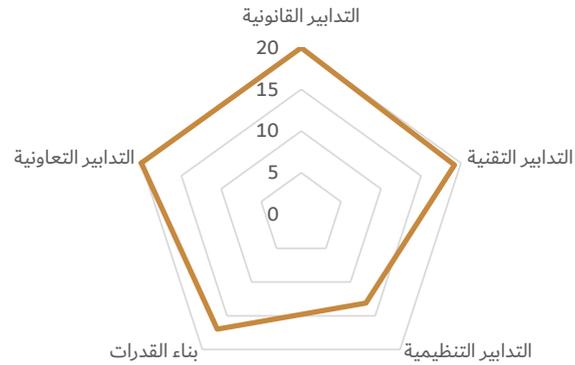
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
12,87	13,86	4,87	7,85	11,02	50,47

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية أذربيجان

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية

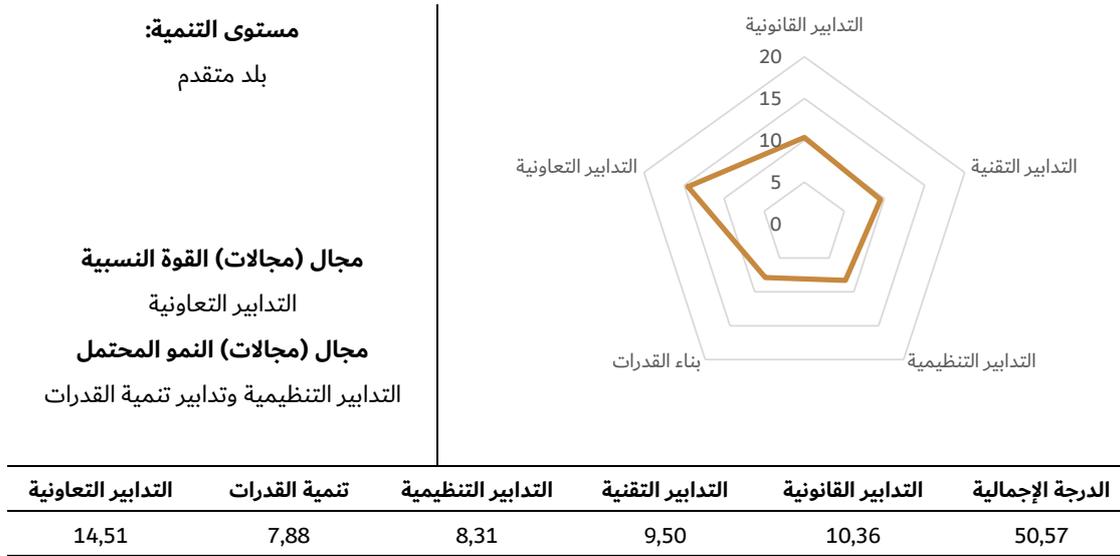


التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,19	13,14	16,99	20,00	89,31

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

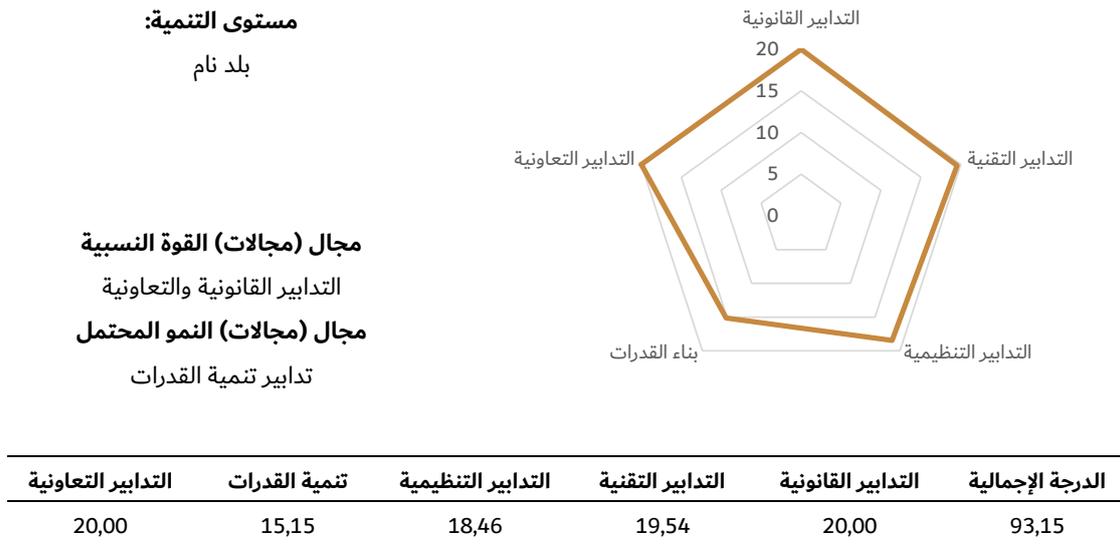
الرقم القياسي العالمي للأمن السيبراني لعام 2020

جمهورية بيلاروس



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كازاخستان

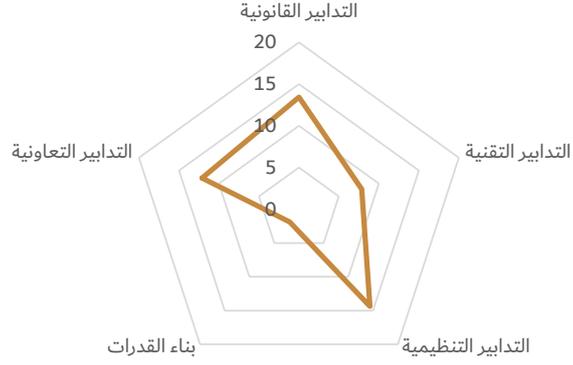


المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية قيرغيزستان

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التنظيمية والقانونية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



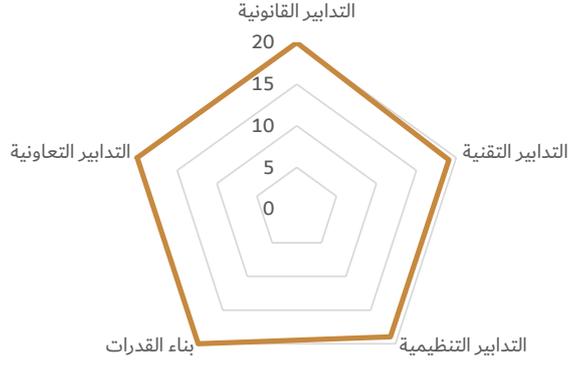
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
12,11	1,87	14,37	7,85	13,43	49,64

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الاتحاد الروسي

مستوى التنمية:
بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية وتدابير تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	20,00	18,98	19,08	20,00	98,06

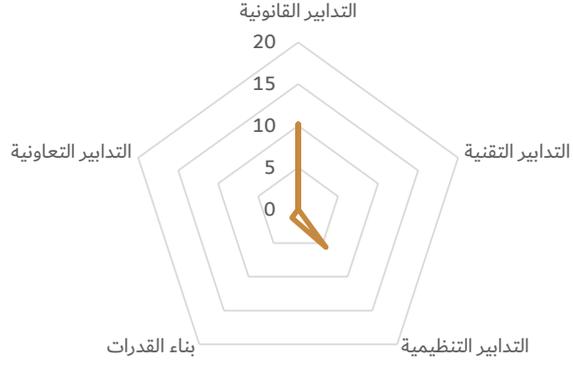
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الرقم القياسي العالمي للأمن السيبراني لعام 2020

جمهورية طاجيكستان**

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
0,00	1,25	5,63	0,00	10,22	17,10

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

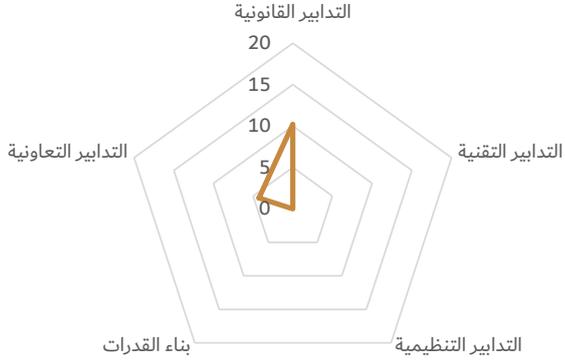
** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

تركمانستان**

مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية والتنظيمية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
4,26	0,00	0,00	0,00	10,22	14,48

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

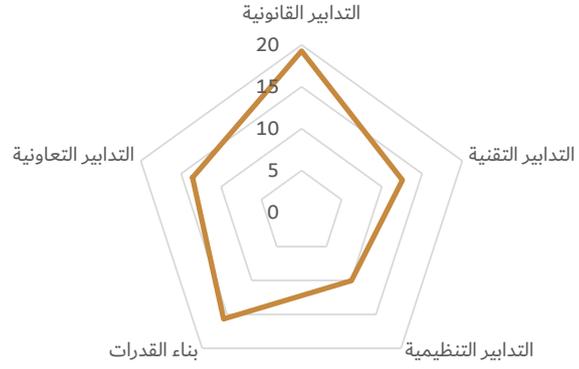
** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

جمهورية أوزبكستان

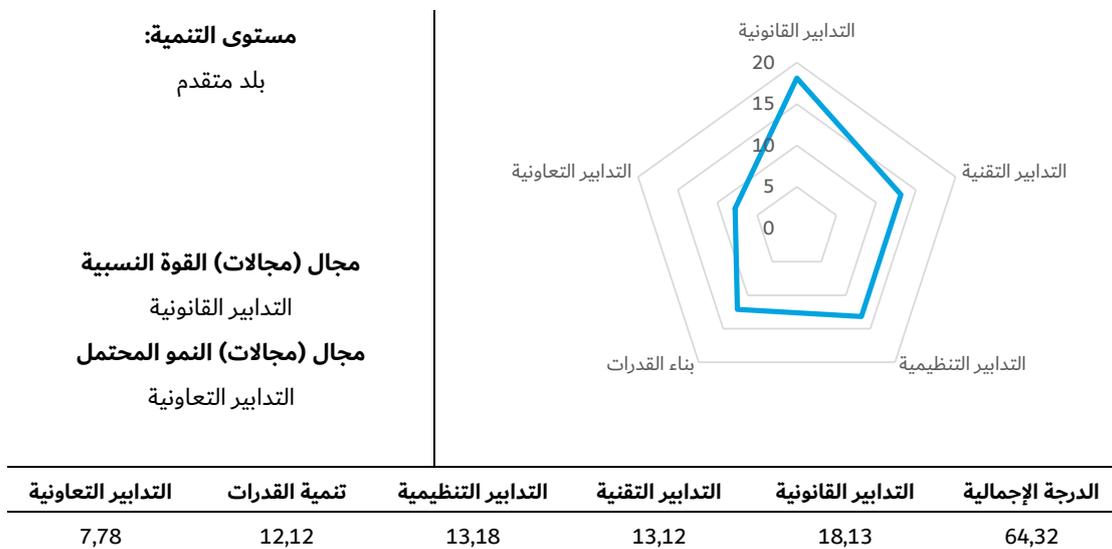
مستوى التنمية:
بلد نام، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية

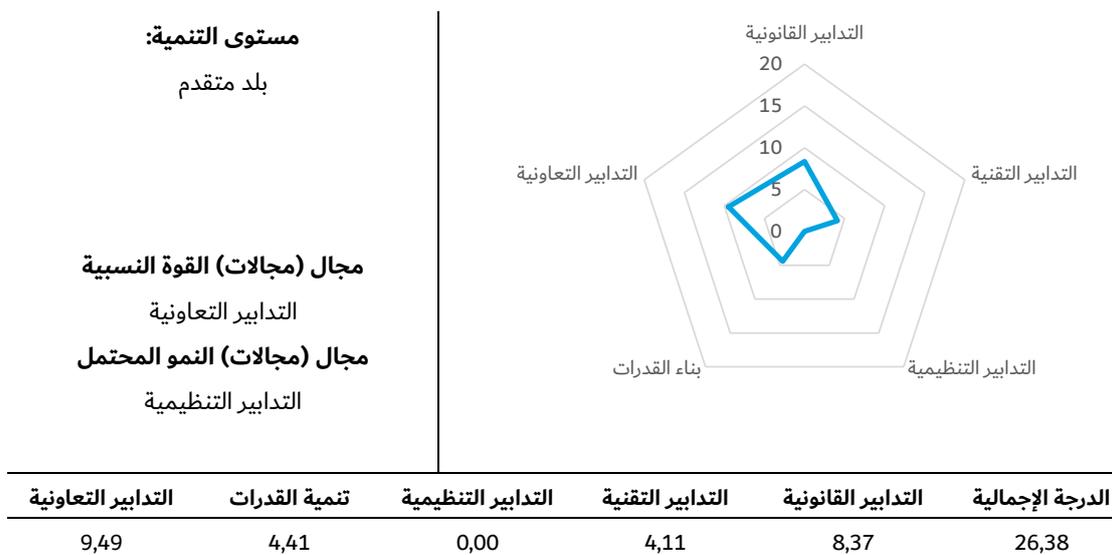


التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
13,56	15,68	10,05	12,56	19,27	71,11

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020



المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

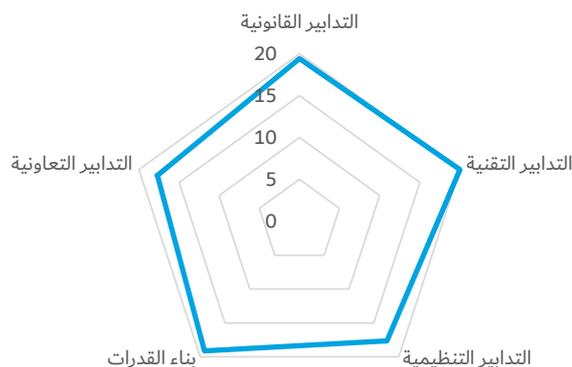
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التقنية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية والتعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
17,70	19,13	17,64	20,00	19,43	93,89

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

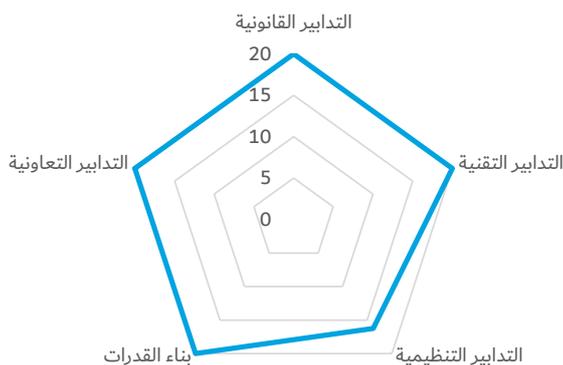
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية والتعاونية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	20,00	16,25	20,00	20,00	96,25

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

البوسنة والهرسك

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
8,33	3,12	1,02	6,56	10,41	29,44

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية بلغاريا

مستوى التنمية:

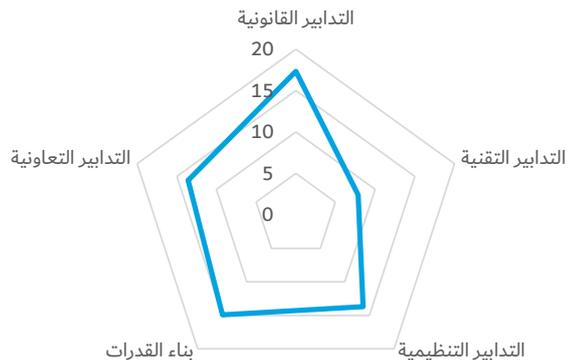
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
13,57	14,92	13,72	7,84	17,34	67,38

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية كرواتيا

مستوى التنمية:

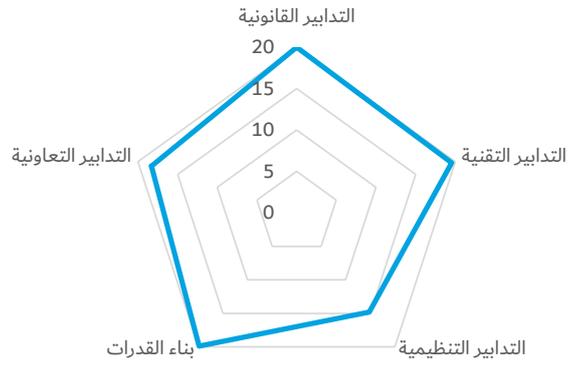
بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير القانونية وتدابير تنمية القدرات

مجالات (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
18,29	19,89	14,80	19,54	20,00	92,53

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية قبرص

مستوى التنمية:

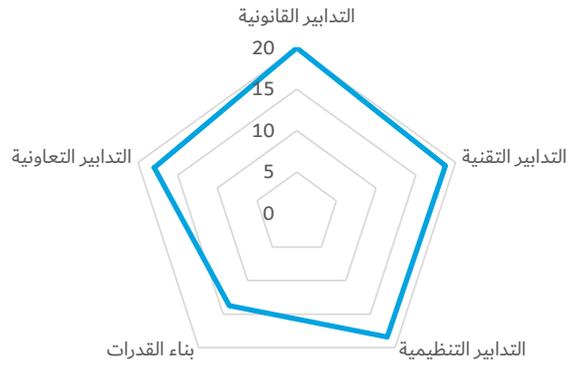
بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير القانونية

مجالات (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
17,94	13,73	18,41	18,73	20,00	88,82

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الجمهورية التشيكية

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التقنية والقانونية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
18,89	19,00	14,20	9,14	13,14	74,37

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الدنمارك

مستوى التنمية:

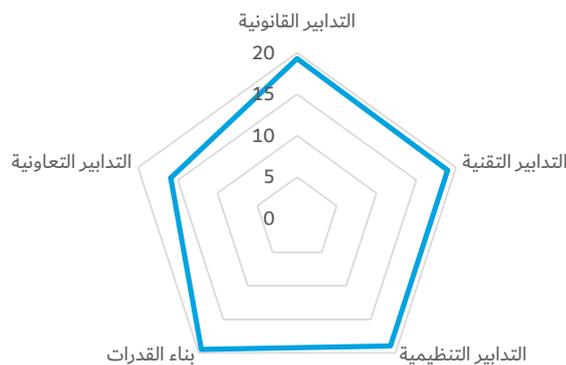
بلد متقدم

مجال (مجالات) القوة النسبية

تنمية القدرات والتدابير القانونية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
19,30	18,94	18,98	19,48	15,89	92,60

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

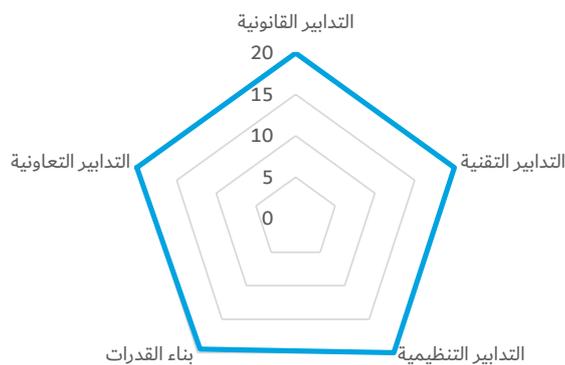
جمهورية إستونيا

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية والتنظيمية
والتعاونية

مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	19,48	20,00	20,00	20,00	99,48

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

فنلندا

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية والتعاونية

مجال (مجالات) النمو المحتمل
التدابير التنظيمية



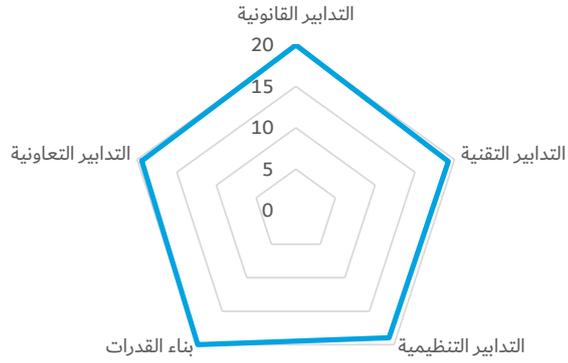
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	17,74	14,33	20,00	20,00	92,07

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

بلد متقدم

مجالات (مجالات) القوة النسبية
التدابير القانونية وتدابير تنمية القدرات
مجالات (مجالات) النمو المحتمل
التدابير التنظيمية



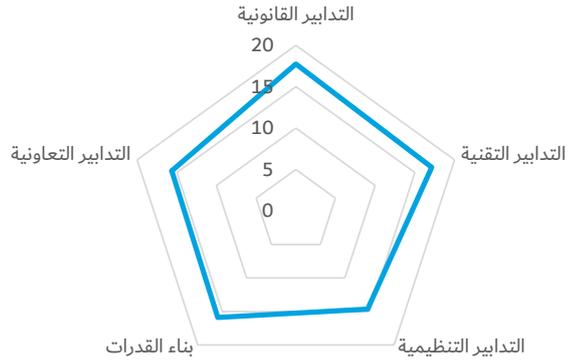
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	20,00	18,98	19,21	20,00	97,60

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

بلد نام

مجالات (مجالات) القوة النسبية
التدابير القانونية
مجالات (مجالات) النمو المحتمل
التدابير التنظيمية والتعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,63	15,89	14,67	17,13	17,75	81,07

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية ألمانيا الاتحادية

مستوى التنمية:

بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير القانونية والتقنية وتدابير تنمية القدرات والتدابير التعاونية

مجالات (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	19,48	18,98	19,54	20,00	97,41

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

اليونان

مستوى التنمية:

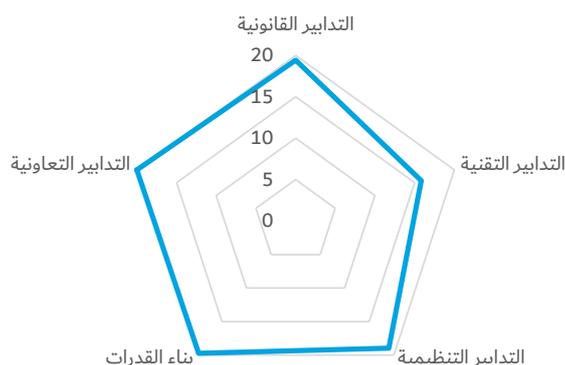
بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير التعاونية والتقنية وتدابير تنمية القدرات والتدابير القانونية

مجالات (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	19,74	18,98	15,83	19,43	93,98

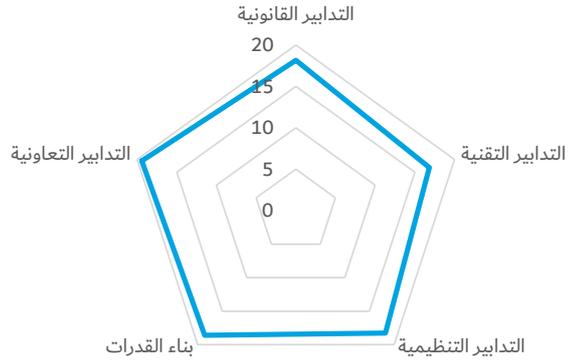
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

هنغاريا

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية
التدابير التعاونية وتدابير تنمية القدرات
مجال (مجالات) النمو المحتمل
التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	18,60	18,29	16,82	18,16	91,28

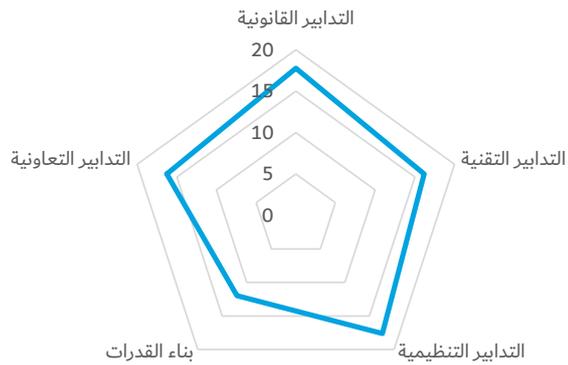
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

أيسلندا

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية والتنظيمية
مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
16,25	11,99	17,62	16,17	17,78	79,81

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

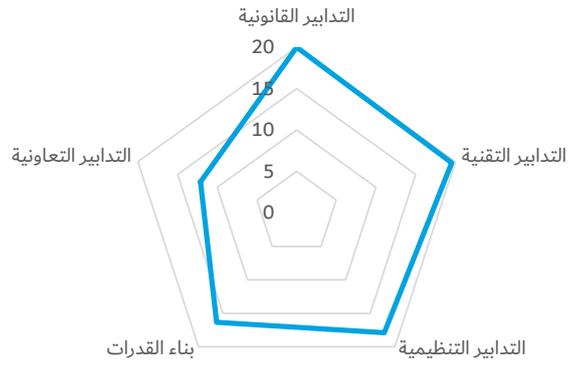
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,54	17,89	16,32	12,11	85,86

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

مستوى التنمية:

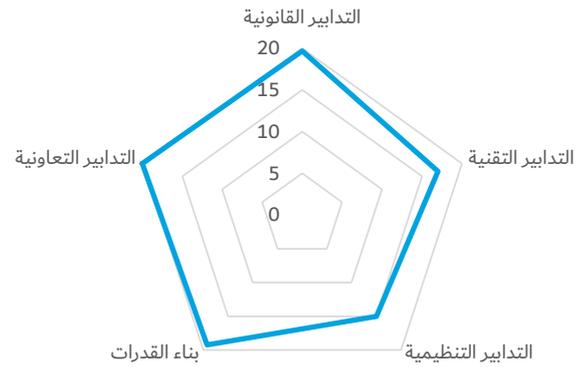
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التعاونية والقانونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
19,68	16,99	15,02	19,24	20,00	90,93

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

مستوى التنمية:

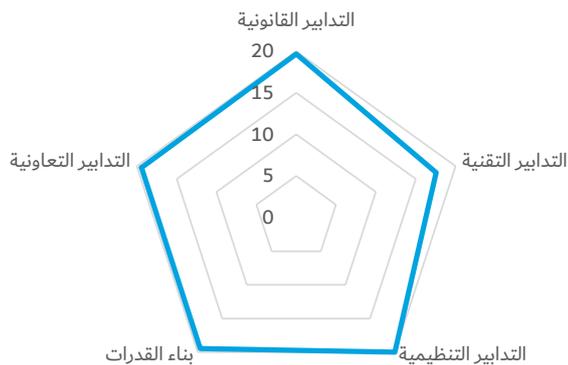
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التنظيمية

مجال (مجالات) النمو المحتمل

التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	19,48	20,00	17,56	19,68	96,13

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

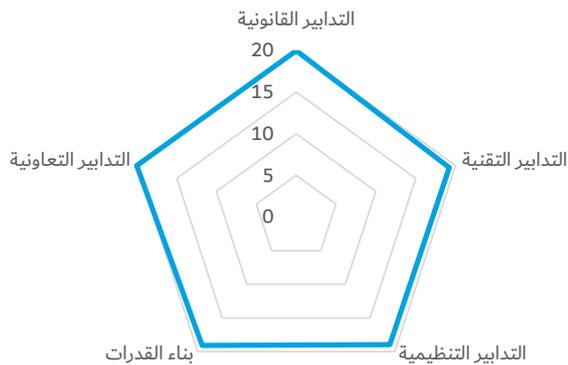
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتعاونية والتقنية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



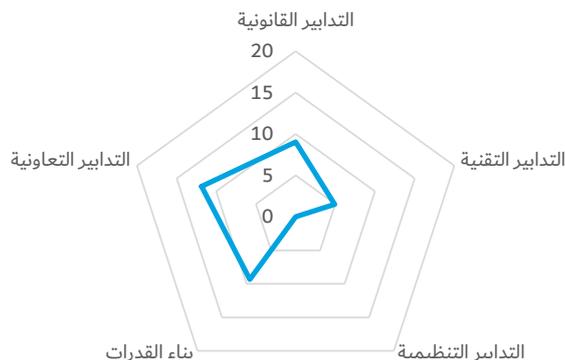
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	19,09	18,98	19,21	20,00	97,28

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

إمارة ليختنشتاين**

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجالات (مجالات) القوة النسبية
التدابير التعاونية
مجالات (مجالات) النمو المحتمل
التدابير التنظيمية



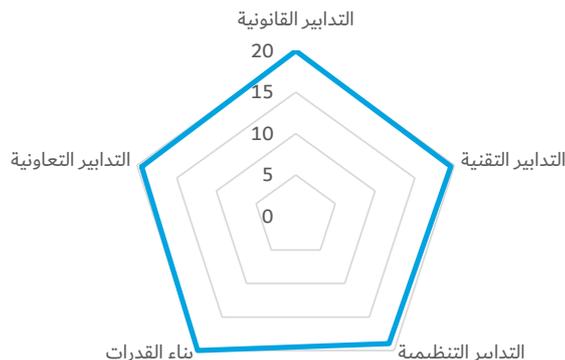
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
9,04	4,93	0,00	9,34	11,85	35,15

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

جمهورية ليتوانيا

مستوى التنمية:
بلد متقدم

مجالات (مجالات) القوة النسبية
التدابير القانونية وتنمية القدرات
والتدابير التعاونية
مجالات (مجالات) النمو المحتمل
التدابير التنظيمية

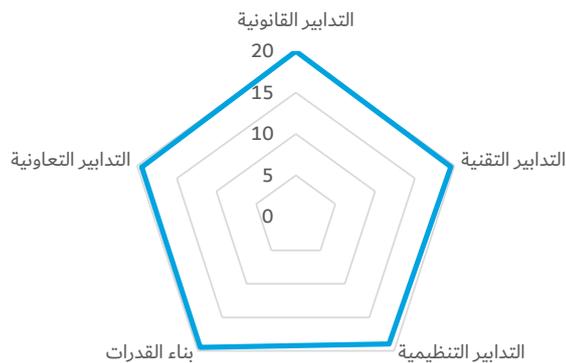


التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	19,54	18,98	20,00	19,41	97,93

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020.

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	19,48	18,98	19,54	20,00	97,41

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2021

مستوى التنمية:
بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,89	18,76	13,41	15,59	20,00	83,65

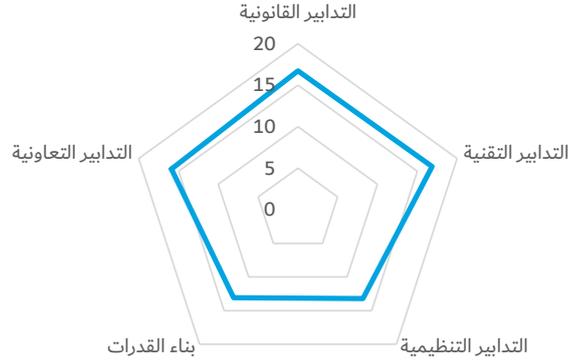
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية مولدوفا

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجالات (مجالات) القوة النسبية
التدابير القانونية والتقنية

مجالات (مجالات) النمو المحتمل
التدابير التنظيمية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
16,73	16,86	13,21	13,09	15,89	75,78

المصدر: الإصدار الرابع للرقم القياسي العالمي للأمن السيبراني للاتحاد، 2020

إمارة موناكو

مستوى التنمية:
بلد متقدم

مجالات (مجالات) القوة النسبية
التدابير القانونية وتنمية القدرات والتدابير التعاونية

مجالات (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
16,00	12,77	12,70	13,75	17,34	72,57

المصدر: الإصدار الرابع للرقم القياسي العالمي للأمن السيبراني للاتحاد، 2021

الجبل الأسود

مستوى التنمية:

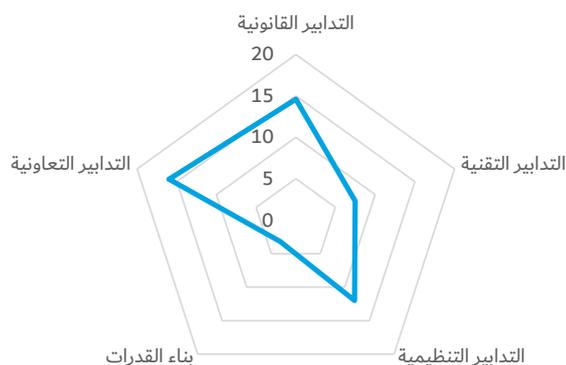
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
15,97	3,18	12,00	7,48	14,61	53,23

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مملكة هولندا**

مستوى التنمية:

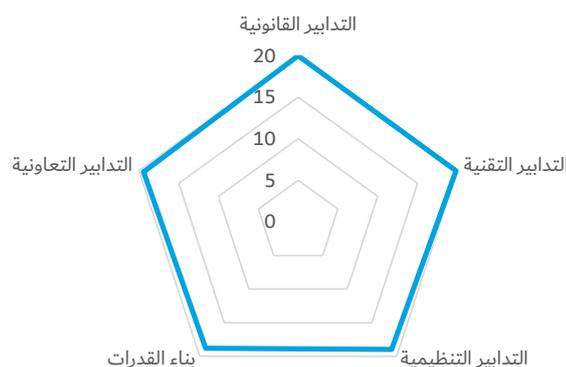
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية والتعاونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
19,41	18,82	18,98	19,84	20,00	97,05

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

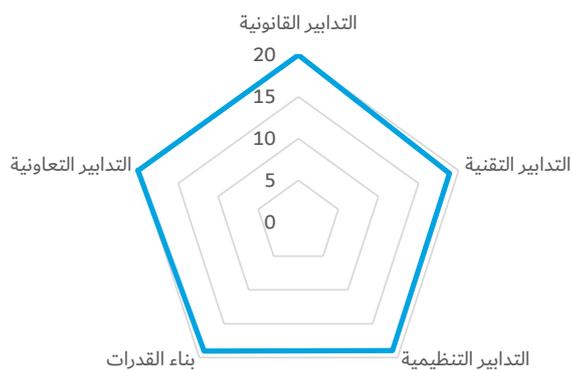
بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير القانونية والتعاونية

مجالات (مجالات) النمو المحتمل

التدابير التقنية والتنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	18,86	18,98	19,04	20,00	96,89

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

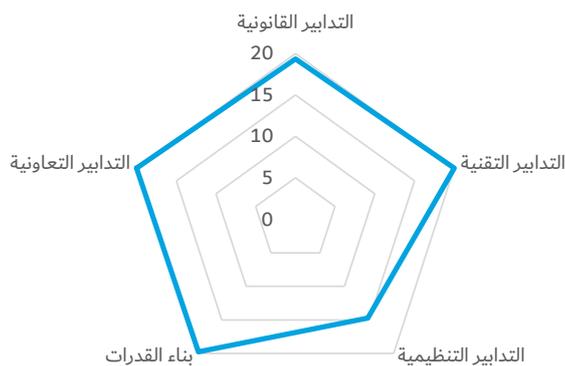
بلد متقدم

مجالات (مجالات) القوة النسبية

التدابير التقنية والتعاونية

مجالات (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
19,35	20,00	14,74	19,77	20,00	93,86

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

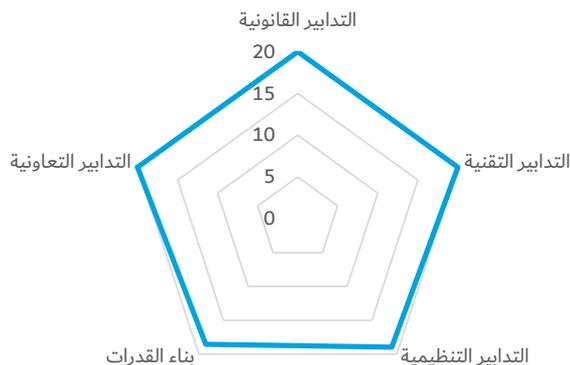
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتقنية والتعاونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية وتدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	18,34	18,98	20,00	20,00	97,32

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

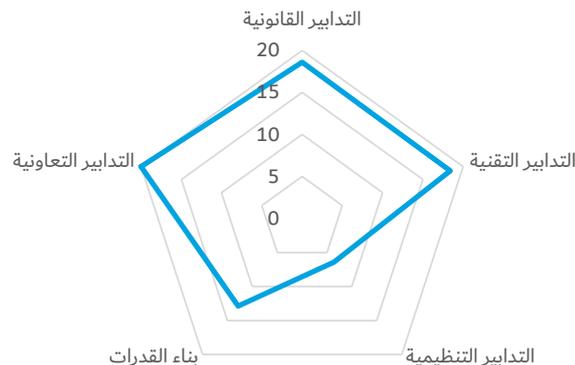
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير التعاونية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	12,88	6,42	18,40	18,60	76,29

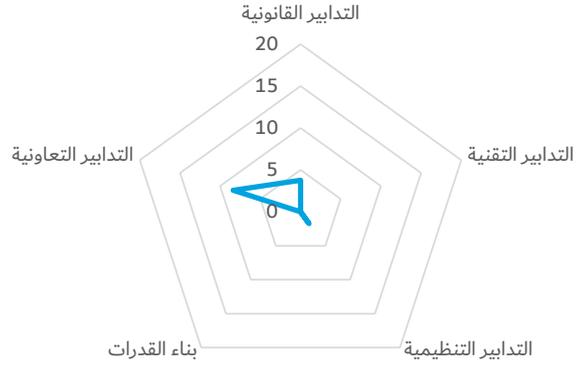
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سان مارينو

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التعاونية

مجال (مجالات) النمو المحتمل
التدابير التقنية وتدابير تنمية القدرات



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
3,77	0,00	1,69	0,00	8,37	13,83

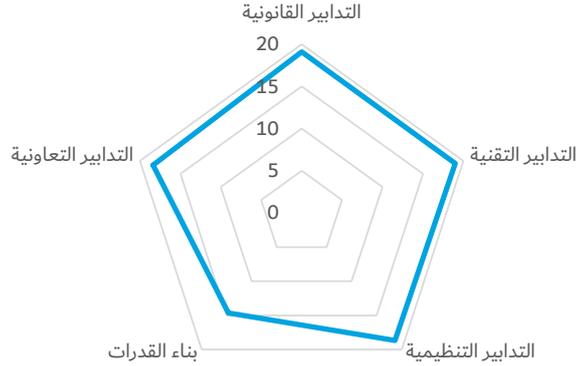
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية صربيا

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية

مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



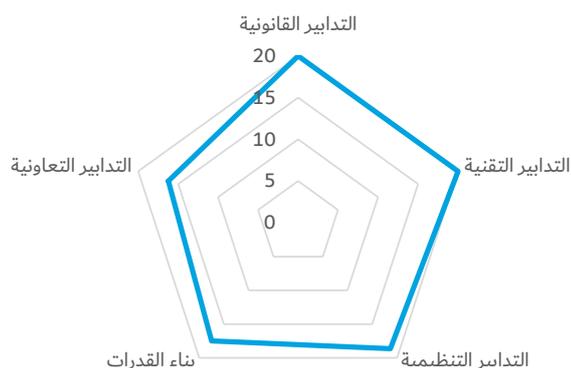
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
19,10	18,99	18,67	14,66	18,38	89,80

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سلوفاكيا

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتقنية
مجال (مجالات) النمو المحتمل
التدابير التعاونية



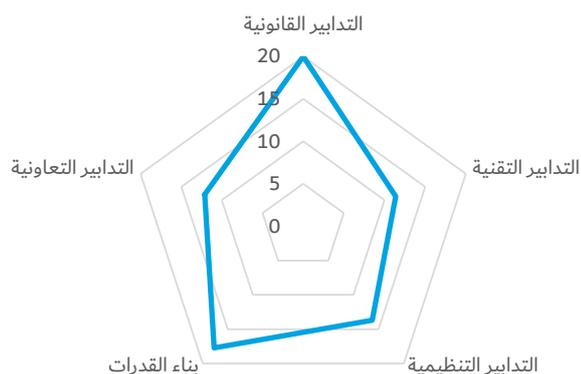
التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
16,22	17,50	18,64	20	20	92,36

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية سلوفينيا

مستوى التنمية:
بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
12,11	17,72	13,71	11,38	20	74,93

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتعاونية وتدابير تنمية القدرات والتدابير التقنية

مجال (مجالات) النمو المحتمل

التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	20,00	18,98	19,54	20,00	98,52

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

مستوى التنمية:

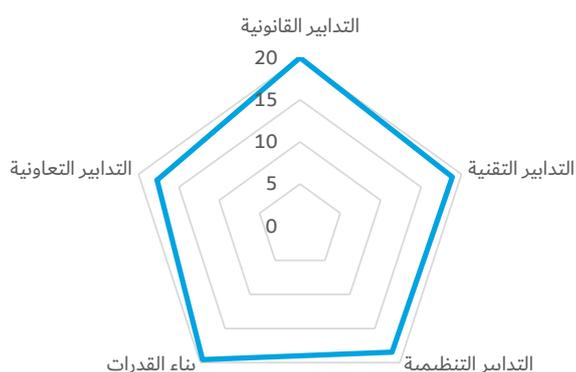
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التعاونية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
17,70	19,57	18,46	18,86	20,00	94,59

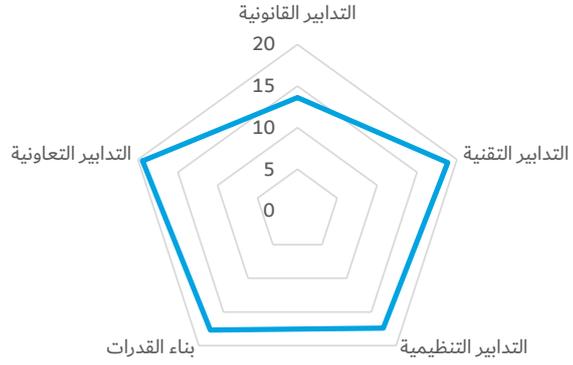
المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الرقم القياسي العالمي للأمن السيبراني لعام 2020

الاتحاد السويسري**

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير التعاونية والتقنية
مجال (مجالات) النمو المحتمل
التدابير القانونية



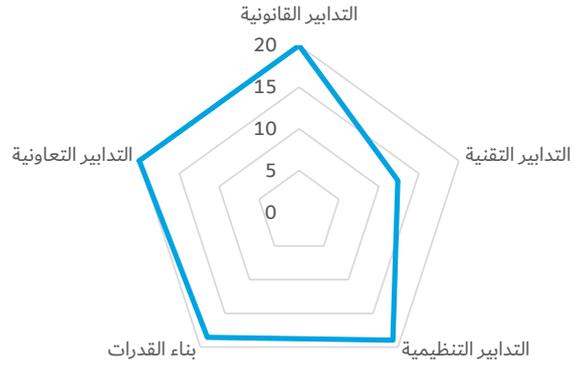
التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
13,62	18,85	17,40	17,69	19,41	86,97

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

جمهورية مقدونيا الشمالية

مستوى التنمية:
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية
مجال (مجالات) النمو المحتمل
التدابير التقنية



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية	الدرجة الإجمالية
20,00	12,37	18,98	18,57	20,00	89,92

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

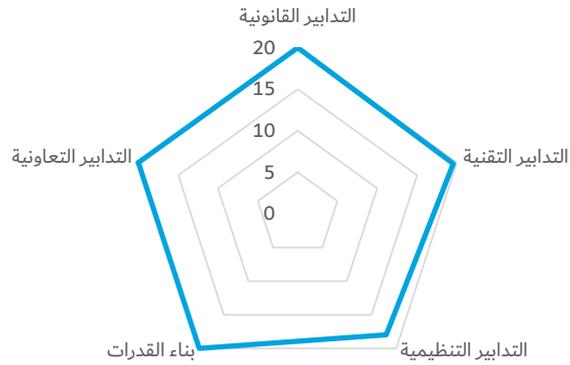
تركيا

مستوى التنمية:

بلد نام

مجال (مجالات) القوة النسبية
التدابير القانونية والتعاونية والتقنية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل
التدابير التنظيمية



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
20,00	20,00	17,96	19,54	20,00	97,50

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

أوكرانيا

مستوى التنمية:

بلد متقدم

مجال (مجالات) القوة النسبية
التدابير القانونية

مجال (مجالات) النمو المحتمل
تدابير تنمية القدرات



التدابير التعاونية	تنمية القدرات	التدابير التنظيمية	التدابير التقنية	التدابير القانونية	الدرجة الإجمالية
12,87	10,94	13,06	11,60	17,46	65,93

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

مستوى التنمية:

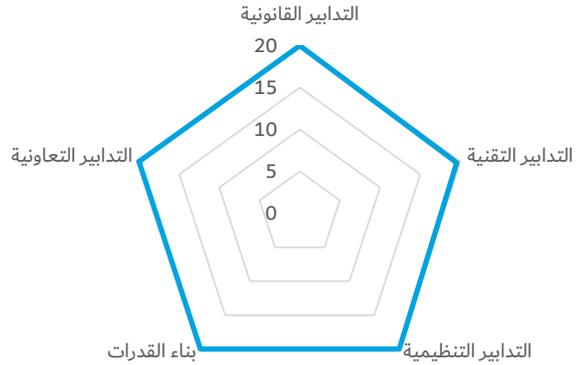
بلد متقدم

مجال (مجالات) القوة النسبية

التدابير القانونية والتنظيمية والتعاونية
وتدابير تنمية القدرات

مجال (مجالات) النمو المحتمل

التدابير التقنية



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	التدابير التعاونية	تنمية القدرات
99,54	20,00	19,54	20,00	20,00	20,00

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

الفايكان*

مستوى التنمية:

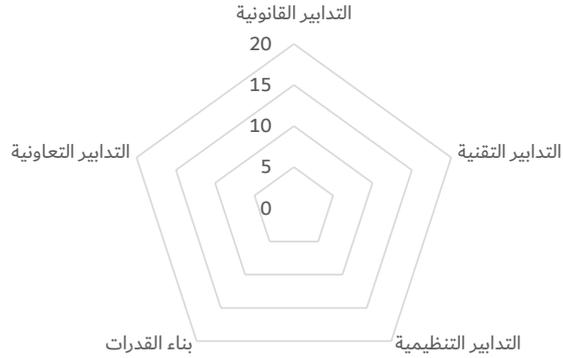
بلد متقدم، بلد غير ساحلي

مجال (مجالات) القوة النسبية

لا يوجد

مجال (مجالات) النمو المحتمل

لا يوجد



الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
0	0	0	0	0	0

المصدر: الإصدار الرابع للرقمي القياسي العالمي للأمن السيبراني للاتحاد، 2020

** لا يوجد رد على الاستبيان/بيانات جمعها الفريق المعني بالرقم القياسي العالمي للأمن السيبراني

* لا توجد بيانات

مسرد المصطلحات

المختصر	التعريف
CERT	فريق الاستجابة للطوارئ الحاسوبية، يحمل العلامة التجارية لجامعة كارنيغي ميلون (Computer Emergency Response Team, trademarked by Carnegie Mellon University)
CI	بنية تحتية (Critical Infrastructure)
CIRT*	فريق الاستجابة للحوادث الحاسوبية، انظر المصطلحات ذات الصلة CERT، CSIRT (Computer Incident Response Team, see related terms CSIRTs, CERTs)
CSIRT	فريق الاستجابة للحوادث الأمنية الحاسوبية (Computer Security Incident Response Team)
DPP	حماية البيانات والخصوصية (Data and Privacy Protection)
EU	الاتحاد الأوروبي (European Union)
GCI-1/2/3/4	صيغة الرقم القياسي العالمي للأمن السيبراني (The iteration of the Global Cybersecurity Index)
GDPR	لائحة حماية البيانات العامة (الاتحاد الأوروبي (EU)) (General Data Protection Regulation (EU))
ICT	تكنولوجيا المعلومات والاتصالات (Information and Communication Technology)
ITU	الاتحاد الدولي للاتصالات (International Telecommunication Union)
LDC	أقل البلدان نمواً (Least Developed Countries)
LLDC	البلدان النامية غير الساحلية (Landlocked Developed Countries)
MLAT	معاهدة المساعدة القانونية المتبادلة (Mutual Legal Assistance Treaty)
MSME	الشركات متناهية الصغر والصغيرة والمتوسطة (Micro, small, and medium-sized enterprise)
NCS	الاستراتيجية الوطنية للأمن السيبراني (National Cybersecurity Strategy)
NGO	منظمة غير حكومية (Non-Government Organization)
ODC	بلدان نامية أخرى (Other Developing Countries)
OT	التكنولوجيا التشغيلية (Operational Technology)
PPP	الشراكة بين القطاعين العام والخاص (Public Private Partnership)
SIDS	الدول الجزرية الصغيرة النامية (Small Island Development States)
SME	الشركات الصغيرة والمتوسطة (Small and medium-sized enterprises)
UN	الأمم المتحدة (United Nations)

الملحق A: المنهجية

A1 نطاق الرقم القياسي وإطار عمله

ولاية الرقم القياسي العالمي للأمن السيبراني (GCI) مستمدة من القرار 130 (المراجع في دبي، 2018) بشأن تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات. وعلى وجه التحديد، تُدعى البلدان "إلى دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك الرقم القياسي العالمي للأمن السيبراني (GCI)، من أجل تشجيع الاستراتيجيات الحكومية وتبادل المعلومات عن الجهود المبذولة عبر الصناعات والقطاعات". والهدف من الرقم القياسي تعزيز ثقة عالمية للأمن السيبراني ودمجها في صميم تكنولوجيا المعلومات والاتصالات.

الجدول A1: المشاركة في الرقم القياسي العالمي للأمن السيبراني وسنوات جمع البيانات

GCI-4	GCI-3	GCI-2	GCI-1	
169	155	136	105	البلدان التي توفر جهة اتصال
2020	2018-2017	2016	2014-2013	سنوات جمع البيانات
2020	2019	2017	2015	سنة النشر

وجرت صياغة الرقم القياسي على أساس البيانات المقدمة من أعضاء الاتحاد، بما في ذلك الأفراد والخبراء وأصحاب المصلحة في الصناعة المهتمين كشركاء مساهمين مع معهد السياسة الاستراتيجية في أستراليا، وFIRST (متتدى أفرقة الأمن والاستجابة للحوادث)، وجامعة غرونوبل (فرنسا)، وجامعة إنديانا، وإنتربول، والمركز الإقليمي المعني بالأمن السيبراني في المنطقة العربية التابع للاتحاد في عُمان، والوكالة الكورية للإنترنت والأمن، والجهاز القومي لتنظيم الاتصالات (NTRA)، في مصر، وRed Team Cyber، ومعهد بوتوماك لدراسة السياسات العامة، ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، وجامعة جامايكا للتكنولوجيا، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، والبنك الدولي.

نطاق الرقم القياسي

الرقم القياسي العالمي للأمن السيبراني (GCI) هو مؤشر مركب للمؤشرات يتطور في كل صيغة ويتيح مراقبة مستوى الالتزام بالأمن السيبراني في إطار الركائز الخمس لبرنامج الأمن السيبراني العالمي (GCA)، وتتمثل أهدافه الرئيسية في قياس:

- نوع ومستوى وتطور الالتزام بالأمن السيبراني مع مرور الوقت داخل البلدان وفيما يتعلق بالبلدان الأخرى.
- التقدم المحرز في التزام البلدان بالأمن السيبراني من منظور عالمي.
- التقدم المحرز في التزام البلدان بالأمن السيبراني من منظور إقليمي.
- فجوة الالتزام بالأمن السيبراني (أي الفرق بين البلدان من حيث مستوى مشاركتها في مبادرات الأمن السيبراني).

والهدف من الرقم القياسي مساعدة البلدان في تحديد مجالات التحسين في مجال الأمن السيبراني وتشجيعها على اتخاذ إجراءات تجاه تلك المجالات. وسيكون ذلك أيضاً فرصة للمساعدة في رفع المستوى العام للالتزام بالأمن السيبراني على الصعيد العالمي وتنسيق الممارسات وتعزيز ثقافة عالمية للأمن السيبراني. ويهدف الرقم القياسي إلى توضيح الأمثلة الناجحة على الأمن السيبراني التي يمكن أن تكون بمثابة ممارسات ومبادئ توجيهية جيدة للبلدان ذات البيئات الوطنية المتماثلة.

A2 إطار التعاون في مجال الأمن السيبراني للاتحاد

الأمن السيبراني مجال متعدد التخصصات ويشمل تطبيقه جميع القطاعات والصناعات وأصحاب المصلحة، رأسياً وأفقياً على السواء. ولذلك، يتعين على القوى السياسية والاقتصادية والاجتماعية بذل جهود لزيادة تنمية القدرات. ويمكن تحقيق ذلك من خلال أجهزة إنفاذ القانون وإدارات العدالة والمؤسسات التعليمية والوزارات ومشغلي القطاع الخاص ومطوري التكنولوجيا والشراكات بين القطاعين العام والخاص والتعاون داخل الدولة.

ويهدف إطار الاتحاد للتعاون الدولي بين أصحاب المصلحة المتعددين في مجال الأمن السيبراني إلى بناء أوجه التآزر بين المبادرات الحالية والمستقبلية ويركز على الركائز الخمس التالية التي تشكل اللبنة الأساسية لثقافة وطنية للأمن السيبراني.

الجدول A2: وصف ركائز الرقم القياسي العالمي للأمن السيبراني لعام 2020

التدابير القانونية
تدابير قائمة على وجود أطر قانونية تتناول الأمن السيبراني والجريمة السيبرانية.
تخول التدابير القانونية (بما في ذلك التشريعات المتعلقة بالرسائل الإحتجاجية ولوائحها واحتوائها) أي دولة بإنشاء آليات استجابة أساسية من خلال التحقيق في الجرائم وملاحقة مرتكبيها وفرض عقوبات على عدم الامتثال للقانون أو خرقه. ويحدد الإطار التشريعي الحد الأدنى من أساس السلوك الذي يمكن بناء المزيد من قدرات الأمن السيبراني على أساسه. ويتمثل الهدف أساساً في وضع تشريعات كافية من أجل موازنة الممارسات على الصعيد الإقليمي/الدولي وتبسيط مكافحة الجريمة السيبرانية على المستوى الدولي.
التدابير التقنية
تدابير قائمة على وجود مؤسسات تقنية وإطار تقني يتناول الأمن السيبراني.
لا يمكن تعزيز كفاءة تطوير واستخدام تكنولوجيا المعلومات والاتصالات إلا في بيئة تسودها الثقة والأمن. ولذلك يتعين على البلدان وضع وتثبيت معايير أمنية وخطط اعتماد دنيا مقبولة فيما يتعلق بالتطبيقات والأنظمة البرمجية. وينبغي استكمال هذه الجهود بإنشاء هيئة وطنية تتعامل مع الحوادث السيبرانية وكيان حكومي موثوق وإطار وطني لمراقبة الحوادث والتحذير منها والاستجابة لها.
التدابير التنظيمية
تدابير قائمة على وجود مؤسسات وسياسات واستراتيجيات التنسيق لتطوير الأمن السيبراني على الصعيد الوطني.
تشمل التدابير التنظيمية تحديد أهداف الأمن السيبراني والخطط الاستراتيجية، فضلاً عن التعريف الرسمي للأدوار والمسؤوليات والمساءلة المؤسسية لضمان تنفيذها. ولا غنى عن هذه التدابير لتأييد وضع وتنفيذ وضع فعال للأمن السيبراني. ويجب أن تحدد الدولة غايات وأهدافاً استراتيجية واسعة، إلى جانب خطة شاملة في التنفيذ والتسليم والقياس. ويجب أن تكون الوكالات الوطنية حاضرة لتنفيذ الاستراتيجية وتقييم النتائج. وبدون استراتيجية وطنية، ونموذج إدارة، وهيئة إشرافية، تتضارب الجهود المبذولة في القطاعات المختلفة، مما يحول دون بذل جهود لتحقيق الموازنة الفعالة في تطوير الأمن السيبراني.
تدابير تنمية القدرات
تدابير قائمة على وجود برامج البحث والتطوير والتعليم والتدريب والمهنيين المعتمدين ووكالات القطاع العام التي تعزز تنمية القدرات.
يشمل تنمية القدرات حملات توعية عامة، وإطاراً لإصدار الشهادات واعتماد المهنيين في مجال الأمن السيبراني، ودورات تدريبية مهنية في مجال الأمن السيبراني أو برامج تعليمية أو مناهج دراسية، وما إلى ذلك. وهذه الركيزة جزء لا يتجزأ من الركائز الثلاث الأولى (القانونية والتقنية والتنظيمية). وغالباً ما يتم التعامل مع الأمن السيبراني من منظور تكنولوجي على الرغم من وجود العديد من الآثار الاجتماعية والاقتصادية والسياسية. وتنمية القدرات البشرية والمؤسسية أمر أساسي لإذكاء الوعي والمعرفة والدراية عبر القطاعات من أجل إيجاد حلول منهجية ومناسبة، وتعزيز تنمية قدرات المهنيين المؤهلين.
التدابير التعاونية
تدابير قائمة على وجود شراكات وأطر تعاونية وشبكات لتبادل المعلومات.
نظراً إلى مستوى التوصل البيئي غير المسبوق بين الدول، يعد الأمن السيبراني مسؤولية مشتركة وتحدياً عابراً للحدود الوطنية. ويمكن لزيادة التعاون أن تمكن من تطوير قدرات أقوى بكثير في مجال الأمن السيبراني، مما يساعد على التخفيف من المخاطر السيبرانية وتمكين تسحين التحقيق، والقبض على العملاء الخبثاء ومقاضاتهم.

A3 التغييرات الرئيسية حسب الركيزة

التدابير القانونية

تتيح التدابير القانونية قياس التدخلات القانونية في مجال الأمن السيبراني، وقد تم تحديثها لتجسد بشكل أفضل القانون الموضوعي الوطني المتعلق بالأمن السيبراني.

- استناداً إلى توصيات فريق التشاور لإدارة مكتب تنمية الاتصالات، لم يعد القانون الإجرائي يقاس في الرقم القياسي العالمي للأمن السيبراني، وبدلاً من ذلك، يتم التأكيد على مزيد من الوضوح في العديد من المجالات بما في ذلك سرقة الهوية والتحرشات عبر الإنترنت والعنصرية.

- وُضعت الأسئلة المندرجة في إطار التدابير القانونية في البداية تبعاً لتوصيات اتفاقيات مثل اتفاقية بودابست بشأن الجريمة السيبرانية. غير أن الإجابات تركز الآن على إبراز القوانين الوطنية المطبقة فقط وليس على جمع التصديقات على هذه الاتفاقيات. ومع ذلك، ونظراً لتأثير الاتفاقيات الدولية ودورها في إنشاء التزامات ملزمة، يجري الآن قياس الاتفاقات الدولية مثل اتفاقية بودابست في إطار الأنشطة الدولية للتدابير التعاونية.
- مع تزايد عدد الأشخاص الذين يستخدمون الإنترنت، يتطلب الفضاء السيبراني الجدير بالثقة الذي يعزز التنوع والشمول أيضاً دراسة قضايا مثل الخصوصية، فضلاً عن التحرش والترهيب والاستمالة واستغلال الأطفال في المواد الإباحية والعنصرية.

التدابير التقنية

أعيدت هيكلة الركيزة التقنية للتعبير على نحو أفضل عن كيفية عمل الأفرقة CIRT، بما في ذلك:

- فريق الاستجابة للحوادث الحاسوبية - تم دمج الأفرقة CIRT الحكومية والوطنية في مؤشر واحد.
- شهادة CIRT عنصر مهم في تقديم رؤى حول القدرة على معالجة الحوادث السيبرانية. ولتقييم مستويات نضج الفريق CIRT الوطني¹، أضيف نظام اعتماد SIM3. ويستخدم الفريق TF-CSIRT/المقدم الموثوق نظام SIM3 كأساس للتقييم والأعضاء "المعتمدين" الذين وصلوا إلى أعلى مرحلة من النضج.

التدابير التنظيمية

- بما أن الأمن السيبراني عملية مستمرة، تُشجع البلدان على إعادة النظر بانتظام في الاستراتيجيات الوطنية للأمن السيبراني (كل خمس سنوات على الأقل) لتقييم ما إذا كانت الاستراتيجية الوطنية للأمن السيبراني لا تزال ذات صلة بالنظر إلى بيئة المخاطر المتغيرة، وما إذا كانت لا تزال تجسد الأهداف الوطنية ولفهم التعديلات اللازمة. واستناداً إلى هذه التوصية، تلقت البلدان التي لم تؤكد من جديد أو تحدّث استراتيجيتها الوطنية بشأن الأمن السيبراني في السنوات الخمس الماضية نقاطاً جزئية بشأن المؤشرات المتعلقة بالاستراتيجية الوطنية للأمن السيبراني.
- ينبغي أن يكون تطوير آليات لحماية الأطفال على الإنترنت من بين الأولويات الحيوية للبلدان خاصة عندما أجبرت جائحة كوفيد-19- الأطفال على الدراسة عبر الإنترنت. وعلى الرغم من أن الإنترنت تجلب منافع كبيرة لتعليم الأطفال ونموهم، فإنها تعرضهم أيضاً لمخاطرها. وقد اتخذت معظم البلدان مبادرات لدعم حماية الأطفال على الإنترنت من خلال جهود مثل إنشاء مواقع إلكترونية ووسائل التواصل الاجتماعي مع مواد تعليمية مخصصة وألعاب إعلامية وأدلة للأطفال والآباء والمعلمين. ولتمييز بين التدخلات المخصصة وتلك المنظمة ضمن استراتيجية أوسع ومحددة، حصلت الأخيرة على علامات كاملة، في حين حصلت البلدان التي لديها مبادرات لمرة واحدة أو متفرقة على علامات جزئية.

تدابير تنمية القدرات

ظلت هذه الركيزة مستقرة من حيث مؤشراتنا منذ الصيغة الثانية للرقم القياسي. وفي هذه الصيغة، اتسع النطاق ليشمل إذكاء الوعي بالدعم الحكومي للشركات الصغيرة والمتوسطة (SME) نظراً لاضطلاعها بدور هام كجهات فاعلة في الاقتصاد الرقمي وسلاسل التوريد، وبأني ذلك في فترة تحوّل نحو التجارة الإلكترونية واحتياج الشركات الصغيرة والمتوسطة إلى الدعم في إدارة المخاطر السيبرانية.

تدابير التعاون

تبين هذه الركيزة ما إذا كانت الاتفاقات موقعة أو مصدق عليها بغض النظر عما إذا كانت ملزمة قانوناً. وقد تم توضيح الاتفاقات التي تندرج في إطار الاتفاقات الثنائية والاتفاقات متعددة الأطراف. وأصبحت اتفاقية بودابست تقع الآن تحت النشاط الدولي بعد أن كانت تندرج سابقاً في إطار الاتفاقات متعددة الأطراف.

A4 المنهجية الحسائية

يوفر الاستبيان المستخدم في الرقم القياسي العالمي للأمن السيبراني قيمة للمؤشرات العشرين التي أنشئت من خلال 82 سؤالاً. وهذا يحقق المستوى المطلوب من التفاصيل ويحسن دقة الأجوبة وجودتها. ويمكن العثور على المؤشرات في استبيان الرقم القياسي (الملحق B).

¹ الأفرقة CIRT المعروفة أيضاً باسم CSIRT/CERT هي كيانات تنظيمية تُسند إليها مسؤولية تسيق ودعم الاستجابة للحوادث أو الأحداث الأمنية الحاسوبية على الصعيد الوطني.

وتم اختيار المؤشرات المستخدمة لحساب الرقم القياسي استناداً إلى:

- أهمية الركائز الخمس للبرنامج العالمي للأمن السيبراني؛
- الصلة بالأهداف الرئيسية للرقم القياسي وإطاره المفاهيمي؛
- تيسر البيانات وجودتها؛
- إمكانية التحقق من خلال البيانات الثانوية.

ويستند الرقم القياسي إلى خريطة تطوير الأمن السيبراني التي يمكن لأي بلد أن يأخذها في الاعتبار عند تحسين التزامه بالأمن السيبراني. ويستند الاستبيان إلى خمس ركائز مختلفة متميزة بخمسة ألوان محددة. ويشير عمق المسار في الرسوم البيانية الواردة في هذا التقرير إلى مستوى تطوير أعلى للالتزام.

ويقدم هذا التقرير الاتجاهات الإقليمية والعالمية. ولضمان الدقة، طُلب من البلدان دعم إجابتها من خلال ميزة تحميل الوثائق الداعمة وعناوين URL. وأضيف قسم للتعليق على كل ركيزة للسماح للبلدان بتقديم الممارسات الجيدة التي تبين التجارب المتعلقة بتأثير تطورها في مجال الأمن السيبراني.

وعُرضت على البلدان أجوبة ثنائية أو ثلاثية على 82 سؤالاً من المؤشرات العشرين للركائز الخمس، واستخدم قسم التعليقات لتفاصيل مرحلة التنفيذ في حالة وجود بند في مرحلة الصياغة أو في مرحلة التنفيذ.

وخضعت الاستبيانات بعد إعادتها لعمليتي تحقق من جانب كيانيين مختلفين، وقُدمت نقاط جزئية إذا كانت الإجابة تشير إلى مرحلة الصياغة أو مرحلة التنفيذ/أو إذا لم تتم الإجابة على جميع بنود السؤال على وجه التحديد. وأتاح هذا الأسلوب من التقييم الثلاثي تجنب التقييم القائم على الرأي والتحيز الذاتي من خلال جدول يحتوي على بنود محددة لتقديم إجابة إيجابية وجزئية.

ولهذا الغرض، قُدمت الطبعة الرابعة من استبيان الرقم القياسي العالمي للأمن السيبراني وأي وثائق ذات صلة من أمانة مكتب تنمية الاتصالات إلى اجتماع فريق المقرر المعني بالمسألة 3 للجنة الدراسات 2 في أكتوبر 2019، حيث تمت الموافقة على الاستبيان قبل إصداره. وفي مارس 2020، خلال اجتماع لجنة الدراسات 2، قام مكتب تنمية الاتصالات بتقديم معلومات محدثة بهذا الشأن في إطار المسألة 3 واستشارة البلدان لتعيين خبراء في مجال الأمن السيبراني للمشاركة في عملية الترجيح.

السير العام لعملية الرقم القياسي العالمي للأمن السيبراني

1 تُرسل رسالة دعوة إلى جميع الدول الأعضاء في الاتحاد ودولة فلسطين، لإبلاغها بالمبادرة، وطلب تعيين جهة اتصال مسؤولة عن جمع جميع البيانات ذات الصلة وملء استبيان الرقم القياسي العالمي للأمن السيبراني عبر الإنترنت. وخلال المسح الإلكتروني، دعا الاتحاد رسمياً جهة الاتصال المعتمدة إلى الإجابة على الاستبيان.

2 جمع البيانات الأولية (للبلدان التي لا ترد على الاستبيان):

- يضع الاتحاد مشروعاً أولياً للرد على الاستبيان باستعمال البيانات المتاحة للجُمهور والبحوث على الإنترنت.
- يُرسل مشروع الاستبيان إلى جهات الاتصال لاستعراضه.
- تقوم جهات الاتصال بتحسين دقة مشروع الاستبيان وإعادته.
- يُرسل مشروع الاستبيان المصحح إلى كل جهة اتصال للموافقة النهائية عليه.
- يُستخدم الاستبيان المتحقق منه لأغراض التحليل والتقييم والتصنيف.

3 جمع البيانات الثانوية (للبلدان التي لا ترد على الاستبيان):

- يحدد الاتحاد الردود الناقصة والوثائق الداعمة والروابط وما إلى ذلك
- تقوم جهة الاتصال بتحسين دقة الأجوبة عند الضرورة.
- يُرسل مشروع الاستبيان المصحح إلى كل جهة اتصال للموافقة النهائية عليه.
- يُستخدم الاستبيان المتحقق منه لأغراض التحليل والتقييم والتصنيف.

ملاحظة: إذا لم يوفر أحد البلدان جهة اتصال تُعنى باستبيان الرقم القياسي، يعتمد الاتحاد إلى إقامة الاتصال مع جهة الاتصال المؤسسية في الدليل العالمي للاتحاد.

الترجيح

على عكس الصيغ السابقة التي تستخدم مقياساً من 0 إلى 1، تستخدم هذه الصيغة للرقم القياسي مقياساً من 0 إلى 100، مع ترجيح كل ركيزة عند 20 نقطة.

وكمؤشر مرجح مركب، تخصص قيمة ترجيحية لكل مؤشر ومؤشر فرعي ومؤشر دون فرعي نظراً للأهمية النسبية لمجموعة المؤشرات. ويمكن أن يكون للقيمة الترجيحية أثر كبير على الدرجات النهائية، وستسفر التقنيات المختلفة عن تصنيفات مختلفة.

وتابع الرقم القياسي نهجاً تشاركياً باستخدام عملية تخصيص الميزانية (BAP). وهي تعتبر القيم الترجيحية في الأساس، أحكاماً قيمية، وينبغي أن تأخذ في الحسبان مجموعة واسعة من مدخلات الخبراء.

وفي إطار نهج تخصيص الميزانية، كان للخبراء "ميزانية" معينة يمكنهم تخصيصها ضمن مجموعة مؤشرات، مع تخصيص قيمة أكبر للمؤشرات التي قُيِّمت باعتبارها أكثر أهمية. وطلب إلى الخبراء تقديم توصيات بشأن الترجيح فيما يتعلق بالركائز التي لديهم خبرة فيها.

ولم تأخذ عملية الترجيح في الحسبان الجودة الإحصائية للبيانات نظراً لأن جميع ردود البلدان التي تستند إليها البيانات تم الإبلاغ عنها كبيانات استقصاء تحقق منها فريق الاتحاد.

مشاركة فريق الخبراء المعني بالترجيح

في أكتوبر 2020، دُعيت الدول الأعضاء في الاتحاد وأعضاء القطاع الخاص من خلال رسالة معممة إلى ترشيح خبراء للمشاركة في هذه الصيغة للرقم القياسي العالمي للأمن السيبراني. وينتمي الخبراء المعينون إلى الهيئات الأكاديمية ومراكز الفكر ووزارات تكنولوجيا المعلومات والاتصالات والهيئات التنظيمية ومنظمات وضع المعايير.

ودُعي الخبراء الذين ساهموا في الصيغ السابقة للرقم القياسي العالمي للأمن السيبراني أيضاً إلى المساهمة بتوصيات الترجيح.

وشارك في الاجتماع 84 خبيراً طلب منهم تقديم توصيات بشأن الترجيح فيما يتعلق بالركائز المتعلقة بمجالات خبراتهم.

التجميع

تم تجميع مجموعات المؤشرات باستخدام المتوسطات الحسابية المرجحة. وهذا يعني أن أي بلد يسجل نتائج سيئة في مجال ما يمكن أن يستعيد بعض درجاته من خلال الأداء الجيد في أماكن أخرى.

وكما جاء في كتيب منظمة التعاون والتنمية في الميدان الاقتصادي بشأن المؤشرات المركبة، فإن "المنفعة الهامشية من الزيادة في الدرجة المطلقة المنخفضة ستكون أعلى بكثير مما هي عليه في الدرجة المطلقة العالية تحت التجميع الهندسي. وبالتالي، سيكون للبلد حافز كبير لمعالجة تلك القطاعات/الأنشطة/البدايل ذات الدرجة المنخفضة إذا كان التجميع هندسياً وليس خطياً" (33). غير أنه لأغراض الوضوح والفهم، اعتُبر النهج الخطي أكثر قابلية للفهم والتنفيذ.

تحليل الحساسية

نظراً لأهمية الترجيح بالنسبة لدرجات البلدان النهائية، أجريت تحليلات الحساسية، شملت ما يلي:

- إدراج/استبعاد المؤشرات الفردية؛
- مخططات مختلفة للترجيح (الترجيح المتساوي، طريقة تخصيص الميزانية، القيم القصوى لتوصيات الخبراء)؛
- أنظمة تجميع مختلفة (متوسطات مرجحة، مضافة).

المرتبات

صُنفت البلدان حسب درجاتها النهائية باستخدام طريقة تصنيف "كثيفة". وتؤدي الدرجات المتساوية إلى نفس المرتبة. ويحصل البلد الذي يلي بلدين أو أكثر من البلدان التي تحتل مرتبة متساوية، على الرقم الترتيبي التالي.

الملحق B: الرقم القياسي العالمي للأمن السيبراني (الطبعة الرابعة)

صاغ أسئلة هذا الاستبيان وراجعها اجتماع فريق المقرر المعني بالمسألة 3/2 لقطاع تنمية الاتصالات: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل تطوير ثقافة الأمن السيبراني. وكان الاجتماع بمثابة قناة لالتماس موافقة الأعضاء على إصدار الطبعة الرابعة من الرقم القياسي العالمي للأمن السيبراني.

ويتألف الاستبيان من خمسة أقسام منفصلة، حيث تكون الإجابة على أسئلة كل الأقسام، باستثناء الإجابات بنعم/لا، مصحوبة بمربعات لوضع علامة عليها. وينبغي استكمال الاستبيان على الإنترنت. وزود كل مستجيب (عن طريق رسالة إلكترونية رسمية من الاتحاد) بعنوان URL فريد ومعلومات تسجيل الدخول لتقديم أجوبته. ويمكن الاستبيان المستجيبين أيضاً من تحميل الوثائق (وعناوين URL) ذات الصلة لكل سؤال كمعلومات داعمة. والمعلومات المقدمة من المستجيبين لهذا الاستبيان يفترض ألا تكون سرية الطابع.

الجدول B1: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير القانونية

1	القانون الموضوعي بشأن الأمن السيبراني الشرح: يشير مصطلح القانون الموضوعي إلى جميع فئات القوانين العامة والخاصة، بما في ذلك قوانين العقود والعقارات والضرر والوصية والقانون الجنائي التي تؤسس الحقوق وتحددها وتنظمها.
1.1	هل لديكم قانون موضوعي بشأن السلوك القانوني على الإنترنت؟ <input type="checkbox"/> نعم <input type="checkbox"/> لا يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق
1.1.1	هل لديكم قوانين موضوعية بشأن النفاذ القانوني إلى الأجهزة وأجهزة الحاسوب والبيانات؟ الشرح: النفاذ - هو القدرة على الاتصال بنظام أو بدلاً من ذلك التفاعل معه ووسيلة هذا الاتصال، من أجل استخدام موارد النظام في تداول المعلومات أو اكتساب معارف من المعلومات المتضمنة في النظام أو التحكم في مكونات النظام ووظائفه (المبادرة الوطنية لوظائف ودراسات الأمن السيبراني)؛ يُقصد "بنظام الحاسوب" أو النظام - جهاز أو مجموعة من الأجهزة الموصولة بينياً أو أي أجهزة ذات صلة والتي يقوم واحداً منها أو أكثر، حسب البرنامج، بالمعالجة الآلية للبيانات (مجلس أوروبا - الاتفاقية بشأن الجريمة السيبرانية) البيانات الحاسوبية - يقصد "بالبيانات الحاسوبية" أي تمثيل لوقائع أو معلومات أو مفاهيم في صورة ملائمة لمعالجتها في نظام حاسوبي، بما في ذلك وضع برنامج مناسب يمكن نظام الحاسوب من أداء وظيفة ما (مجلس أوروبا - الاتفاقية بشأن الجريمة السيبرانية)؛ <input type="checkbox"/> نعم <input type="checkbox"/> لا يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق
2.1.1	هل لديكم قانون موضوعي بشأن التدخلات غير القانونية (عبر إدخال البيانات وتعديلها وإلغائها) على الأجهزة والبيانات والأنظمة الحاسوبية؟ الشرح: التداخل على نظام حاسوبي - تعطيل خطير متعمد وغير مصرح به لوظائف نظام حاسوبي. قد يشمل ذلك إدخال بيانات في الحاسوب أو إرسالها أو تعطيلها أو حذفها أو إتلافها أو تحويلها أو شطبها. التداخل على البيانات - القيام عن عمد وبدون تصريح بتعطيل بيانات حاسوب أو حذفها أو إتلافها أو تحويلها أو شطبها. <input type="checkbox"/> نعم <input type="checkbox"/> لا يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق

الجدول B1: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير القانونية (تابع)

<p>3.1.1 هل لديك قوانين موضوعية بشأن الاعتراض غير القانوني للأجهزة والأنظمة الحاسوبية والبيانات؟ الشرح: الاعتراض غير القانوني - القيام عن عمد وبدون ترخيص بالإرسال غير العمومي لبيانات حاسوبية من أو داخل حاسوب أو نظام إلكتروني آخر، عبر وسائل تقنية.</p> <p><input type="checkbox"/> نعم <input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق</p>
<p>4.1.1 هل لديك قوانين موضوعية بشأن سرقة الهوية والبيانات على الإنترنت؟ الشرح: سرقة الهوية على الإنترنت - سرقة معلومات شخصية، مثل الأسماء أو العناوين أو تاريخ الميلاد أو بيانات الاتصال أو الحسابات المصرفية. وقد يقع هذا الأمر نتيجة الاحتيال والقرصنة على الحسابات الإلكترونية واستخلاص المعلومات من وسائل التواصل الاجتماعي أو النفاذ غير القانوني إلى قواعد البيانات.</p> <p><input type="checkbox"/> نعم <input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق</p>
<p>2.1 هل لديك ترتيبات بشأن أعمال التزوير ذات الصلة بأجهزة الحاسوب (القرصنة/انتهاكات حقوق التأليف والنشر)؟ الشرح: القيام بدون ترخيص بإدخال أو تعديل أو حذف بيانات حاسوبية نتيجة بيانات غير موثوقة بنية اعتبارها أو التصرف فيها لأغراض قانونية كما لو كانت موثوقة لتكريس تصميم احتيالي أو غير سوي.</p> <p><input type="checkbox"/> نعم <input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق</p>
<p>3.1 هل لديك قوانين موضوعية بشأن السلامة على الإنترنت؟ الشرح: السلامة على الخط - تشير إلى تعظيم سلامة الإنترنت من المخاطر الأمنية المختلفة التي تحيق بالمعلومات الخاصة والشخصية والمعلومات المرتبطة بالملكية، فضلاً عن تعزيز الحماية الذاتية للمستخدمين من الجرائم السيبرانية.</p>
<p>1.3.1 هل لديك ترتيبات/تدابير قانونية بشأن الاعتداءات ذات الصلة بالمواد العنصرية التي تحض على كراهية الآخرين؟ الشرح: تدابير لمنع مختلف أشكال الخطاب الذي يحض على الكراهية على الإنترنت وأشكال عدم التسامح الأخرى بسبب العرق أو اللون أو الديانة أو النسب أو الأصل القومي أو الإثني أو التوجه الجنسي أو الهوية الجنسانية أو الإعاقة أو الوضع الاجتماعي أو أي خصائص أخرى.</p> <p><input type="checkbox"/> نعم <input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق</p>
<p>2.3.1 هل لديك ترتيبات/تدابير قانونية بشأن التحرش والإساءة إلى الكرامة/السلامة الشخصية على الإنترنت؟ الشرح: التحرش أو التهيب السيبرانيان - الرسائل المرسلة عبر البريد الإلكتروني أو المراسلة المباشرة أو مواقع الويب المسيئة التي تهدف إلى تهيب فرد أو مجموعة من الأفراد أو التحرش بهم من خلال هجمات ذات طابع شخصي.</p> <p><input type="checkbox"/> نعم <input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق</p>

الجدول B1: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير القانونية (تابع)

3.3.1	<p>لديكم ترتيبات/تدابير قانونية بشأن حماية الأطفال على الإنترنت؟</p> <p>الشرح: القوانين التي توضح أن أي جريمة وكل جريمة ترتكب ضد أي طفل في العالم الحقيقي يمكن أن ترتكب أيضاً على الإنترنت أو أي شبكة إلكترونية أخرى. وقد يكون من الضروري أيضاً وضع قوانين جديدة أو تكييف القوانين القائمة لتجريم بعض أنواع السلوك التي لا يمكن أن تحدث إلا على الإنترنت، مثل إغراء الأطفال عن بُعد بأداء أو مشاهدة أفعال جنسية، أو تجهيز الأطفال لمقابلتهم في العالم الحقيقي لأغراض جنسية. (المبادئ التوجيهية للاتحاد من أجل واضعي السياسات بشأن حماية الأطفال على الإنترنت).</p> <p style="text-align: right;"> <input type="checkbox"/> نعم <input type="checkbox"/> لا </p> <p style="text-align: right;">يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p style="text-align: right;">يرجى تقديم الوثائق</p>
(2)	<p>هل هناك أي لوائح للأمن السيبراني تتعلق بـ...</p> <p>الشرح: اللوائح عبارة عن قواعد يستند إليها أو يقصد بها تنفيذ جزء محدد من التشريعات. تقوم بإنفاذ اللوائح عادةً الهيئات التنظيمية التي تشكل أو يوكل إليها تنفيذ أهداف أو أحكام أي تشريع.</p> <p>ومن هنا، فإن أي لوائح للأمن السيبراني تنطوي على وضع مبادئ تلتزم بها الأطراف المعنية المختلفة، تنشأ وتشكل جزءاً من عملية تنفيذ القوانين التي تتعامل مع حماية البيانات والتبليغ عن الانتهاكات ومتطلبات منح الشهادات/التقييم في مجال الأمن السيبراني وتنفيذ تدابير الأمن السيبراني ومتطلبات مراجعة الأمن السيبراني وحماية الخصوصية وحماية الأطفال على الإنترنت والتوقيعات الرقمية والمعاملات الإلكترونية ومسؤولية موردي خدمات الإنترنت.</p>
1.2	<p>حماية البيانات الشخصية/الخصوصية؟</p> <p>الشرح: لوائح بشأن حماية البيانات الشخصية من كل ما هو غير مرخص به من نفاذ أو تعديل أو تدمير أو استعمال. والخصوصية في الإنترنت هي مستوى الخصوصية والأمن للبيانات الشخصية التي تنشر عبر الإنترنت. وهو مصطلح فضفاض يشير إلى مجموعة متنوعة من العوامل والتقنيات والتكنولوجيات التي تستخدم لحماية البيانات والاتصالات والأفضليات الحساسة والخاصة؛ ومن أمثلة هذه التشريعات قانون حماية البيانات.</p> <p style="text-align: right;"> <input type="checkbox"/> نعم <input type="checkbox"/> لا </p> <p style="text-align: right;">يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p style="text-align: right;">يرجى تقديم الوثائق</p>
2.2	<p>التبليغ عن انتهاكات/حوادث البيانات؟</p> <p>الشرح: قوانين أو لوائح التبليغ عن الانتهاكات هي تلك التي تلزم أي كيان يتعرض لانتهاك ما بإبلاغ السلطات وعملائه والأطراف الأخرى عن الانتهاك واتخاذ خطوات أخرى لعلاج الأضرار الناجمة عن الانتهاك. وتسنّ هذه القوانين استجابة إلى العدد المتصاعد من الانتهاكات لقواعد بيانات المستهلكين التي تتضمن معلومات شخصية يمكن التعرف على هوية أصحابها من خلالها.</p> <p style="text-align: right;"> <input type="checkbox"/> نعم <input type="checkbox"/> لا </p> <p style="text-align: right;">يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p style="text-align: right;">يرجى تقديم الوثائق</p>
3.2	<p>متطلبات مراجعة الأمن السيبراني؟</p> <p>الشرح: تعني مراجعة الأمن التقييم النظامي والدوري لأمن نظام المعلومات. وقد تشمل المراجعة النمطية تقييم زمن التشكيلة المادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين.</p> <p style="text-align: right;"> <input type="checkbox"/> نعم <input type="checkbox"/> لا </p> <p style="text-align: right;">يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p style="text-align: right;">يرجى تقديم الوثائق</p>

الجدول B1: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير القانونية (تابع)

4.2	تنفيذ المعايير؟
<p>الشرح: وجود إطار (أطر) معتمدة من الحكومة (أو تحظى بتأييدها) من أجل تنفيذ معايير الأمن السيبراني المعترف بها دولياً داخل القطاع العام (الوكالات الحكومية) وداخل البنى التحتية الحرجة (حتى ولو كان القطاع الخاص هو من يقوم بتشغيلها). وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تقدم معايير المعلومات المهيكلية (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وفريق التداخل بين الرموز (ISI)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وقوات الأمن الداخلي (ISF)، وRFC، والمعايير الدولية لمراجعة الحسابات (ISA)، واللجنة الكهروتقنية الدولية (IEC)، والمجلس الوطني للبحوث البيئية (NERC)، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، ومعايير معالجة المعلومات الفيدرالية (FIPS)، ومعلومات التحكم بالبروتوكول (PCI)، وخدمة أمن الدفاع (DSS)، وغيرها.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
5.2	تحديد البنى التحتية الوطنية الحرجة للمعلومات وحمايتها؟
<p>الشرح: تضم البنى التحتية الحرجة الأنظمة الأساسية الحاسمة بالنسبة للسلامة والأمن والأمن الاقتصادي والصحة العامة للدولة. وقد تشمل هذه الأنظمة، على سبيل الذكر وليس الحصر، أنظمة الدفاع والشؤون المصرفية والمالية والاتصالات والطاقة وما إلى ذلك.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
<p>يرجى تقديم بعض من أفضل الممارسات/الإنجازات/أوجه التقدم الجارية التي اشترك/يشترك فيها بلدك فيما يتعلق بالمجالات القانونية كجزء من أنشطة الأمن السيبراني.</p> <p>استعمل إطار التعليقات من أجل أي ممارسة/ممارسات تفصيلية مع إضافة روابط كإثبات أو قدم وثيقة/وثائق بما في ذلك روابط كإثبات</p>	

الجدول B2: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التقنية

<p>1 الأفرقة CERT/CSIRT/CIRT الوطنية/الحكومية.</p> <p>الشرح: الأفرقة CERT-CSIRT-CIRT: أفرقة الاستجابة للحوادث الحاسوبية، كيانات تنظيمية مملوثة من الموظفين، تكلف بمسؤولية تنسيق ودعم الاستجابة للحوادث أو الأحداث الأمنية الحاسوبية على الصعيد الوطني أو الحكومي.</p> <p>ملاحظة: يتم التمييز في بعض الأوقات بين أفرقة الاستجابة للحوادث الحاسوبية الوطنية والحكومية ككيانات منفصلة/مختلفة - فأفرقة الاستجابة للحوادث الحاسوبية الحكومية تخدم هيئات حكومية، بينما تخدم أفرقة الاستجابة للحوادث الحاسوبية الوطنية الهيئات الوطنية، بما في ذلك القطاع الخاص والمواطنين. ويشار إليها في بعض الأوقات ككيان واحد.</p>	<p>1.1 هل هناك أفرقة CERT/CSIRT/CIRT وطنية/حكومية؟</p> <p>الشرح: مدعومة بقرار من الحكومة أو تشكل جزءاً من الهياكل الحكومية أو الوطنية.</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
<p>2.1 هل الفريق CERT/CSIRT/CIRT الوطني أو الحكومي لديكم ...</p>	<p>1.2.1 يطور أو ينفذ أنشطة توعية بشأن الأمن السيبراني؟</p> <p>الشرح: جهود تشجيع إطلاق حملات دعائية على نطاق واسع لتوعية الدولة بالسلوك السيبراني الآمن على الخط.</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
<p>2.2.1 إجراء تمارين للأمن السيبراني بانتظام مثل التدريبات السيبرانية؟</p> <p>الشرح: حادث مخطط تقوم خلاله منظمة ما بمحاكاة خلل سيبراني من أجل تطوير أو اختبار إمكانات مثل المنع أو الاكتشاف أو التخفيف من الآثار أو الاستجابة أو الاستعادة فيما يتعلق بحالات الخلل هذه. هل تجري هذا التمارين بصورة دورية أو متكررة؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>	<p>3.2.1 توفير نشرات للجمهور؟</p> <p>الشرح: نشرات الأفرقة CIRT: عرض المعلومات على جمهور العامة بشأن التهديدات السيبرانية الناشئة والإجراءات التي يوصى باتخاذها.</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
<p>4.2.1 المساهمة في قضايا حماية الأطفال على الإنترنت؟</p> <p>الشرح: توفر الأفرقة CERT/CSIRT/CIRT الدعم مثل حملات التوعية والإبلاغ عن الحوادث المتعلقة بالأطفال وتوفير المواد التثقيفية بشأن حماية الأطفال على الإنترنت، وأمور أخرى.</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>	

الجدول B2: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التقنية (تابع)

3.1	هل الأفرقة CIRT المذكورة أعلاه (CERT أو CSIRT) منضمة إلى منتدى أفرقة الأمن والاستجابة للحوادث (FIRST)؟ الشرح: عضوية كاملة أو جهة اتصال بالمنتدى FIRST. www.first.org	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
4.1	هل الأفرقة CIRT المذكورة أعلاه (CERT أو CSIRT) منضمة إلى أي فريق CIRT إقليمي؟ الشرح: أي علاقة رسمية أو غير رسمية مع أي فريق CERT آخر داخل أو خارج البلاد، جزء من أي فريق CERT إقليمي. تشمل أمثلة الأفرقة CERT الإقليمية APCERT وAFRICACERT وEGC وOIC وOAS.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
5.1	هل مستوى اكتمال خدمات الأفرقة CIRT أو CSIRT أو CERT معتمد من برنامج إصدار الشهادات TI طبقاً للمعيار TF-CSIRT-SIM3؟ الشرح: المعيار SIM3 هو الأساس لمنح الشهادات للأفرقة CIRT.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2	الأفرقة CERT/CSIRT/CIRT القطاعية الشرح: الفريق CERT/CSIRT/CIRT القطاعي هو كيان يتعامل مع حوادث الأمن أو الأمن السيبراني الحاسوبية التي تؤثر على قطاع بعينه. وتشكل الأفرقة CERT القطاعية عادةً من أجل القطاعات الحساسة مثل الرعاية الصحية والمرافق العامة والهيئات الأكاديمية وخدمات الطوارئ والقطاع المالي. ويقدم الفريق CERT القطاعي خدماته لهيئات من قطاع وحيد فقط.	
1.2	هل يوجد في بلدكم أفرقة CERT/CSIRT/CIRT قطاعية؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2.2	هل تقوم الأفرقة CERT/CSIRT/CIRT القطاعية لديكم بما يلي:	
1.2.2	تطوير وتنفيذ أنشطة توعية بشأن الأمن السيبراني في القطاع؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2.2.2	تشارك بنشاط في التدريبات السيبرانية الوطنية؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	

الجدول B2: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التقنية (تابع)

3.2.2	عرض معلومات عن الحوادث المتعلقة بالقطاع على الجهات التابعة؟ الشرح: عرض معلومات عن التهديدات السيبرانية الناشئة والإجراءات التي يوصى باتخاذها.
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
(3) الإطار الوطني لتنفيذ معايير الأمن السيبراني	
الشرح: اعتماد إطار (أطر) من أجل تنفيذ معايير الأمن السيبراني المعترف بها دولياً داخل القطاع العام (الوكالات الحكومية) وداخل البنى التحتية الحرجة (حتى ولو كان القطاع الخاص هو من يقوم بتشغيلها). وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تقدم معايير المعلومات المهيكلية (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وفريق التداخل بين الرموز (ISI)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وقوات الأمن الداخلي (ISF)، وRFC، والمعايير الدولية لمراجعة الحسابات (ISA)، واللجنة الكهروتقنية الدولية (IEC)، والمجلس الوطني للبحوث البيئية (NERC)، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، ومعايير معالجة المعلومات الفيدرالية (FIPS)، ومعلومات التحكم بالبروتوكول (PCI)، وخدمة أمن الدفاع (DSS)، وغيرها.	
1.3	هل يوجد إطار لتنفيذ/اعتماد معايير الأمن السيبراني؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
2.3	هل يتضمن الإطار معايير دولية أو أي معايير أخرى ذات صلة؟ الشرح: من قطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) وISO/IEC وNIST وANSI/ISA وغيرهم.
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
(4) حماية الأطفال على الإنترنت	
الشرح: يقيس هذا المؤشر مدى وجود وكالة وطنية مكرسة لحماية الطفل على الخط ومدى تيسر رقم هاتف وطني للإبلاغ عن القضايا المرتبطة بوجود الأطفال على الإنترنت، وأي آليات وقدرات تقنية يتم نشرها للمساعدة في حماية الأطفال على الإنترنت، وأي نشاط تنفذه مؤسسات حكومية أو غير حكومية لتوفير المعارف والدعم لأصحاب المصلحة بشأن كيفية حماية الأطفال على الإنترنت، ومد توفر خط هاتف وعنوان بريد إلكتروني ومواقع ويب وغيرها يمكن للأطراف المعنية أن تستخدمها في الإبلاغ عن الحوادث أو الشواغل ذات الصلة بحماية الأطفال على الإنترنت (COP).	
1.4	هل هناك أي آليات أو قدرات إبلاغ تم نشرها للمساعدة في حماية الأطفال على الإنترنت؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
يرجى تقديم بعض من أفضل الممارسات/الإنجازات/أوجه التقدم الجارية التي اشترك/بشرك فيها بلدك فيما يتعلق بالمجالات التقنية كجزء من أنشطة الأمن السيبراني.	
استعمل إطار التعليقات من أجل أي ممارسة/ممارسات تفصيلية مع إضافة روابط كإثبات أو قدم وثيقة/وثائق بما في ذلك روابط كإثبات	

الجدول B3: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التنظيمية

1	الاستراتيجية الوطنية للأمن السيبراني
<p>الشرح: وضع سياسات للنهوض بالأمن السيبراني كأولوية من الأولويات الوطنية الملحة. وينبغي للاستراتيجية الوطنية للأمن السيبراني أن تنص على الحفاظ على وجود بنى تحتية حرجة للمعلومات تتسم بالقدرة على الصمود والاعتمادية، بما في ذلك أمن وسلامة المواطنين؛ وحماية مواد وأصول الملكية الفكرية الخاصة بالمواطنين والمنظمات والدولة؛ والتعاطي مع الهجمات السيبرانية على البنى التحتية الحرجة ومنعها؛ وتدنية الأضرار والتقليل للحد الأدنى لزممن الاستعادة من الهجمات السيبرانية.</p>	
1.1	هل لدى بلدكم استراتيجية/سياسة وطنية للأمن السيبراني؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
<p>هل تتناول حماية البنى التحتية الوطنية الحرجة للمعلومات، بما ذلك قطاع الاتصالات؟</p> <p>الشرح: أي نظام معلومات مادي أو افتراضي يقوم بالتحكم أو معالجة أو إرسال أو استقبال أو تخزين معلومات إلكترونية في أي صورة كانت، بما في ذلك بيانات أو صوت أو فيديو تعد حيوية في سير عمل أي بنية تحتية حرجة؛ حيوية لدرجة أن عدم قدرة هذه الأنظمة أو إصابتها بالدمار قد تترتب عليه أثار ضارة بالأمن القومي أو الأمن الاقتصادي القومي أو الصحة والسلامة العامة القومية.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
<p>هل تتضمن إشارة إلى الخطة الوطنية للقدرة على الصمود؟</p> <p>الشرح: تضمن الخطة الوطنية للقدرة على الصمود قدرة البلاد على مقاومة واستيعاب التأثيرات الناجمة عن أي أخطار والتكيف معها والتعافي (بما في ذلك الأخطار الطبيعية أو الاصطناعية) في الوقت المناسب وبكفاءة، بما في ذلك من خلال حفظ واستعادة خدماتها ووظائفها الأساسية بالاعتماد على جهة خارجية.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
<p>هل الاستراتيجية الوطنية للأمن السيبراني تنقح وتحدث بشكل مستمر؟</p> <p>الشرح: تُحدد إدارة دورة حياة الاستراتيجية وتحدث الاستراتيجية طبقاً للتطورات الوطنية والتكنولوجية والاجتماعية والاقتصادية والسياسية التي يمكن أن تؤثر على الوضع الوطني للأمن السيبراني.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
<p>هل استراتيجية الأمن السيبراني منفتحة على أي شكل من أشكال التشاور مع خبراء وطنيين يعملون في مجال الأمن السيبراني؟</p> <p>الشرح: تكون الاستراتيجية مفتوحة للتشاور بالنسبة لجميع أصحاب المصلحة المعنيين، بما في ذلك مشغلو البنى التحتية الحرجة وموردو خدمات الإنترنت والهيئات الأكاديمية وما إلى ذلك.</p>	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	

الجدول B3: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التنظيمية (تابع)

2.1	هل توجد خطة عمل/ خارطة طريق محددة لتنفيذ إدارة الأمن السيبراني؟
	الشرح: خطة استراتيجية تحدد النتائج الوطنية للأمن السيبراني بما في ذلك الخطوات والمعالم الرئيسية اللازمة لتنفيذها.
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
3.1	هل توجد استراتيجية وطنية لحماية الأطفال على الإنترنت؟
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
(2)	الوكالة المسؤولة
	الشرح: الوكالة المسؤولة عن تنفيذ الاستراتيجية/السياسية الوطنية للأمن السيبراني يمكن أن تضم لجاناً دائمة أو أفرقة عمل رسمية أو مجالس استشارية أو مراكز متعددة الاختصاصات. وقد يتولى كيان كهذا أيضاً المسؤولية المباشرة للفريق الوطني CIRT الوطني. وقد تكون الوكالة المسؤولة داخل الحكومة أو قد تكون لها سلطة ضم وكالات وهيئات وطنية أخرى لتنفيذ السياسات واعتماد المعايير.
1.2	هل توجد وكالة مسؤولة عن تنسيق الأمن السيبراني على الصعيد الوطني؟
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
1.1.2	هل توجد وكالة وطنية تتولى الإشراف على حماية البنى التحتية الوطنية الحرجة للمعلومات؟
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
2.2	هل توجد وكالة وطنية تتولى الإشراف على تطوير القدرات الوطنية في مجال الأمن السيبراني؟
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
3.2	هل توجد وكالة تتولى الإشراف على مبادرات حماية الأطفال على الإنترنت على الصعيد الوطني؟
	الشرح: وجود وكالة وطنية مخصصة للإشراف على حماية الأطفال على الإنترنت وتعزيزها.
	<input type="checkbox"/> نعم
	<input type="checkbox"/> لا
	يرجى تقديم روابط/ مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
(3)	مقاييس الأمن السيبراني
	الشرح: وجود أي ممارسات تقييم وطنية أو قطاعية معترف بها رسمياً أو يفضل استعمالها في قياس تطور الأمن السيبراني واستراتيجيات تقييم المخاطر ومراجعات الأمن السيبراني وغيرها من الأدوات والأنشطة الخاصة بقياس أو تقييم الأداء الناتج من أجل إجراء تحسينات في المستقبل. على سبيل المثال، طبقاً للمعيار ISO/IEC 27004 المعني بالقياسات المتعلقة بإدارة أمن المعلومات.

الجدول B3: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التنظيمية (تابع)

1.3	هل تجرى أي مراجعات للأمن السيبراني على الصعيد الوطني؟ الشرح: المراجعة الخاصة بالأمن هي تقييم نظامي لأمن أحد أنظمة المعلومات عن طريق قياس إلى أي مدى يلتزم بمجموعة من المعايير المحددة. والمراجعة الكاملة تتولى عادةً تقييم أمن التشكيلة المادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين. وقد تلزم الهيئات التنظيمية البنى التحتية الحرجة التي يديرها القطاع الخاص بإجراء تقييمات دورية للوضع الأمني ورفع تقارير بالنتائج.
	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق
2.3	هل توجد مقاييس لتقييم المخاطر المرتبطة بالفضاء السيبراني على الصعيد الوطني؟ الشرح: عملية تشمل تحديد المخاطر وتحليلها وتقييمها.
	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق
3.3	هل توجد تدابير لتقييم مستوى تطور الأمن السيبراني على الصعيد الوطني؟ الشرح: نهج لقياس مستوى تطور الأمن السيبراني على الصعيد الوطني.
	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق
	يرجى تقديم بعض من أفضل الممارسات/الإنجازات/أوجه التقدم الجارية التي اشترك/بشترك فيها بلدك فيما يتعلق بالتدابير التنظيمية كجزء من أنشطة الأمن السيبراني. استعمل إطار التعليقات من أجل أي ممارسة/ممارسات تفصيلية مع إضافة روابط كإثبات أو قدم وثيقة/وثائق بما في ذلك روابط كإثبات

الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات

(1)	حملات التوعية العامة بالأمن السيبراني الشرح: تشمل التوعية العامة الجهود التي تبذل في سبيل تشجيع وصول حملات التوعية إلى أكبر عدد ممكن من المواطنين والاستفادة من المنظمات غير الحكومية والمؤسسات والمنظمات وموردي خدمات الإنترنت والمكتبات ومنظمات التجارة المحلية والمراكز المجتمعية وكلليات المجتمعات المحلية وبرامج تعليم الكبار والمدارس ومنظمات أولياء الأمور-المعلمين من أجل توصيل الرسالة إلى الجميع بشأن السلوك الآمن من الناحية السيبرانية على الشبكة. ويتضمن ذلك إجراءات من قبيل إنشاء بوابات ومواقع شبكية لإذكاء الوعي، ونشر مواد الدعم وغيرها من الأنشطة الأخرى.
1.1	هل توجد حملات توعية عامة تستهدف قطاع بعينه مثل الشركات الصغيرة والمتوسطة وشركات القطاع الخاص والوكالات الحكومية؟
	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق

الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات (تابع)

2.1	هل توجد حملات توعية عامة تستهدف المجتمع المدني؟ الشرح: المنظمات غير الحكومية، منظمات المجتمعات المحلية.
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
3.1	هل توجد حملات توعية عامة تستهدف المواطنين؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
4.1	هل توجد حملات توعية عامة تستهدف كبار السن؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
5.1	هل توجد حملات توعية عامة تستهدف الأشخاص ذوي الاحتياجات الخاصة؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
6.1	هل توجد حملات توعية عامة تضم أولياء الأمور والمعلمين والأطفال (تتعلق بحماية الأطفال على الإنترنت)؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	
(2) تدريب مهنيي الأمن السيبراني	
الشرح: وجود برامج تدريب مهني خاصة بالقطاعات لزيادة الوعي لدى الجمهور العام (أي تخصيص يوم أو أسبوع أو شهر وطني للتوعية بالأمن السيبراني) وتشجيع تثقيف قوة العمل من مختلف التخصصات (التقنية والعلوم الاجتماعية وغيرها) بالأمن السيبراني وتشجيع منح الشهادات للمهنيين في أي من القطاعين العام أو الخاص.	
ويشمل ذلك أيضاً التدريب على الأمن السيبراني لضباط إنفاذ القوانين والعاملين في المجال التشريعي والقانوني ووضع برامج تدريب مهنية وتقنية يمكن تخصيصها لضباط الشرطة ووكلاء الإنفاذ والقضاة والمدعين العموم ومحامي المحاكم العليا ووكلاء النائب العام والمحامين وقضاة المحاكم العليا وغيرهم من الأشخاص العاملين في مجال القانون وإنفاذه. ويشمل هذا المؤشر أيضاً وجود إطار معتمد (مؤيد) أو أطر معتمدة (مؤيدة) من الحكومة منح الشهادات واعتماد المهنيين من خلال معايير معترف بها دولياً للأمن السيبراني. وتشمل هذه الشهادات وأوراق الاعتماد والمعايير على سبيل الذكر وليس الحصر: معارف أمن الحوسبة السحابية (تحالف أمن الحوسبة السحابية) و CISP و SSCP و CSSLP و CBK والتحليل الجنائي في مجال الأمن السيبراني (ISC ²) وغيرها.	
1.2	هل تطور حكومتك أو تدعم دورات التدريب المهني في مجال الأمن السيبراني؟
الشرح: تشجيع مناهج الأمن السيبراني بين قوة العمل (التقنية والعلوم الاجتماعية وما إلى ذلك، وتشجيع منح الشهادات للمهنيين في أي من القطاعين العام أو الخاص.	
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
يرجى تقديم روابط/مواقع إلكترونية (URL)	
يرجى تقديم الوثائق	

الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات (تابع)

2.2	هل يوجد برنامج اعتماد لمهنيي الأمن السيبراني في بلدكم؟ الشرح: معاهد تعتمد مهنيي الأمن السيبراني أو أي آليات أخرى ذات صلة.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
3.2	هل توجد برامج/دورات تدريب/مناهج تعليمية خاصة بقطاع وطني بعينه من أجل المهنيين العاملين في مجال الأمن السيبراني؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
1.3.2	هل توجد برامج/دورات تدريب/مناهج تعليمية خاصة بقطاع وطني بعينه من أجل العاملين في مجال إنفاذ القانون؟ الشرح: عملية رسمية للأمن السيبراني لتتقيف العاملين في المجال القانوني (ضباط الشرطة ووكالات إنفاذ القانون) بشأن أمن الحاسوب.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2.3.2	هل توجد برامج/دورات تدريب/مناهج تعليمية خاصة بقطاع وطني بعينه من أجل العاملين في مجال القضاء وغيرهم من العاملين في المجال القانوني؟ الشرح: تدريب على الأمن السيبراني أو تدريب تقني يمكن تخصيصه لضباط الشرطة ووكلاء الإنفاذ والقضاة والمدعين العموم ومحامي المحاكم العليا ووكلاء النائب العام والمحامين وقضاة المحاكم العليا وغيرهم من الأشخاص العاملين في مجال القانون وإنفاذه.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
3.3.2	هل توجد برامج/دورات تدريب/مناهج تعليمية خاصة بقطاع وطني بعينه من أجل الشركات الصغيرة والمتوسطة/شركات القطاع الخاص؟ الشرح: دورات تدريب على الممارسات الجيدة/تطوير القدرات بشأن الأمن السيبراني لحماية أعمالهم وما إلى ذلك، من خلال الاستخدام الأمثل للخدمات الإلكترونية.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
4.3.2	هل توجد برامج/دورات تدريب/مناهج تعليمية خاصة بقطاع وطني بعينه من أجل مسؤولي القطاع العام/المسؤولين الحكوميين الآخرين؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	

الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات (تابع)

<p>3) هل تقوم حكومتكم/منظمتكم بوضع أو دعم أي برامج تعليمية أو مناهج أكاديمية في مجال الأمن السيبراني...</p> <p>الشرح: وجود وتشجيع مناهج وبرامج تعليم وطنية لتدريب جيل الشباب على المهارات والمهن المتعلقة بالأمن السيبراني في المدارس والكليات والجامعات ومؤسسات التعلم الأخرى. وتشمل المهن المتعلقة بالأمن السيبراني، على سبيل الذكر وليس الحصر، محلي الشفراء وخبراء الأدلة الجنائية الرقمية والمستجيبين لحالات الحوادث والمعماريين الأمنيين ومختبري الاختراق.</p>	
1.3	<p>في التعليم الأساسي؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
2.3	<p>في التعليم الثانوي؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
3.3	<p>في التعليم العالي؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
<p>4) برامج البحث والتطوير في مجال الأمن السيبراني</p> <p>الشرح: يقىس هذا المؤشر الاستثمار في برامج البحث والتطوير الوطنية في مجال الأمن السيبراني في المؤسسات التي قد تكون تابعة للقطاع العام أو القطاع الخاص أو أكاديمية أو غير حكومية أو دولية. ويتناول أيضاً وجود هيئة مؤسسية معترف بها على الصعيد الوطني للإشراف على البرامج. وتشمل برامج البحث الخاصة بالأمن السيبراني، على سبيل الذكر وليس الحصر، تحليل البرمجيات الضارة والأبحاث في مجال التشفير والبحث في مواطن ضعف الأنظمة ونماذج ومفاهيم الأمن. وتشير برامج التطوير الخاصة بالأمن السيبراني إلى تطوير حلول خاصة بالعتاد أو البرمجيات تشمل، على سبيل الذكر وليس الحصر، جدران الحماية وأنظمة منع الاقتحام ومضادات البرمجيات الروبوتية والوحدات النمطية لأمن العتاد. يلزم وجود هيئة وطنية حاکمة لزيادة التنسيق بين مختلف المؤسسات وتقاسم الموارد.</p>	
1.4	<p>هل توجد أنشطة بحث وتطوير في مجال الأمن السيبراني على الصعيد الوطني؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
1.1.4	<p>هل توجد برامج بحث وتطوير في مجال الأمن السيبراني للقطاع الخاص؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>
2.1.4	<p>هل توجد برامج بحث وتطوير في مجال الأمن السيبراني للقطاع العام؟</p> <p><input type="checkbox"/> نعم</p> <p><input type="checkbox"/> لا</p> <p>يرجى تقديم روابط/مواقع إلكترونية (URL)</p> <p>يرجى تقديم الوثائق</p>

الجدول B4: استبيان الرقم القياسي العالمي للأمن السيبراني: تدابير تنمية القدرات (تابع)

3.1.4	هل تشارك مؤسسات التعليم العالي، مثل الهيئات الأكاديمية والجامعات في أعمال البحث والتطوير؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
	يرجى تقديم روابط/مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
(5)	الصناعة الوطنية للأمن السيبراني
	الشرح: من شأن وجود بيئة اقتصادية وسياسية واجتماعية مؤاتية تدعم تطوير الأمن السيبراني أن يحفز نمو قطاع خاص حول الأمن السيبراني. ووجود حملات للتوعية العامة وتطوير لقوة العمل وبناء للقدرات وحوافز حكومية من شأنه أن يدفع بظهور سوق لمنتجات وخدمات الأمن السيبراني. ووجود صناعة داخلية للأمن السيبراني يعد شاهداً على هذه البيئة المؤاتية ويدفع بنمو المشاريع المبتدئة في مجال الأمن السيبراني وأسواق التأمين السيبراني المرتبطة بها.
1.5	هل توجد صناعة وطنية للأمن السيبراني؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
	يرجى تقديم روابط/مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
(6)	هل توجد أي آليات تحفيز حكومية ...
	الشرح: يبحث هذا المؤشر أي جهود تحفيزية تبذلها الحكومة لتشجيع تنمية القدرات في مجال الأمن السيبراني، سواء من خلال الإعفاءات الضريبية وتقديم المنح والاعتمادات والقروض وتدابير المرافق وغيرها من الحوافز الاقتصادية والمالية، بما في ذلك تخصيص هيئة مؤسسية معترف بها وطنياً للإشراف على أنشطة تنمية القدرات في مجال الأمن السيبراني. وتزيد الحوافز من الطلب على الخدمات والمنتجات المتعلقة بالأمن السيبراني، مما يحسن من القدرات الدفاعية في مواجهة التهديدات السيبرانية.
1.6	من أجل تشجيع تطوير القدرات في مجال الأمن السيبراني؟
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
	يرجى تقديم روابط/مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
2.6	من أجل تطوير صناعة للأمن السيبراني؟
	الشرح: دعم المشاريع المبتدئة في مجال خدمات الأمن السيبراني في الهيئات الأكاديمية وغيرها
<input type="checkbox"/>	نعم
<input type="checkbox"/>	لا
	يرجى تقديم روابط/مواقع إلكترونية (URL)
	يرجى تقديم الوثائق
	يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بتدابير تنمية القدرات كجزء من أنشطة الأمن السيبراني.
	استعمل إطار التعليقات من أجل أي ممارسة/ممارسات تفصيلية مع إضافة روابط كإثبات أو قدم وثيقة/وثائق بما في ذلك روابط كإثبات

الجدول B5: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التعاونية

(1)	الاتفاقات الثنائية بشأن التعاون في مجال الأمن السيبراني مع بلدان أخرى
	الشرح: تشير الاتفاقات الثنائية (اتفاقات بين طرفين) إلى أي شركات وطنية أو قطاعية معترف بها رسمياً لتبادل معلومات الأمن السيبراني أو أصوله عبر الحدود بين الحكومة وحكومة أجنبية أخرى أو كيان إقليمي أو منظمة دولية (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيا والموارد الأخرى). يقاس المؤشر أيضاً مدى تبادل المعلومات المتعلقة بالتهديدات. ويشير مصطلح تنمية القدرات إلى تبادل الأدوات المهنية وزيادة إشراك الخبراء وغير ذلك.

الجدول B5: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التعاونية (تابع)

1.1	هل لديكم اتفاقات ثنائية بشأن التعاون في مجال الأمن السيبراني مع بلدان أخرى؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق
	هل تبادل المعلومات جزء من الاتفاق (الاتفاقات)؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	الشرح: يشير تبادل المعلومات إلى الممارسات التي تدور حول تبادل المعلومات غير الحساسة.		
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق
	هل تنمية القدرات جزء من الاتفاق (الاتفاقات)؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	الشرح: القدرة على تشجيع الدورات التدريبية الرامية إلى تعزيز المهارات والكفاءات والقدرات للمهنيين الوطنيين العاملين في مجال الأمن السيبراني من خلال التعاون لضمان بذل كل الجهود الجماعية لمواجهة التهديدات السيبرانية.		
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق
	هل المساعدة القانونية المتبادلة جزء من الاتفاق (الاتفاقات)؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	الشرح: مساعدة متبادلة بين بلدين أو أكثر بغرض جمع وتبادل المعلومات سعياً إلى إنفاذ القانونين العام أو الجنائي.		
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق
2	مشاركة الحكومة في الآليات الدولية المتعلقة بأنشطة الأمن السيبراني		
	الشرح: قد تشمل أيضاً التصديق على اتفاقات دولية بخصوص الأمن السيبراني، مثل اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية واتفاقية بودابست بشأن الجريمة السيبرانية وغيرها.		
1.2	هل تشارك حكومتك/منظمتك في آليات دولية متعلقة بأنشطة الأمن السيبراني؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق
3	اتفاقات متعددة الأطراف في مجال الأمن السيبراني		
	الشرح: تشير الاتفاقات متعددة الأطراف (اتفاقات بين طرف وأطراف متعددة) إلى أي برامج وطنية أو قطاعية معترف بها رسمياً من أجل تبادل معلومات أو أصول الأمن السيبراني عبر الحدود بين الحكومة وحكومات أجنبية أو منظمات دولية متعددة (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيا والموارد الأخرى).		
1.3	هل لدى حكومتك اتفاقات متعددة الأطراف بشأن التعاون في مجال الأمن السيبراني؟	<input type="checkbox"/> نعم	<input type="checkbox"/> لا
	يرجى تقديم روابط /مواقع إلكترونية (URL)		يرجى تقديم الوثائق

الجدول B5: استبيان الرقم القياسي العالمي للأمن السيبراني: التدابير التعاونية (تابع)

1.1.3	هل تبادل المعلومات جزء من الاتفاق (الاتفاقات)؟ الشرح: يشير تبادل المعلومات إلى الممارسات التي تدور حول تبادل المعلومات غير الحساسة.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2.1.3	هل تنمية القدرات جزء من الاتفاق (الاتفاقات)؟ الشرح: القدرة على تشجيع الدورات التدريبية الرامية إلى تعزيز المهارات والكفاءات والقدرات للمهنيين الوطنيين العاملين في مجال الأمن السيبراني من خلال التعاون لضمان بذل كل الجهود الجماعية لمواجهة التهديدات السيبرانية.	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
(4)	الشراكات بين القطاعين العام والخاص (PPP) الشرح: يشير مصطلح الشراكات بين القطاعين العام والخاص (PPP) إلى مشاريع مشتركة بين القطاعين العام والخاص. ويمكن قياس مؤشر الأداء هذا من خلال عدد الشراكات الوطنية أو القطاعية المعترف بها رسمياً بين القطاعين العام والخاص لتبادل معلومات الأمن السيبراني وأصوله (الأشخاص والعمليات والأدوات) بين القطاعين العام والخاص (أي الشراكات الرسمية للتعاون أو تبادل المعلومات و/أو الخبرات و/أو التكنولوجيا و/أو الموارد)، وطنياً أو دولياً.	
1.4	هل تشارك حكومتك في شراكات بين القطاعين العام والخاص مع شركات منشأة محلياً؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
2.4	هل تشارك حكومتك في شراكات بين القطاعين العام والخاص مع شركات مملوكة لجهات أجنبية في بلدكم؟	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
(5)	شراكات بين الوكالات الشرح: يشير مؤشر الأداء هذا إلى أي شراكات رسمية بين الوكالات الحكومية المختلفة داخل دولة وطنية (لا يشير إلى الشراكات الدولية). ويمكن أن يشير إلى الشراكات بشأن تبادل المعلومات أو الأصول بين الوزارات والدوائر والبرامج ومؤسسات القطاع العام الأخرى.	
1.5	هل توجد شراكات/اتفاقات بين الوكالات فيما بين الهيئات الحكومية المختلفة تتعلق بالأمن السيبراني؟ الشرح: التعاون بين الوزارات أو الوكالات المختصة	<input type="checkbox"/> نعم <input type="checkbox"/> لا
	يرجى تقديم روابط/مواقع إلكترونية (URL) يرجى تقديم الوثائق	
	يرجى تقديم بعض من أفضل الممارسات/الإنجازات/أوجه التقدم الجارية التي اشترك/يشترك فيها بلدك فيما يتعلق بالتدابير التعاونية كجزء من أنشطة الأمن السيبراني. استعمل إطار التعليقات من أجل أي ممارسة/ممارسات تفصيلية مع إضافة روابط كإثبات أو قدم وثيقة/وثائق بما في ذلك روابط كإثبات	

مكتب نائب المدير ودائرة تنسيق العمليات الميدانية
للحضور الإقليمي (DDR)

الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المدير

Place des Nations
CH-1211 Geneva 20
Switzerland
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Place des Nations
CH-1211 Geneva 20
Switzerland
Email: bdttdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

دائرة الشراكات من أجل التنمية
الرقمية (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

دائرة محور المعارف الرقمية (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

دائرة الشبكات الرقمية والمجتمع الرقمي
(DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

زيمبابوي
مكتب المنطقة للاتحاد

TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare - Zimbabwe
Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

السنغال
مكتب المنطقة للاتحاد

8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar - Yoff - Senegal
Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

الكاميرون
مكتب المنطقة للاتحاد

Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé - Cameroon
Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

إفريقيا
إثيوبيا
المكتب الإقليمي للاتحاد

Gambia Road
Leghar Ethio Telecom Bldg, 3rd floor
P.O. Box 60 005
Addis Ababa - Ethiopia
Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

هندوراس
مكتب المنطقة للاتحاد

Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cia
Apartado Postal 976
Tegucigalpa - Honduras
Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

شيلي
مكتب المنطقة للاتحاد

Merced 753, Piso 4
Santiago de Chile
Chile
Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

بربادوس
مكتب المنطقة للاتحاد

United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown - Barbados
Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

البرازيل
المكتب الإقليمي للاتحاد

SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia - DF - Brazil
Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

كومونولث الدول المستقلة
الاتحاد الروسي
المكتب الإقليمي للاتحاد

4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itumoscow@itu.int
Tel.: +7 495 926 6070

إندونيسيا
مكتب المنطقة للاتحاد

Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 - Indonesia
Email: itu-ro-asiapacific@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

آسيا - المحيط الهادئ
تايلاند
المكتب الإقليمي للاتحاد

4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi - Bangkok 10210 - Thailand
Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 - 8
+66 2 575 0055

الدول العربية
مصر
المكتب الإقليمي للاتحاد

Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt
Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

أوروبا
سويسرا

الاتحاد الدولي للاتصالات (ITU)
مكتب أوروبا (EUR)

Place des Nations
CH-1211 Geneva 20 - Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

الاتحاد الدولي للاتصالات

Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-33926-5



نُشرت في سويسرا

2022، جنيف،

إصدار الصور: Shutterstock