الأمن السيبراني في مصر
دراسة تحليلية لتكامل الأداء وفق المؤشرات الدولية

د. هشام مصطفى كمال الدين أحمد
المدرس بقسم الوثائق والمكتبات والمعلومات
كلية الآداب – جامعة المنصورة
heshamabc@mans.edu.eg

تاريخ الاستلام: 27 يناير 2025 **تاريخ القبول: 6 فبراير 2025**

المستخلص

تهدف هذه الدراسة إلى تحليل تدابير الأمن السيبراني المتبعة في مصر وتقييم مدى توافقها مع المعايير الدولية من خلال مقارنة الأداء المصري مع المؤشرات الدولية الرئيسية، مثل المؤشر العالمي للأمن السيبراني (GCI)، مؤشر الأمن السيبراني الوطني(NCSI) ، مؤشر القوى السيبرانية الوطنية(NPCI) ، ومؤشر الجاهزية الشبكية .(NRI) اعتمدت الدراسة على المنهج التحليلي المقارن لتحليل بيانات المؤشرات وتقييم الفجوات بين السياسات المتبعة في مصر وبين المتطلبات العالمية. وقد توصلت الدراسة إلى أن مصر قد حققت تقدماً ملحوظاً في تصنيفها ضمن الدول العشر الأولى وفقاً لمؤشر GCI في عام 2024. ومع ذلك، كشفت النتائج عن تباين كبير بين تصنيف مصر في GCI مقارنة ببقية المؤشرات، مما يعكس فجوة بين السياسات المتبعة والتطبيق الفعلي للتدابير السيبرانية. كما أظهرت الدراسة ضرورة استخدام مؤشرات إضافية لتقييم كفاءة تطبيق الأمن السيبراني في مصر بشكل دقيق. وفي ضوء النتائج، أوصت الدراسة بضرورة مراجعة وتحسين تطبيق السياسات الحالية للأمن السيبراني في مصر، مع التركيز على تعزيز التعاون الإقليمي والدولي، وتطوير البنية التحتية التقنية، وزيادة الاستثمار في مجال البحث والابتكار. كما أكدت على أهمية وضع خطط استراتيجية لإدارة المخاطر وتعزيز التوعية وبناء القدرات لمواجهة التهديدات السيبرانية المتزايدة.

الكلمات المفتاحية: الأمن السيبراني؛ مؤشرات الأمن السيبراني؛ التدابير السيبرانية؛ الأمن السيبراني في مصر.

أولاً: المقدمة المنهجية:

1- المقدمة:

في عالمنا الحديث، اصبح الاعتماد على التقنيات السيبرانية أكثر من أي وقت مضى، حيث يتصل بالإنترنت أكثر من خمسة مليارات شخص. ويتم يوميًا إنتاج أكثر من عشرة مليارات جيجابايت من البيانات عبر الإنترنت، مع توقعات بتجاوز عدد الأجهزة النشطة المتصلة بالإنترنت 24 مليار جهاز بحلول عام 2030. هذا التحول الرقمي المتسارع يشمل مختلف المجالات، بدءًا من المعاملات التجارية والتمويل، وصولًا إلى الترفيه، الاتصالات، السياسة، والأمن.

ورغم ما جلبته الرقمنة من مزايا وراحة في حياتنا، إلا أنها صاحبتها مخاطر وتهديدات غير مسبوقة. فيوميًا، يتم اختراق أكثر من 250 ألف صفحة ويب، وفي المتوسط تحدث 70 مليون هجمة إلكترونية يوميًا وفقًا لتقارير شركة Check Point، المزود الرائد لحلول الأمن السيبراني. وقد بلغت قيمة سوق الجرائم الإلكترونية عالميًا نحو 6 تريليونات دولار في عام 2021.

لقد أصبحت مفاهيم مثل الهجمات السيبرانية، الجرائم الإلكترونية، الصراعات الإلكترونية، وحتى الحرب الإلكترونية، والتنمر السيبراني جزءًا لا يتجزأ من حديثنا اليومي في السنوات الأخيرة، مما أدى إلى تحول الفضاء السيبراني إلى بيئة شديدة الفوضى مليئة بالتهديدات المتزايدة. وفي ظل هذا المشهد المقلق، اضطرت الدول وأصحاب المصلحة في الفضاء الإلكتروني إلى اتخاذ تدابير حاسمة لتعزيز الأمن السيبراني، الذي بات خلال العقد الماضي يتصدر جداول أعمال الأمن الوطنية والدولية باعتباره إحدى القضايا الأكثر إلحاحًا حول العالم.

هناك ارتباط تام بين الأمن السيبراني والتنمية المستدامة والنمو الشامل عالميًّا، لذا فحماية المعلومات أمر في غاية الأهمية للقطاعات كلها، وفي أبعاد التنمية المستدامة جميعها من حيث الأمن الغذائي، وأمن الصحة والتعليم والموارد والقطاعات كافة. وقد كشف تقرير المخاطر العالمية لعام 2023 ، أن الأمن السيبراني يعد من أهم المخاطر التي تواجه الاقتصاد العالمي، والذي يأتي في المرتبة الرابعة من بين المخاطر كافة التي تواجه العالم، ومن أبرزها على الأجلين القصير والطويل.

ومن خلال استعراض الأدبيات البحثية في العقد الأخير حول معالجة موضوع الأمن السيبراني في مصر، لوحظ تركيز الدراسات على تناول الأطر النظرية لمفهوم الأمن السيبراني وأنواع واشكال التهديدات السيبرانية وجهود مكافحة الجرائم الإلكترونية، في حين كانت الدراسات التي تقيم التدابير المتبعة في مصر ومدى توافقها مع المؤشرات العالمية قليلة نسبيا وإن لم تكن نادرة، وهو ما تسعى هذه الدراسة إلى معالجته. في هذا الإطار، فتهدف الدراسة إلى تحليل واقع الأداء المصري في مجال الأمن السيبراني، مع التركيز على السياسات والإستراتيجيات المتبعة، ومقارنتها بالمؤشرات الدولية، والإجابة على السؤال: "هل التدابير الحالية للأمن السيبراني في مصر كافية وفعّالة وفقًا للمؤشرات الدولية؟

2- مشكلة الدراسة:

في العصر الرقمي الذي نعيشه اليوم، أصبح الأمن السيبراني ركيزة أساسية لضمان استقرار الأفراد والمؤسسات والدول على حد سواء. مع التوسع المتسارع في استخدام الإنترنت والتكنولوجيا الرقمية، تزداد التهديدات السيبرانية التي تستهدف المعلومات الحساسة والأنظمة الحيوية مثل البنية التحتية، الاقتصاد، والأمن الوطني. تطور الهجمات الإلكترونية وأساليب الاختراق يعزز الحاجة الملحة إلى تبني استراتيجيات فعّالة تضمن الأمان الرقمي.

الأمن السيبراني ليس مجرد وسيلة لحماية البيانات الشخصية، بل هو عنصر حيوي لتعزيز ثقة المستخدمين في الخدمات الرقمية وضمان استمرارية الأعمال في مواجهة التحديات المتنامية.

في هذا الإطار، عملت هيئات دولية ومؤسسات متخصصة في تكنولوجيا المعلومات والاتصالات على تطوير أدوات وتقارير تقييمية تدعم الدول في قياس فعالية تدابيرها لحماية الأمن السيبراني. وتشمل هذه التقارير تقييم مرتكزات أساسية مثل الأطر القانونية والتشريعية، البنية التحتية الرقمية، التمويل، ريادة الأعمال، التعليم، البحث العلمي، الابتكار، والتعاون المحلي والدولي. من خلال هذه الأدوات، يمكن للدول تحليل نقاط قوتها وضعفها، مما يساعدها في تحسين استراتيجياتها الأمنية وتعزيز جاهزيتها لمواجهة التهديدات السيبرانية.

حققت مصر في عام 2024 تقدمًا بارزًا في مجال الأمن السيبراني، حيث صُنفت ضمن الدول العشر الأولى عالميًا وفقًا للمؤشر العالمي للأمن السيبراني .(GCI) ورغم أن هذا التصنيف يعكس التزامًا كبيرًا بتبني السياسات والتدابير الأمنية، إلا أن مستوى التطبيق الفعلي لهذه التدابير يبقى المحك الأساسي.

ورغم تقدم مصر، فإن حصول أي دولة على قيمة 100% في المؤشر يُظهر حاجة ملحة لمراجعة المؤشرات الفرعية لهذا المؤشر GCI. فلا يمكن لأي دولة، بما في ذلك مصر، تحقيق تأمين كامل بنسبة 100%، خاصة مع استمرار وقوع هجمات سيبرانية بمستويات مختلفة. كما أن حصول مصر على الدرجة النهائية يعني ببساطة أن أي تقدم سوف تحققه في المستقبل لن يكون له أي انعكاس على قيمة المؤشر الخاص بها نظرًا لوصولها إلى الدرجة القصوى.

لذلك، يُعد الاعتماد على مؤشرات إضافية، مثل مؤشر الأمن السيبراني الوطني (NCSI)، مؤشر القوى السيبرانية الوطنية (NPCI)، ومؤشر الجاهزية الشبكية (NRI)، أمرًا ضروريًا لتقييم كفاءة التطبيق الفعلي. بناءً على ذلك، تحدد إشكالية الدراسة: إلى أي مدى يعكس تصنيف مصر المتقدم في مؤشر GCI التزامها الفعلي بتبني تدابير الأمن السيبراني؟ وهل هذا التصنيف يعكس كفاءة التطبيق مقارنة بالمؤشرات الدولية الأخرى؟

3- **أهمية الدراسة**:

تنبع أهمية الدراسة من أهمية موضوع الأمن السيبراني وضرورة سعي الدول إلى اتخاذ التدابير اللازمة لمكافحة التهديدات السيبرانية، إضافة إلى الاهتمام العالمي بتوفير مؤشرات قياس وتحليل التدابير المتخذة لتحقيق الأمن السيبراني. بالنسبة لمصر، تكتسب الدراسة أهميتها من خلال النقاط التالية:

1- تُعد هذه الدراسة، حسب علم الباحث، الأولى من نوعها التي تقدم تحليلًا معمقًا وشاملًا لتقييم واقع التطبيق الفعلي للتدابير المتخذة في مصر لتعزيز الأمن السيبراني، بما يتماشى مع المؤشرات الدولية.

2- تسلط الدراسة الضوء على المعايير والمناهج العالمية المستخدمة لقياس وتقييم مؤشرات الأداء في مجال الأمن السيبراني، مما يوفر إطارًا موضوعيًا وموثوقًا لإجراء المقارنة.

3- تستعرض الدراسة تأثير تطبيق التدابير الفعلية المتبعة في مصر لتعزيز الأمن السيبراني على ترتيبها في مؤشرات الأمن السيبراني الدولية، مما يبرز الأبعاد العملية للسياسات الحالية.

4- تحلل الدراسة الفجوات بين السياسات المعتمدة وواقع التطبيق الفعلي لتدابير الأمن السيبراني في مصر وفقًا لمؤشرات الأداء العالمية، مما يساعد في تحديد مجالات التطوير.

5- تقدم الدراسة توصيات عملية لتحسين تطبيق التدابير المتبعة في مصر لتعزيز الأمن السيبراني، مستندةً إلى الفجوات المحددة بالمقارنة مع المؤشرات العالمية، بما يسهم في تحقيق تقدم مستدام.

4- أهداف الدراسة:

تسعى الدراسة إلى تحقيق مجموعة من الأهداف تتمثل في:

1- تحليل وتقييم التدابير المتبعة في مصر لتعزيز الأمن السيبراني، مع التركيز على مدى توافقها مع المعايير والمؤشرات الدولية.

2- الكشف عن نقاط القوة ونواحي القصور في الأداء المصري بمجال الأمن السيبراني، بما يُبرز الجوانب المميزة والتحديات القائمة.

3- تحليل حجم الفجوة بين التقييم المثالي لمصر في مؤشر GCI والأداء الفعلي في المؤشرات الأخرى (NCSI, NPCI, NRI).

4- تقديم توصيات عملية قابلة للتطبيق لتحسين الأداء السيبراني في مصر، مستندةً إلى الفرص المتاحة والنتائج المستخلصة من التحليل، ولتعزيز كفاءة واستدامة التدابير المتخذة.

5- تساؤلات الدراسة:

1- ما هو مفهوم الأمن السيبراني؟ وما هي المرتكزات الأساسية التي تعتمد عليها الدول لتعزيز أمنها السيبراني؟

2- ما هي المؤشرات الدولية الرئيسية المستخدمة لتقييم التدابير الوطنية في مجال الأمن السيبراني؟

3- هل تختلف منهجيات تقييم الدول وفقًا للمرتكزات الأساسية في مؤشرات الأمن السيبراني الدولية؟

4- ما مدى ملاءمة وكفاية التدابير القانونية والتشريعية المصرية في مجال الأمن السيبراني؟ وكيف تتوافق مع المؤشرات الدولية؟

5- ما مدى جاهزية القدرات التقنية والبنية التحتية الرقمية في مصر لتعزيز الأمن السيبراني؟

6- إلى أي مدى يسهم مستوى التعاون الإقليمي والدولي لمصر في تعزيز أدائها في مجال الأمن السيبراني وفقًا للمؤشرات الدولية؟

7- هل تمتلك مصر مراكز متخصصة وخطة استراتيجية لإدارة المخاطر وتعزيز المرونة السيبرانية؟ وما مدى كفاءة أدائها مقارنةً بالمؤشرات الدولية؟

8- هل لدى مصر خطة واضحة للتوعية وبناء القدارات تعزز من أمنها السيبراني؟

9- هل حجم الاستثمارات الحكومية في مشروعات الأمن السيبراني ودعم الشركات الناشئة كافٍ لتعزيز الأمن السيبراني في مصر؟

10- ما هو حجم الفجوة بين التقييم المثالي لمصر في مؤشر GCI وتقييم الأداء الفعلي في المؤشرات الأخرى (NCSI, NPCI, NRI)؟

11- ما هي التوصيات العملية التي يمكن تقديمها للاستفادة من الفرص المتاحة لتعزيز الأداء المصري في مجال الأمن السيبراني؟

6- حدود الدراسة:

- ✓ الحدود الموضوعية: تغطي الدراسة موضوع تحليل وتقييم التدابير المتخذة في مصر لتعزيز الأمن السيبراني وفقًا للمؤشرات الدولية .
- ✓ الحدود الزمنية: اقتصر نطاق الدراسة على التقارير الدولية والمحلية التي تغطي الفترة الزمنية من 2023 إلى 2024.
- ✓ الحدود الجغرافية: تقتصر الدراسة على تناول جمهورية مصر العربية.

7- منهج الدراسة:

اقتضت الدراسة الحالية نظراً لطبيعتها، وأهدافها استخدام اكثر من منهج حيث تعتمد الدراسة على المنهج الوصفي التحليلي (تحليل المضمون) لدراسة التدابير المتبعة في مصر لتعزيز الأمن السيبراني، مع التركيز على ست ركائز رئيسية: الحوكمة والسياسات، القدرات التقنية، التعاون الدولي، إدارة المخاطر، التوعية، والاستثمار، وتحليل مدى كفايتها وفقًا للمؤشرات العالمية. كما تعتمد الدراسة على المنهج الإحصائي الوصفي لوصف وتحليل البيانات الرقمية المتعلقة بمؤشرات التدابير المصرية، التي تم جمعها من تقارير إحصائية لمؤشرات الأمن السيبراني الدولية بين 2023 و2024، لتفسير النتائج وتحليلها.

8- مصطلحات الدراسة:

1- الفضاء السيبراني. [1]

تعرف وزارة الدفاع الأمريكية للفضاء السيبراني هو: "مجال يتميز باستخدام التقنيات الإلكترونية والأنظمة الكهرومغناطيسية لتخزين وتعديل وتبادل البيانات عبر الإنترنت والبنى التحتية المادية المرتبطة بها."

2- الأمن السيبراني. [2]

يُعرِّف المعهد الوطني للمعايير والتقنية (NIST) الأمن السيبراني على أنه "الحماية من الأضرار واستعادة أنظمة الحاسب وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات".

مؤشرات الأمن السيبراني. [3]

هي أدوات أو مقاييس تُستخدم لتقييم فعالية الإجراءات الأمنية المتبعة في حماية المعلومات والأنظمة الإلكترونية. وتساعد هذه المؤشرات في قياس مدى قوة الدفاعات السيبرانية، وتحديد الثغرات، وتوجيه التحسينات المستمرة.

9- الدراسات السابقة:

في هذا السياق تم البحث بقواعد البيانات المحلية والدولية ببنك المعرفة المصري حول الدراسات التي تتناول الأمن السيبراني وتقييم تدابير الدول وفق المؤشرات العالمية وذلك باستخدام عدد من المصطلحات البحثية باللغتين العربية والانجليزية وهي:

- الأمن السيبراني Cybersecurity.
- التدابير السيبرانية Cyber Measures.
- مؤشرات الأمن السيبراني الدولية International Cybersecurity Indicators.
- مؤشر الأمن السيبراني العالمي Global Cybersecurity Index (GCI)
- المؤشر الوطني للأمن السيبراني National Cyber Security Index (NCSI)
- مؤشر القوى السيبرانية الوطنية National Cyber Power Index (NCPI)
- مؤشر الجاهزية الشبكية Network Readiness Index (NRI)

وبالبحث في بنك المعرفة المصري فيما يتعلق بمصطلحات الدراسات "التدابير السيبرانية"، و "مؤشرات الأمن السيبراني الدولية" سواء باللغة العربية أو باللغة الإنجليزية لم يتوفر للباحث أي نتائج عن دراسات تتناول مؤشرات الأمن السيبراني سواء في مصر أو في أي من الدول العربية ومن ثم فالدراسة الحالية تعد أول دراسة تتناول هذا الموضوع من هذه الزاوية على حد علم الباحث. في حين عند توسيع نطاق البحث باستخدام مصطلح "الأمن

السيبراني" حيث تم تحديد العديد من الدراسات التي تتناول مجال الامن السيبراني ولكن من زوايا معالجة أخرى تختلف تماما عن موضوع الدراسة الحالية حيث امكن تصنيف تلك الدراسات تحت:

أولاً: دراسات تأطيرية عن الأمن السيبراني تهدف إلى وضع إطار عام أو خارطة مفاهيمية للموضوع.

ثانياً: دراسات تتناول تقييم مستوى الوعي لدي فئة محددة حول الأمن السيبراني.

ثالثاً: دراسات تتناول متطلبات تحقيق الأمن السيبراني في مؤسسات محددة بعينها.

أولاً: الدراسات التأطيرية عن الأمن السيبراني:

قدمت البداينة، ذياب[4] عام (2024) دراسة حول الإرهاب السيبراني والتقنيات الناشئة، حيث استعرضت مكونات الفضاء السيبراني وتطوره كحاضنة للإرهاب السيبراني. وركزت الدراسة على مفهوم الإرهاب السيبراني وأشكاله، طرق الهجمات الإرهابية السيبرانية، والحرب السيبرانية. كما ناقشت العلاقة بين الإرهاب السيبراني والتقنيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء، وطرحت التحديات التي يواجهها الأمن الوطني السيبراني والسيادة الوطنية.

وفي نفس العام قدم **البدوي، حبيب.** (2024) [5] دراسة حول الحرب الرقمية والأمن السيبراني، حيث استعرض مظاهر الحرب السيبرانية ودور الأمن السيبراني في التخفيف من آثارها. شملت الدراسة ثلاث خطوات رئيسية: جمع البيانات حول أنواع الحرب السيبرانية وتدابير الأمن السيبراني، التحليل والتوليف لتحديد الأنماط والمفاهيم الرئيسية، وأخيراً الهيكلة والكتابة حيث تم تنظيم المعلومات في تسلسل منطقي لدعم أهداف الدراسة.

وفي ذات السياق سعت **عبدالقادر، إيمان** [6] في عام (2024). لدراسة أثر الفضاء السيبراني على الأمن القومي العربي بين 2011 و2023. اعتمدت الدراسة على المنهج الوصفي، وناقشت العلاقة بين الفضاء السيبراني والأمن القومي، وتأثيره على الأمن القومي العربي. كما استعرضت التحديات التي تواجه الأمن السيبراني في الدول العربية وركائز لمواجهتها. أوصت الدراسة بتوفير منح دراسية في مجال الأمن السيبراني للدول التي تفتقر إلى الكوادر المدربة، لحين إنشاء مؤسسات تعليمية متخصصة.

كما وقدم **ناصف، أحمد مصطفى** [7] في عام (2023) دراسة حول دمج الأمن السيبراني في منظومة الأمن القومي المصري. تناولت الدراسة تعريف الأمن السيبراني وعلاقته بأمن المعلومات، بالإضافة إلى المخاطر التي تهددها. أكدت على أهمية الأمن السيبراني كجزء أساسي من الأمن القومي، ووضحت كيفية دمجه في هذه المنظومة. كما استعرضت التحديات في مواجهة الجرائم الإلكترونية وأوصت بتنظيم دورات تدريبية متقدمة لتعزيز الوعي بأهمية الأمن السيبراني في حماية الأمن القومي.

وفي نفس العام 2023 أعدت **آل مداوى** [8] دراسة تناولت الأمن السيبراني بالمملكة العربية السعودية من حيث تعريفه، أهميته، أنواعه، إستراتيجيات الوقاية من الهجمات السيبرانية. تناولت نبذة تاريخية عن الأمن السيبراني، وبينت أنواع الأمن السيبراني، ودوافع اهتمام الدول بالأمن السيبراني، كما حددت جهود المملكة السعودية في مجال الأمن السيبراني، وحددت إستراتيجيات للوقاية من الهجمات السيبرانية، وأوضحت التشريعات التي وضعتها المملكة في مكافحة الجرائم الإلكترونية، وسلطت الضوء على الاتحاد السعودي وعلاقته بالأمن السيبراني والبرمجة والدرونز. اختتمت الدراسة بالنتائج التي تحققت بالمملكة العربية السعودية بالحصول على المرتبة الثانية عالميًا في مؤشر الأمن السيبراني، وذلك ضمن تقرير الكتاب السنوي للتنافسية العالمية لعام (2022).

في عام (2021) قدم **المزيني، عبدالعزيز بن أحمد** [9] دراسة تأطيرية استعرضت الأمن السيبراني كواجب للدولة الحديثة ووسائل تحقيقه التنظيمية. تناولت تعريف الأمن السيبراني وخصائصه، والأساس الفقهي والنظامي

له. أكدت الدراسة على ضرورة وضع استراتيجية وطنية للأمن السيبراني وضوابط ومعايير رقابية لتحقيقه. واختتمت بتأكيد على أهمية نشر الوعي بين أفراد المجتمع لضمان المسؤولية والوعي بالأمن السيبراني.

ثانياً: دراسات تتناول تقييم مستوى الوعي لدي فئة محددة حول الأمن السيبراني.

في عام 2024 قدم **الضفيري، ناجي بدر**[10] دراسة حول مستوى الوعي بالأمن السيبراني وتوظيف التكنولوجيا في التدريس لدى معلمي المرحلة المتوسطة بالكويت. استخدم المنهج الوصفي المسحي مع عينة من 124 من معلمي ومعلمات المرحلة المتوسطة بمنطقة العاصمة. أظهرت النتائج أن الوعي بالأمن السيبراني كان دون المستوى المطلوب، بينما كان توظيف التكنولوجيا في التدريس متوسطًا. كما تبين وجود علاقة إيجابية مؤثرة بين الوعي بالأمن السيبراني وتوظيف التكنولوجيا في التدريس.

بينما في عام 2022 قدم **الحبيب، ماجد بن عبدالله بن محمد** [11] دراسة هدفت إلى التعرف على درجة الوعي بمفاهيم الأمن السيبراني، ودرجة الوعي بتطبيقات الأمن السيبراني، وأبرز سبل تعزيز الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية من وجهة نظرهم، ولتحقيق هذا الهدف استخدم الباحث المنهج الوصفي المسحي، وقد تمثلت أهم نتائج الدراسة في أن أفراد مجتمع الدراسة يملكون درجة (عالية) من الوعى بمفاهيم الأمن السيبراني، وأن أفراد مجتمع الدراسة يملكون درجة (عالية) من الوعي بتطبيقات الأمن السيبراني، وهو ما يشير إلى ارتفاع مستوى معرفة أفراد مجتمع الدراسة بتطبيقات الأمن السيبراني. وأن أفراد مجتمع الدراسة موافقون على سبل تعزيز الوعي بالأمن السيبراني. وأوصت الدراسة بتفعيل كلية التربية لعدد من الإجراءات التي تساهم في رفع درجة الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بالكلية.

وفي نفس العام قدمت **فرج، علياء عمر كامل إبراهيم** [12] دراسة حول دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز. استخدمت الدراسة المنهج الوصفي وطبقت استبانة على 125 عضوًا من هيئة التدريس. توصلت إلى أن دواعي تعزيز الثقافة السيبرانية جاءت بدرجة متوسطة، حيث تصدرت الدواعي المجتمعية ثم المعرفية، تلتها الدواعي التقنية. أوصت الدراسة بزيادة الوعي بالأمن السيبراني بين الطلاب وتصميم حملات توعية بالمخاطر السيبرانية.

أما في عام 2021 فقد أجرت **أنديجاني، دلال صالح** [13] دراسة هدفت إلى التعرف على ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية والتعرف على الفئات المستهدفة بتعزيز الوعي بثقافة الأمن السيبراني والتعرف على التوصيات لتعزيز الوعي بثقافة الأمن السيبرانى لدى الفئات المستهدفة من عام 2015 إلى عام 2020 في عدد من قواعد البيانات. واتبعت الدراسة السبع مراحل لمنهج المراجعة المنهجية للدراسات السابقة. ووضحت الدراسة العوائد وأهمية الدراسة الاجتماعية والبيئية والاقتصادية والثقافية والمحلية والدولية. وتوصلت الدراسة إلى عدد من النتائج وتم استعراضها من خلال الإجابة على أسئلة الدراسة. وكذلك أوصت الدراسة بعدة توصيات بناء على نتيجة المراجعة المنهجية.

ثالثاً: دراسات تتناول متطلبات تحقيق الأمن السيبراني في مؤسسات محددة بعينها.

قدمت **المنيع، الجوهرة عبد الرحمن** [14] عام 2022 دراسة هدفت إلى التعرف على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030. استخدمت الدراسة المنهج الوصفي التحليلي وركزت على موظفي التقنيات في ثلاث جامعات سعودية هي: (جامعة أم القرى، جامعة الإمام عبد الرحمن بن فيصل، جامعة

الإمام محمد بن سعود الإسلامية)، أظهرت النتائج أن هناك توافقًا متوسطًا على تحقيق الأمن السيبراني، مع وجود معوقات مثل تدني خبرة الموظفين وضعف التعاون بين التقنيين. كما أظهرت الدراسة اتفاقًا كبيرًا على متطلبات تحقيق الأمن السيبراني وقدمت مقترحات مثل توعية الموظفين بمخاطر استخدام الأجهزة الشخصية وحوافز لدعم العاملين المبدعين في هذا المجال.

وفي نفس العام قدم **العتيبي، فهد، البرهمتوشي** [15] دراسة سعت لتناول واقع المدن الذكية السعودية وتحدياتها الأمنية السيبرانية في ضوء رؤية المملكة 2030. شملت الدراسة تحليل واقع سبع مدن ذكية (الرياض، نيوم، مكة المكرمة، المدينة المنورة، جدة، الأحساء، وينبع) باستخدام مصفوفة مؤشرات لتقييم المقومات وتم إعداد استبانة تقييمية طبقت على (٦٠) من أعضاء هيئة التدريس المتخصصين في الجامعات السعودية والمصرية. وقد أبرزت الدراسة وجود تحديات أمنية منها الهجمات السيبرانية، قرصنة البيانات، وانتهاك الخصوصية، وقدمت 10 توصيات لمواجهة هذه التحديات وتعزيز الأمن السيبراني في المدن الذكية.

بينما في عام 2021 قدم **عبدالحميد، عماد الدين محمد كامل** [16] دراسة هدفت إلى التعرف على استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي. واستعرضت مؤشر الأمن السيبراني العالمي وركائزه، وتحديات الأمن القومي في الفضاء السيبراني، وحوادث الأمن السيبراني لعام 2020. كما ناقشت استراتيجية الأمن السيبراني للقطاع المالي لتعزيز الاقتصاد الرقمي والتجارة الدولية. أوصت الدراسة بمراجعات دورية للأمن السيبراني المرتبط بأصول التشفير، وحذرت من شراء منظومات حماية سيبرانية قد تهدد الأمن الاقتصادي والقومي.

وفي نفس العام قدمت **السيد، نهى مجدي محمد** [17] دراسة هدفت لتحليل علاقة الأمن السيبراني بالمضمون الإعلامي في ظل رؤية مصر 2030. استخدمت المنهج الوصفي التحليلي واستبيانًا شمل 32 أستاذًا جامعيًا ومتخصصًا في الإعلام وتقنية المعلومات والأمن السيبراني بكليتي الإعلام والهندسة، أكدت النتائج أهمية الأمن السيبراني في حماية المضمون الإعلامي، مشيرة إلى عدم تطبيق كامل لآليات الأمن السيبراني في الإعلام الإلكتروني، مما يستدعي جهودًا تشريعية ورقابية فعّالة.

كذلك في عام 2021 قدمت **الغامدي، عهود أحمد** [18] دراسة لتحليل دور الأمن السيبراني في تحقيق الميزة التنافسية بمطار الملك عبدالعزيز بجدة، باستخدام المنهج الوصفي التحليلي واستبانة لجمع البيانات. أظهرت النتائج دورًا إيجابيًا للسرية، الخصوصية، والتعزيز في تحقيق الميزة التنافسية، وأوصت الباحثة بالاستمرار في تعزيز الأمن السيبراني كجزء من الأمن الوطني السعودي.

وفي توجه مختلف قدم **براون، رافائيل دين** [19] عام 2018 دراسة هدفت إلى تقديم نموذجا لتعزيز قدرات الأمن السيبراني (Q–C2M2) في دولة قطر ضمن إطار تشريعي. وتناول البحث نموذجا أصيلا لتعزيز قدرات الأمن السيبراني مع تسليط الضوء على غرضه وخصائصه واعتماده. كما عرضت الدراسة نماذجا لتعزيز قدرات الأمن السيبراني الحالية والمعترف بها عالميا، وتناولت دراسة عن الأمن السيبراني في دولة قطر باستخدام الوثائق المتاحة، وذلك بناء على منهجية التحليل الموضوعي للوثائق. كما قدمت الدراسة تحليلا مقارنا لنماذج تعزيز قدرات الأمن السيبراني في ضوء الأمن السيبراني القطري. لتحديد الثغرات الموجودة في سياسة تأمين المعلومات الوطنية القطرية بشكل عام، ودليل تأمين المعلومات الوطنية القطرية بشكل خاص.

التعليق على الدراسات السابقة:

نظرا لحداثة موضوع الأمن السيبراني وأهميته فقد تعددت زوايا تناول الموضوع بالدراسات السابقة ومن خلال استعراض هذه الدراسات، يمكن التأكيد على اختلاف الدراسة الحالية في زاوية تناولها ومعالجتها لموضوع الأمن السيبراني، وعلى الرغم من الاختلاف إلا أن ذلك لم يمنع الباحث من الاستفادة من تلك الدراسات، خاصة تلك التي ساهمت في تأطير الجوانب النظرية لموضوع الأمن السيبراني ومعالجة أبعاده المختلفة وخاصة ما يرتبط منها بعلاقة الأمن السيبراني بالأمن القومي. كما ساعدت الباحث أيضا في تحديد منهج البحث المناسب لإجراء الدراسة الحالية.

ثانياً: الاطار النظري للدراسة:

1- مفهوم الأمن السيبراني:

على الرغم من أهمية الأمن السيبراني، فإنه لا يوجد تعريف موحد، أو مصطلح مشترك لشرح الأمن السيبراني. حيث تستهدف التعريفات الحالية إلى حد كبير الأكاديميين أو الخبراء التقنيين، ولكنها غير مفهومة بشكل كبير بالنسبة لغير الخبراء وسوف تستعرض الدراسة أبرز تلك التعريفات على سبيل المثال لا الحصر:

قام المعهد الوطني للمعايير والتقنية (NIST)[20] بتعريف الأمن السيبراني على أنه: "القدرة على الحماية أو الدفاع من الهجمات السيبرانية، عند استخدام الفضاء السيبراني."

فيما طوّر الاتحاد الدولي للاتصالات (ITU)[21] من أجل الاستخدام العملي ، تعريفًا شاملًا وواضحًا للأمن السيبراني يشمل تقريبًا كل جانب من جوانب الأمن السيبراني :"الأمن السيبراني هو مجموعة من الأدوات والسياسات ومفاهيم الأمان والضمانات الأمنية والمبادئ التوجيهية وإدارة المخاطر والأساليب والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة وأصول المستخدم"

ووفقاً للهيئة الوطنية للأمن السيبراني السعودية،[22] يعرف الأمن السيبراني على أنه حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي وغيرها.

كما يعرفه المركز الوطني للامن السيبراني البحريني [23] بأنه " هو عملية حماية الأنظمة والبيانات والاتصالات والشبكات الموجودة والمتصلة بالإنترنت ضد الهجمات الرقمية. فهذه الهجمات، التي يشار إليها عادة باسم "الهجمات السيبرانية"، ما هي إلا محاولة اختراق، أو تعديل أو تعطيل أو دخول أو استخدام غير مشروع؛ وبالتالي، يمكن أن تتراوح الهجمات السيبرانية من تثبيت رموز برمجية ضارة على جهاز حاسوب شخصي وصولا إلى محاولة تدمير البنية التحتية لدول بأكملها."

في حين تُعرّفه وزارة الدفاع الأمريكية [24] بأنه: «جميع الإجراءات التنظيمية المطلوبة لضمان حماية أمن المعلومات بجميع أشكالها (الإلكترونية والمادية)، وأمن الأنظمة والشبكات حيث يتم تخزين المعلومات والوصول إليها ومعالجتها ونقلها، بما في ذلك الاحتياطات المُتخذة للوقاية من الجريمة، والهجوم، والتخريب، والتجسس، والحوادث".

وفي ضوء التعريفات السابقة يمكن استنتاج أن الأمن السيبراني ما هو إلا مجموعة من الإجراءات التنظيمية، والتقنيات، والسياسات التي تهدف إلى حماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات

التشغيلية، وما تحتويه من بيانات وخدمات من الاختراق أو التعديل أو الاستخدام غير المشروع. كما يشمل حماية البنية التحتية الرقمية ضد الهجمات السيبرانية، وضمان سلامة العمليات المرتبطة بالفضاء السيبراني، بما في ذلك الوقاية من الجريمة السيبرانية، والتجسس، والتخريب.

علاقة الامن السيبراني (Cybersecurity) بأمن المعلومات (Information Security)

الأمن السيبراني وأمن المعلومات مفهومان مترابطان ولكنهما يختلفان في النطاق والتركيز. يشير الأمن السيبراني إلى حماية الأنظمة والشبكات والتطبيقات الرقمية من الهجمات الإلكترونية والتهديدات السيبرانية، مثل البرمجيات الخبيثة وهجمات الفدية ويركز بشكل خاص على تأمين الفضاء السيبراني باستخدام تقنيات مثل جدران الحماية، أنظمة كشف التهديدات، والتشفير. من ناحية أخرى، يهتم أمن المعلومات بحماية البيانات والمعلومات بجميع أشكالها – الرقمية والمادية – من الوصول غير المصرح به أو التعديل أو الإتلاف، مع ضمان السرية والتكامل والتوافر. وعلى الرغم من أن الأمن السيبراني يُعد جزءًا من أمن المعلومات، إلا أن الأخير أوسع نطاقًا، حيث يشمل حماية المعلومات بغض النظر عن وسيطها ويعمل كلا المجالين معًا لضمان بيئة آمنة للمعلومات والبنية التحتية الرقمية.

أنواع التهديدات السيبرانية التي يتصدى لها الأمن السيبراني:

الأمن السيبراني يتصدى لعدة أنواع من التهديدات السيبرانية، والتي يمكن تصنيفها إلى ثلاث فئات رئيسية:[25]

1- **التهديدات الإلكترونية (Cyber Threats)** تشمل الهجمات التي تستهدف أنظمة الحوسبة والشبكات مثل البرمجيات الخبيثة (Malware)، وهجمات الفدية (Ransomware)، والتصيد الاحتيالي (Phishing)، والاختراق (Hacking) لاستغلال الثغرات الأمنية وسرقة البيانات أو تعطيل العمليات.

2- التهديدات المادية (Physical Threats) وتشير إلى المخاطر التي تستهدف البنية التحتية التقنية، مما قد يؤدي إلى إتلافها أو تعطيلها أو فقدان البيانات التي تحتويها.

3- التهديدات البشرية (Human Threats): تنشأ عن أخطاء الأفراد أو نوايا خبيثة، مثل إرسال معلومات حساسة بالخطأ، فقدان كلمات المرور، أو التهديدات الداخلية من موظفين يسربون أو يعبثون بالبيانات. تتطلب مواجهة هذه التهديدات تعزيز الوعي الأمني، سياسات صارمة لإدارة الوصول، ومراقبة الأنشطة.

أهمية الأمن السيبراني للأمن القومي للدول:

مفهوم الأمن القومي:

كان الأمن القومي يُعرَّف تقليديًا بالدفاعات العسكرية ضد التهديدات ذات الطابع العسكري، لكن ثبتت محدودية هذا التعريف، مما استدعى صياغة مفهوم أوسع. ووفقًا لمؤسسة "Heritage" الفكرية الأمريكية، يُعرف الأمن القومي بأنه حفظ الأمة من الأخطار الخارجية، وحماية القوات المسلحة، وأسرار الدولة، والأمن الداخلي، إلى جانب حماية المصالح الجيوسياسية والاقتصادية.

لقد تعددت مجالات الأمن القومي، لتشمل المجال السياسي الذي يتمثل في الحفاظ على وحدة وسلامة أراضي الدولة من أي تهديدات داخلية أو خارجية، والمجال الاقتصادي الذي يهدف إلى تنمية الموارد الاقتصادية للدولة وتحقيق التنمية الاقتصادية المستدامة،[26] والمجال الاجتماعي الذي يعبر عن قدرة الدولة على حماية قيمها الأيديولوجية،[27] والمجال العسكري/الأمني الذي يركز على تعزيز القدرات العسكرية للدولة. إضافةً إلى ذلك، يشمل الأمن القومي المجال السيبراني، الذي يتجسد في الإجراءات والتقنيات المستخدمة لحماية الأنظمة الإلكترونية المختلفة للدولة من الهجمات السيبرانية.[28]

أبرز جوانب أهمية الأمن السيبراني للأمن القومي: [29] [30]

الأمن السيبراني أصبح حجر الزاوية في تحقيق الأمن القومي للدول، وذلك لما يقدمه من حماية ضد التهديدات المختلفة التي يفرضها الفضاء السيبراني. يتضح ذلك من خلال أبرز الجوانب التالية:

1- حماية البنية التحتية الحيوية: تأمين شبكات الطاقة، المياه، النقل، والاتصالات من الهجمات التي قد تسبب شللًا في الخدمات الأساسية أو تؤثر على استقرار الدول خلال الحروب السيبرانية.

2- مكافحة الجرائم والإرهاب السيبراني: منع استغلال الفضاء الإلكتروني لنشر الفوضى، زعزعة الاستقرار، أو الدعاية الإرهابية.

3- حماية البيانات الحساسة: تأمين المعلومات السرية للدولة للحفاظ على سيادتها ومنع التجسس أو التسريب.

4- التصدي للحروب السيبرانية: تطوير استراتيجيات قوية لحماية المصالح الوطنية من الهجمات الإلكترونية.

5- التأثير السياسي: مواجهة استغلال الفضاء السيبراني لتوجيه الرأي العام وإدارة الحروب النفسية.

6- التأثير الاجتماعي: حماية القيم الاجتماعية من التغيير الأيديولوجي ومنع استخدام الفضاء لنشر الإرهاب.

7- التأثير الاقتصادي: تقليل الخسائر الناتجة عن الهجمات على المؤسسات الكبرى وضمان استقرار النظام المالي.

8- تعزيز الثقة والتعاون الدولي: ضمان استمرارية العمليات الرقمية وتعزيز الثقة في التكنولوجيا والدول كشركاء دوليين موثوقين.

مؤشرات الامن السيبراني Cybersecurity indicators:

مؤشر الأمن السيبراني Cybersecurity indicators وفقاً للهيئة الوطنية للأمن السيبراني [31]هي أدوات قياس تستخدم لتقييم مدى جاهزية الدول أو المؤسسات في مواجهة التهديدات السيبرانية وحماية بنيتها التحتية الرقمية. تستند هذه المؤشرات إلى مجموعة من الركائز والمعايير، مثل الحوكمة، القدرات التقنية، التعاون الدولي، وإدارة المخاطر، لتقديم رؤية شاملة عن الأداء السيبراني. وتُسهم هذه المؤشرات في تحديد نقاط القوة والضعف، توجيه السياسات الاستراتيجية، وتعزيز القدرة على مواجهة التحديات السيبرانية المتزايدة. وتبرز أهمية استخدام هذه المؤشرات في العديد من الجوانب، أهمها:

1. **تقييم الجاهزية السيبرانية:** تساعد المؤشرات الدولية مثل **GCI** و**NCSI** الدول على قياس كفاءتها في التصدي للهجمات السيبرانية من خلال تحليل الأداء في مجالات مثل الحوكمة، التقنية، وإدارة المخاطر، يمكن للدول التعرف على مدى جاهزيتها واستعدادها للأحداث السيبرانية.

2. **تحديد نقاط القوة والضعف:** تُظهر هذه المؤشرات المجالات التي تحقق فيها الدول تقدمًا، وتلك التي تحتاج إلى تحسين. على سبيل المثال، إذا أظهر مؤشر ما ضعفًا في التعاون الإقليمي، يمكن للدولة اتخاذ خطوات لتعزيز شراكاتها مع الدول الأخرى.

3. **تعزيز التنافسية العالمية:** يُسهم الأداء الجيد في المؤشرات الدولية في تحسين صورة الدولة على المستوى العالمي، مما يعزز ثقة الشركاء الدوليين والمستثمرين فيها.

4. **توجيه السياسات والاستراتيجيات:** تساعد المؤشرات الدول على تصميم استراتيجيات فعّالة للأمن السيبراني بناءً على بيانات دقيقة وموثوقة. كما تتيح مقارنة الأداء مع الدول الأخرى لتبني أفضل الممارسات.

5. **تعزيز التعاون الدولي:** تُبرز المؤشرات المجالات التي يمكن للدول أن تتعاون فيها مع الدول الأخرى، مثل تبادل المعلومات حول التهديدات السيبرانية أو المشاركة في تدريبات سيبرانية مشتركة.

6. **زيادة الوعي بالأمن السيبراني:** تُسهم المؤشرات في رفع مستوى الوعي بين الحكومات والمجتمع حول أهمية الأمن السيبراني وأثره على الأمن القومي والاقتصاد.

7. **تحفيز الابتكار والتطوير التقني:** تُشجع المؤشرات الدول على الاستثمار في تقنيات جديدة وتعزيز البحث العلمي في مجال الأمن السيبراني للوصول إلى مستويات أعلى من الحماية.

وهناك العديد من مؤشرات الآمن السيبراني تتباين فيما بينها من حيث جهة الإصدار وحدود التغطية الجغرافية والهدف منها، وبعد دراسة مسحية لبعض تلك المؤشرات أمكن تقسيمها إلى ثلاث فئات هي:

1- مؤشرات تهتم بتقييم تدابير الأمن السيبراني على مستوى الدول.

2- مؤشرات تهتم بتقييم تدابير الأمن السيبراني على مستوى الهيئات والمنظمات.

3- مؤشرات تهتم بجوانب اخري (أنواع الهجمات السيبرانية، برامج المكافحة الجديدة بالأسواق ...الخ) لتقييم تدابير الامن السيبراني

ونظرا لطبيعة الدراسة وأهدافها فسوف تقتصر المقارنة على المؤشرات التي تهتم بتقييم تدابير الأمن السيبراني بالدول ويوضح جدول (1) مقارنة بين اشهر تلك المؤشرات:

جدول (1) مؤشرات الأمن السيبراني الدولية

م	المؤشر	الجهة المطورة	عدد الدول بالمؤشر	منهجية البحث	عدد المؤشرات indicators	النتائج المقدمة Rank or Score
1	Cyber Maturity in the ASIA-PACIFIC Region	The Australian Strategic Policy Institute	23	Secondary	11	Score
2	National Cyber Security Index (NCSI)	Estonian e-Governance Academy & Estonian Foreign Ministry	160	Primary & Secondary	12	Rank & Score
3	Global Cybersecurity Index (GCI)	International Telecommunication Union	193	Primary & Secondary	20	Rank & Score
4	Kaspersky Cybersecurity Index	Kaspersky Lab & B2B International	21	Primary	3	Score
5	Asia-Pacific Cybersecurity Dashboard	BSA, Software Alliance	10	Secondary	31	none
6	Cyber Readiness Index 2.0 (CRI 2.0)	Potomac Institute for Policy Studies	125	Primary & Secondary	7	Score
7	National Cyber Power Index (NCPI)	the Belfer Center, Harvard Kennedy School	30	Secondary	7	Rank & Score

Rank & Score	12	Primary & Secondary	133	World Economic Forum in partnership with INSEAD	Network Readiness Index - NRI	8

في ضوء معطيات جدول (1) فقد تم اختيار المؤشرات (NCSI, GCI, NCPI, NRI) كأدوات لتقييم تدابير الأمن السيبراني في مصر للأسباب التالية:

1- أن الجهات المطورة لتلك المؤشرات هي جهات دولية ذات ثقل في المجال (أكاديمية الحكومة الإلكترونية الإستونية ووزارة الشؤون الخارجية الإستونية، الاتحاد الدولي للاتصالات (ITU)، جامعة هارفارد، والمنتدى الاقتصادي العالمي).

2- لم تركز تلك المؤشرات على نطاق جغرافي محدد مثل مؤشر (Asia-Pacific Cybersecurity Dashboard أسيا والمحيط الهادي) وانما امتدت تغطيتها إلى نطاق عالمي.

3- منهجية الحصول على البيانات والمعلومات لديها متنوعة وشاملة وتعتمد على البحث الثانوي Secondary وتُعنى بالحصول على البيانات من مصادر موجودة مسبقًا تم جمعها ونشرها من قبل جهات أخرى كما يعتمد على منهجية البحث الأولي Primary على جمع البيانات مباشرة من جهات عدة داخل الدولة.

4- تقدم تلك المؤشرات نتائج متنوعة في شكلين الأول Scoreيشير إلى الدرجة التي حصلت عليها الدولة بناءً على أدائها في معايير أو مؤشرات محددة. بالإضافة إلى Rank يشير إلى المرتبة التي حصلت عليها الدولة بالمقارنة بالدول الأخرى في نفس السياق.

ثالثاً: النتائج والتوصيات:

1- تقييم الآداء المصري في ضوء مؤشرات الأمن السيبراني العالمية لعام 2024:

1- مؤشر الأمن السيبراني العالمي (GCI): [32]

ينشر الاتحاد الدولي للاتصالات مؤشره العالمي للأمن السيبراني (GCI) منذ عام 2015، ونشر منه حتى الآن خمسة إصدارات (في أعوام 2015، 2017، 2018، و2020 و 2023). تجدر الإشارة إلى أن مؤشر (GCI) لا يقيس مستوى الأمن السيبراني بحد ذاته، بل هو مؤشر يعكس "**الالتزام**" بالأمن السيبراني، بناءً على منهجية تعتمد على البيانات التي تقدمها الدول الأعضاء، والتي يبلغ عددها 193 دولة.

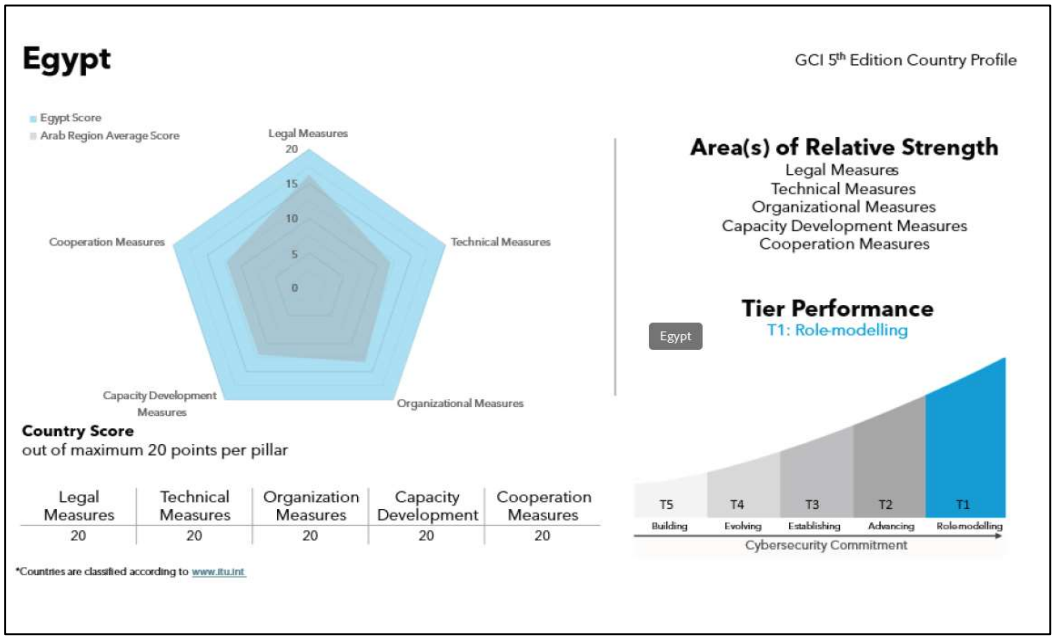
يعتمد المؤشر على استبيان يتألف من 150 سؤالًا. وفي الإصدارات الأخيرة، بدأ الاتحاد الدولي للاتصالات أيضًا في جمع البيانات من مصادر مفتوحة ويقوم مؤشر (GCI) بقياس التزامات الدول الأعضاء في مجال الأمن السيبراني عبر خمس ركائز رئيسية يتم قياسها من خلال (20) مؤشر فرعي كما يوضح جدول (2):

جدول (2) منهجية مؤشر الأمن السيبراني العالمي (GCI)

الركائز		مؤشرات القياس	الوزن النسبي
1- التدابير القانونية			20%
1/1	قانون الجريمة السيبرانية		
2/1	لوائح الأمن السيبراني		
2- التدابير التقنية			20%
1/2	فريق التصدي للطوارئ الحاسوبية/فريق التصدي للحوادث الحاسوبية /فريق التصدي للحوادث الأمنية الحاسوبية أو مركز ا لعمليات الأمنية، على الصعيد الوطني		
2/2	أفرقة التصدي للطوارئ الحاسوبية/أفرقة التصدي للحوادث الحاسوبية /أفرقة التصدي للحوادث الأمنية الحاسوبية أو مراكز العمليات الأمنية، على صعيد القطاعات		

3/2	الإطار الوطني لتنفيذ معايير الأمن السيبراني	
3- التدابير التنظيمية		20%
1/3	الاستراتيجية الوطنية للأمن السيبراني	
2/3	الوكالة المسؤولة	
3/3	مقاييس الأمن السيبراني	
4/3	استراتيجيات ومبادرات حماية الأطفال على الإنترنت	
4- تدابير تنمية القدرات		20%
1/4	حملات التوعية العامة في مجال الأمن السيبراني	
2/4	تدريب المهنيين العاملين في مجال الأمن السيبراني	
3/4	البرامج التعليمية المتعلقة بالأمن السيبراني في إطار المناهج الأكاديمية الوطنية	
4/4	برامج البحث والتطوير (R&D) في مجال الأمن السيبراني	
5/4	صناعة الأمن السيبراني الوطنية	
6/4	آليات تقديم الحوافز الحكومية	
5- تدابير التعاون		20%
1/5	الاتفاقات الثنائية في مجال الأمن السيبراني	
2/5	اتفاقات الأمن السيبراني المتعددة الأط راف المعقودة مع بلدان أخرى	
3/5	معاهدات المساعدة القانونية المتبادلة 25 (MLAT) المتعلقة بالأمن السيبراني	
4/5	الشراكات بين القطاعين العام والخاص (PPP)	
5/5	الشرا كات بين الوكالات	

ووفقا لتقييم المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات 2024" صنفت مصر ضمن دول الفئة الأولى والتي تضم 47 دولة من بين 193 دولة بالتقرير وتأتي مصر في المرتبة (9) عالميًا بنتيجة بلغت 100 نقطة وقد شهد أداؤها في مجال الأمن السيبراني تحسنًا ملحوظًا، حيث ارتفعت من المركز 27 في عام 2014 إلى المركز 23 في عام 2020. وصولا للترتيب الحالي.



شكل (1) مصر بمؤشر الامن السيبراني العالمي 2023

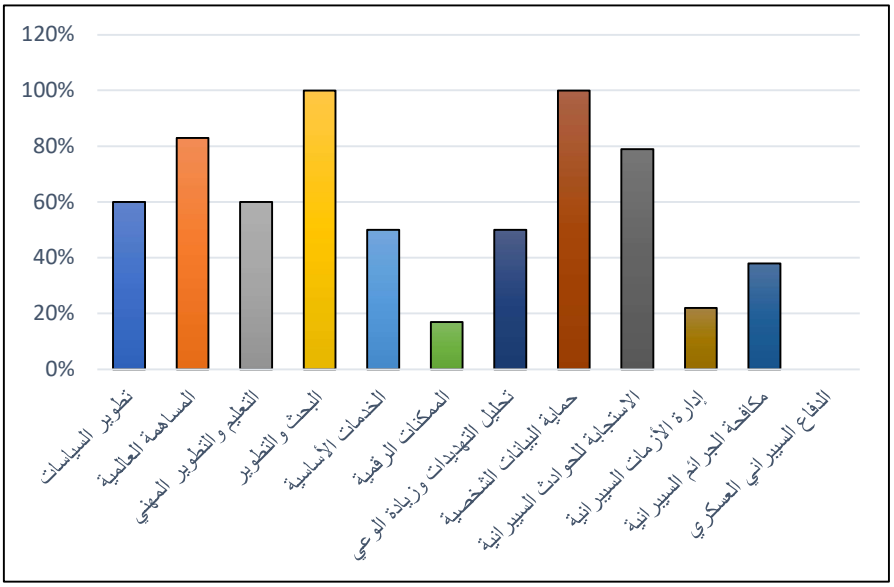
2- مؤشر الأمن السيبراني الوطني (NCSI) The National Cyber Security Index: [33]

تم إعداد مؤشر الأمن السيبراني الوطني (NCSI) من قبل أكاديمية الحوكمة الإلكترونية في إستونيا لقياس

قدرات الأمن السيبراني للحكومات(eGA) the Estonian e-Governance Academy ويستند هذا المؤشر إلى تقييم ثلاث ركائز أساسية (الإستراتيجية، والوقائية، والإستجابة) ويتم قياس هذه الركائز عبر12 مؤشر فرعي ويخصص لكل مؤشر وزن نسبي من النقاط وفقا لاهميته في منهج التقييم وقد جاء ترتيب مصر وفقًا لتقييم عام 2024 في الترتيب (42) عالميًا من بين (140) دولة بنتيجة بلغت 50.83 نقطة كما يوضح جدول (3) وهو مؤشر جيد يعبر عن تحسن ملحوظ في الأداء عن الترتيب المسجل عام 2021 حيث ارتفع ترتيب مصر من المركز 61 من 167 دولة في ذلك العام وصولا للترتيب الحالي.

جدول (3) تقييم أداء مصر في ضوء مؤشر الأمن السيبراني الوطني (NCSI) لعام 2023

الركائز	مؤشرات القياس	النقاط	النسبة
1- مؤشرات الأمن السيبراني الاستراتيجية			
1/1	تطوير السياسات	9/15	60%
2/1	المساهمة العالمية	5/6	83%
3/1	التعليم والتطوير المهني	6/10	60%
4/1	البحث والتطوير	4/4	100%
2- مؤشرات الأمن السيبراني الوقائية			
1/2	الخدمات الأساسية	6/12	50%
2/2	الممكنات الرقمية	2/12	17%
3/2	تحليل التهديدات وزيادة الوعي	6/12	50%
4/2	حماية البيانات الشخصية	4/4	100%
3- مؤشرات الأمن السيبراني الاستجابية			
1/3	الاستجابة للحوادث السيبرانية	11/14	79%
2/3	إدارة الأزمات السيبرانية	2/9	22%
3/3	مكافحة الجرائم السيبرانية	6/16	38%
4/3	الدفاع السيبراني العسكري	0/6	0%



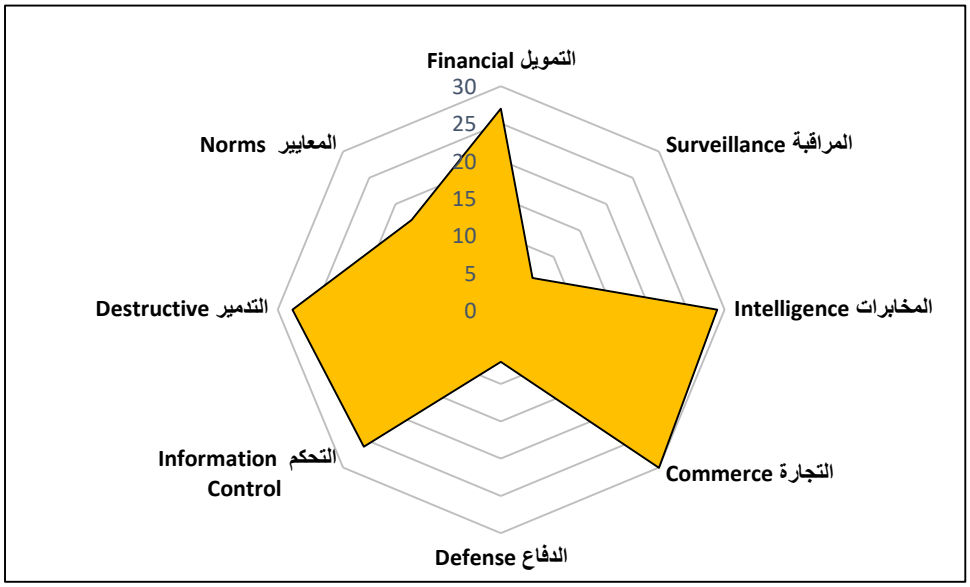
شكل (2) تقييم أداء مصر في ضوء مؤشر الأمن السيبراني الوطني (NCSI) لعام 2023

3- مؤشر القوى السيبرانية الوطنية (National Cyber Power Index (NCPI: [34]

مؤشر تم تقديمه لأول مرة عام 2020 من قبل جامعة هارفارد عبر مشروع Cyber Power Project التابع لكلية بيلفر للعلوم والسياسة الدولية. ويقيس NCPI القدرة السيبرانية لـ 30 دولة بناءً على سبعة أهداف وطنية تسعى إليها الدول باستخدام الوسائل السيبرانية ، وهي مسح الجماعات المحلية ومراقبتها، تقوية الدفاعات السيبرانية الوطنية وتعزيزها، التحكم في بيئة المعلومات ومعالجتها، جمع المعلومات الاستخبارية الأجنبية للأمن القومي، تحقيق مكاسب تجارية أو تعزيز نمو الصناعة المحلية، تدمير أو تعطيل البنية التحتية للعدو وقدراته، وأخيراً تحديد القواعد والمعايير التقنية السيبرانية الدولية. وبناءً على هذه الأهداف، يقيس مؤشر NCPI على وجه التحديد أهداف البلدان وقدراتها في ستة مجالات تشمل (المراقبة، الدفاع، التحكم في المعلومات، الاستخبارات، التجارة، والمعيير والأعراف) وقد جاء ترتيب مصر وفق تقرير 2023/2022 في المرتبة (24) بين (30) دولة وهى مرتبة متأخرة وعلى الرغم من ذلك يمكن استشعار تحسن طفيف خاصة بالمقارنة مع ترتيبها في المركز الأخير عام 2021/2020 وجاء تقييم مصر في الركائز عام 2023 على النحو التالي:

جدول (4) مصر في مؤشر القوى السيبرانية الوطنية (NCPI) 2022

الركيزة	التمويل Financial	المراقبة Surveillance	المخابرات Intelligence	التجارة Commerce	الدفاع Defense	التحكم Information Control	التدمير Destructive	المعايير Norms
الترتيب	27	6	29	30	7	26	28	17



شكل (3) مصر في مؤشر القوى السيبرانية الوطنية (NCPI) 2023

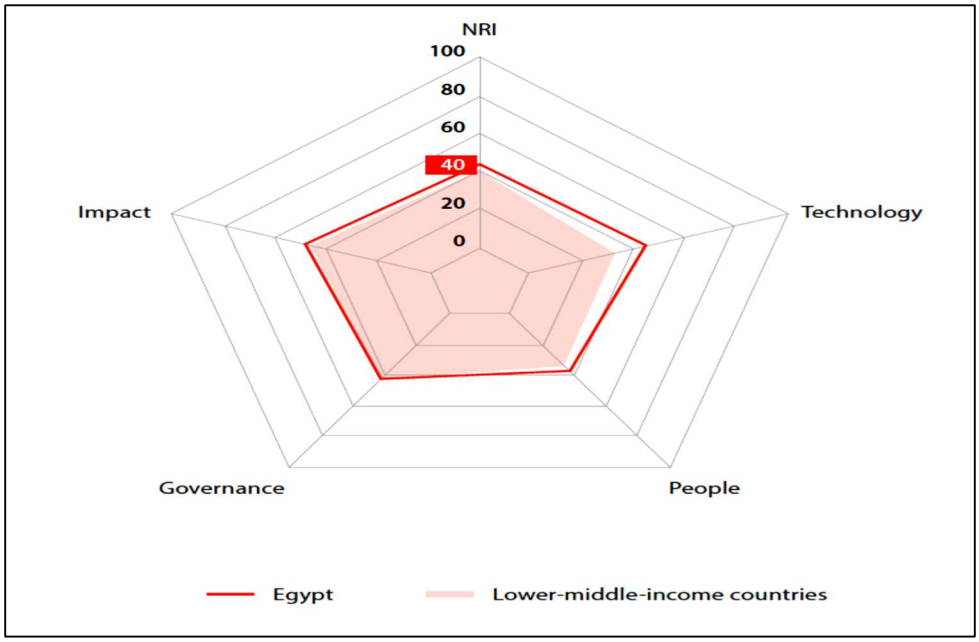
4- مؤشر الجاهزية الشبكية (Network Readiness Index – NRI): [35]

مؤشر الجاهزية الشبكية (NRI) هو تصنيف عالمي يقيس مدى جاهزية الدول للاستفادة من التكنولوجيا الرقمية والاتصال الشبكي لتحفيز التنمية الاقتصادية والاجتماعية تم إطلاقه لأول مرة في عام 2002 من قبل المنتدى الاقتصادي العالمي بالشراكة مع INSEAD في الوقت الحالي، يتم إدارته بواسطة مؤسسة Portulans

Institute. ويتكون المؤشر من 4 ركائز رئيسية، يتم قياسها بواسطة (12) مؤشر فرعي، وقد جاء ترتيب مصر وفق تقرير عام 2024 في المرتبة (85) بين 133 دولة، متأخرة بذلك عن ترتيبها في عام 2022 حيث سجلت الترتيب (73). وجاء تقييم مصر 2024 في الركائز الاربع على النحو الذي يوضحه جدول (5) التالي:

جدول (5) مصر في مؤشر الجاهزية الشبكية (Network Readiness Index – NRI) 2024

الركيزة	المؤشر الفرعي	الدرجة	الترتيب
1–التكنولوجيا (Technology)		44.83	56
1/1	– البنية التحتية الرقمية	74.79	38
1/2	– استخدام التكنولوجيا	28.59	55
1/3	– تقنيات المستقبل (إنترنت الأشياء، الذكاء الاصطناعي	31.12	83
2–الأفراد (People)		36.94	93
2/1	– المهارات الرقمية	44.62	84
2/2	– التعليم والتدريب	31.27	90
2/3	–المشاركة الرقمية للأفراد والشركات	34.93	79
3–الحوكمة (Governance)		46.99	99
3/1	– سياسات الخصوصية	31.97	98
3/2	– الأطر القانونية والتنظيمية	56.11	102
3/3	– تكافؤ الفرص	52.88	86
4– التأثير (Impact)		48.94	95
4/1	– التأثير على الاقتصاد	43.47	26
4/2	– تحسين جودة الحياة	41.53	114
4/3	– الابتكار الرقمي وريادة الأعمال	61.82	83



شكل (4) قيم مصر في مؤشر الجاهزية الشبكية 2024 (NRI)

2– إشكالية تحليل واقع الامن السيبراني في مصر في ضوء المؤشرات العالمية:

وبالنظر إلى النتائج التي كشفت عنها تقارير المؤشرات الأربع (GCI, NCSI, NPCI, NRI)، سوف نلاحظ

أن هناك تباين بين تلك النتائج. وبالدراسة والتحليل لأهداف ومنهجية بناء تلك المؤشرات، أمكن تحديد أسباب هذا التباين في العوامل التالية:

1- اختلاف نطاق التغطية والأهداف:

يُركز كل مؤشر على نطاق معين ويستهدف غاية مختلفة، مما يفسر التباين في النتائج. فعلى سبيل المثال، يُعنى مؤشر GCI بقياس النضج العام للأمن السيبراني بمستوى الدولة، بينما يستهدف مؤشر NCSI تقييم الإجراءات التقنية والقانونية للدولة، في حين يركز مؤشر NPCI اهتمامه بقياس القوة السيبرانية للدولة من حيث قدراتها الهجومية والدفاعية في الفضاء السيبراني، ويهدف مؤشر NRI إلى تقييم جاهزية الشبكات من حيث البنية التحتية الرقمية وقدرة الدولة على الاستفادة من تقنيات المعلومات والاتصالات. هذا التنوع في النطاق يؤدي إلى اختلاف النتائج النهائية لكل مؤشر.

2- الاختلاف في منهجيات القياس:

مؤشر GCI يركز بشكل أساسي على مدى التزام الدول بتطوير سياسات وتشريعات الأمن السيبراني، وتقييم الجهود المؤسسية والتعاون الدولي في هذا المجال. بالتالي، يمكن أن تحصل دولة على درجة عالية إذا أظهرت التزامًا قويًا بتطوير الإطار القانوني والتنظيمي، حتى لو لم تكن هناك نتائج فعلية ملموسة من حيث التطبيق العملي.

أما **مؤشرات NCSI, NPCI & NRI** فتعطي وزنًا أكبر للنتائج العملية ومدى كفاءة الأنظمة الأمنية المطبقة في مواجهة التهديدات السيبرانية الحقيقية. هذه المؤشرات تميل إلى تقييم الأداء الفعلي بدلًا من السياسات والخطط.

3- التفاوت الزمني لتحديث البيانات:

تعتمد المؤشرات على تقارير دورية قد تختلف في توقيت النشر وتحديث البيانات، مما يؤدي إلى تباين في انعكاس الأحداث والتطورات الأخيرة.

4- السياقات المحلية والإقليمية:

تختلف الدول من حيث جاهزيتها السيبرانية والقوة السيبرانية، ما يبرز الحاجة لتفسير النتائج في ضوء السياق المحلي الخاص بكل دولة. هذه الاختلافات قد تكون أكثر وضوحًا عند مقارنة الدول ذات الموارد المحدودة مع الدول ذات القدرات السيبرانية المتقدمة.

5- الاختلاف في الأولويات الوطنية:

تضع كل دولة أولويات مختلفة تتعلق بالأمن السيبراني، مثل تعزيز القوة السيبرانية، الاستثمار في البنية التحتية الرقمية، أو التركيز على الحماية القانونية، مما يؤدي إلى تفاوت في الأداء بين المؤشرات".

وعلى الرغم من عوامل التباين السابقة بين المؤشرات محل الدراسة، إلا أن هناك العديد من المرتكزات والمؤشرات الفرعية المشتركة التي يمكن البناء عليها لاستخلاص قائمة مرجعية شاملة تُسهم في تقييم أداء الأمن السيبراني المصري بشكل دقيق وفعّال. ويوضح جدول (6) هذه المرتكزات والمؤشرات الفرعية المقترحة.

جدول (6) المنهجية المقترحة لمؤشر الأمن السيبراني

الركيزة الرئيسية	المؤشرات الفرعية
1-الحوكمة والسياسات	- عدد التشريعات المتعلقة بالأمن السيبراني التي تم اعتمادها.
	- إنشاء هيئات وطنية مختصة بالأمن السيبراني.
	- مدي الالتزام بمعايير واطر الأمن السيبراني.
2-القدرات التقنية والبنية التحتية	- توفر مراكز العمليات الأمنية .(SOC)
	- جاهزية البنية الشبكية للتعامل مع التهديدات السيبرانية.
	- وجود منصات رقمية لتنسيق الجهود الأمنية بين القطاعات.
3-التعاون الإقليمي والدولي	- عدد الاتفاقيات الموقعة مع دول أخرى للتعاون السيبراني.
	- المشاركة في التمارين الإقليمية والدولية لمحاكاة الهجمات السيبرانية.
	- التفاعل مع المنظمات الدولية مثل ENISA والاتحاد الأوروبي.
4-إدارة المخاطر والمرونة السيبرانية	- عدد الهجمات السيبرانية التي تم رصدها والاستجابة لها.
	- وجود خطط طوارئ للتعامل مع حوادث الفضاء السيبراني.
	- عدد الاختبارات الدورية للتأكد من جاهزية الأنظمة ضد التهديدات.
5-التوعية وبناء القدرات	- عدد البرامج التدريبية في مجال الأمن السيبراني.
	- مستوى إدراج الأمن السيبراني في المناهج التعليمية.
	- حملات التوعية العامة التي تهدف إلى نشر ثقافة الأمن السيبراني.
6-الاستثمارات والابتكار	- حجم الميزانية الوطنية المخصصة للأمن السيبراني.
	- عدد المشاريع البحثية في مجال الأمن السيبراني.
	- عدد الشركات الناشئة المتخصصة في الأمن السيبراني المدعومة من الحكومة

في ضوء المرتكزات والمؤشرات الفرعية المقترحة في جدول (6)، يمكننا تحليل نقاط التباين والتشابه بين المؤشرات الأربع (GCI, NCSI, NPCI, NRI) كما هو موضح في جدول (7).

جدول (7) مقارنة بين المؤشرات في ضوء المرتكزات والمؤشرات الفرعية المقترحة لتقييم تدابير الأمن السيبراني في مصر

الركيزة الرئيسية	• مؤشر GCI	• مؤشر NCSI	• مؤشر NCPI	• مؤشر NRI
1- الحوكمة والسياسات	• يقيّم وجود استراتيجيات سيبرانية شاملة على مستوى الدولة. • يقيم مستوى التنسيق بين الهيئات الحكومية والقطاع الخاص. • يقيم الامتثال للقوانين والتشريعات الدولية.	• تقييم استراتيجيات الأمن السيبراني الوطنية. • يقيم وجود هيئات حكومية متخصصة بالأمن السيبراني.	• يقيم مدى تعزيز الحوكمة المؤسسية للأمن السيبراني. • يقيم مدى تطور الإطار القانوني والسياسات الوطنية.	• يقيم جاهزية الشبكات الوطنية وتنظيم السياسة الرقمية. • يقيم مدى التنسيق بين السياسات الوطنية في المجال
2- القدرات التقنية والبنية التحتية	• يقيم القدرة على مواجهة التهديدات باستخدام تقنيات حديثة • يقيم مدى القدرة على تطبيق إجراءات الكشف عن الهجمات	• تقييم قدرة الدولة على حماية البنية التحتية الحيوية. • يقيم وجود مراكز عمليات الأمن السيبراني (SOC)	• يقيم مدى تعزيز القدرات التقنية في مجال الأمن السيبراني على مستوى المؤسسات • يقيس حجم الاستثمار في البنية التحتية الرقمية	• يقيم مستوى الابتكار واستخدام التقنيات في البنية التحتية الرقمية. • يقيم مدى جاهزية الشبكات في التعامل مع التهديدات السيبرانية
3- التعاون الإقليمي والدولي	• قياس مستوى التعاون الدولي بين الدول في مجال الأمن السيبراني • يقيم مستوى الشراكات مع منظمات دولية مثل ENISA.	• يقيم التعاون الإقليمي والدولي في مجال تبادل المعلومات والتهديدات.	• يقيم حجم التعاون المؤسسي على مستوى الدولة والقطاع الخاص. • يقيم التعاون مع المنظمات الدولية في مجال تبادل المعلومات	• يقيم قدرة الدولة على التنسيق مع الدول الأخرى في البنية التحتية الرقمية. • يقيم التعاون بين الدول في مجالات الشبكات العالمية.

4- إدارة المخاطر والمرونة السيبرانية	• تقييم مستوى الاستجابة للأزمات السيبرانية وإدارة المخاطر	• يقيم وجود خطط للطوارئ وتدابير لمواجهة الهجمات السيبرانية • يقيم خطط اختبار جاهزية الأنظمة الوطنية.	• يقيم قدرة الدولة على التكيف مع المخاطر السيبرانية المستجدة.	• قياس مستوى مرونة الشبكات أمام التهديدات السيبرانية في الدولة.
5- التوعية وبناء القدرات	• يقيم وجود برامج تدريبية متخصصة لتطوير المهارات في الأمن السيبراني. • يقيم حجم ثقافة الوعي بالأمن السيبراني بين المواطنين.	• تقييم مستوى التعليم الأمني السيبراني في المؤسسات التعليمية. • يقيم خطط تدريب العاملين في القطاع العام والخاص على الأمن السيبراني.	• قياس مستوى تطور المهارات في الأمن السيبراني داخل المؤسسات • يقيم برامج التدريب الموجهة للأفراد في مواجهة التهديدات السيبرانية.	• يقيم مدى جاهزية القوى العاملة في مجال الشبكات الرقمية والتقنيات الحديثة.
6-الاستثمارات والابتكار	• قياس حجم الاستثمارات في مجال البحث والتطوير السيبراني. • يقيم مدى تطبيق حلول مبتكرة للتصدي للهجمات.	• قياس الاستثمارات الوطنية في البنية التحتية للأمن السيبراني • يقيم حجم الابتكار في مجال الأمن السيبراني من خلال المشروعات البحثية.	• يقيس حجم استثمار الدولة في الابتكار وتطوير القدرات السيبرانية على المستوى المحلي.	• يقيس حجم الاستثمارات في شبكات البنية التحتية الرقمية. • يقيم مدى دعم الابتكار في تقنيات الأمن السيبراني ومرونة الشبكات.

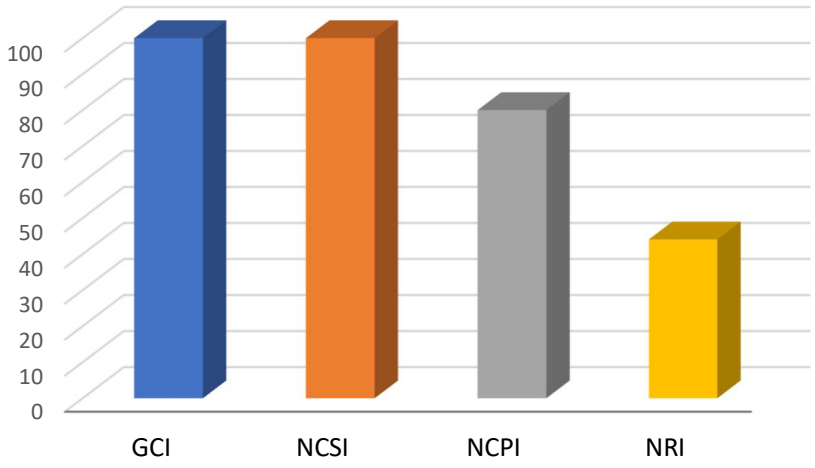
3- تحليل نقاط القوة والضعف في أداء الأمن السيبراني في مصر وفقاً للمؤشرات العالمية والمرتكزات المقترحة:

3/1 الحوكمة والسياسات:

تُعتبر الجرائم في الفضاء السيبراني رخيصة ومربحة ومنخفضة المخاطر، مما يبرز أهمية وجود بيئة آمنة ومنظمة. ويُعد القانون أداة فعالة لتحقيق ذلك، حيث يساعد الدول في وضع الأسس القانونية اللازمة، وتطوير آليات استجابة قوية للتحقيق والمقاضاة، وفرض عقوبات رادعة لضمان حماية استقرار الفضاء السيبراني.

جدول (8) تحليل أداء مصر في مجال الحوكمة والسياسات المتعلقة بالأمن السيبراني وفق المؤشرات الدولية للأمن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%100	%80	%44.08	%81.02	جيد جدا



شكل (5) تحليل أداء مصر في مجال الحوكمة والسياسات وفق المؤشرات الدولية للأمن السيبراني

ولما كان الهدف من الإجراءات القانونية ليس فقط إصدار اللوائح، بل أيضًا تنفيذها وتطبيقها. فقد أظهرت مصر أداءً

جيدًا في البعد القانوني وفقًا للأطر الدولية للمراقبة. فوفقًا **لمؤشر الأمن السيبراني العالمي (GCI)** لعام 2024، حصلت مصر على درجة تقييم (20/20) بمتوسط (100%) في مؤشر التدابير القانونية كما وبلغت درجة مصر في **مؤشر الأمن السيبراني الوطني (NCSI)** لعام 2024 (100%) في ثلاث مؤشرات هي؛ المؤشر الفرعي "الجرائم الإلكترونية في القانون الوطني" والمؤشر الفرعي "أحكام القانون الاجرائي" والمؤشر الفرعي "حماية البيانات الشخصية" وبعد احتساب متوسط مجموع درجات المؤشرات الثلاث تكون مصر قد حصلت على (100%) نقطة. أما في **مؤشر القوة السيبرانية NCPI** فقد تناول تقييم الحوكمة والسياسات السيبرانية في مؤشرين فرعيين هما "مؤشر المراقبة" وجاءت مصر بالترتيب (6/30) وبدرجة (54.84/60) وبنسبة (90.8%)، "ومؤشر التجارة" في الترتيب (30/30) وبدرجة (4/34) وبنسبة (11.67%) وبحساب متوسط درجات مصر في هاذين المؤشرين بلغ حوالي (51.32%) درجة ، في حين غطي **مؤشر الجاهزية الشبكية (NRI)** اللوائح القانونية بمرتكز الحوكمة ومن خلال المؤشر الفرعي "سياسات الخصوصية" حققت مصر درجة (31.97%) ومؤشر "الاطر التنظيمية والقانونية" وحققت درجة (56.11%) وبحساب متوسط درجات مصر في هاذين المؤشرين بلغ حوالي (44.08%) درجة وبالتالي فإن المتوسط العام للأداء القانوني لمصر بناءً على تقييم هذه المصادر الأربع (مؤشر GCI، مؤشر NGCI، ومؤشر NCPI ومؤشر NRI) يبلغ حوالي (100/81.02) وهي قيمة جيدة جداً تعكس أن مصر قد حققت نجاحًا ملحوظاً في الجانب القانوني والتشريعي الخاص بالأمن السيبراني ومكافحة الجرائم السيبرانية.

نقاط القوة:

1- التشريعات المتعلقة بالأمن السيبراني التي تم اعتمادها. [36]

في السنوات الأخيرة، أولت مصر اهتمامًا كبيرًا بتطوير الإطار التشريعي والتنظيمي للأمن السيبراني لحماية البنية التحتية المعلوماتية ومكافحة الجرائم السيبرانية. [٨٨] فصدر قانون تنظيم خدمات الاتصالات **(رقم 10 لسنة 2003)**، والقانون **(رقم 15 لسنة 2004)** بتنظيم التوقيع الالكتروني، وكان قرار مجلس الوزراء **(رقم 2259 لسنة 2014)** هو الأكثر شمولًا فيما يتعلق بانشاء المجلس الاعلي للامن السيبراني. وقانون مكافحة الإرهاب **(رقم 94 لسنة 2015)** يتضمن بنودًا متعلقة بمكافحة الإرهاب السيبراني والتصدي لاستخدام التكنولوجيا والإنترنت في الترويج للأفكار الإرهابية أو التنسيق للهجمات. كما أصدرت الحكومة المصرية العديد من اللوائح القانونية المستقلة كقانون مكافحة جرائم تقنية المعلومات **(رقم 175 لسنة 2018)**، وقانون الجرائم الإلكترونية **(رقم 175 لسنة 2018)** ، وقانون حماية المستهلك في السوق الرقمي **(رقم 181 لسنة 2018)**، بالإضافة إلى التعديلات الدستورية في 23 أبريل 2019 حيث نصت **(المادة 31)** من الدستور المصري على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"، كما أصدرت مصر قانون حماية البيانات الشخصية **(رقم 151 لسنة 2020)**.

2- الهيئات الوطنية المختصة بالأمن السيبراني.

• أكد الاتحاد الدولي للاتصالات أن مصر اتخذت خطوات مهمة لدعم الأمن السيبراني، من أهمها: تأسيس مجلس أعلى للأمن السيبراني عام 2015 ، ووضع استراتيجية وطنية للأمن السيبراني 2017 -2021 ، إلى جانب تأسيس المركز الوطني للاستعداد لطوارئ الحاسبات والشركات EG-CERT.

3- مدي الالتزام بمعايير واطر الأمن السيبراني.

أقر المركز الوطني للاستعداد لطوارئ الحاسبات والشركات EG-CERT مجموعة من الأطر ومعايير حوكمة الأمن السيبراني للمؤسسات بهدف مساعدتها على الحماية من الهجمات الإلكترونية. وتوفر هذه الأطر والمعايير مجموعة من

أفضل الممارسات التي يمكن اتباعها لتحسين وضع الأمن السيبراني لديها. [37]

نقاط الضعف:

على الرغم من الجهود المبذولة لتحسين البنية التشريعية للأمن السيبراني في مصر إلا أن هناك العديد من التحديات التي تواجهها في هذا المجال:

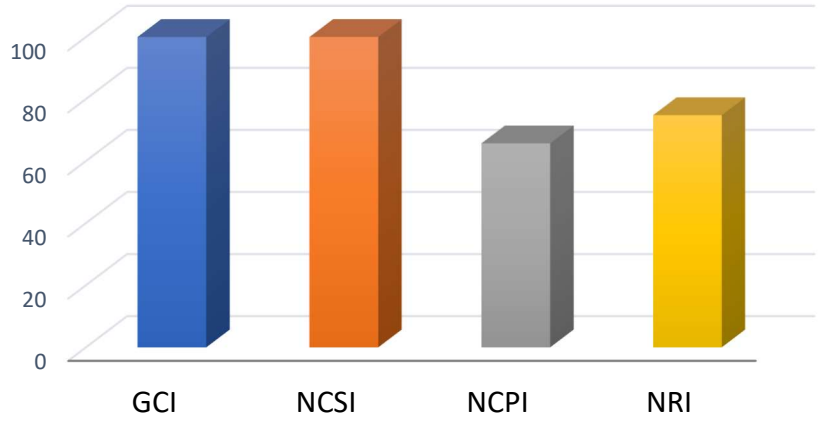
- القوانين المتعلقة بالأمن السيبراني في مصر موجودة ولكنها متفرقة كمواد في قوانين مختلفة مثل قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية وقانون مكافحة الإرهاب في حين لم يصدر حتى الآن إطار قانوني موحد يعرف ماهية الامن السيبراني ويغطي جميع جوانبه بشكل شامل مثل حماية البنية التحتية الحرجة، والحوكمة، والتعاون الدولي.
- في ظل تسارع التهديدات السيبرانية فإن القوانين الحالية تحتاج إلى تحديث دوري لمواكبة التطورات التقنية والتهديدات السيبرانية المتجددة وهو مايمثل تحديا أمام المشرع المصري.
- نقص كوادر إنفاذ القانون المؤهلة والمدربة لتنفيذ قوانين الأمن السيبراني بشكل فعال كما أن بعض الجهات قد تفتقر إلى الوعي الكامل بالمتطلبات القانونية.
- ضعف التشريعات التي تلزم الجهات المسؤولة عن البنية التحتية بتطبيق تدابير أمنية صارمة. ترتبط بالأمن السيبراني.
- عدم صدور لائحة تنفيذية لقانون حماية البيانات الشخصية.
- رغم شمولية اللوائح القانونية من منظور الأمن الوقائي، إلا أن الإطار القانوني يبدو أقل قوة فيما يتعلق بضمان الحقوق وحماية البيانات الشخصية والحريات على الإنترنت.
- البطء في تسوية القضايا والنزاعات في مجال الامن السيبراني .

3/2 القدرات التقنية والبنية التحتية:

تطوير القدرات التقنية والبنية التحتية التكنولوجية عنصر أساسي لتعزيز الأمن السيبراني، ورغم التباين بين المؤشرات العالمية محل الدراسة في تقييم هذه القدرات، إلا أنها تتفق على ثلاث ركائز رئيسية: كفاءة مشغلي البنية التحتية، جاهزية الشبكات لمواجهة التهديدات، والمنصات الرقمية لتنسيق الجهود الأمنية بين القطاعات.

جدول (9) تحليل أداء مصر في مجال القدرات التقنية والبنية التحتية وفق المؤشرات الدولية للأمن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%100	%65.7	%95.50	%90.3	ممتاز



شكل (6) تحليل أداء مصر في مجال القدرات التقنية والبنية التحتية وفق المؤشرات الدولية للأمن السيبراني

في ضوء منهجية مؤشرات التقييم لم يتناول **مؤشر الأمن السيبراني العالمي (GCI)** تقييم تقني للبنية التحتية" وأنما اهتم

بتقييم التدابير التقنية لحماية البنية التحتية وقد حصلت مصر على درجة (20/20) وبنسبة (100%) كذلك في **مؤشر الأمن السيبراني الوطني (NCSI)** فقد تم تناول البنية التحتية من منظور تقييم مشغلى البنية التحتية للمعلومات في المؤشر الفرعي " "تحديد البنية التحتية للمعلومات الحيوية"" وقد حصلت مصر فيه على درجة (3/3) بنسبة (100%) أما في **مؤشر القوة السيبرانية NCPI** فقد تناول تقييم البنية التحتية في ثلاث مؤشرات فرعية هى "مؤشر المراقبة" وجاءت مصر بالترتيب (6/30) وبدرجة (54.84/60) وبنسبة (90.8%)، "ومؤشر الدفاع " في الترتيب (7/30) وبدرجة (52.38/60) وبنسبة (87.3%) ومؤشر "التحكم بالمعلومات" في الترتيب (26/30) وبدرجة (12.41) وبنسبة (19%) وبحساب متوسط درجات مصر في هذه المؤشرات بلغ حوالي (65.7%) درجة ، في حين غطي **مؤشر الجاهزية الشبكية (NRI)** جاهزية البنية التحتية الشبكية للأمن السيبراني بمرتكز الحوكمة حيث حققت مصر الترتيب (30) بدرجة (95.50%) وبالتالي فإن المتوسط العام لجاهزية البنية التحتية لمصر بناءً على تقييم هذه المصادر الأربع (مؤشر GCI، مؤشر NGCI، ومؤشر NCPI ومؤشر NRI) يبلغ حوالي (100/90.3) وهي قيمة ممتازة تعكس أن مصر قد حققت نجاحًا ملحوظاً في الجانب القدرة التقنية والبنية التحتية الخاصة بالحماية من الهجمات السيبرانية.

نقاط القوة:

1- مشغلي البنية التحتية الحيوية للمعلومات.

- المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) [38] يُعد بمثابة مركز وطني مسؤول من الجهاز القومي لتنظيم الاتصالات (NTRA) ويعمل كمركز وطني للرد على الحوادث السيبرانية، ويقدم خدمات تحليل التهديدات، وتنسيق الاستجابة مع الهيئات الحكومية، ويدعم قطاعات حيوية مثل الصحة، الطاقة، والنقل في حماية شبكاتها الرقمية.
- مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي (EG-FinCIRT) [39] هو وحدة متخصصة تهدف إلى حماية البنية التحتية الرقمية للنظام المالي والمصرفي في مصر.
- تلعب الهيئة القومية لتنظيم الاتصالات (NTRA) دورًا حيويًا في الإشراف على قطاع الاتصالات، بما في ذلك البنية التحتية الحيوية للمعلومات. وتتمثل مهمتها في ضمان أمن ومرونة شبكات وخدمات الاتصالات التي تُعد جزءًا من البنية التحتية الحيوية للمعلومات. وقد أصدرت الهيئة عدة أطر تنظيمية مختلفة.
- تم إنشاء المجلس الأعلى للأمن السيبراني المصري " (ESCC) [40] يعتمد تقييم مستوى الأمان والتصاريح والمواصفات للأشخاص العاملين في البنى التحتية الحيوية للاتصالات والمعلومات."
- تم انشاء المركز المصري للاستجابة لطوارئ الحاسب الالي "سيرت" في عام 2012 بهدف توفير نظام مبكر ضد البرمجيات الخبيثة والهجمات الالكترونية ضد البنية التحتية الحيوية للمعلومات المصرية.

2- جاهزية البنية الشبكية للتعامل مع التهديدات السيبرانية.

- صنف مؤشر مصر من الدول المتقدمة من حيث تدابير الأمن السيبراني حيث جاءت في مؤشر الجاهزية الشبكية NRI في الترتيب (30) من بين (133) دولة بنقاط (100/90.3)

3- المنصات الرقمية لتنسيق الجهود الأمنية بين القطاعات:

في مصر يتم استخدام عدد من **المنصات الأمنية السيبرانية** داخل مراكز عمليات الأمن السيبراني (SOC) لبعض القطاعات الحكومية أو القطاع الخاص:

القطاع الحكومي:

- **المركز المصري للاستجابة للطوارئ المعلوماتية (EG-CERT)** يستخدم منصات SIEM (Security Information

(and Event management مثل IBM QRadar لرصد وتحليل الحوادث كما يعتمد على أنظمة SOAR لتحسين الاستجابة للحوادث، ويدمج أدوات تحليل التهديدات مثل Threat Intelligence Platforms للتنبؤ بالتهديدات المستقبلية، وقد تم تطوير البنية التحتية لمنصة المركز للتوافق مع المعايير الدولية والتوجيهات مثل NIS2.

- **مركز SOC للبنك المركزي المصري** ويعتمد على منصات CrowdStrike Falcon وCarbon Black لحماية النقاط النهائية ويستخدم أنظمة كشف التهديدات (IDS/IPS) لمراقبة الشبكات المالية، بالإضافة إلى منصة IBM QRadar للتحليل المتقدم للتهديدات.
- **مركز SOC الخاص بشركة المصرية للاتصالات WE** يستخدم أدوات مثل Cisco Secure X ومنصات SIEM لمراقبة البنية التحتية.
- **مركز SOC بقطاع البترول والغاز** يعتمد على أدوات حماية البنية التحتية الحرجة مثل Palo Alto Networks وDarktrace. كما يتم استخدام أنظمة إدارة نقاط الضعف (Vulnerability Management) مثل Nessus لتحليل الثغرات.

القطاع الخاص:

- شركات التكنولوجيا الكبيرة العاملة في مصر مثل IBM وCisco تعتمد على منصات SIEM. وأدوات SOAR لتحليل البيانات.
- شركات قطاع الاتصالات مثل شركات اورانج وفودافون تعتمد على حلول متطورة مثل **Elastic Stack** و**ThreatConnect** لتحليل البيانات وتبادل المعلومات.
- البنوك الخاصة مثل بنك**CIB** وبنك **QNB**، لديها مراكز SOC تعتمد على أدوات حماية النقاط النهائية (Endpoint Detection and Response – EDR) وأنظمة كشف ومنع التهديدات.

نقاط الضعف

مصر تواجه مجموعة من التحديات المتعلقة بالبنية التحتية التكنولوجية التي تؤثر على قدرتها على تحقيق مستوى عالٍ من الأمن السيبراني مقارنة بالمؤشرات العالمية مثل مؤشر الأمن السيبراني العالمي (GCI)، والمؤشر الوطني للأمن السيبراني (NCSI)، ومؤشر القوة السيبرانية (NCPI). مؤشر الجاهزية الشبكية (NRI) ومن أبرز التحديات:

- لا توجد منصات وطنية خاصة بكافة القطاعات الحيوية لتنسيق الجهود الأمنية بين القطاعات المختلفة.
- نقص العاملين المؤهلين لإدارة وصيانة البنية التحتية الرقمية وفقًا للمعايير العالمية مما يؤدي إلى تأخير في تنفيذ استراتيجيات الأمن السيبراني والاستجابة للحوادث.
- قلة الاستثمارات في التقنيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء لدعم الأمن السيبراني مما يقلل من القدرة على تحسين كفاءة أنظمة الأمن السيبراني واستباق التهديدات المتطورة.
- عدم وجود وعي كافٍ حول أهمية حماية البنية التحتية الرقمية مما يؤدي إلى تجاهل إجراءات الأمان الأساسية، ويجعل الأنظمة أكثر عرضة للهجمات السيبرانية.

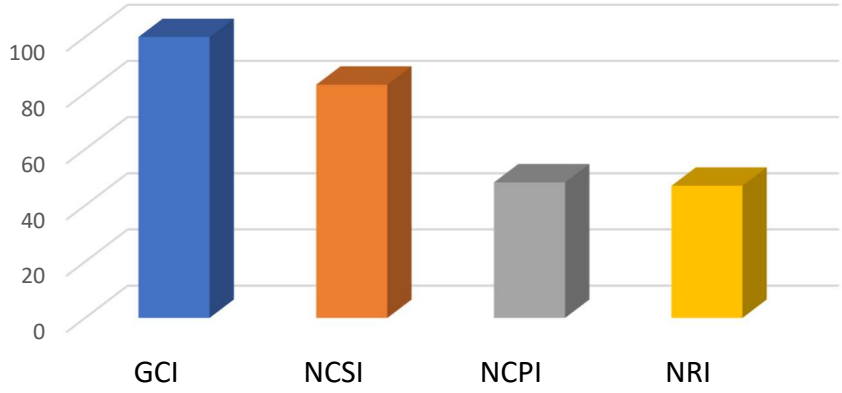
3/3- التعاون الإقليمي والدولي:

يعد التعاون الإقليمي والدولي في مجال الأمن السيبراني ضروري لمواجهة التهديدات العابرة للحدود، حيث يعزز تبادل المعلومات والخبرات، ويُسهم في تطوير استراتيجيات موحدة لمكافحة الجرائم السيبرانية. كما يدعم بناء قدرات الدول الأقل تجهيزًا لضمان الأمن الرقمي العالمي ويعرض جدول (10) تحليل لأداء مصر في مجال التعاون

الإقليمي والدولي المتعلق بالأمن السيبراني وفق ثلاث مؤشرات تشمل؛ مؤشر الاتفاقات الموقعة مع دول أخرى للتعاون السيبراني، مؤشر المشاركة في التمارين الإقليمية والدولية لمحاكاة الهجمات السيبرانية، ومؤشر التفاعل مع المنظمات الدولية.

جدول (10) تحليل أداء مصر في مجال التعاون الإقليمي والدولي وفق المؤشرات الدولية للأمن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%83	%48.2	%46.99	%69.5	جيد



شكل (7) تحليل أداء مصر في مجال التعاون الإقليمي والدولي وفق المؤشرات الدولية للأمن السيبراني

حققت مصر أداءً جيداً وإن كان اقل من أدائها في المؤشرين السابقين فوفقًا **لمؤشر الأمن السيبراني العالمي (GCI)** لعام 2024، حصلت مصر على درجة تقييم (20/20) ممتاز بمتوسط (100%) بمؤشر تدابير التعاون كما وبلغت درجة مصر في **مؤشر الأمن السيبراني الوطني (NCSI)** لعام 2024 (83%) في مؤشر " المساهمة العالمية". أما في **مؤشر القوة السيبرانية NCPI** فقد تناول تقييم التعاون الدولي في أربع مؤشرات فرعية هى "الأعراف NORMS" وجاءت مصر بالترتيب (17/30) وبدرجة (31.34/60) وبنسبة (52%)، "ومؤشر الدفاع " في الترتيب (7/30) وبدرجة (53.8/65) وبنسبة (82.7%) ومؤشر "الاستخبارات" في الترتيب (29/30) وبدرجة (6.10) وبنسبة (10%) وبحساب متوسط درجات مصر في هذه المؤشرات بلغ حوالي (65.7%) درجة ، في حين غطي **مؤشر الجاهزية الشبكية (NRI)** التعاون بمرتكز الحوكمة (Governance) حيث حققت مصر درجة (46.99%) وبالتالي فإن المتوسط العام لجاهزية البنية التحتية لمصر بناءً على تقييم هذه المصادر الأربع (مؤشر GCI، مؤشر NGCI، ومؤشر NCPI ومؤشر NRI) يبلغ حوالي (100/69.5) وهي قيمة جيدة نوعاً ما.

نقاط القوة

1- الاتفاقيات الموقعة مع دول أخرى للتعاون السيبراني

وقعت مصر العديد من الاتفاقات مع العديد من الدول مثل:

الاتفاقات الدولية:

- اتفاقية الشراكة الاستراتيجية والشاملة بين جمهورية مصر العربية والاتحاد الأوروبي في عام 2024[41]
- اتفاقية التعاون بين مصر وروسيا في عام 2018 في مجال الأمن السيبراني على مستوى البنية التحتية الرقمية.

- اتفاقية التعاون بين مصر والهند عام 2023 في مجال الأمن السيبراني. [42]
- اتفاقية التعاون بين مصر وماليزيا في مجال الأمن السيبراني. [43]

الاتفاقات العربية:

- اتفاقية مصر والإمارات لتعزيز التعاون في مجال الأمن السيبراني عام 2018 لدعم وتعزيز الأمن السيبراني من خلال تدريب الكوادر، تبادل المعلومات، وتطوير آليات استجابة مشتركة.
- اتفاقية مصر والسعودية لتعزيز التعاون في مجال الأمن السيبراني عام 2020 لتبادل المعلومات والخبرات حول حماية الأنظمة الرقمية ومكافحة الهجمات السيبرانية.
- اتفاقية بين مصر والأردن للتعاون في مجال الأمن السيبراني2020 لتعزيز التنسيق المشترك في مواجهة الهجمات السيبرانية، وحماية الأنظمة الحساسة. [44]
- توقيع مذكرة تفاهم للتعاون بين مصر والجزائر في مجال الاتصالات وتكنولوجيا المعلومات في يونيو 2023 بهدف تبادل الخبرات في مجال الأمن السيبراني. [45]

الاتفاقات مع الشركات العالمية:

- اتفاقية التعاون مع شركة ترينـد مايكرو trend-micro 2022 [46]
- اتفاقية التعاون مع كاسبرسكي Kaspersky [47]

2- المشاركة في التمارين الدولية لمحاكاة الهجمات السيبرانية.

رصدت المؤشرات مشاركة مصر بفعالية في العديد من التمارين الإقليمية والدولية لمحاكاة الهجمات السيبرانية ومنها:

التمارين الدولية:

- **تمرين "Arab Cyber Drill"** الثامن وتنظمه جامعة الدول العربية بالتعاون مع هيئات الأمن السيبراني في الدول العربية. يهدف إلى محاكاة الهجمات السيبرانية التي قد تستهدف أنظمة المؤسسات الحكومية والبنية التحتية الحيوية في الدول العربية. [48]
- مناورة تقييم الجاهزية الدولية **CyberEX2020** وفاز المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بالمركز الثاني، مجتازًا جميع مراحل المناورة بنجاح وفي زمن قياسي.
- المناورة السيبرانية الـ11 التي ينظمها المركز الإقليمي العربي للأمن السيبراني تحت مظلة الاتحاد الدولي للاتصالات (ITU-ARCC)[49]

التمارين المحلية:

في اطار برنامج مناورة سيبرانية 360 ينظم المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) مناورة سيبرانية افتراضية بمشاركة العديد من الهيئات والجهات الحكومية بهدف اختبار مدى استجابة وجاهزية قطاعات البنية المعلوماتية الحرجة في الدولة المصرية لمواجهة أية تهديدات أو حوادث سيبرانية، عن طريق محاكاة سيناريوهات هجمات سيبرانية. [50]

3- التفاعل مع المنظمات الدولية:

رصدت المؤشرات تفاعل مصر مع بعض الجهات الدولية مثل:

- التعاون بين المركز الوطني للاستعداد لطوارئ الحاسب والشبكات **(EG|CERT)** ومنظمة التعاون الإسلامي للمراكز الوطنية للأمن السيبراني والسلامة المعلوماتية **(OIC-CERT)** [51]
- اتفاقية تعاون بين المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) والمركز الإقليمي العربي للأمن السيبراني بالاتحاد الدولي للاتصالات (ITU-RCC) بسلطنة عمان في مجال الأمن السيبراني. [52]

نقاط الضعف

هناك بعض العوامل التي رصدتها المؤشرات تؤثر على الأداء المصري في هذا المرتكز وهي:

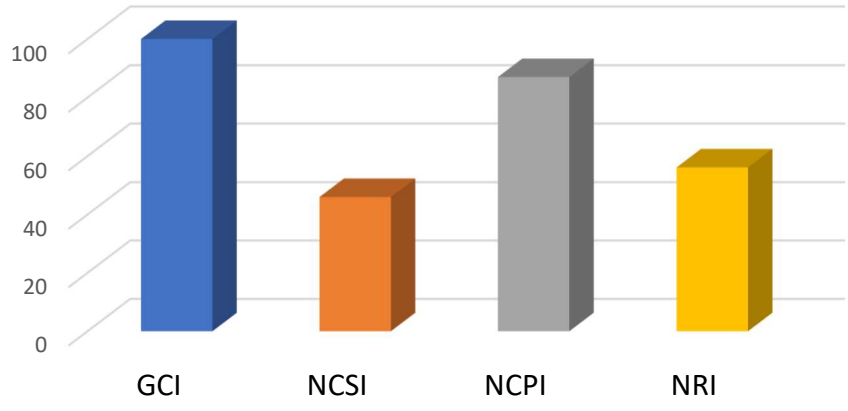
- تركز مصر على حماية البنية التحتية الحيوية كأولوية قصوى، إلا أنها لا تولي نفس القدر من الاهتمام لحماية البيانات الشخصية، مما قد يحد من فعالية التعاون مع دول أخرى تعتبر حماية البيانات الشخصية أولوية رئيسية لتعزيز حقوق الإنسان.
- نتيجة عدم وجود إطار قانوني مصري موحد يعرف ماهية الامن السيبراني ويغطي جميع جوانبه بشكل شامل مثل حماية البنية التحتية الحرجة، والحوكمة، والتعاون الدولي. أدى الى بطء توقيع الاتفاقات وتاخر تنفيذ المشاريع المشتركة.
- تواجه مصر صعوبات في إقناع الدول أو الجهات الشريكة بمشاركة معلومات حساسة حول الهجمات أو نقاط الضعف.
- وجود مصر في وسط العديد من التوترات الأقليمية والعالمية بين التكتلات الدولية وسياسة استقطاب الدول تعيق التعاون الدولى.

3/4 إدارة المخاطر والمرونة السيبرانية:

يقصد بمفهوم إدارة المخاطر السيبرانية Cyber Risk Management إجراءات الدول لتحديد وتقييم ومعالجة التهديدات التي تواجه الأنظمة والبنية التحتية الرقمية لتقليل تأثيرها، من خلال تقييم نقاط الضعف، وتطبيق خطط وقائية، ورصد الأنظمة باستخدام الذكاء الاصطناعي لاكتشاف التهديدات المحتملة. أما المرونة السيبرانية Cyber Resilience فيقصد بها قدرة الأنظمة على التحضير للهجمات السيبرانية، والتعامل معها، والتعافي منها بأقل تأثير على الأعمال، من خلال تطوير استراتيجيات وقائية، وتنفيذ خطط طوارئ لضمان استمرارية الأعمال، وإصلاح الأنظمة المتضررة وتحليل الهجمات لتعزيز الحماية مستقبلاً.

جدول (11) تحليل أداء مصر في مجال إدارة المخاطر والمرونة السيبرانية وفق المؤشرات الدولية للامن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%46	%87	%56.11	%72.3	جيد



شكل (8) تحليل أداء مصر في مجال إدارة المخاطر والمرونة السيبرانية وفق المؤشرات الدولية للامن السيبراني

حققت مصر أداءً جيداً فوفقًا **لمؤشر الأمن السيبراني العالمي (GCI)** لعام 2024، حصلت مصر على درجة تقييم (20/20) ممتاز بمتوسط (100%) بمؤشر التدابير التنظيمية أما في **مؤشر الأمن السيبراني الوطني (NCSI)** لعام

2024 فقد تم تقييم أداء مصر في مجال إدارة المخاطر والمرونة السيبرانية في ثلاث مؤشرات هي مؤشر " الاستجابة للحوادث السيبرانية" وجاءت درجة مصر (11/14) وبنسبة (79%)، ومؤشر "إدارة الازمات السيبرانية بدرجة (2/9) بنسبة (22%)، ومؤشر مكافحة الجرائم السيبرانية بدرجة (6/16) وبنسبة (38%) وبالتالي يصبح المتوسط الكلي (46%) أما في **مؤشر القوة السيبرانية NCPI** فقد تناول تقييم إدارة المخاطر والمرونة السيبرانية في مؤشر الدفاع " في الترتيب (7/30) وبدرجة (52.4/65) وبنسبة (87%)، في حين غطي **مؤشر الجاهزية الشبكية (NRI)** الاستجابة والمرونة ضمن مؤشر "الأطر القانونية والتنظيمية بمرتكز الحوكمة (Governance) حيث حققت مصر درجة (56.11%) وبالتالي فإن المتوسط العام لجاهزية البنية التحتية لمصر بناءً على تقييم هذه المصادر الأربع (مؤشر GCI، مؤشر NGCI، ومؤشر NCPI ومؤشر NRI) يبلغ حوالي (100/72.3) وهي قيمة جيدة.

نقاط القوة

1- عدد الهجمات السيبرانية التي تم رصدها والاستجابة لها.

على الرغم من عدم توفر إحصائية حكومية بعدد الهجمات فإن تقرير لشركة "كاسبرسكي Kaspersky " المتخصصة في خدمات الأمن السيبراني أشار إلى أن الشركة أوقفت وكشفت نحو 13 مليون هجمة سيبرانية على مصر خلال الربع الأول من عام 2023. وقد ركزت تلك الهجمات على الحسابات المصرفية وبيانات مختلف العملاء في القطاع المصرفي المصري بنسبة 186% خلال الربع الأول من العام الجاري مقارنة بنفس الفترة من عام 2022. كما أشار التقرير إن هناك زيادة مضطردة في هجمات القرصنة التي استهدفت نظام المعلومات في قطاع التجزئة المصرفية في مصر، بالإضافة إلى زيادة هجمات التصيد الاحتيالي عبر البريد الإلكتروني والرسائل النصية القصيرة. وقد تعرض ما يقرب من 75 ألف مستخدم في مصر خلال الربع الأول من عام 2023 لهجمات التصيد الاحتيالي، بالإضافة إلى تعرض بعض المؤسسات الحكومية المصرية لهجمات شنتها فرق قرصنة دولية في عام 2022 بهدف التجسس وسرقة بيانات العملاء.

2- وجود خطط طوارئ للتعامل مع حوادث الفضاء السيبراني.

- قامت مصر بتطوير خطط طوارئ للتعامل مع الحوادث السيبرانية عبر المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) بالجهاز القومي لتنظيم الاتصالات.[54]
- يوجد فريق استجابة لطوارئ الحاسوب (CERT) مُعين بمسؤوليات وطنية للكشف عن الحوادث السيبرانية والاستجابة لها.
- في عام 2016 تم الإعلان عن استراتيجية الأمن السيبراني الوطنية، التي تهدف إلى حماية أمن المعلومات في جميع القطاعات الحيوية في الدولة، مثل الاتصالات، الطاقة، النقل، والقطاع المالي. [55]
- في عام 2018 تم **تأسيس المجلس الأعلى للأمن السيبراني،** كهيئة معنية بالإشراف على تنفيذ هذه الاستراتيجية وتنسيق الجهود بين مختلف الجهات.

3- عدد الاختبارات الدورية للتأكد من جاهزية الأنظمة ضد التهديدات.

شهد عام 2022 اطلاق اول مناورة سيبرانية وطنية تستهدف القطاعات الحيوية الحرجة و المراكز القطاعية حيث قام المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EGCERT) بالتعاون مع مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء، بتنفيذ أول مناورة سيبرانية بهدف قياس مدى الجاهزية والاستجابة لمواجهة الهجمات السيبرانية على المستوى الوطني، والتصدي لمختلف الهجمات الإلكترونية تنفيذًا للاستراتيجية الوطنية للأمن السيبراني. [65]

نقاط الضعف

- عدم توفر إحصائية حكومية بعدد الهجمات السيبرانية التي تعرضت لها القطاعات المختلفة بمصر.

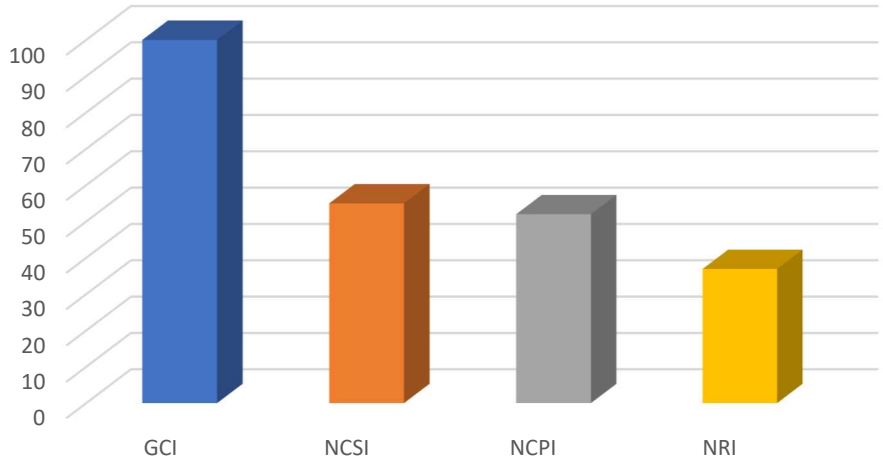
- عدم وضوح عدد الاختبارات الدورية للتأكد من جاهزية الأنظمة ضد التهديدات.

3/5 التوعية وبناء القدرات:

تعد التوعية وبناء القدرات السيبرانية عنصرًا محوريًا في تحقيق الأمن السيبراني، حيث تسعى إلى تعزيز المعرفة والفهم بأهمية حماية الفضاء الرقمي، إلى جانب تطوير مهارات الأفراد والمؤسسات للتعامل مع التهديدات المتزايدة. هذه الركيزة الأساسية تمثل حجر الزاوية في جهود مصر لتأمين بنيتها الرقمية ودعم استقرارها السيبراني في مواجهة التحديات المتغيرة.

جدول (12) تحليل أداء مصر في مجال التوعية وبناء القدرات وفق المؤشرات الدولية للامن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%55	%52	%36.94	%61	جيد



شكل (9) تحليل أداء مصر في مجال التوعية وبناء القدرات وفق المؤشرات الدولية للامن السيبراني

وفقًا **لمؤشر الأمن السيبراني العالمي (GCI)** لعام 2024، حصلت مصر على درجة تقييم (20/20) ممتاز بمتوسط (100%) بمؤشر تدابير تنمية القدرات أما في **مؤشر الأمن السيبراني الوطني (NCSI)** فقد تم تقييم التوعية تنمية القدرات في مؤشرين هما مؤشر " التعليم والتطوير المهني" وحصلت مصر فيه على تقدير (60%) وفي مؤشر "تحليل التهديدات وزيادة الوعي" وحصلت على (50%) ومن ثم فالمتوسط بلغ بهذا لهاذين المؤشرين (55%). وبالنسبة **لمؤشر القوة السيبرانية NCPI** فقد تناول تقييم التوعية وبناء القدرات ضمن مؤشر "الأعراف NORMS" وجاءت مصر بالترتيب (17/30) وبدرجة (31.34/60) وبنسبة (52%)، وأخيرا في مؤشر **مؤشر الجاهزية الشبكية (NRI)** تم التقييم بمرتكز الأفراد (People) حيث حققت مصر درجة (36.94%) وبحساب المتوسط الإجمالي لقيم تلك المؤشرات نجد أن مصر حصلت على نسبة (61%) وهي نسبة تشير إلى الحاجة لبذل مزيد من الجهد في هذا المحور.

نقاط القوة

1- عدد البرامج التدريبية في مجال الأمن السيبراني.

- قام معهد تكنولوجيا المعلومات (ITI) – الذراع التدريبي لوزارة الاتصالات وتكنولوجيا المعلومات – بإطلاق أكاديمية الأمن السيبراني في إطار مبادرة "سايبر مصر 360" وتهدف إلى تقديم خدمات تدريبية وتعليمية لقطاعات مختلفة بدءاً من النشء في سن المدرسة إلي طلبة الجامعات وشباب الخريجين وصولاً إلى العاملين المتخصصين وغير المتخصصين في مجال أمن المعلومات وقد بلغ عدد خريجي الأكاديمية الذين التحقوا بسوق العمل المصري والمتدربين 7000 طالب

ومستفيد. [57]

2- مستوى إدراج الأمن السيبراني في المناهج التعليمية: [58]

- يوجد بمصر أربعة جامعات أهلية وحكومية تقدم برامج متخصصة في الأمن السيبراني وهى: (جامعة مصر للمعلوماتية، وكلية الحاسبات والذكاء الاصطناعي بجامعة القاهرة، وكلية الحاسبات والذكاء الاصطناعي بجامعة حلوان، وكلية الهندسة الالكترونية بجامعة المنوفية) إلى جانب جامعة خاصة واحدة (كلية الحاسبات بجامعة TKH- مؤسسة جامعات المعرفة الدولية-كوفنتري - فرع مصر)
- توقيع مذكرة تفاهم بين وزارة الاتصالات وتكنولوجيا المعلومات، وجامعة ولاية أوهايو الأمريكية Ohio State University في (2020) لتقديم برنامج ماجستير تقني في مجال الأمن السيبراني. [59]

3- حملات التوعية العامة التي تهدف إلى نشر ثقافة الأمن السيبراني.

- يشرف المجلس الأعلى للأمن السيبراني المصري على تنظيم واطلاق حملات وطنيه دوريه للتعريف بمخاطر الاختراقات السيبرانيه في مختلف القطاعات وتنظيم ورش عمل ودورات للتوعيه بالأمن السيبراني علي المستوى القطاعي. [60]
- من نماذج المبادرات الناجحة مبادرة "**تعليم عال آمن رقميا**" [61] في مصر وتنفذها وزارة الاتصالات وتكنولوجيا المعلومات من خلال المركز المصري للاستجابة لطوارئ الحاسبات EG-CERT وبالتعاون مع وزارة التعليم العالي والبحث العلمي وشركة الشرق الأوسط لأنظمة الاتصالات (MCS) بهدف تعزيز الوعي بالأمن السيبراني وحماية البيانات في قطاع التعليم العالي والبحث العلمي في مصر.

نقاط الضعف

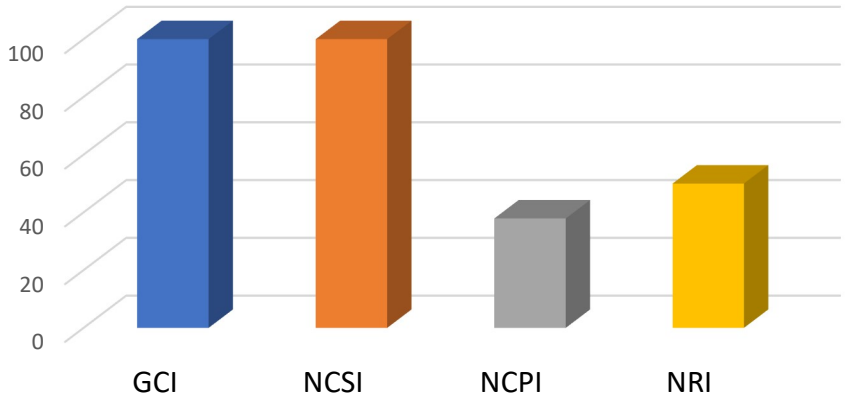
- ندرة وجود تخصصات دراسية وجامعية في مجال الأمن السيبراني في مصر فنسبة المؤسسات التعليمية والتي سبق ذكرها مقارنة بحجم الجامعات في مصر لا تشكل سوى (6%) فقط.
- عدم قدرة البنية التحتية للمؤسسات التعليمية في مصر من معامل وشبكات وبرامج على استيعاب المستجدات التكنولوجية في مجال الامن السيبراني بنفس سرعة المؤسسات التعليمية العالمية نفسها.
- غياب التنسيق فيما يخص التسويق لمخرجات البرامج التعليمية والتدريبية المختصة في الأمن السيبراني في مصر.
- تباين مستوى الوعي قد يواجه بعض الموظفين صعوبة في فهم موضوعات الأمن السيبراني بسبب غياب الخبرة التقنية.
- الاستمرارية في التدريب من الضروري توفير برامج تدريب دورية لتحديث المعارف والمهارات في مواجهة التهديدات المستمرة.

3/6 الاستثمارات والابتكار:

يعد تقييم الاستثمارات والابتكار في مجال الأمن السيبراني ذو أهمية كبيرة في تعزيز قدرة الدول والشركات على مواجهة التحديات السيبرانية المتزايدة. ويشمل هذا التقييم تقييم: حجم الميزانية الوطنية المخصصة للأمن السيبراني، عدد المشاريع البحثية في مجال الأمن السيبراني، عدد الشركات الناشئة المتخصصة في الأمن السيبراني المدعومة من الحكومة.

جدول (13) تحليل أداء مصر في مجال الاستثمارات والابتكار وفق المؤشرات الدولية للامن السيبراني

المؤشر	GCI	NCSI	NCPI	NRI	المتوسط	المستوى
النسبة	%100	%100	%37.9	%50	%72	جيد



شكل (10) تحليل أداء مصر في مجال الاستثمارات والابتكار وفق المؤشرات الدولية للامن السيبراني

وفقًا **لمؤشر الأمن السيبراني العالمي (GCI)** لعام 2024، حصلت مصر على درجة تقييم (20/20) ممتاز بمتوسط (100%) بمؤشرات "برامج البحث والتطوير"، "صناعة الأمن السيبراني الوطنية"، و"آليات تقديم الحوافز الحكومية" ولم يختلف **مؤشر الأمن السيبراني الوطني (NCSI) عن المؤشر السابق فقد حصلت مصر على تقييم (100%) بمؤشر "البحث والتطوير R&D"**. ولم يتناول المؤشر حجم الاستثمار بالتقييم، وبالنسبة **لمؤشر القوة السيبرانية NCPI** فقد تناول تقييم الابتكار ضمن مؤشر "الأعراف NORMS" وجاءت مصر بالترتيب (15/30) وبدرجة (35.55/60) وبنسبة (59.25%)، كما تم تقييم التمويل **بالمؤشر المالي "Financial** حيث حصلت مصر على (16.48%) وهي درجة ضعيفة تعكس ضعف التمويل وأخيرا في مؤشر **مؤشر الجاهزية الشبكية (NRI)** تم التقييم بمرتكز الأفراد (People) حيث حققت مصر درجة (36.94%) وبحساب المتوسط الإجمالي لقيم تلك المؤشرات نجد أن مصر حصلت على نسبة (72%).

نقاط القوة [62]

1- حجم الميزانية الوطنية المخصصة للأمن السيبراني.

- على الرغم من أن حجم الميزانية المخصصة للأمن السيبراني في مصر قد لا يتم الإعلان عنه بشكل علني أو تفصيلي. إلا ان جهود الدولة في انشاء المجلس الأعلى للأمن السيبراني والذي حدد من ضمن أهدافه التأكد من توافر التمويل اللازم لضمان تنفيذ منظومة الامن السيبراني، بالإضافة إلى استثمار الدولة في البنية التحتية من خلال تخصيص جزء من ميزانيتها لتمويل وتطوير مراكز الاستجابة للطوارئ السيبرانية (CERT) وأيضا تخصيص ميزانية لدعم التعاون مع منظمات دولية في مجال الأمن السيبراني، مثل الاتحاد الأوروبي والمبادرة الأفريقية للأمن السيبراني كل الجهود السابقة تؤشر إلى وجود تمويل متزايد.

2- حجم المشاريع البحثية في مجال الأمن السيبراني

- جاءت مصر في المركز الأول على مستوى قارة إفريقيا في عدد الأبحاث في مجال الذكاء الاصطناعي والامن السيبراني، بإجمالي 6985 بحثًا منشورًا، وقد إستأثرت الجهات المانحة التابعة لوزارة التعليم العالي والبحث العلمي بتمويل 30% من المشروعات البحثية.

3- عدد الشركات الناشئة

- احتلت مصر المركز الأول على مستوى الشرق الأوسط وشمال أفريقيا من حيث عدد الصفقات الموجهة لتمويل شركات الأمن السيبراني الناشئة في مصر خلال عام 2023 حيث أستأثرت مصر بـ (40%) من حجم التمويل مما يدل على القدرة التنافسية العالية للقطاع واستعداده للنمو في مصر كما بلغت حجم الاستثمارات الموجهة للشركات الناشئة في مجال الأمن السيبراني في مصر (750 الف دولار).

نقاط الضعف

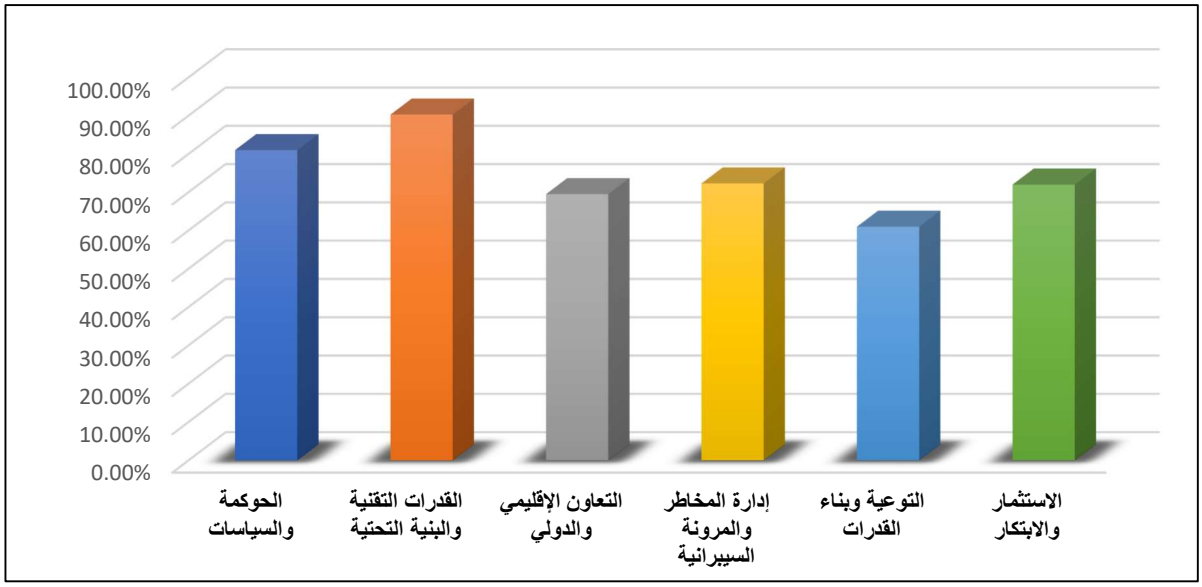
- الصعوبة البالغة في الحصول على معلومات عن حجم الميزانية الوطنية المخصصة للاستثمار ودعم شركات الأمن السيبراني يوحي بعدم اهتمام الدولة بالمستثمرين في مجال الأمن السيبراني على المستوى القومي ويدعم حالة التخوف من السوق المصري سواء من رواد الأعمال المحلين أو المستثمرين الأجانب.
- الضغوط الاقتصادية التي تعاني منها مصر تؤثر على حجم التمويل المخصص لبرامج البحث والتطوير والابتكار بالامن السيبراني فوفقا لتقرير مؤشر الابتكار العالمي (GII) الصادر عن المنظمة العالمية للملكية الفكرية (WIPO) لعام 2023 أتت مصر من بين الاقتصاديات المتوسطة الدخل التي سجلت نموا في البحث والتطوير في الفترة من 2021-2023 وبلغ 3.9% فقط.
- هجرة العقول المصرية في مجال الامن السيبراني نتيجة ضعف الفرص وانخفاض الرواتب يؤثر سلبا على مشروعات البحث والابتكار في مجال الامن السيبراني في مصر.
- بلغ عدد شركات الأمن السيبراني الناشئة المصرية المتخصصة (3) شركات فقط تم انشاؤهم خلال الفترة (2014-2023) وهو عدد ضعيف للغاية.
- ثقة العملاء بشركات الأمن السيبراني الكبرى الموجودة بالفعل تحد من الطلب على الشركات الناشئة مما يخلق أمامها صعوبات في المنافسة.
- غياب التخصص فكثير من الشركات العاملة في مجال تكنولوجيا المعلومات والاتصالات وشركات البرمجة تقدم خدمات في مجال الامن السيبراني إلى جانب خدماتها الأساسية مما يحد من الطلب على الشركات المتخصصة في الأمن السيبراني فقط.
- انخفاض حجم التمويل الممنوح للشركات الناشئة في مصر بنسبة 17.5% عام 2023 مقارنة بالتمويلات الممنوحة خلال عام 2022 ليصل 608 ملايين دولار.
- عدم تمييز شركات الأمن السيبراني الناشئة بأية لائحة أو قانون أو نص يسهل أعمال تلك الشركات على وجه الخصوص.

رابعاً: خلاصة تحليل مدي تكامل الآداء المصري في مجال الأمن السيبراني المصري وفق نتائج المؤشرات العالمية:

في ضوء التحليل السابق لمؤشرات الأمن السيبراني محل الدراسة ونقاط القوة الضعف التي تم رصدها بالتحليل يُظهر الجدول أدناه تقييم الأداء العام للأمن السيبراني في مصر وفقا لتقييم مختلف المرتكزات الرئيسية:

جدول (15) تقييم الأداء العام للأمن السيبراني في مصر وفق المرتكزات الرئيسية

المرتكز	الحوكمة والسياسات	القدرات التقنية والبنية التحتية	التعاون الإقليمي والدولي	إدارة المخاطر والمرونة السيبرانية	التوعية وبناء القدرات	الاستثمار والابتكار
متوسط	81.02%	90.3%	69.5%	72.3%	61%	72%



شكل (11) حجم تباين الأداء بين المرتكزات المختلفة المتعلقة بالأمن السيبراني في مصر

يعكس جدول (14) حجم تباين الأداء بين المرتكزات المختلفة المتعلقة بالأمن السيبراني في مصر. حيث يظهر تفوقًا واضحًا في "القدرات التقنية والبنية التحتية" (90.3%)، والحوكمة والسياسات (81.02%) مما يشير إلى جاهزية تقنية وبنية تحتية قوية، ونظام حوكمة وسياسات ملائم. في المقابل، تمثل التوعية وبناء القدرات (61%) نقطة ضعف تحتاج إلى تعزيز، وهو أمر حيوي لتحسين ثقافة الأمن السيبراني. الأداء المتوسط في "التعاون الإقليمي والدولي (69.5%) وإدارة المخاطر والمرونة السيبرانية (72.3%) يشير إلى وجود فرص لتحسين التنسيق والاستجابة للأزمات.

بينما وللوقوف على حجم الفجوة بين التقييم المثالي لمصر في مؤشر GCI وباقي المؤشرات يوضح جدول (15) مقارنة بين تقييم الأداء المصري في مؤشر الأمن السيبراني العالمي GCI من جانب ومتوسط مجموع القيم بمؤشرات (NCSI, NPCI & NRI) من جانب أخر:

جدول (15) حجم الفجوة بين تقييم مؤشر GCI وباقي المؤشرات (NCSI, NPCI & NRI)

المرتكز	الحوكمة والسياسات	القدرات التقنية والبنية التحتية	التعاون الإقليمي والدولي	إدارة المخاطر والمرونة السيبرانية	التوعية وبناء القدرات	الاستثمار والابتكار
GCI	100%	100%	100%	100%	100%	100%
NCSI	100%	100%	83%	46%	55%	100%
NPCI	80%	65.7%	48.2%	87%	52%	37.9%
NRI	44.08%	95.5%	46.99%	56.11%	36.94%	50%
متوسط مجموع القيم بمؤشرات (NCSI, NPCI & NRI)	74.6%	87%	59%	63%	48%	62.6%

في ضوء تحليل الجدول، يتضح وجود تباين ملحوظ بين تقييم مؤشر GCI ومتوسط القيم المسجلة في مؤشرات NCSI وNPCI وNRI، ما يسلط الضوء على فجوة بين التصنيف المثالي الممنوح لمصر من (100%) GCI والأداء الفعلي على أرض الواقع.

فبالنظر إلى مرتكز **الحوكمة والسياسات**، نجد أن تقييم GCI يشير إلى أداء مثالي بنسبة 100%، بينما يبلغ متوسط القيم الأخرى بالمؤشرات الثلاث 74.6%. هذا التباين، البالغ 25.4 نقطة، يعكس أن السياسات والتشريعات التي وضعتها مصر قوية نظرياً على الورق، لكنها قد تفتقر إلى التنفيذ الفعلي أو إلى تأثير واضح على الأداء العملي للأمن السيبراني.

فيما يتعلق **بالقدرات التقنية والبنية التحتية**، تظهر البيانات توافقًا نسبيًا بين مؤشر GCI ومتوسط المؤشرات الأخرى، حيث يبلغ التباين 13 نقطة فقط. يعكس هذا القرب جهودًا حقيقية لتحسين البنية التحتية التقنية، لكنه يبرز في الوقت ذاته أن هناك مجالًا للتطوير لتحقيق مستوى مثالي فعلي.

أما في مرتكز **التعاون الإقليمي والدولي**، فإن التباين يتسع بشكل كبير ليصل إلى 41 نقطة، حيث يشير متوسط القيم الأخرى إلى 59% فقط. هذا يوضح وجود تحديات في تحقيق التكامل مع الجهود الإقليمية والدولية، وهو جانب بالغ الأهمية لتعزيز الأمن السيبراني في مواجهة تهديدات عابرة للحدود.

وعلى صعيد **إدارة المخاطر والمرونة السيبرانية**، يظهر تباين قدره 37 نقطة، حيث يشير متوسط الأداء بالمؤشرات الثلاث إلى 63% وتعكس هذه الفجوة أن قدرة مصر على التصدي الفعلي للهجمات السيبرانية والتعامل مع المخاطر ما زالت دون المستوى الذي يعكسه تصنيف GCI المثالي.

في حين التباين الأكبر يُلاحظ في مرتكز **التوعية وبناء القدرات**، حيث يبلغ متوسط القيم بالمؤشرات الثلاث 48% فقط، مقارنة بـ100% في GCI، بفارق 52 نقطة. وهذا يشير إلى قصور واضح في رفع مستوى الوعي السيبراني وتطوير الكفاءات البشرية اللازمة، وهو مجال يتطلب استثمارات أكبر لتحقيق تقدم ملموس.

وأخيرًا، فيما يخص **الاستثمار والابتكار**، فإن التباين يصل إلى 37.4 نقطة، حيث يبلغ متوسط القيم بالمؤشرات الثلاث 62.6% ويعكس ذلك تحديات في تحفيز الابتكار وتوفير التمويل للبحث في مجال الأمن السيبراني.

بصورة عامة، يظهر التحليل أن تقييم GCI لمصر لا يعكس بدقة الأداء العملي في جميع المرتكزات، حيث إن الأداء الفعلي في مجالات التوعية، التعاون الدولي، وإدارة المخاطر يحتاج إلى تحسينات جذرية. فالتقدير المثالي لمصر (100/100) في مؤشر GCI يعد إنجازًا رمزيًا يعكس جهودًا كبيرة على المستوى التشريعي والتنظيمي، لكنه لا يعني بالضرورة أن البيئة السيبرانية في مصر محصنة بالكامل أو أنها أكثر كفاءة مقارنة بدول أخرى. وأن الأداء المتفاوت في المؤشرات الأخرى يشير إلى وجود حاجة ملحة لتطوير تطبيق عملي يتماشى مع الالتزامات النظرية، ويدعو لمراجعة شاملة واستراتيجية تعزز النتائج الفعلية وتغطي أبعاد الأمن السيبراني كافة.

خامساً: التوصيات:

1- وضع إطار قانوني شامل ومتكامل يغطي جميع جوانب الأمن السيبراني.
2- تحديث القوانين بشكل دوري وإجراء مراجعات مستمرة للتشريعات لتواكب التطورات التكنولوجية.
3- تطوير أطر قانونية للشركات الناشئة في مجال الأمن السيبراني.
4- إطلاق حملات توعية لتعريف الأفراد والمؤسسات بالقوانين والمسؤوليات المتعلقة بالأمن السيبراني.
5- العمل على تطوير اتفاقيات تعاون دولية ملزمة لتبادل المعلومات السيبرانية ومواجهة التهديدات.
6- إنشاء منصات وطنية خاصة بالقطاعات الحيوية لتنسيق الجهود الأمنية بين القطاعات المختلفة.

7- تطوير برامج تدريبية مخصصة للعاملين بالقطاعات الحيوية لبناء كوادر مؤهلة في إدارة البنية التحتية السيبرانية.

8- إرساء أطر قانونية موحدة للتعاون الدولي في مجال الأمن السيبراني.

9- إقامة منصات للتواصل المباشر بين الدول لزيادة الشفافية وبناء الثقة في تبادل المعلومات السيبرانية.

10- دعم الدول ذات القدرات الضعيفة في المجال التكنولوجي من خلال توفير التدريب والمساعدة التقنية.

11- التوسع في إنشاء برامج أكاديمية جديدة في الجامعات المصرية تركز على الأمن السيبراني، بما في ذلك درجات البكالوريوس، والماجستير، والدكتوراه.

12- تقديم حوافز للجامعات لإنشاء كليات أو أقسام متخصصة في مجال الأمن السيبراني بالتعاون مع مؤسسات دولية.

13- دمج الأمن السيبراني في المناهج التعليمية للمراحل المختلفة (الابتدائية، الإعدادية، الثانوية) لزيادة الوعي في مرحلة مبكرة.

14- تخصيص ميزانية وطنية لدعم البنية التحتية في الجامعات المصرية لمواكبة المستجدات العالمية في الأمن السيبراني.

15- تعزيز التسويق لمخرجات البرامج التعليمية من خلال إنشاء مكاتب للتنسيق بين الجامعات وسوق العمل لتسهيل توظيف الخريجين في قطاعات الأمن السيبراني.

16- تخصيص ميزانيات حكومية أكبر لدعم مشاريع التكنولوجيا مثل الذكاء الاصطناعي والأمن السيبراني.

المصادر والمراجع:

1- James E. Cartwright, Joint Terminology for Cyberspace Operations, Memorandum for Chiefs of the Military Services, Washington, D.C. 20318-9999, p. 7.

2- ناصف، أحمد مصطفى. (2023). "دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي". *مجلة المال والتجارة، ع645* ، 24 .32 – متاح في :
تم الاطلاع في 2025/1/2 http://search.mandumah.com/Record/1363433

3- ما هو المؤشر العالمي للأمن السيبراني؟. المركز الوطني للامن السيبراني. الأردن. متاح في:
تم الاطلاع 2025/1/2 https://www.safeonline.jo/Default/Ar

4- البداينة، ذياب. (2024). "الإرهاب السيبراني والتقنيات الناشئة: تحديات الأمن الوطني السيبراني والسيادة الوطنية". *مجلة الدراسات القانونية والأمنية، مج4, ع1* ، 7 .72 – متاح في:
تم الاطلاع 2024/12/28 http://search.mandumah.com/Record/1467103

5- البدوي، حبيب. (2024). "الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله تعزيز الدفاعات". *مجلة بحوث الإعلام الرقمي*، ع3 ، 154 – 180. متاح في:
تم الاطلاع 2024/12/28 http://search.mandumah.com/Record/1497116

6- عبدالقادر، إيمان. (2024). "أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من 2011 حتى 2023". *مجلة الأمن القومي والإستراتيجية، مج2, ع3* ، 98 .111 – متاح في:
تم الاطلاع 2024/12/28 http://search.mandumah.com/Record/1440297

7- ناصف، أحمد مصطفى. (2023). مصدر سابق.

8- آل مداوى، علي. (2023). "الأمن السيبراني: تعريفه – أهميته – أنواعه – استراتيجيات الوقاية من الهجمات السيبرانية". *مجلة الدراسات الدولية، ع34* ، 115 .124 – متاح في:
http://search.mandumah.com/Record/1454807 2024/12/28 تم الاطلاع

9- المزيني، عبدالعزيز بن أحمد. (2022). "الأمن السيبراني واجب من واجبات الدولة الحديثة ووسائل تحقيقه التنظيمية: دراسة تأصيلية مقارنة". *مجلة قضاء، ع29* ، 492 .542 – متاح في:
http://search.mandumah.com/Record/1349659 2024/12/28 تم الاطلاع

10- الضفيري، ناجي بدر، العنزي، إبراهيم غازي، و العنزي، دلال فرحان نافع. (2024). "الوعي بالأمن السيبراني لدى معلمي المرحلة المتوسطة بدولة الكويت وعلاقته بمستوى توظيفهم للتكنولوجيا في التدريس". *مجلة الدراسات والبحوث التربوية، مج4, ع11* ، 1 .42 – متاح في:
http://search.mandumah.com/Record/1475468 2024/12/28 تم الاطلاع

11- الحبيب، ماجد بن عبدالله بن محمد. (2022). "درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم". *مجلة العلوم التربوية، ع30*، 269-326. متاح في:
http://search.mandumah.com/Record/1274697 2024/12/28 تم الاطلاع

12- فرج، علياء عمر كامل إبراهيم (2022). "دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي : جامعة الأمير سطام بن عبد العزيز نموذجا". *المجلة التربوية لكلية التربية بجامعة سوهاج*. ع. 94، ج.1. ص ص 510-737. متاح في:
https://edusohag.journals.ekb.eg/article_212365_d8eb0c9783cebf97a18a4d7a20a2f5e8.pdf
2024/12/28 تم الاطلاع

13- أنديجاني، دلال صالح، و فلمبان، فدوى ياسين نور الدين. (2021). "ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية". *المجلة العربية للمعلوماتية وأمن المعلومات، ع5* ، 75 .102 – متاح في: http://search.mandumah.com/Record/1189463 تم الاطلاع 2024/12/28

14- المنيع، الجوهرة عبد الرحمن. (2022). "متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030". *مجلة كلية التربية*. مج. 38، ع. 1.
http://search.shamaa.org/PDF/Articles/EGJfeau/JfeauVol38No1Y2022/jfeau_2022-v38-n1_156-194.pdf 2024/12/28 تم الاطلاع

15- العتيبي، فهد، البرهمتوشي، حسنين محمد، كاتب، فارس، و موصلي، ريان. (2022). "واقع المدن الذكية السعودية وتحدياتها الأمنية السيبرانية وحلولها في ضوء رؤية المملكة 2030 م". *مجلة جامعة الملك عبدالعزيز – الآداب والعلوم الإنسانية، مج30, ع6* ، 73 .113 – مسترجع من
http://search.mandumah.com/Record/1360342 2024/12/28 تم الاطلاع

16- عبدالحميد، عماد الدين محمد كامل. (2021)."استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي: دراسة في العملات الرقمية للبنوك المركزية : الحلقة الثانية". *مجلة الاقتصاد الإسلامي، مج41, ع486*، 31-41. متاح في: http://search.mandumah.com/Record/1267059 تم الاطلاع 2024/12/28

17- السيد، نهى مجدي محمد. (2021). "الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030". *المجلة العربية لبحوث الإعلام والاتصال، ع35* ، 484 .514 – متاح في:
http://search.mandumah.com/Record/1252316 2024/12/28 تم الاطلاع

18- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله. (2021). "دور الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبدالعزيز الدولي بجدة". *مجلة العلوم الإقتصادية والإدارية والقانونية، مج5, ع9* ، 144 .164 – متاح في:
تم الاطلاع 2024/12/28 http://search.mandumah.com/Record/1176003

19- براون، رافائيل دين. (2018). "نحو نموذج لتعزيز كفاءة الأمن السيبراني في قطر ضمن الإطار التشريعي". *المجلة الدولية للقانون*، مج7, ع4 ، 9 – 44. متاح في:
تم الاطلاع 2024/12/17 http://search.mandumah.com/Record/1142117

20- Cybersecurity Framework. National Institute of Standards and Technology (NIST). Available at: https://www.nist.gov/cyberframework last seen 12/1/2025

21- تعريف الأمن السيبراني »، الاتحاد الدولي للاتصالات، متاح في :
https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx .
تم الاطلاع 2025/1/25

22- ما هو الأمن السيبراني؟. المملكة العربية السعودية. هيئة الاتصالات والفضاء والتقنية. متاح في:
https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx تم الاطلاع 2025 /1/25

23- ما هو الأمن السيبراني؟. المركز الوطني للامن السيبراني. مملكة البحرين. متاح في:
https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html last seen 12/1/2025

24- James E. Cartwright, op.cit, p. 7.

25- ناصف، أحمد مصطفى. (2023). مصدر سابق. ص

26- Kim R. Holmes, (2015), What is national Security, Washington, The Heritage Foundation, p. 23- p. 19

27- Jude Blanchette (2020), Ideological Security as National Security, Washington, Center for Strategic and International Studies, p. 4

28- Kim R. Holmes, op.cit, p. 19

29- عبدالقادر، إيمان. (2024). مصدر سابق. ص99

30- ناصف، أحمد مصطفى. (2023). مصدر سابق. ص27

31- مؤشر الأمن السيبراني وفقاً للهيئة الوطنية للأمن السيبراني. متاح في:
https://tahwul.com/cybersecurity-index/ 2025 /1/25 تم الاطلاع

32- Global Cybersecurity Index 2024. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf last accessed 12/1/2025

33- NCSI: Ranking - National Cyber Security Index. Available at: https://ncsi.ega.ee/country/eg/ last accessed 12/1/2025

34- The National Cyber Power Index (NCPI). Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2022 last accessed 12/1/2025

35- Network Readiness Index 2024. Available at: https://networkreadinessindex.org/countries last accessed 12/1/2025

36- الإطار القانوني للأمن السيبراني في مصر. مركز المعلومات ودعم اتخاذ القرار. مصر. متاح في:
https://www.idsc.gov.eg/Studies%20and%20Policy%20Papers/details/10385

تم الاطلاع 2025 /1/25

37- معايير وأطر الأمن السيبراني. المركز الوطني للإستعداد لطوارئ الحاسبات والشبكات. مصر. متاح في: https://egcert.eg/ar/cybersecurity-frameworks-and-standards/ تم الاطلاع 2025 /1/25

38- المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT). متاح في: https://egcert.eg/ar/ تم الاطلاع 2025 /1/25

39- مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي (EG-FinCIRT) بالبنك المركزي المصري. متاح في: https://www.egfincirt.org.eg/ar/ تم الاطلاع 2025/1/18

40- المجلس الأعلى للأمن السيبراني المصري (ESCC) . متاح في: https://escc.gov.eg/ تم الاطلاع 2025 /1/25

41- إعلان مشترك بشأن الشراكة الاستراتيجية والشاملة بين جمهورية مصر العربية والاتحاد الأوروبي. متاح في: https://ec.europa.eu/commission/presscorner/api/files/attachment/877828/مشروع-اعلان-مشترك-نهائي-عربي-مصر.pdf تم الاطلاع 2025/1/18

42- اتفاقية التعاون مع الهند: تبادل المعلومات وبناء القدرات في مجال الامن السيبراني . متاح في: https://egcert.eg/ar/news/cooperation-with-india/ تم الاطلاع 2025/1/18

43- مصر وماليزيا توقعان اتفاقية تعاون في مجال الأمن السيبراني . متاح في: https://egcert.eg/ar/news/م-في-تعاون-اتفاقية-توقعان-وماليزيا-مصر/

44- مصر توقع اتفاقية تعاون مع الأردن في مجال الأمن السيبراني. متاح في: https://egcert.eg/ar/news/jordan/ تم الاطلاع 2025/1/18

45- شركات الأمن السيبراني الناشئة: جهود مصرية وفرص عالمية. مجلس الوزراء المصري. مركز معلومات دعم اتخاذ القرار. مصدر سابق. ص 54.

46- اتفاقية التعاون مع شركة تريند مايكرو trend-micro. متاح في: https://egcert.eg/ar/news/trend-micro/ تم الاطلاع 2025/1/21

47- اتفاقية التعاون مع كاسبرسكي Kaspersky. متاح في: https://egcert.eg/ar/news/egcert-kaspersky-mou/ تم الاطلاع 2025/1/15

48- مصر تفوز بالمناورة السيبرانية خلال الأسبوع الإقليمي للأمن السيبراني . متاح في: https://egcert.eg/ar/news/ا-خلال-السيبرانية-المناورة-تفوز-مصر/ تم الاطلاع 2025/1/18

49- مناورة المركز الإقليمي العربي للأمن السيبراني: متاح في: https://egcert.eg/ar/news/مصر-تتصدر-مناورة-المركز-الإقليمي-العرب/ تم الاطلاع 2025/1/18

50- مناورة سيبرانية بمشاركة جهات وهيئات حكومية : متاح في: https://egcert.eg/ar/news/cyberdrill1/

51- تعاون مشترك بين المركز الوطني للاستعداد لطوارئ الحاسبات و OIC-CERT لوضع سياسات وضوابط الأمن السيبراني. متاح في: https://egcert.eg/ar/news/oic-certcooperation/ تم الاطلاع 2025/1/16

52- تعاون إقليمي اتفاقية التعاون مع (ITU-RCC) في مجال الأمن السيبراني. متاح في: https://egcert.eg/ar/news/cooperation-with-itu-rcc/ تم الاطلاع 2025/1/16

53-Daily News Egypt, Kaspersky Tackles 13 Million Cyberattacks in Egypt During 1Q 2023, Daily News Egypt, May 8, 2023, Available online: https://shorturl.at/tGW18 , Accessible on September 25, 2023.

54- خطة الاستجابة والتصعيد لمواجهة الهجمات السيبرانية. متاح في:
https://egcert.eg/wp-content/uploads/Response-and-escalation-cybersecurity-plan.pdf
تم الاطلاع 1/25/ 2025
55- الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣-٢٠٢٧. متاح في:
https://mcit.gov.eg/Upcont/Documents/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf تم الاطلاع 1/25/ 2025
56- مناورة سيبرانية بمشاركة جهات وهيئات حكومية : متاح في:
https://egcert.eg/ar/news/national-first-cyberdrill/ تم الاطلاع 1/25/ 2025
57- أكاديمية الأمن السيبراني. مصر. متاح في:
https://maharatech.gov.eg/mod/page/view.php?id=14161 تم الاطلاع 1/25/ 2025
58- شركات الأمن السيبراني الناشئة: جهود مصرية وفرص عالمية. مجلس الوزراء المصري. مركز معلومات دعم اتخاذ القرار. ص 34. متاح في:
https://idsc.gov.eg/upload/DocumentLibrary/AttachmentA/10386/6.pdf تم الاطلاع 1/20/ 2025
59- نفس المصدر. ص 59.
60- برامج التوعية. EG-CERT. متاح في:
https://egcert.eg/ar/?s=%D8%A7%D9%84%D8%AA%D9%88%D8%B9%D9%8A%D8%A9 تم الاطلاع 1/20/ 2025
61- مبادرة "تعليم عال آمن رقميا" . متاح في:
https://egcert.eg/ar/news/8-الحاس-لطوارئ-للاستعداد-الوطني-المركز تم الاطلاع 1/25/ 2025
62- شركات الأمن السيبراني الناشئة: جهود مصرية وفرص عالمية. مجلس الوزراء المصري. مركز معلومات دعم اتخاذ القرار. مصدر سابق. ص 43.

Cybersecurity in Egypt

An Analytical Study of Performance Integration According to International Indicators

Dr. Hesham Mostafa Kamal Elden Ahmed
Lecturer of Information, Department of Documents, Libraries, and Information, Faculty of Arts, Mansoura University
heshamabc@mans.edu.eg

Abstract

This study aims to analyze the cybersecurity measures adopted in Egypt and assess their alignment with international standards by comparing Egypt's performance with key international indicators, such as the Global Cybersecurity Index (GCI), the National Cybersecurity Index (NCSI), the National Cyber Power Index (NPCI), and the Network Readiness Index (NRI). The study adopted a comparative analytical approach to analyze indicator data and assess the gaps between Egypt's policies and global requirements.

The study found that Egypt made significant progress by ranking among the top ten countries according to the GCI in 2024. However, the results revealed a considerable disparity between Egypt's GCI ranking and other indicators, reflecting a gap between the adopted policies and the actual implementation of cybersecurity measures. The study also highlighted the need for additional indicators to accurately assess the effectiveness of Egypt's cybersecurity application.

Based on the findings, the study recommended the need to review and improve the actual implementation of current cybersecurity policies in Egypt, focusing on enhancing regional and international cooperation, developing technical infrastructure, and increasing investment in research and innovation. It also emphasized the importance of establishing strategic risk management plans and promoting awareness and capacity building to address the growing cybersecurity threats.

Keywords:

Cybersecurity; Cybersecurity Indicators; Cyber Measures; Cybersecurity in Egypt