Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
رؤى أمنية

رؤية أمنية في مؤشر الأمن السيبراني العالمي 2020

Security Vision in the Global Cybersecurity Index 2020

الرسائل الأساسية:

- شَهِدَ مؤشرُ الأمن السيبراني 2020 تقدُّمًا ملحوظًا للدول العربية، وخصوصًا المملكة العربية السعودية والإمارات العربية المتحدة على حساب عدد من دول العالم المتقدم في مجال التكنولوجيا، مثل: اليابان والهند.
- تتميز معظم الدول العربية في تطبيق التدابير القانونية أو التنظيمية أو تدابير تنمية القدرات، سواء أكان ذلك بصورة منفردة أم بالجمع بينها، كما أن معظمها في انتظار تطوير التدابير الفنية للحفاظ على الأمن السيبراني بصورة أكبر.
- معظم الدول العربية قد قطعت شوطًا جيدًا تجاه صياغة تشريعات لحماية البيانات، وخصوصًا في ظل تحدي انتشار الجرائم الإلكترونية.
- نسبة كبيرة من الدول التي تمتلك إستراتيجية وطنية للأمن السيبراني لا تُجري تقييمات دورية لتلك الإستراتيجيات، فمن بين 98 دولة لديها إستراتيجية وطنية للأمن السيبراني، هناك 60 دولة فقط تُجري تقييمات دورية لتحديث إستراتيجيتها من بينها 6 دول عربية فقط.

المقدمة

يُعَدّ مؤشر الأمن السيبراني العالمي 2020، الصادر عن الاتحاد الدولي للاتصالات (ITU) في عام 2023، رؤيةً أمنيةً استشرافيةً لحالة الأمن السيبراني العالمي؛ حيث يهدف التقرير إلى فهم التزامات الدول الأعضاء في الاتحاد تجاه الأمن السيبراني بشكل أفضل، وتحديد الثغرات، وتشجيع دمج الممارسات الجيدة، فضلًا عن تقديم رؤى مفيدة للبلدان لتحسين أوضاع الأمن السيبراني لديها، وذلك من خلال استطلاع رأي تم تعميمه على الدول الأعضاء يضم 82 سؤالًا حول التزامات الدول بشأن الأمن السيبراني.

وينقسم المؤشر إلى 4 فصول؛ أولها يتناول خلفية وسياق مؤشر الأمن السيبراني، الذي يُبَيِّن التغيير الواضح في نتائج المؤشر منذ نشأته عام 2015 وحتى الآن؛ حيث أدت الثورة التكنولوجية الهائلة التي

يمر بها العالم إلى حدوث تغييرات جذرية في نتائج المؤشر، كما يتناول الفصل الثاني الركائز الخمس الرئيسة التي شملتها استطلاعات الرأي التي اعتمد عليها المؤشر، ويتناول الفصل الثالث أبرز نتائج المؤشر وترتيب الدول التي شملها المؤشر على المستويين العالمي والإقليمي، وأخيرًا يدرس الفصل الرابع حالة كل دولة وفقًا لنتائج المؤشر، كما يضع المؤشر رؤية مستقبلية لتحسين استجابة الدول لتهديدات الأمن السيبراني المختلفة، فضلًا عن وضع مجموعة من التوصيات للدول التي شملها المؤشر للاستفادة من مزاياها التنافسية وتعزيز أمنها السيبراني.

الشكل رقم 1 - الركائز الأساسية للأمن السيبراني

وبشكل عام، يُشير المؤشِّر إلى أن جائحة كورونا كان لها تأثير واضح على الأمن السيبراني العالمي؛ حيث إنه مع انتشار الوباء في إبريل 2020 ارتفعت نسبة مستخدمي الإنترنت بنسبة 30% عن الفترة السابقة للجائحة، وهو الأمر الذي أظهر للعالم أهمية الأمن السيبراني في ضوء المخاطر التي ظهرت في تلك الفترة؛ لذا يُعد مؤشر الأمن السيبراني نقطة انطلاق مهمة لفهم تأثير الجائحة على جهود الأمن السيبراني العالمية، ويوضِّح الشكل رقم (1) المحاور الرئيسة التي اعتمدت عليها نتائج المؤشر.

الدول الـ 10 الأولى عالميًّا وفقًا لنتائج المؤشر

وفقًا لنتائج المؤشر، تحتل الولايات المتحدة الأمريكية المرتبة الأولى عالميًّا في مؤشر الأمن السيبراني، وكما يتضح من الجدول رقم (1) فهناك دولتان عربيتان ضمن الدول العشر الأولى عالميًّا في مؤشر الأمن السيبراني، وهما: المملكة العربية السعودية (تحتل المرتبة الثانية عالميًّا)، والإمارات العربية المتحدة (تحتل

المرتبة الخامسة عالميًا)، وهو ما يدل على تفوق تلك الدولتين في المؤشر على عدد من الدول المتقدمة الأخرى في مجال التكنولوجيا، مثل: اليابان (تحتل المرتبة السابعة عالميًا)، والهند (تحتل المرتبة العاشرة عالميًا).

الجدول رقم 1 - الدول العشر الأولى وفقًا لنتائج مؤشر الأمن السيبراني

الترتيب	قيمة المؤشر	الدولة
1	100	الولايات المتحدة الأمريكية
2	99.54	المملكة المتحدة
2	99.54	المملكة العربية السعودية
3	99.48	إستونيا
4	98.52	كوريا الجنوبية
4	98.52	سنغافورة
4	98.52	إسبانيا
5	98.06	روسيا
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

Source: (The International Telecommunication Union, 2023).

ترتيب الدول العربية وفقًا لنتائج المؤشر

وبالنسبة للدول العربية، وكما يتضح من الجدول رقم (2) فقد جاءت المملكة العربية السعودية في المرتبة الأولى، تلتها الإمارات العربية المتحدة في المرتبة الثانية، ثم سلطنة عمان في المرتبة الثالثة، وجمهورية مصر العربية في المرتبة الرابعة، ثم قطر في المرتبة الخامسة، وبالنظر إلى نقاط القوة الحالية نجد أن معظم الدول العربية تتميز في تطبيق التدابير القانونية أو التنظيمية أو تدابير تنمية القدرات، سواء أكان ذلك بصورة منفردة أم بالجمع بينها، كما أن معظمها في انتظار تطوير التدابير الفنية للحفاظ على الأمن السيبراني بصورة أكبر.

الجدول رقم 2 - ترتيب الدول العربية في مؤشر الأمن السيبراني 2020

الدولة	قيمة المؤشر	الترتيب العالمي	نقاط القوة الحالية	نقاط القوة المحتملة
المملكة العربية السعودية	99.54	2	التدابير القانونية، والتنظيمية، وتنمية القدرات	التدابير الفنية
الإمارات العربية المتحدة	98.06	5	التدابير الفنية، والتعاونية، وتنمية القدرات	التدابير التنظيمية
سلطة عمان	96.04	21	التدابير القانونية، والتنظيمية، وتنمية القدرات	التدابير الفنية
جمهورية مصر العربية	95.48	23	التدابير القانونية والتنظيمية	التدابير الفنية
قطر	94.5	27	التدابير القانونية، وتنمية القدرات	التدابير الفنية
تونس	86.23	45	التدابير القانونية والفنية	التدابير التنظيمية
المملكة المغربية	82.41	50	التدابير القانونية والتعاونية	التدابير التنظيمية
البحرين	77.86	60	التدابير القانونية	التدابير الفنية
الكويت	75.07	65	التدابير القانونية	التدابير التنظيمية
الأردن	70.96	71	التدابير القانونية	التدابير الفنية
السودان	35.03	102	التدابير الفنية	التدابير التعاونية
الجزائر	33.95	104	التدابير القانونية	التدابير التنظيمية
لبنان	30.44	109	التدابير القانونية	التدابير التعاونية
ليبيا	28.78	113	التدابير الفنية، والتعاونية	التدابير القانونية، والتنظيمية
فلسطين	25.18	122	التدابير الفنية	التدابير التعاونية
سوريا	22.14	126	التدابير القانونية	وتنمية القدرات، والتدابير التعاونية
العراق	20.71	129	التدابير التنظيمية	التدابير القانونية
موريتانيا	18.94	133	التدابير القانونية	التدابير الفنية، والتعاونية، وتنمية القدرات

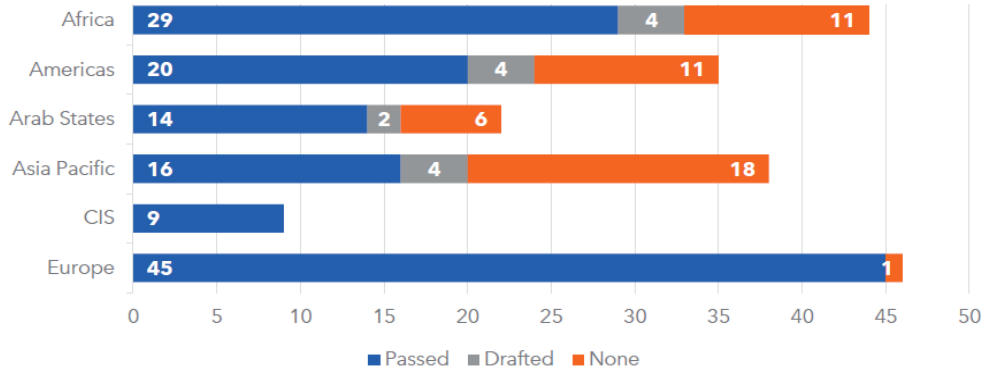
الدولة	قيمة المؤشر	الترتيب العالمي	نقاط القوة الحالية	نقاط القوة المحتملة
الصومال	17.25	137	التدابير التنظيمية والتعاونية	التدابير القانونية
جزر القمر	3.72	175	التدابير التعاونية	التدابير القانونية، والفنية، وتنمية وبناء القدرات
جيبوتي	1.73	179	التدابير القانونية	التدابير الفنية، والتنظيمية، والتعاونية، وتنمية القدرات
اليمن	0	182	-	-

Source: (The International Telecommunication Union, 2023).

نتائج المؤشر فيما يتعلَّق بالركائز الأساسية للأمن السيبراني

أولًا: التدابير القانونية Legal Measures:

أوضح المؤشر أن هناك العديد من دول العالم لديها بالفعل تشريعات لحماية البيانات، وضمان الخصوصية؛ حيث تمتلك 133 دولةً لوائح وقوانين لحماية البيانات، من بينها 14 دولة عربية، وهو ما يدل على أن معظم الدول العربية قد قطعت شوطًا جيدًا تجاه صياغة تشريعات لحماية البيانات، وخصوصًا في ظل تحدي انتشار الجرائم الإلكترونية، كما هو موضح في الشكل رقم (2).



Source: ITU

Source: (The International Telecommunication Union, 2023).

الشكل رقم 2 - عدد الدول التي لديها تشريعات خاصة بحماية البيانات

وفيما يتعلَّق بالتشريعات الخاصة بالحماية من الاختراقات وحوادث سرقة البيانات، هناك 12 دولة عربية لديها تشريعات سارية في هذا الشأن، في حين لا تمتلك 10 دول عربية هذا النوع من التشريعات حتى الآن.

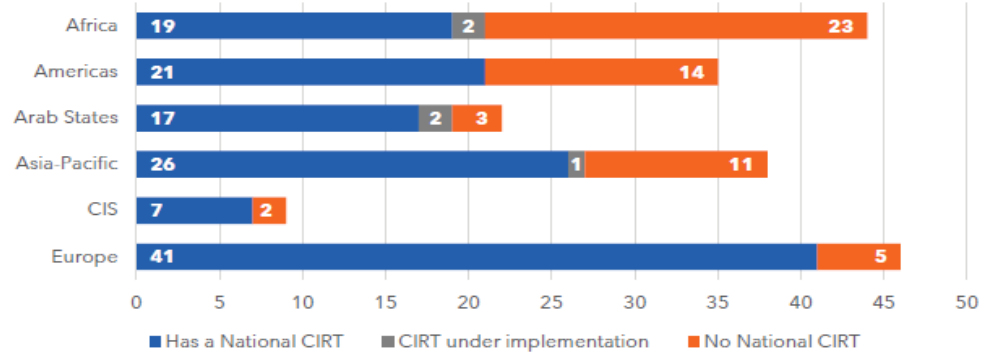
ووفقًا للمؤشر، فإنه على الرغم من أن هناك العديد من الدول التي لديها إجراءات تشريعية لمواجهة النشاط غير القانوني عبر الإنترنت، فإن تلك التشريعات لا تولي الاهتمام الكافي لحماية الهوية عبر الإنترنت وكذلك حماية البيانات من السرقة؛ حيث إن هناك 97 دولة على مستوى العالم تمتلك تشريعات تتعلَّق بسرقة البيانات الشخصية، في حين أن هناك 80 دولة لا تمتلك مثل تلك التشريعات على الإطلاق.

وبالنسبة للدول العربية، هناك 17 دولة لديها تشريعات بخصوص الوصول غير المشروع للبيانات، في حين أن هناك 5 دول فقط لا تمتلك مثل تلك التشريعات.

ويقيس المؤشر السلوك المعادي للمجتمع عبر الإنترنت، من خلال دراسته لكل من المضايقات والعنصرية والكراهية للأجانب عبر الإنترنت؛ حيث أن هناك 100 دولة تمتلك تشريعات لمواجهة هذا النوع من المضايقات من بينها 11 دولة عربية.

ثانيًا: التدابير الفنية Technical Measures:

وفقًا للمؤشر، فإنه بنهاية عام 2020 تَمَكَّنَت 131 دولة حول العالم من تشكيل فِرَقٍ وطنيةٍ للاستجابة للحوادث السيبرانية (CIRTs)، وتحظى أوروبا بالنصيب الأكبر في عدد فِرَقِ الاستجابة للحوادث السيبرانية بإجمالي 41 دولة، وكان نصيب الوطن العربي 17 دولة لديها فِرَقٌ موجودة بالفعل ودولتين لديهما فِرَقُ استجابةٍ تحت الإنشاء، وهو ما يتضح في الشكل رقم (3).



Source: ITU

Source: (The International Telecommunication Union, 2023).

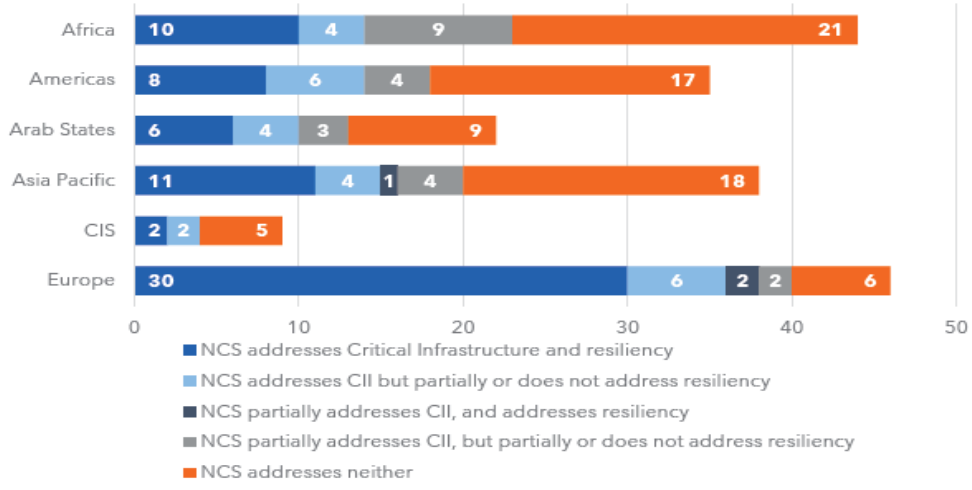
الشكل رقم 3 - عدد الدول التي تمتلك فِرَق استجابة وطنية للحوادث السيبرانية

هذا، وقد أوضح المؤشر أنه على الرغم من امتلاك العديد من دول العالم لِفِرَقِ استجابة للحوادث السيبرانية، فإن معظمها لا يمتلك فِرَق استجابة متخصصة في قطاعات معينة، ففي المنطقة العربية هناك 10 دول فقط تمتلك فِرَقَ استجابةٍ مختصةٍ بقطاع مُعين، مقابل 12 دولة لا تمتلك أيّ فرق استجابة قطاعية.

ثالثًا: التدابير التنظيمية Organizational Measures:

وفقًا للمؤشر، فهناك 127 دولةً لديها إستراتيجية وطنية للأمن السيبراني، ومع ذلك فقد أظهرت 60 دولة فقط تقدُّمًا في وضع أهداف واضحة من خلال مراجعة وتطوير الإستراتيجية أو تحديث خطة عملها.

ومن بين التدابير التنظيمية أيضًا جهود حماية البنية التحتية الحيوية في مواجهة مخاطر الأمن السيبراني، وعلى الرغم من أهميتها، فإن العديد من البلدان لا تتناولها ضمن إستراتيجيتها للأمن السيبراني، فوفقًا للشكل رقم (4) هناك 6 دول عربية تتناول البنية التحتية الحيوية والمرونة في إستراتيجية الأمن السيبراني، و4 دول تتناول البنية التحتية الحيوية ولكنها تتناول المرونة بشكل جزئي، و3 دول تتناول البنية التحتية الحيوية بشكل جزئي ولكنها لا تشتمل على المرونة، مقابل 9 دول لا تتناول أيٍّ من البنية التحتية ولا المرونة.



Source: ITU

Source: (The International Telecommunication Union, 2023).

الشكل رقم 4 - الدول التي تتناول البنية التحتية الحيوية والمرونة في إستراتيجية الأمن السيبراني

وفي هذا السياق، أشار التقرير إلى أن أكثر من نصف دول العالم الأقل نموًّا لا تمتلك فِرَقَ استجابةٍ لحوادث الإنترنت، و60% منها لا تمتلك أو لم تبدأ في عملية تطوير إستراتيجية وطنية للأمن السيبراني، وبالتالي، فإن وجود إستراتيجية وطنية للأمن السيبراني هو خطوة أولى إيجابية لموقف الأمن السيبراني في الدولة، مع ضرورة إجراء تحديثات ومراجعات منتظمة، فمن بين 98 دولة لديها إستراتيجية وطنية للأمن السيبراني، هناك 60 دولة فقط تُجري تقييمات دورية لتحديث إستراتيجيتها من بينها 6 دول عربية فقط.

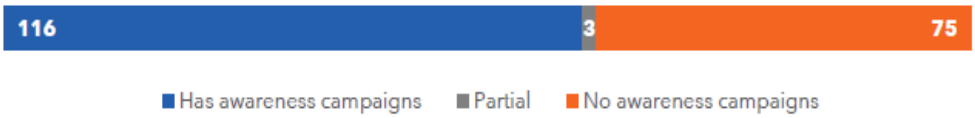
ووفقًا للتقرير، من بين الدول التي تُجري تقييمات دورية للإستراتيجية الوطنية للأمن السيبراني، هناك 88 دولة على مستوى العالم من بينها 9 دول عربية فقط تقوم بعمليات تدقيق وتحديث على المستوى المحلي للإستراتيجية.

وبالتالي، فمعظم دول العالم لا تمتلك مقاييس محلية لتقييم المخاطر المرتبطة بالفضاء السيبراني؛ حيث أن 75 دولة فقط على مستوى العالم تمتلك مقاييس محلية لمواجهة مخاطر الأمن السيبراني من بينها 9 دول عربية، وهو ما قد يزيد من صعوبة تقييم المخاطر الحالية وتحديد أولويات التدخل للحفاظ على الأمن السيبراني.

رابعًا: تدابير تنمية القدرات Capacity development measures:

هناك حاجة ماسّة إلى تنمية قدرات الأمن السيبراني في دول العالم وبالأخص الدول الأقل نموًّا، وذلك من خلال الخطوات التالية:

1. زيادة الوعي العام بالأمن السيبراني بما يجعل المواطنين والشركات والحكومات مستعدين لمواجهة المخاطر السيبرانية التي قد تظهر فيما بعد.
2. تقديم حملات توعية مخصصة لذوي الاحتياجات الخاصة وكبار السن؛ حيث إنه وفقًا لتقديرات عام 2021، فإن 18% فقط من دول العالم توفر حملات توعية بمخاطر الأمن السيبراني لتلك الفئة من المجتمع.
3. التركيز في حملات التوعية على الشركات الصغيرة والمتوسطة؛ حيث يوضِّح الشكل رقم (5) أن 60% من دول العالم لديها حملات توعية بمخاطر الأمن السيبراني موجهة للشركات الصغيرة والمتوسطة.



Source: (The International Telecommunication Union, 2023).

الشكل رقم 5 - عدد الدول التي تمتلك حملات توعية بمخاطر الأمن السيبراني تستهدف كل من الشركات الصغيرة والمتوسطة، والقطاع الخاص، والمؤسسات الحكومية

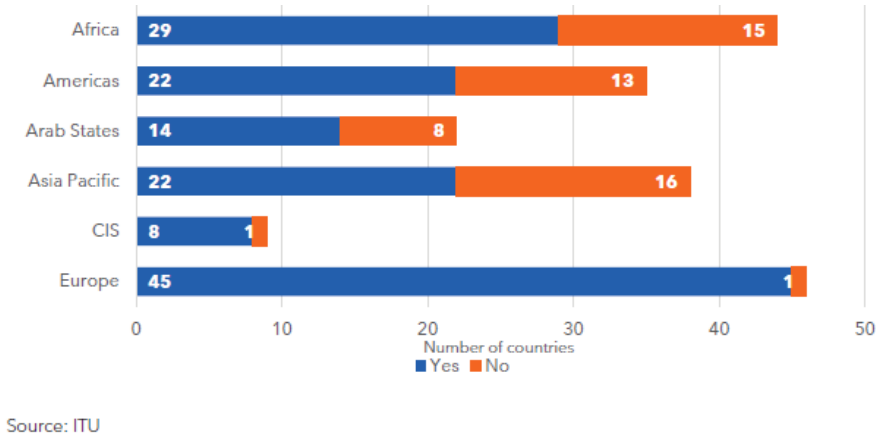
4. الحاجة إلى توفير برامج تعليمية لتدريب متخصصين في مجال الأمن السيبراني، وخصوصًا أن هناك 46% فقط من دول العالم لديها برامج تدريبية مخصصة لمجال الأمن السيبراني.
5. انتشار دورات الأمن السيبراني للتعليم الابتدائي والثانوي؛ حيث ارتفع عدد الدول التي توفر تلك الدورات للمرحلة الابتدائية من 46 دولة إلى 55 دولة خلال عامي 2018 و2020، كما ارتفع عدد الدول التي تُقَدِّم تلك الدورات إلى المرحلة الثانوية من 54 إلى 67 خلال الفترة نفسها.
6. الحاجة إلى زيادة الحوافز الحكومية لتطوير الأمن السيبراني؛ حيث أن هناك 124 دولة حول العالم لم تُقَدِّم أي حوافز للأمن السيبراني، من بينهم 13 دولة عربية.

خامسًا: التدابير التعاونية Cooperative measures:

يُعَدُّ التعاونُ بين الدول هو الأداة الرئيسة لمواجهة مخاطر الأمن السيبراني المتزايدة، وخصوصًا أنها مخاطر عابرة للحدود الوطنية، الأمر الذي يستدعي تنسيق الحد الأدنى من تدابير الأمن، وتبادل المعلومات والممارسات الجيدة، وتدوين قواعد السلوك، وذلك من خلال الآتي:

1. **الاتفاقات الثنائية والمتعددة الأطراف**، هناك 90 دولة فقط لديها اتفاقيات ثنائية في مجال الأمن السيبراني، من بينها 11 دولة عربية وفقا للتقرير.

   ووفقًا لنتائج المؤشر، فمن المرجَّح أن يكون لدى الدول اتفاقيات متعددة الأطراف بصورة أكبر من الاتفاقيات الثنائية؛ حيث أن هناك ما يزيد على 57% من الدول التي وَقَّعَت على اتفاقية متعددة الأطراف من بينها 12 دولة عربية.
2. **المشاركة في الأنشطة الدولية**، فوفقًا لنتائج المؤشر، شاركت 140 دولة في أنشطة دولية، مثل: مؤتمرات الأمن السيبراني، وورش العمل، والشراكات، والاتفاقيات مع دول أخرى، من بينها 14 دولة عربية، كما يتضِّح في الشكل رقم (6).



Source: (The International Telecommunication Union, 2023).

الشكل رقم 6 - الدول المشاركة في الأنشطة الدولية وفقًا للإقليم

3. **الشراكة بين القطاعين العام والخاص**، فوفقًا للمؤشر هناك 86 دولة منخرطة أو ستنخرط قريبًا في شراكة بين القطاعين العام والخاص، سواء أكان ذلك على المستوى المحلي أم الدولي، وهو ما يتضح في الجدول رقم (3).

الجدول رقم 3 - عدد الدول المشاركة في شراكات محلية أو دولية بين القطاعين العام والخاص

	International PPP	International PPP in progress	No international PPP
Domestic PPP	62	0	14
Domestic PPP in progress	1	0	0
No domestic PPP	12	1	104

Source: (The International Telecommunication Union, 2023).

الخاتمة:

بناءً على ما سبق، أوضح المؤشر أنه بحلول عام 2030، فمن المتوقَّع أن يكون 90% من سكان العالم متصلين بالإنترنت، وبالتالي فهناك حاجة متزايدة إلى تعزيز الأمن السيبراني لضمان وجود حلول رقمية آمنة وجديرة بالثقة.

وفي هذا الإطار، يُمكن استعراض مجموعة من التوصيات إلى صُنَّاع القرار في العالم بصفة عامة، والتي يُمكن تطبيقها على الوطن العربي لتعزيز جهود مواجهة المخاطر السيبرانية وتعزيز الأمن السيبراني، وذلك من خلال ما يأتي:

1. ضرورة العمل من خلال نهج متعدد التخصصات؛ لمراجعة جميع ركائز مبادرة جنيف الدولية، وتعزيز التعاون بين دول العالم في مواجهة تحديات الأمن السيبراني، وخصوصًا في الدول الأقل نموًّا، والدول الجزرية الصغيرة النامية، والبلدان النامية غير الساحلية.
2. ضرورة معالجة نقاط القوة والضعف في جهود الدول لتعزيز الأمن السيبراني والاستفادة من مزاياها التنافسية لتعزيز القدرات الإلكترونية والصحة العامة.
3. ضرورة إجراء تقييمات دورية لالتزامات الدول بجهود تعزيز الأمن السيبراني، بما في ذلك المقاييس ذات الصلة.
4. التطوير المستمر لِفِرَقِ الاستجابة الوطنية لحوادث الإنترنت، ومواصلة إنشاء فِرَقِ استجابةٍ وطنيةٍ لحوادث الإنترنت تكون متخصصة في قطاعات بعينها.
5. مراقبة وتحديث الإستراتيجيات الوطنية للأمن السيبراني مع وضع خططٍ واضحةٍ للتنفيذ.
6. الشمول والتنوع، لا سيما فيما يتعلَّق بالمجموعات الممثلة تمثيلًا ناقصًا، مثل: النساء والشباب، ضمن القوى العاملة في مجال الأمن السيبراني.
7. المشاركة المنتظمة في الأنشطة الدولية لتبادل الممارسات الجيدة، ودراسات الحالة، وتحسين القدرة على التأهب والاستجابة لمخاطر الأمن السيبراني.
8. تحسين قدرة الأمن السيبراني للشركات الصغيرة والمتوسطة ومتناهية الصغر (MSMEs).
9. المشاركة المنتظمة لجميع أصحاب المصلحة المَعْنِيِّين بالأمن السيبراني، بما في ذلك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني.
10. هناك حاجة ملحة للعمل على تطوير برامج أمن نُظم المعلومات، وتعزيز قدرتها على الصمود في مواجهة التهديدات السيبرانية.
11. ضرورة تحديد فرص وتحديات الأمن السيبراني المستقبلية ذات الصلة بتقنيات الثورة الصناعية الرابعة، وتصميم الحلول التي تساعد على بناء الثقة.

12. ضرورة تعزيز ثقافة الحوكمة الإلكترونية بحيث تضع كُلُّ مؤسسةٍ ماليةٍ إستراتيجيةَ الأمنِ السيبرانيِّ الخاصة بها وفقًا لممارسات إدارة المخاطر.
13. تعزيز تضافر الجهود لوضع مؤشرات نوعية مناسبة لقياس المخاطر السيبرانية فيما يتعلَّق بغسل الأموال وتمويل الإرهاب.
14. تعميق التعاون بين الدول العربية في مجال حماية الأمن السيبراني؛ من أجل وضع وتطوير الإستراتيجيات الوطنية للأمن السيبراني، وتفعيل دور المؤسسات المتعلقة بالأمن السيبراني على غرار المجلس الأعلى للأمن السيبراني المصري، الذي تم إنشاؤه بقرار السيد رئيس الوزراء رقم 1630 لعام 2016.
15. تعزيز الجهود الإقليمية والدولية لمعاقبة المتورطين في الهجمات السيبرانية المختلفة، وذلك من خلال التعاون بين أجهزة إنفاذ القانون والسلطات المعنية بحماية الأمن السيبراني بين الدول العربية بصفة خاصة، والعالم ككل بصفة عامة.
16. ضرورة إجراء مسحٍ وطنيٍّ للتشريعات القائمة ذات الصلة بالأمن السيبراني؛ تمهيدًا لوضع سياسات تشريعية عربية فعالة تستند إلى أسس علمية واضحة ولا تتسم بالتكرار، فضلًا عن تحديث تلك التشريعات؛ لتكون أكثر فعالية.

المراجع:

- The International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2020. Geneva, Switzerland.

Received 08 July 2023; Accepted 12 July 2023; Available Online 12 Oct. 2023.

Rania Soliman Saadeldin
Faculty of Economics and Political Science, Cairo University Egypt

رانيا سليمان سعد الدين
كلية الاقتصاد والعلوم السياسية، جامعة القاهرة
جمهورية مصر العربية

Keywords: security studies, cybersecurity, global risks

الكلمات المفتاحية:
الدراسات الأمنية، الأمن السيبراني، المخاطر العالمية

Production and hosting by NAUSS

* Corresponding Author: Rania Soliman Saadeldin
Email: kaboudouh@nauss.edu.sa
doi: 10.26735/VFTR8994