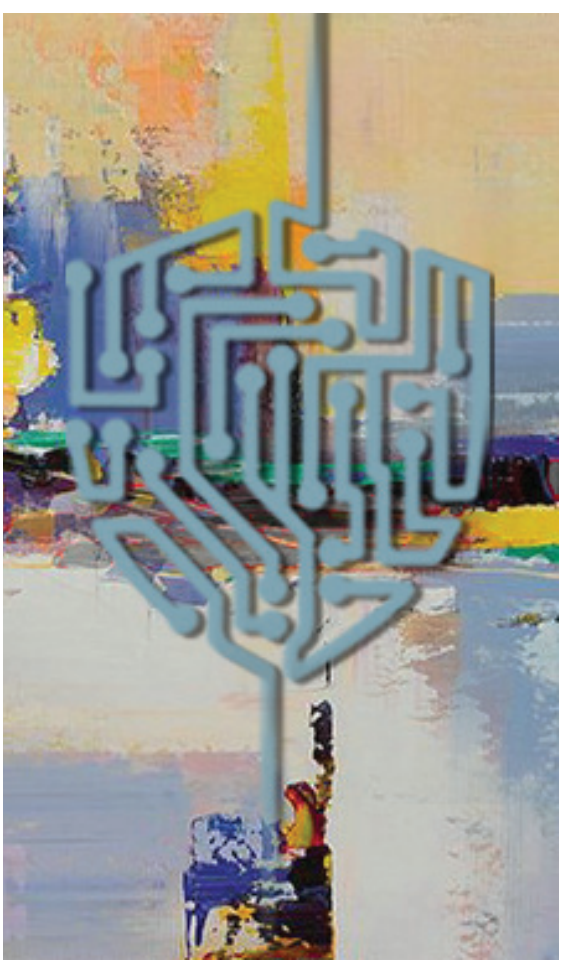
رئاسة مجلس الوزراء
المجلس الأعلى للأمن السيبراني

وزارة الاتصالات
وتكنولوجيا المعلومات

الاستراتيجية الوطنية للأمن السيبراني
٢٠٢٣ - ٢٠٢٧



قـائمة الجـداول

قـائمة الـرسـوم التـوضيحية

١ الأمن السيبراني في مصر

١,١ أهمية استراتيجية الأمن السيبراني لمصر

تتمثل أهمية وجود استراتيجية وطنية للأمن السيبراني في نقطتين أساسيتين، أولهما هو التصدي للحوادث السيبرانية التي تزايدت من حيث عددها ومصادرها، وثانيهما هو صناعة فرص للسوق المصرية عن طريق بناء كوادر بشرية وتطوير صناعة وطنية تشارك في زيادة إجمالي الناتج المحلي (GDP).

من المهم إجراء تقييم للوضع الراهن لحالة الأمن السيبراني في مصر وذلك لتحديد عناصر الاستراتيجية الوطنية للأمن السيبراني بدقة. سيتم عرض التهديدات والفرص ونقاط القوة والضعف بشيء من التفصيل في الفقرات التالية.

١,٢ المخاطر

تزايدت أعداد الهجمات السيبرانية في الأعوام السابقة بشكل كبير، كما تسببت الهجمات السيبرانية في خسائر ضخمة للاقتصاد العالمي مما يشكل عبئًا كبيرًا على ميزانيات الدول. هذا بالإضافة إلى الخسائر الأخرى مثل توقف بعض الخدمات الحيوية عن العمل والإضرار بسمعة الشركات والأفراد.

ومن الجدير بالذكر أن مصادر التهديدات السيبرانية تنوعت لتشمل الجريمة السيبرانية (Cyber Crime) والحرب السيبرانية (Cyber War) والإرهاب (Terrorists) والتهديدات الداخلية (Insiders) وتهديدات الهواة (Script Kiddies). وسيتم شرحها تفصيلا في الفقرات التالية.

١,٢,١ الجريمة السيبرانية (Cyber Crime):

إن الجريمة السيبرانية هي المسؤولة بصورة أساسية عن تطوير وترويج برامج ضارة من أجل الكسب المالي أو القرصنة بقصد سرقة البيانات و/أو الشبكات أو إتلافها أو تحريفها. وقد أصبحت تلك الهجمات شرسة وتنتشر في العالم بشكل متزايد كما يوضحه الاستخدام المتزايد لبرامج طلب الفدية (ransomware) والتهديدات بهجوم حجب الخدمة (DDoS) لأغراض تشويه الصورة أو الابتزاز.

١,٢,٢ الحرب السيبرانية (Cyber War):

هي تهديدات تقوم بها دول وجماعات ترعاها دول وذلك لاختراق القطاعات الحرجة في دول أخرى مثل قطاعات الطاقة والاتصالات والبنوك وغيرها، وذلك من أجل التجسس أو مكاسب سياسية واستراتيجية أو بغرض التخريب فقط.

ومن الجدير بالذكر أن العديد من الدول قد أعلنت صراحة عن امتلاكها لقدرات هجومية سيبرانية لغرض الدفاع عن النفس من هذه التهديدات.

١,٢,٣ الإرهاب (Terrorists):

على الرغم من القدرات السيبرانية المتواضعة للإرهابيين، فإنه من المتوقع خلال الأعوام القليلة القادمة أن تزداد هذه القدرات على إحداث أضرار بالغة مما يجعلها على خريطة التهديدات المحتملة.

١,٢,٤ التهديدات الداخلية (Insiders):

مع تزايد استخدام تكنولوجيا المعلومات داخل المؤسسات، تتزايد احتمالات المخاطر الناتجة، قصدًا أو بدون قصد، من الموظفين المخولين باستخدام أنظمة المعلومات. فقد يكون هؤلاء الموظفون مصدرًا لتهديد المؤسسات عن طريق سرقة بيانات حساسة تؤدي إلى خسائر مادية جسيمة أو إلى تهديد سمعة المؤسسة.

وقد يعرّض الموظف بيانات المؤسسة الحساسة للخطر بدون قصد عن طريق بعض الهجمات السيبرانية مثل التصّيد الإلكتروني (Phishing) أو الهندسة الاجتماعية (Social Engineering).

١,٢,٥ الهواة (Script Kiddies):

هم مجموعة أشخاص أصحاب مهارات سيبرانية محدودة، ولكنهم يستخدمون برامج مجهزة ذات قدرات تخريبية عالية إذا صادفت نقاط ضعف في أنظمة المعلومات الموجودة في المؤسسات.

١,٣ الفرص

على الرغم من الآثار التخريبية للتهديدات السيبرانية، فإنه يمكن استغلال هذه التهديدات لبناء صناعة وطنية للأمن السيبراني تستوعب الكثير من الشباب القادرين على تطوير وتشغيل برمجيات الأمن السيبراني ونشر الوعي بين أفراد المجتمع عامة والعاملين في المؤسسات المالكة/المشغلة للبنية التحتية الحرجة.

كما أنه من المتوقع عالميًا أن يرتفع الإنفاق على الأمن السيبراني للبنية التحتية الحرجة.

١,٤ نقاط القوة

تتمثل نقاط القوة في إقبال الطلاب على مجال الاتصالات وتكنولوجيا المعلومات في مرحلة التعليم الجامعي. بالإضافة إلى ذلك فإن النمو الملحوظ في البنية التحتية لقطاع الاتصالات وتكنولوجيا المعلومات يعتبر جاذبًا لخدمات الأمن السيبراني.

١,٥ التحـديات

مـازال البحـث العلمـي فـي مجـال الأمـن السـيبراني فـي مراحلـه الأولـى، وهـو مـا يضـع علـى كاهلنـا عـبء بنـاء بنيـة تحتيـة للبحـث العلمـي فـي هـذا المجـال. هـذا بالإضافـة إلـى دمـج برامـج الأمـن السـيبراني فـي مناهـج المراحـل التعليميـة المختلفـة. وكذلـك فمـن التحديـات عـدم وجـود إطـار ملـزم ينسـق العمـل بيـن الجهـات الحكوميـة والجهـات المالكة/المشـغلة للبنيـة التحتيـة الحرجـة. ملخـص تحليـل نقـاط القـوة والتحديـات والمخاطـر والفـرص موضـح فـي (**جـدول ١**)

١,٦ مصادر تطوير الاستراتيجية

اعتمد وضع وتطوير الاستراتيجية الوطنية للأمن السيبراني على كل من:

- استراتيجية مصر ٢٠٣٠
- تجارب الدول الرائدة في مجال إدارة الأمن السيبراني
- الخبراء الأكاديميين والشركات العاملة في مجالي الأمن السيبراني وتكنولوجيا المعلومات
- الأبحاث في مجال الأمن السيبراني

جـدول ١: ملخص تحليـل نقـاط القـوة، التحـديـات، المخـاطر، والفـرص (SWOT Analysis)

نقاط القوة

- زيـادة أعـدادا طـلاب وأعضـاء هيئـة التدريـس فـي الجامعـات التكنولوجيـة
- نمو قطاع الاتصالات وتكنولوجيا المعلومات

التحـديـات

- تطويـر البنيـة التحتيـة للبحـث العلمـي فـي مجـال الأمـن السـيبراني
- دمـج برامـج الأمـن السـيبراني فـي مناهـج المراحـل المختلفـة للتعليـم
- إطـار ملـزم ينسـق العمـل بيـن الجهـات المالكـة/ المشـغلة للبنيـة التحتيـة الحرجـة

المخـاطر

- زيادة أعداد الهجمات السيبرانية
- تنوع مصادر التهديد السيبراني
- زيادة الخسائر المادية

الفـرص

- إنشاء صناعة وطنية للأمن السيبراني
- فـرص عمـل للشـباب العامليـن فـي مجـال الأمـن السـيبراني

٢ الاستراتيجية

٢,١ الـرؤية

الفضاء السيبراني المصري مؤمّن وقادر على الصمود ويشجع الازدهار الاقتصادي.

٢,٢ المهمة

قيادة الجهود الوطنية لفهم وإدارة مخاطر الفضاء السيبراني

٢,٣ الغطاء التشريعي

تنص المادة (٣١) من الدسـتـور المصـري (ينايـر ٢٠١٤) على أن أمن الفضاء المعلوماتي جـزء أساسـي مـن منظومة الاقتصـاد والأمـن القومـي، وتلتـزم الدولـة باتخـاذ التدابيـر اللازمـة للحفـاظ عليـه على النحو الـذي ينظمـه القانون.

٢,٤ برامج الاستراتيجية الوطنية

تغطـي برامـج الخطـة الاسـتراتيجية سـتة مجـالات رئيسـية (**رسـم توضيحـي ١**) وهي: بناء إطـار تشـريعي متكامل، تغيـر ثقافـة المجتمـع حـول الامـن السـيبراني، تعزيـز الشـراكة الوطنيـة، بنـاء دفاعـات سـيبرانية قويـة وقـادرة علـى الصمـود، تشـجيع البحـث العلمـي وتعزيـز الابتـكار والنمـو، تعزيـز التعـاون الدولـي.

بـرامج الخطـة الاستراتيجية للأمـن السيبراني
٢٠٢٣ -٢٠٢٧

- بنـاء إطـار تشريعي متكـامل
- تعـزيز الشـراكة الـوطنية
- بنـاء دفاعات سيبرانية قوية وقـادرة على الصمـود
- تعـزيز التعـاون الـدولى
- تغيير ثقـافة المجتمع حول الأمن السيبراني
- تشـجيع البحث العلمي وتعـزيز الابتكـار والنمـو

رسـم توضيحي ١: برامج الخطة الاستراتيجية الوطنية للأمن السيبراني

٣ برامج بنـاء إطـار تشـريعي متكامل

الجريمـة الإلكترونيـة هـي فعـل يتسـبب بضـرر جسـيم للأفـراد أو المؤسسـات بهـدف إفشـاء أسـرار أمنيـة مهمـة تخص مؤسسـات مهمة بالدولة أو بيانات وحسـابات بنكية خاصة بالأفراد وكذلك تشـويه سـمعة الضحايا مـن أجل تحقيق مكاسـب ماديـة أو خدمـة أهـداف سياسـية باسـتخدام الحاسـوب ووسـائل الاتصـال الحديثـة مثـل الإنترنـت.

وتتشـابه الجريمـة الإلكترونيـة مـع الجريمـة العاديـة فـي عناصرهـا مـن حيـث وجـود الجانـي والضحيـة وفعـل الجريمـة، ولكـن تختلـف عـن الجريمـة العاديـة باختلاف البيئات والوسـائل المسـتخدمة، فالوسـيلة المسـتخدمة هـي التكنولوجيا الحديثـة ووسـائل الاتصـال الحديثـة والشـبكات المعلوماتية.

٣,١ الهيكل التشريعي

قـام المشـرع المصـري بسـن تشـريعات تعمـل فـي محوريـن أساسـيين (**رسـم توضيحـي ٢**)، وهمـا تجريـم الجانـي عـن طريـق قانـون جرائـم تقنيـة المعلومـات رقـم ١٧٥ لسـنة ٢٠١٨ وفـرض الضوابـط والمعاييـر القياسـية علـى المؤسسـات لحمايـة كل مـن البيانـات والمعلومـات وكذلـك الأنظمـة المعلوماتيـة عـن طريـق قانـون حمايـة البيانـات الشـخصية رقـم ١٥١ لسـنة ٢٠٢٠ وجـاري العمـل علـى قانـون الأمـن السـيبراني.

محـــاور عمـل قـوانين الأمن السيبراني

- تجـريـم الجـانـي
  - قـانـون مكـافحـة جرئم تقنية المعلـومات رقـم ١٧٥ لسنة ٢٠١٨
- فـرض الضـوابـط والمعـايير القيـاسـية
  - قـانـون حمـاية البيـانـات الشـخصية رقـم ١٥١ لسنة ٢٠٢٠
  - قـانـون الأمن السـيبراني

رسم توضيحي ٢: محاور عمل قوانين الأمن السيبراني

٣,١,١ تجـريم الجـاني

قـام المشـرع المصـري بسـن قانـون مكافحـة جرائـم تقنيـة المعلومـات «قانـون رقـم ١٧٥ لسـنة ٢٠١٨» بيّـن فيـه الأنـواع المختلفـة لجرائـم تقنيـة المعلومـات والعقوبـات المصاحبـة لهـا، وبهـذا يكـون الاتجـاه الأول فـي التشـريع قـد تـم أخـذه فـي الاعتبـار. كمـا تـم إصـدار اللائحـة التنفيذيـة لهـذا القانـون.

٣,١,٢ فرض الضوابط والمعايير القياسية على المؤسسات

قانون رقم ١٥١ لسنة ٢٠٢٠

قـام المشـرع المصـري بسـن قانـون رقـم ١٥١ لسـنة ٢٠٢٠ وذلـك بهـدف حمايـة البيانـات الشـخصية عـن طريـق قيـام مركـز حمايـة البيانـات الشـخصية بتنظيـم معالجـة وإتاحـة البيانـات الشـخصية، وبهـذا يكـون البنـد الأول مـن الاتجـاه الثانـي قـد تـم أخـذه فـي الاعتبـار.

قانون الأمن السيبراني

لكـي يكتمـل البنـاء التشـريعي لحمايـة مقـدرات الدولـة المعلوماتيـة (البيانـات الشـخصية والأنظمـة المعلوماتيـة الحرجـة) جـاري العمـل علـى سـن قانـون يقـوم بتحديـد مسـئوليات وصلاحيـات ومهـام المركـز الوطنـي للأمـن السـيبراني علـى غـرار مركـز حمايـة البيانـات الشـخصية، وذلـك لرفـع كفـاءة الأمـن السـيبراني فـي المؤسسـات الحائزة/المشـغلة للبنيـة التحتيـة الحرجـة.

٣,٢ الوضع الحالي للهيكل التشريعي

تـم الانتهـاء مـن المحـور الأول للهيـكل التشـريعي لقوانيـن الأمـن السـيبراني (تجريـم الجانـي)، كمـا تـم الانتهـاء مـن البنـد الأول للمحـور الثانـي (قانـون حمايـة البيانـات الشـخصية)، وجـاري اعتمـاد اللائحـة التنفيذيـة للقانـون. أمـا بالنسـبة للبنـد الثانـي للمحـور الثانـي، فجـاري العمـل علـى إعـداد مسـودة لقانـون الأمـن السـيبراني (**جـدول ٢**).

جـدول ٢ : الـوضـع الحـالي للبنـاء التشـريعي

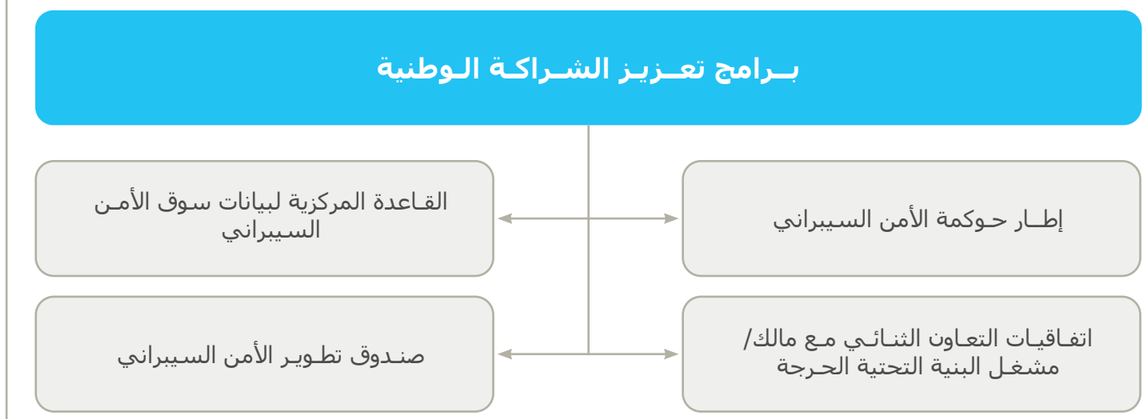
التشـريعـات	المـوقـف الحـالي
قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨	✓
اللائحة التنفيذية - قانون مكافحة جرائم تقنية المعلومات	✓
قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠	✓
اللائحة التنفيذية - قانون حماية البيانات الشخصية	قيد الاعتماد
مسودة قانون الأمن السيبراني	قيد الإعداد

٤ برامج تعزيز الشراكة الوطنية

إن الأمن السيبراني مسئولية جميع المؤسسات سواء كانت المالكة أو المشغلة لبنية معلوماتية. وتتمثل هذه المسئولية في إدراك المخاطر المرتبطة بالبنية المعلوماتية وكيفية حمايتها والجهات المرتبطة بها.

من خلال استراتيجية ٢٠٢٣-٢٠٢٧ ستتعاون الجهات الحكومية وخبراء الأمن السيبراني والتعليم والشركات العاملة في القطاع من أجل المشاركة في وضع وتطوير ومتابعة تنفيذ مبادرات الأمن السيبراني.

تشمل برامج تعزيز الشراكة الوطنية، كما هو مبين في (**رسم توضيحي ٣**)، مبادرات تطوير إطار حوكمة الأمن السيبراني واستحداث اللجنة الاستشارية لصناعة الأمن السيبراني وإبرام اتفاقيات التعاون الثنائي مع مالك / مشغل البنية التحتية الحرجة، إنشاء صندوق تطوير صناعة الأمن السيبراني، وإنشاء قاعدة بيانات إدارة مجال الأمن السيبراني.



رسم توضيحي ٣: برامج تعزيز الشراكة الوطنية

٤,١ إطار حوكمة الأمن السيبراني

تتنوع أدوار الجهات العاملة في مجال الأمن السيبراني بين وضع سياسات أو تنفيذ استراتيجيات أو تقديم خدمات أو تقييم التزامات. ولذلك فإن الهدف من إطار الحوكمة هو وضع هيكل للأمن السيبراني المصري يوضح دور كل جهة (المركز الوطني للأمن السيبراني والمراكز القطاعية ومقدم الخدمة ومسئول الأمن السيبراني ومالك/مشغل البنية المعلوماتية ومالك/مشغل البنية المعلوماتية الحرجة وغير ذلك) ونقاط الاتصال الأساسية والبديلة ومستوى الخدمات المقدمة والوقت المطلوب لتقديمها وكيفية قياس مستوى هذه الخدمة وآليات رفع أداء هذه الخدمات. هذا وسيتم البدء في إنشاء المركز الوطني للأمن السيبراني والمراكز القطاعية والجغرافية والتخصصية طبقا للآتي:

٤,١,١ الهيئة الوطنية للأمن السيبراني

هي هيئة تتبع رئيس الوزراء وتختص بتنظيم العمل في مجال الأمن السيبراني والإشراف على تنفيذ القوانين والالتزامات في ذات المجال في قطاعات الدولة المختلفة.

هذا ويحدد قانون الأمن السيبراني ولائحته التنفيذية صلاحيات ومسئوليات الهيئة والمراكز القطاعية التابعة كافة.

٤,١,٢ المراكز القطاعية والجغرافية والتخصصية

تقوم المراكز القطاعية والجغرافية والتخصصية ببعض أعمال الهيئة في قطاع حكومي معين (الكهرباء أو البترول أو غير ذلك)، أو نطاق جغرافي معين (غرب القاهرة أو جنوب الصعيد او غير ذلك) تحت الإشراف الفني والإداري للهيئة. كما تتعاون وتتكامل هذه المراكز مع بعضها البعض ومع الهيئة الوطنية بهدف الارتقاء بمستوى خدمات الأمن السيبراني في ربوع الجمهورية.

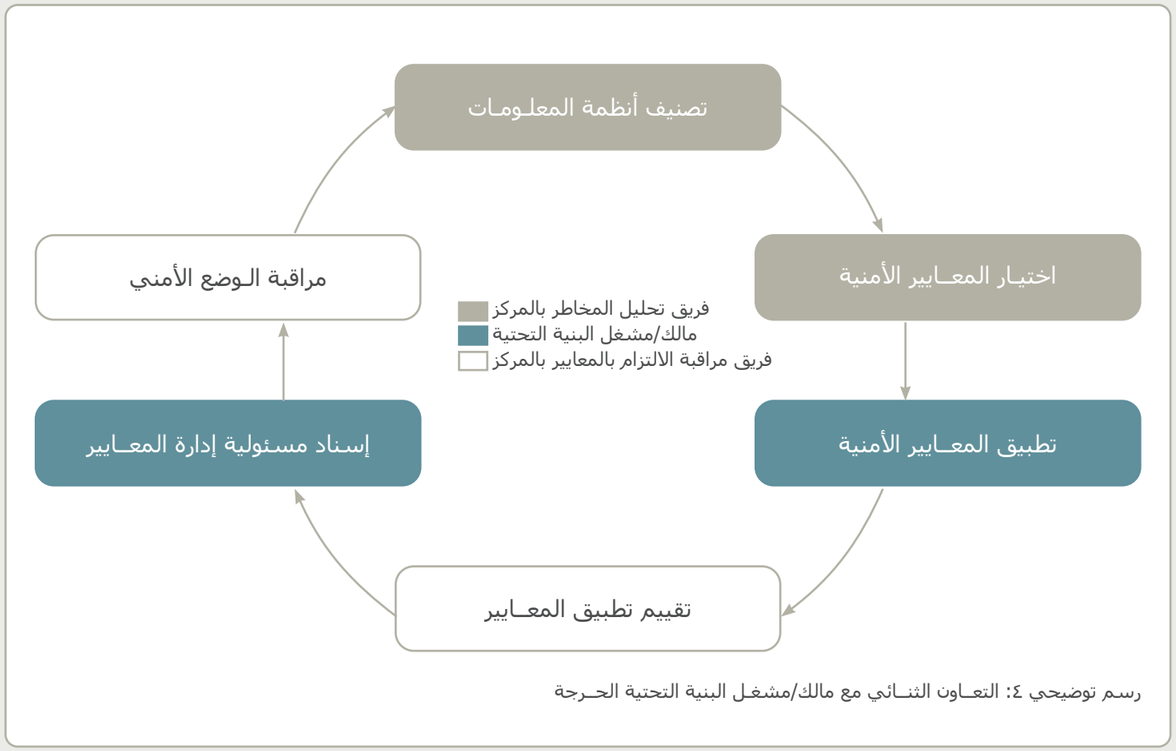
٤,٢ القاعدة المركزية لبيانات سوق الأمن السيبراني

إن وجود قاعدة بيانات مركزية لسوق الأمن السيبراني أمر ضروري لمتابعة تقدم مشاريع الأمن السيبراني ومستوى الخدمات في السوق وأسعارها ومقدرات السوق من الأفراد والشركات والحوادث السيبرانية والعوامل المشتركة بينها وأفضل طرق التصدي لها ووضع خطط مستقبلية لاحتياجات السوق.

كما تساعد قاعدة البيانات كل الشركاء (الهيئة والمراكز التابعة ومالك/مشغل البنية التحتية الحرجة وغير ذلك) على تبادل المعلومات والخبرات السيبرانية للوصول إلى أفضل القرارات.

٤,٣ اتفاقيات التعاون الثنائي مع مالك/مشغل البنية التحتية الحرجة

تغطي إتفاقيات التعاون الثنائي بين المركز ومالك/مشغل البنية التحتية الحرجة ستة جوانب رئيسية، وهي تصنيف أنظمة المعلومات واختيار المعايير الأمنية المناسبة لمستوى المخاطر الأمنية وتطبيق هذه المعايير وتقييم مطابقة تنفيذ التطبيق مع الخطة الموضوعة وإسناد إدارة هذه المعايير للأشخاص المؤهلين داخل المؤسسة ومراقبة التزام جميع الجهات بدمج هذه المعايير في الأعمال اليومية وفي ثقافة المؤسسة. ولتحقيق أعلى مستويات الأمن السيبراني للبنية التحتية المعلوماتية الحرجة سيتم تطبيق أفضل التجارب العالمية في دورة العمل.



رسم توضيحي ٤: التعاون الثنائي مع مالك/مشغل البنية التحتية الحرجة

٤,٤ صندوق تطوير صناعة الأمن السيبراني

لضمان استمرارية أعمال مشاريع الأمن السيبراني ولطبيعة الطوارئ المرتبطة بهذه المشاريع فإنه من الضروري ضمان استمرارية تدفق التمويل. ولذلك فإن دور صندوق تطوير صناعة الأمن السيبراني هو دور محوري في دعم الركائز الأساسية لهذه الصناعة.

رسم توضيحي ٥: صندوق تطوير صناعة الأمن السيبراني

٥ برامج بناء دفاعات سيبرانية قوية وقادرة على الصمود

تشمل برامج بناء دفاعات سيبرانية قوية، كما هو مبين في (**رسم توضيحي ٦: برامج بناء دفاعات سيبرانية قوية وقادرة على الصمود**) التكامل وتعظيم دور مشروعات الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١ ووضع مبادرات دفاعية إضافية، مثل مبادرة clean pipe technology مع مقدمي خدمة الإنترنت لتقليل الهجمات وسوء الاستخدام وتطوير البرنامج المصري EG-Shield للعمل على أجهزة الهاتف المحمول ووضع ضوابط حاكمة للتطبيقات الخاصة بالهواتف المحمولة وخاصة التطبيقات الحكومية والخدمات العامة وكذلك التكنولوجيات الحديثة، مثل IOT, Big Data, Cloud Computing. وكذلك السياسات الأمنية التي تمس أنظمة المعلومات والعاملين عليها.

ذلك بالإضافة إلى المبادرات التي تهدف إلى تحسين مستوى الخدمات في سوق الأمن السيبراني عن طريق إصدار تراخيص لمقدمي الخدمة وكذلك إصدار سجل للخبراء العاملين في المجال مع توضيح مستوى الخبرة وإنشاء أكاديمية للأمن السيبراني تابعة للمركز لرفع مستوى الخبرة للعاملين في المجال.

ومن المبادرات الموجهة إلى القطاع الخاص إنشاء وتطوير موقع لرفع مستوى الأمن السيبراني للشركات الصغيرة ومبادرة رفع مستويات الأمن السيبراني لكبرى الشركات العاملة في الاقتصاد المصري (EGX٣٠).

رسم توضيحي ٦: برامج بناء دفاعات سيبرانية قوية وقادرة على الصمود

٥,١ برامج المشروعات القومية

- التكامل مع مشروعات الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧- ٢٠٢١
- مبادرة clean pipe technology
  هو نوع من الحلول التقنية التي تحمي من هجمات حجب الخدمة (DDoS) قبل أن تؤثر على المواقع الإلكترونية للشركات والمؤسسات المصرية، وبذلك تضمن أن خدمات المؤسسة متاحة للمستخدمين الشرعيين.
- تطوير البرنامج المصري EG- Shield للعمل على أجهزة الهاتف المحمول
- المناورات السيبرانية (National Cyber Crises Exercise)
  وذلك لقياس مدى جاهزية الجهات للتعامل مع الحوادث السيبرانية.

٥,٢ برامج موجهة إلى البنية التحتية الحرجة

- إنشاء المراكز القطاعية في القطاعات الحرجة للدولة
  يعتبر خط الدفاع الأول ضد الحوادث السيبرانية لما له من خبرة في احتياجات هذا القطاع. ويتم تحديد دوره ومسئولياته وتبعيته ومعاملاته المالية وعلاقته مع الجهات الأخرى بالدولة عن طريق المجلس الأعلى للأمن السيبراني.
- مراجعة التزام الجهات الحكومية بمعايير الأمن السيبراني
  وذلك عن طريق زيارات دورية لهذه الجهات.

٥,٣ برامج موجهة إلى القطاع الخاص

- رفع مستويات الأمن السيبراني لكبرى الشركات العاملة في الاقتصاد المصري (EGX٣٠)
  بشكل غير ملزم يقدم المركز استشارات وخدمات مجانية.
- إنشاء وتطوير موقع لرفع مستوى الأمن السيبراني للشركات الصغيرة
  يراعي تصميم هذا الموقع مستوى الوعي المتواضع لأصحاب الشركات الصغيرة عن طريق عرض الإرشادات الأمنية المناسبة لنظام المعلومات المستخدم فقط خطوة بخطوة.

٥,٤ برامج المعايير والسياسات

- وضع ضوابط حاكمة للتطبيقات الخاصة بالهواتف المحمولة خاصة التطبيقات الحكومية والخدمات العامة
- وضع السياسات الأمنية التي تمس أنظمة المعلومات والعاملين عليها
- وضع سياسات وخطط التصدي للمخاطر السيبرانية مثل:
  - خطط التصدي للهجمات السيبرانية (National Cyber Incident Handling Plan)
  - خطط المرونة السيبرانية (National Cyber Resilience Framework)
- وضع ضوابط حاكمة للتكنولوجيات الحديثة، مثل (IOT, Cloud Computing, Big Data)
  مع مراعاة أن تتبنى هذه الضوابط المعايير الدولية، مثل NIST, ISO, FIPS, PCI DSS, NERC, ...

٥,٥ برامج رفع مستوى الخدمات

- إصدار تراخيص لمقدمي خدمات الأمن السيبراني
- إصدار سجل للخبراء العاملين في مجال الأمن السيبراني يوضح مستوى الخبرة
- إنشاء أكاديمية الأمن السيبراني

٦ برامج تعزيز التعاون الدولي

إن التعاون الدولي في مجال الأمن السيبراني هو ضمان لتعزيز المصالح الأمنية والاقتصادية. وبناءً على ذلك فإن دور برامج التعاون الدولي هو تطوير معايير سلوك الدول قبل وفي أثناء وبعد الحوادث السيبرانية وتطبيق القانون الدولي وإدارة الإنترنت (Internet Governance) والابتكار بانتظام بالتعاون مع الدول الأخرى وتيسير سبل الاستثمار في مجال الأمن السيبراني.

تشمل برامج تعزيز التعاون الدولي، كما هو مبين في (**رسم توضيحي ٧: برامج تعزيز التعاون الدولي**)، وضع وتطوير استراتيجية التعاون الدولي في مجال الأمن السيبراني والتي تختص بإرساء مبادئ واتجاهات الدبلوماسية السيبرانية المصرية وفتح آفاق التعاون عربيًا وأفريقيًا وعالميًا ورفع مستوى الابتكار بالتعاون مع الشركاء الدوليين على أن تكون وزارة الخارجية المصرية هي الجهة الوطنية المعنية بإدارة هذا الملف.

برامج تعزيز التعاون الدولى

وضع وتطوير استراتيجية التعاون الدولي في مجال الأمن السيبراني

إرساء مبادئ واتجاهات الدبلوماسية السيرانية المصرية
(The Egyptian Cyber Diplomacy)

الأمن السيبراني

١. تعزيز التعاون من أجل منع الجرائم السيبرانية واكتشافها والتحقيق فيها ومقاضاة مرتكبيها
٢. التعاون على بناء قدرات سيبرانية قوية ومرنة في مصر والمنطقة العربية والأفريقية والعالم
٣. بناء نظام دولى للتعامل مع المعلومات الرقمية المضللة والخاطئة

النمو والابتكار

١. الترابط الإقليمي عن طريق دعم دول المنطقة بخدمات أمن سيبراني آمنة ومجدية اقتصاديًا
٢. حوكمة الإنترنت (سياسات وتقنيات)
٣. تعزيز التعاون مع الشركاء الدوليين قي مجال البحث العلمي، الصناعة، والابتكار

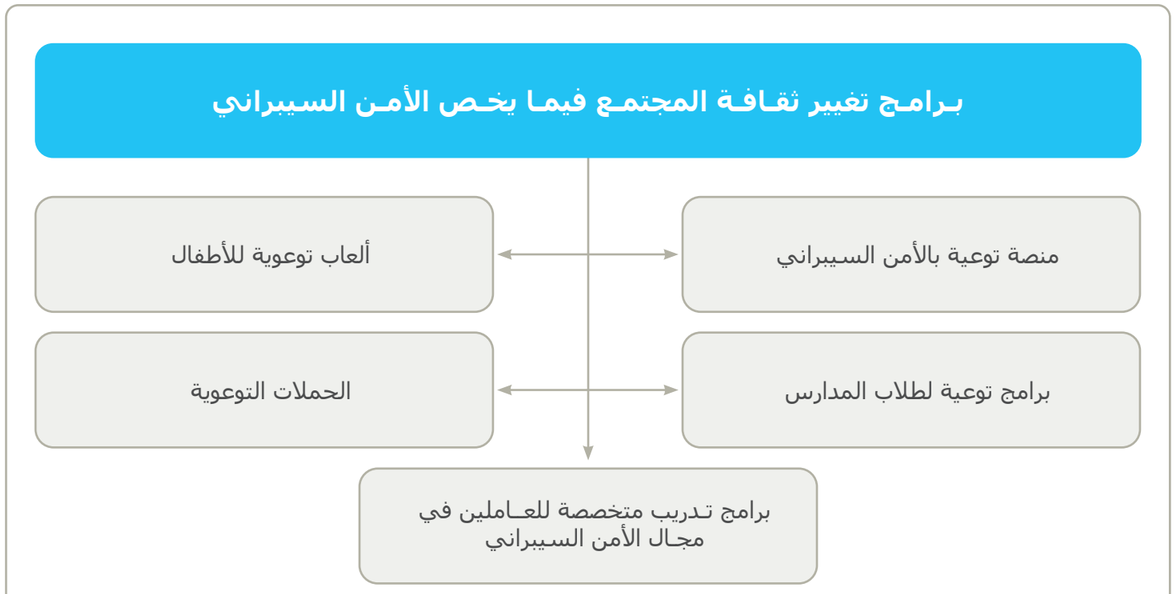
الريادة

طرح مبادرات حول حظر الهجمات السيبرانية على البنية التحتية الحيوية وسبل تحقيق الامن السيبراني على المستويين الإقليمي والدولي

رسم توضيحي ٧: برامج تعزيز التعاون الدولي

٧ برامج تغيير ثقافة المجتمع فيما يخص الأمن السيبراني

تشمل برامج تغيير ثقافة المجتمع فيما يخص الأمن السيبراني، كما هو مبين في (**رسم توضيحي ٨**)، وضع وتطوير برامج توعية فئة مستخدمي الإنترنت المنزلي ووضع وتطوير برامج توعية فئة المستخدمين في الشركات والهيئات والجهات الحكومية والمشاركة في وضع وتطوير مناهج خاصة بتوعية الطلاب في المراحل التعليمية المختلفة بمخاطر الأمن السيبراني.



رسم توضيحي ٨: برامج تعزيز ثقة المجتمع في الفضاء السيبراني

٧,١ منصة التوعية بالأمن السيبراني

تشمل المنصة فيديوهات ومنشورات وإرشادات وغيرها من وسائل التواصل البصري والسمعي للوصول إلى كل فئات المجتمع ونشر المعلومات اللازمة للتعامل مع المخاطر السيبرانية التي قد يتعرض لها الأفراد.

٧,٢ ألعاب توعوية للأطفال

زيادة وعي الأطفال بالمخاطر السيبرانية مهمة تحتاج لاتباع أساليب تواصل غير نمطية، مثل الألعاب التي تمثل جزءًا كبيرًا من أنشطة الأطفال في المراحل العمرية المبكرة من حياتهم. ولذلك تهدف الاستراتيجية إلى وضع وتطوير ألعاب مشوقة موجهة للأطفال تحمل في طياتها التوعية بالمخاطر التي قد يتعرضون لها.

٧,٣ برامج توعية طلاب المدارس

بالإضافة إلى الطرق غير التقليدية في التواصل مع الأطفال، مثل الألعاب، فإن المناهج التخصصية للمراحل التعليمية المختلفة (الابتدائية والإعدادية والثانوية) لها دور كبير في تشكيل وعي الأطفال والشباب. ولذلك تهدف الاستراتيجية إلى وضع وتطوير هذه المناهج باستمرار لمواكبة المتغيرات في هذا المجال.

٧,٤ الحملات التوعوية

تستهدف هذه الحملات كل فئات المجتمع، مثل القطاعين الخاص والعام والمشروعات الصغيرة وكبار السن وأصحاب الهمم والآباء والمعلمين وغيرهم.

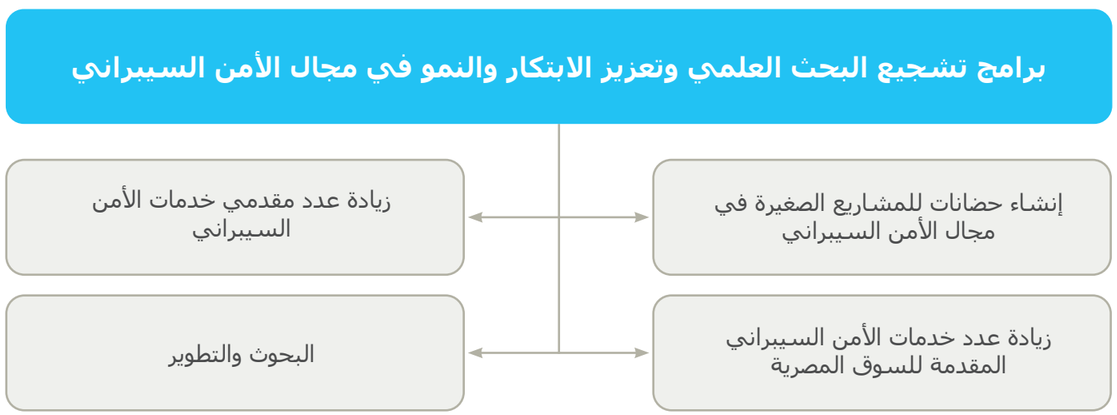
٧,٥ برامج تدريب متخصصة للعاملين في مجال الأمن السيبراني

تهدف هذه المبادرة إلى دعم البرامج الموجودة بالفعل ووضع وتطوير برامج التدريب الوطنية المتخصصة لرفع كفاءة العاملين في المجال.

٨ برامج تشجيع البحث العلمي وتعزيز الابتكار والنمو

تعتمد العديد من الشركات على الثقة في أمن الفضاء السيبراني في الترويج لمنتجاتها. ولذلك فإن الحصول على هذه الثقة يعني أن مصر موقع آمن لتنويع الأعمال والاستثمار.

تشمل برامج تعزيز ثقة المجتمع في الفضاء السيبراني، كما هو مبين في (**رسم توضيحي ٩**)، إنشاء حاضنات للمشاريع الصغيرة في مجال الأمن السيبراني تابعة للمركز وزيادة عدد خدمات الأمن السيبراني المقدمة للسوق المصرية وزيادة عدد مقدمي خدمات الأمن السيبراني، الاهتمام بالبحوث والتطوير.



رسم توضيحي ٩: برامج تعزيز الابتكار والنمو

٨,١ دعم حاضنات المشاريع الصغيرة

يشمل الدعم الفني والإداري والتسويقي والمادي لضمان استمرارية الأعمال ورفع كفاءتها.

٨,٢ زيادة عدد مقدمي الخدمة

عن طريق تشجيع الاستثمار المحلي والأجنبي في مجال الأمن السيبراني

٨,٣ زيادة عدد خدمات الأمن السيبراني

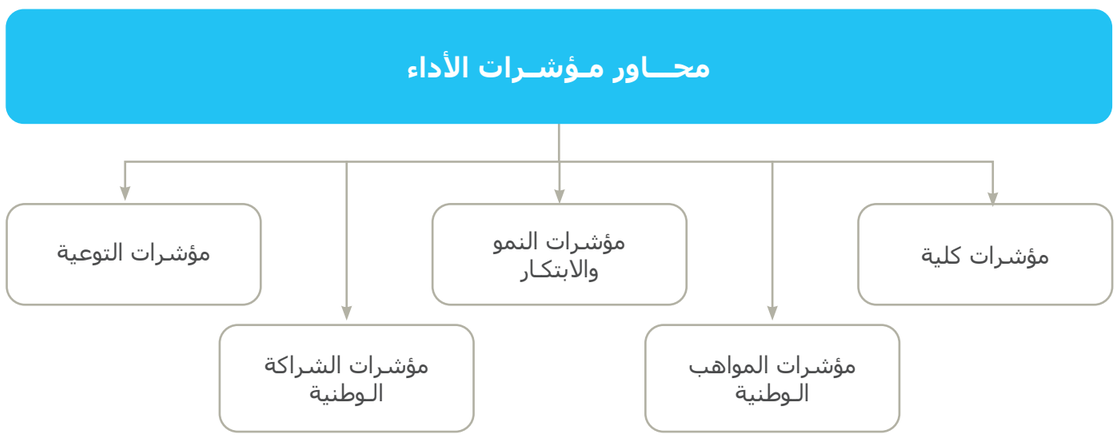
عن طريق توفير الأفراد المدربين والمؤهلين لتقديم هذه الخدمات

٨,٤ البحوث والتطوير

عن طريق التعاون مع الجامعات والمراكز البحثية وشركات القطاعين الخاص والعام والمشروعات الصغيرة

٩ مؤشرات الأداء

إن الهدف من مؤشرات الأداء (Key Performance Indicators) هو متابعة تنفيذ استراتيجية الأمن السيبراني وتحديد بوصلة المسار الصحيح بدقة وتقييم تقدم مشاريع الاستراتيجية باستمرار. وفيما يلي مجموعة من المقاييس الكمية والنوعية لقياس مدى تقدم الرؤية من خال الفحص الملموس. وستقوم معايير التقييم على خمسة محاور رئيسية كما هو مبين في (**رسم توضيحي ١٠**). وسيقوم المركز الوطني للأمن السيبراني بمراقبة تقدم الاستراتيجية من خلال ٢٠ مؤشر أداء فرعيًا.



رسم توضيحي ١٠: محاور مؤشرات الأداء

٩,١ مؤشرات كلية

- إسهام صناعة الأمن السيبراني في تعزيز نمو إجمالي الناتج المحلي القومي (GDP)
- عدد مقدمي خدمات الأمن السيبراني المرخص لهم
- عدد خدمات الأمن السيبراني المقدمة في السوق المصرية

٩,٢ مؤشرات النمو والابتكار

- عدد الأوراق البحثية المنشورة في المجلات العلمية المرموقة
- عدد الجهات التي تقدمت بأوراق بحثية مقبولة
- تمثيل مصر في المحافل الدولية
- تقدم مصر في مؤشرات (GCI)
- عدد المشاريع الصغيرة التي انضمت للحاضنات

٩,٣ مؤشرات التوعية

- عدد حملات التوعية التي تستهدف التجمعات (المدارس والنوادي والجهات الحكومية وغير ذلك)
- عدد المنشورات في وسائل التواصل الاجتماعي المختلفة
- عدد المتابعين على وسائل التواصل
- عدد المشاهدين على وسائل التواصل

٩,٤ مؤشرات المواهب الوطنية

- عدد البرامج التدريبية
- عدد المتقدمين للبرامج التدريبية
- عدد المتخرجين من البرامج التدريبية
- عدد المرخص لهم بمزاولة المهنة
- العدد الإجمالي للخريجين المعينين

٩,٥ مؤشرات الشراكة الوطنية

- عدد اتفاقيات التعاون الثنائي مع الجهات الحكومية
- عدد المشروعات الممولة من صندوق إدارة التعاون
- عدد الجهات الحكومية التي قامت بتعيين مسئول أمن سيبراني (نقطة اتصال)