الجمهورية العربية السورية

وزارة الاتصالات والتقانة

استراتيجية الأمن السيبراني للجمهورية العربية السورية

الملخص التنفيذي

تتزايد التهديدات لأنظمة المعلومات والبيانات مما أدى لتزايد الاهتمام عالمياً بمواضيع الأمن السبراني لحماية الأصول المعلوماتية كونها تشكل أحد أهم الموارد في ظل التطورات التقانية الحديثة، لذلك بدأت الدول بوضع السياسات العامة والاستراتيجيات والسياسات التنفيذية لحماية معلوماتها من (التخريب – التعديل – الحذف – السرقة...)، وتتالت الدعوات للتعاون بين الدول في مجال صياغة استراتيجيات واتفاقيات مشتركة للتصدي لأي محاولة اختراق سبرانية لمعلوماتها، وكان آخرها اللجنة المفتوحة العضوية في الأمم المتحدة التي تُعنى بوضع اتفاقيات دولية شاملة لمكافحة استخدام وسائل تقانة المعلومات لأغراض إجرامية.

اعتمدت وزارة الاتصالات والتقانة الاستراتيجية الوطنية للتحول الرقمي في الخدمات الحكومية الإلكترونية وعملت على تنظيم عمل التطبيقات الإلكترونية، وتشجيع خدمات الدفع الإلكتروني، ونشر الحزمة العريضة، وإدخال المشغل الثالث للاتصالات النقالة الذي سيؤدي إلى تزايد حجم المعلومات والبيانات المتداولة على الشبكة، لذلك تسعى الجمهورية العربية السورية من خلال هذه الاستراتيجية إلى تطوير قدراتها في مجال الأمن السبراني، بهدف تعزيز مستوى حماية الأصول المعلوماتية من المخاطر السبرانية الداخلية والخارجية التي يمكن أن تؤثر بشكل كبير على مقدرات الدولة السورية، وبهدف امتلاك الأدوات التقانية اللازمة للتصدي لهذه المخاطر بما يساهم في تحسين البيئة المحيطة بالأمن السبراني، وزيادة التعاون الدولي، وتحسين الجوانب التنظيمية وبناء القدرات مع نشر الوعي والثقافة الأمنية السبرانية بين أفراد المجتمع لتعزيز الانتقال الآمن بالاقتصاد السوري إلى الاقتصاد الرقمي.

أعدّت وزارة الاتصالات والتقانة هذه الاستراتيجية الخاصة بالأمن السبراني بالتعاون مع الشركاء الاستراتيجيين والتي جاءت بناءً على تحليل الواقع الراهن وأفضل الممارسات العالمية وبما يتوافق مع الاستراتيجية الوطنية للتحول الرقمي وبرنامج سورية ما بعد الحرب، متضمنة سبعة أهداف رئيسية:

1. تأسيس بنية أمن سبراني قوية ومستدامة توفر الحماية المتكاملة للأصول المعلوماتية والتقنية.
2. إدارة فعالة متكاملة لمواجهة التهديدات والتصدي للمخاطر على مستوى الجمهورية العربية السورية. 3. تطوير الجوانب التشريعية والتنظيمية الخاصة بالأمن السبراني.
4. تطوير وصقل الإمكانات الوطنية البشرية والتقنية للأمن السبراني، وبناء الثقافة وإذكاء الوعي المجتمعي للوصول لأفضل الممارسات في مجال الأمن السبراني.
5. تشجيع البحث العلمي والابتكار في مجال الأمن السبراني.
6. تحقيق الحوكمة الفعالة للتنسيق بين جميع الجهات وضمان حُسن التنفيذ.
7. تعزيز التنسيق والتعاون في قضايا الأمن السبراني على المستويين الإقليمي والدولي.

الفهـــــــرس

المقـــــــدمة

تكتسب تكنولوجيا المعلومات والاتصالات أهمية كبيرة في تحقيق التنمية الاقتصادية والاجتماعية، وتزداد الأهمية أكثر في ظل الاعتماد المتزايد على شبكة الإنترنت لتبادل المعلومات والخدمات في الأعمال التجارية والحكومية، وتحول الاقتصاد التقليدي إلى الاقتصاد الرقمي من خلال رقمنة عدد من المجالات والقطاعات المختلفة، إلا أن ذلك أدى أيضاً إلى وجود بيئة ملائمة للجرائم المعلوماتية، لذلك تزايد الاهتمام بالأمن السبراني وأصبح أمن المعلومات الرقمية جزءاً من الأمن الوطني وأمن الأفراد والشركات.

تسعى حكومة الجمهورية العربية السورية إلى تعزيز الاهتمام في مجالات الأمن السبراني، من خلال تطوير السياسات، وتوفير الأدوات اللازمة لحماية الأصول المعلوماتية، وتعزيز القدرات الوطنية في مواجهة المخاطر السبرانية المحتملة. وتشكل هذه الوثيقة التوجهات الوطنية الأساسية وإطار عمل مرجعي للعاملين والمهتمين في مجال الأمن السبراني من القطاعين العام والخاص، بما يضمن الوصول إلى درجات مقبولة في حماية الأصول المعلوماتية وفقاً لأهميتها، ويضمن توزيع الأدوار وتحديد الصلاحيات بين جميع الأطراف سواء داخل المؤسسات أو على المستوى الوطني.

وبناء عليه تم تشكيل فريق من الخبراء المختصين بالأمن السبراني لوضع رؤية عمل مشتركة في مجال أمن الاتصالات والمعلومات من خلال تحليل الواقع الراهن والانطلاق إلى تحديد الأخطار المختلفة التي تهدد نظم المعلومات ووضع السبل الكفيلة بحماية البيانات المتضمنة فيها مع وضع المقترحات الكفيلة بتحقيق هذه الرؤية.

نطـــــاق العمـــل

تركز هذه الاستراتيجية على حماية الجوانب المدنية للفضاء السبراني، وتغطي جميع الجوانب المختلفة للحوكمة، والسياسات التنفيذية والجوانب التشغيلية، والتقنية، والقانونية والتنظيمية للأفراد والشركات والجهات الحكومية وغير الحكومية. وتسلط الضوء على المبادئ الشاملة وأفضل الممارسات التي يتعين النظر فيها لتحقيق وإدارة استراتيجية وطنية للأمن السبراني ووضعها موضع التنفيذ.ويشمل نطاق الاستراتيجية الوطنية للأمن السبراني الأولويات الوطنية فضلاً عن الإطار العام للشراكة والتعاون الدولي بشأن الأمن السبراني وفق المجالات التالية:

1. الحوكمة والامتثال والتنفيذ. 2. التشريع والتنظيم.
3. البنية التحتية وتكنولوجيا الأمن السبراني.
4. بناء القدرات وثقافة الأمن السبراني وإذكاء الوعي.
5. البحث والتطوير وتشجيع الابتكار نحو الاعتماد على الذات. 6. إدارة مخاطر الأمن السبراني.
7. التنسيق والتعاون على المستويين الإقليمي والدولي.

الرؤيـــــــة

" فضاء سبراني آمن وموثوق في جميع المجالات، بما يسهم في حماية المصالح الوطنية ويعزز الثقة في التحول الرقمي"

الأهـــــداف

تسعى هذه الاستراتيجية إلى تحقيق الأهداف الآتية:

1. تأسيس بنية أمن سبراني قوية ومستدامة توفر الحماية المتكاملة للأصول المعلوماتية والتقنية.
2. إدارة فعالة ومتكاملة لمواجهة التهديدات والتصدي للمخاطر على مستوى الجمهورية العربية السورية. 3. تطوير الجوانب التشريعية، والتنظيمية، ووضع القواعد القانونية الملائمة، والإجراءات المتبعة للتصدي للجرائم الخاصة بالأمن السبراني.
4. تطوير وصقل الإمكانات الوطنية البشرية والتقنية للأمن السبراني، وبناء الثقافة وإذكاء الوعي المجتمعي للوصول لأفضل الممارسات في مجال الأمن السبراني.
5. تشجيع الأبحاث والتحقيقات والبحث العلمي في مجال الأمن السبراني. 6. تحقيق الحوكمة الفعالة للتنسيق بين جميع الجهات وضمان حُسن التنفيذ.
7. تعزيز التنسيق والتعاون في قضايا الأمن السبراني على المستويين الإقليمي والدولي.

مدخلات استراتيجية

تعتبر استراتيجية الأمن السبراني إحدى الاستراتيجيات القطاعية في مجال الاتصالات والمعلومات، وتتكامل مع السياسات والاستراتيجيات الأخرى التي يجري اعتمادها أو تنفيذها في سورية بما يضمن اتساق المسارات، حيث هناك مساران استراتيجيان أساسيان في الجمهورية العربية السورية:

أ. البيان الحكومي لعام 2021: والذي تضمّن في جزئه الخاص بوزارة الاتصالات والتقانة ثلاثة برامج تنفيذية أساسية بعيدة المدى (مدة كل منها عشر سنوات):

1. برنامج التحول الرقمي للخدمات الحكومية الإلكترونية. 2. برنامج دعم الصناعات المعلوماتية.
3. برنامج تطوير البنى التحتية لقطاع الاتصالات والمعلومات.

ترتبط استراتيجية الأمن السبراني ارتباطاً وثيقاً بالبرامج الثلاثة، وعلى وجه الخصوص البرنامج الأول، وجاءت الاستراتيجية الوطنية للتحول الرقمي للخدمات الحكومية كخطة تنفيذية متضمنة برنامجاً فرعياً مخصصاً (البرنامج العاشر – أمن المعلومات)، ويهدف إلى وضع السياسات وتوفير الأدوات والمعايير اللازمة لحماية المعلومات والبيانات الوطنية.

ب. وثيقة سورية ما بعد الحرب: يعدّ البرنامج الوطني التنموي لسورية ما بعد الحرب بمثابة الخطة الاستراتيجية التنموية لسورية حتى أفق عام 2030 وما بعد، وهي تظهر توجهات الحكومة السورية وخططها الواعية والهادفة إلى رسم المشهد السوري في المرحلة المقبلة، حيث يمر تنفيذ البرنامج بأربع مراحل رئيسية، وفق ما يلي:

وفيما يخص قطاع الاتصالات وتقانة المعلومات، يركز البرنامج أهدافه الرئيسية على شكل غايات تستهدف قيم العديد من المؤشرات ومنها مؤشرات تطوير الحكومة الإلكترونية والمؤشر العالمي للأمن السبراني، وهي مؤشرات ترتبط بشكل أو بآخر باستراتيجية الأمن السبراني. كما تتسق هذه الاستراتيجية أيضاً مع المسارات الدولية في مجال الأمن السبراني، إذ أطلق الاتحاد الدولي للاتصالات مبادرة البرنامج العالمي للأمن السبراني CGA: Global Cybersecurity Agenda في عام 2007، والتي وُضعت بهدف تعظيم التعاون والكفاءة وتشجيع التعاون مع جميع الشركاء والاستفادة من المبادرات القائمة لتفادي تكرار الجهود، وتتمحور هذه المبادرة حول خمس ركائز رئيسية: الإجراءات القانونية، والإجراءات التقنية، والبنى التنظيمية، وبناء القدرات، والتعاون الدولي.

كما اعتمد مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات لعام 2018 الذي عُقد في دبي القرار 130 بعنوان: تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، ونص القرار على جملة من القضايا تضمنت استخدام إطار البرنامج العالمي للأمن السبراني لمواصلة توجيه عمل الاتحاد بشأن الجهود الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

ويقوم الاتحاد الدولي للاتصالات بإجراء قياس دوري من خلال نموذج أعده خصيصاً لهذا الغرض باسم النموذج العالمي للأمن السبراني Global Cybersecurity Index، وهو يقيس مدى تقدم الدول في كل من الركائز الخمس التي تتضمنها المبادرة، وفي هذا السياق تؤكد تقارير الاتحاد على أن وجود سياسة وطنية للأمن السبراني هو حجر الأساس لركيزة البنى التنظيمية، وقد صيغت هذه الاستراتيجية بالاستفادة من الدليل الاسترشادي الذي أعده الاتحاد لبناء استراتيجيات الأمن السبراني، وقد حُددت أهداف الاستراتيجية بحيث تتوافق مع ركائز مبادرة البرنامج العالمي للأمن السبراني.

تحليل الواقع الراهن

نعرض في هذا القسم تلخيصاً وصفياً لأهم النتائج التي تم التوصل إليها نتيجة تحليل الوضع الراهن للأمن السبراني في سورية، حيث تم إعداد استبيان لدراسة الواقع الراهن جرى توجيهه للجهات الحكومية، بالإضافة إلى المشاهدات المتوفرة لدى فريق العمل في القطاع العام.

مؤشرات الواقع الراهن

أظهرت المؤشرات العالمية المرتبطة بالأمن السبراني في سورية تراجعاً ملحوظاً خلال العامين الماضيين، حيث احتلت سورية موقعاً متأخراً في العام 2020 على المستويين العالمي والعربي على حد سواء، حيث كان مؤشر الأمن السبراني لسورية هو 22,14 % واحتلت المرتبة 126 على المستوى العالمي بتأخر 12 مرتبة عن العام 2018، وتظهر النتائج التفصيلية أن هناك ضعفاً في جميع الركائز بدرجات متفاوتة، وأقلها ضعفاً هي ركيزة الإجراءات القانونية، ويظهر الضعف الأكبر في ركيزتي بناء القدرات وإجراءات التعاون الدولي، تليها ركيزة البنى التنظيمية والتي يتوقع أن تتحسن بعد إقرار هذه الاستراتيجية.

واقع الموارد البشرية

بينت الدراسة التحليلية (المرفق رقم1) لواقع الأمن السبراني نقص خبرة الموارد البشرية العاملة لدى القطاع العام في مواجهة حالات الطوارئ على الشبكة بغض النظر عن نوعها، وعدم القدرة على وضع وتطبيق سياسات أمن المعلومات، ويُعزى ذلك إلى عدم القدرة على استقطاب الكوادر البشرية للعمل في مجال أمن المعلومات بسبب ضعف الأجور، وتدني مستوى التدريب والتأهيل في مجال أمن المعلومات، وهذا ما أدى إلى تراجع واضح في مؤهلات الموارد البشرية العاملة في هذا المجال.

البيئة التشريعية والتنظيمية

- أولت الحكومة السورية خلال السنوات السابقة اهتماماً ملحوظاً بتشريعات الفضاء السبراني، حيث جرى إصدار العديد من القوانين وهي:
  - قانون التوقيع الرقمي وخدمات تقانة المعلومات. - قانون مكافحة الجريمة المعلوماتية.
  - قانون المعاملات الإلكترونية.

  ومازال هناك حاجة لإصدار قانون يتعلق بحماية البيانات الشخصية.
- وقد عملت وزارة الاتصالات والتقانة خلال السنوات السابقة على إعداد بعض السياسات التي تشكل الإطار التنظيمي والمعيار الوطني المتوافق مع المعايير العالمية لإعداد السياسات التنفيذية لأمن المعلومات وصدرت الوثائق الآتية:
  - السياسة الوطنية لأمن المعلومات، والتي تشكل المعيار الوطني لأمن المعلومات.
- السياسة الوطنية للتشفير، والتي تشكل المعيار الوطني للتشفير؛ كما نفذت الوزارة عدداً من الدورات التدريبية وورشات العمل على هذه القوانين والسياسات.

- وبدأت الوزارة بتنظيم خدمات أمن المعلومات من خلال اعتمادية الشركات العاملة في مجال أمن المعلومات، بما يضمن توفر شركات مؤهلة في السوق المحلية مختصة في هذا المجال.
- تم إحداث فرع خاص بمكافحة الجريمة المعلوماتية في وزارة الداخلية، وإحداث محكمة خاصة بالجرائم المعلوماتية وجرائم الاتصالات، مع وجود صعوبات في حسم مسألة الاختصاص القضائي في الجرائم الإلكترونية العابرة للحدود.
- ولكن من الملاحظ عدم توفر سياسات أمن معلومات لدى الجهات الحكومية تتوافق مع السياسة الوطنية لأمن المعلومات؛ بالإضافة إلى عدم وجود وحدة وظيفية متخصصة بأمن المعلومات لدى تلك الجهات، مهمتها المحافظة على البيانات الرقمية والمنظومات المعلوماتية كأحد أهم الأصول لدى المؤسسات في الوقت الراهن.

البيئة الفنية

بينت الدراسة التحليلية لواقع الأمن السبراني عدم وجود مراكز متخصصة بالاستجابة للطوارئ المعلوماتية، وعدم لحظ مشاريع متخصصة بأمن المعلومات.

وقد بينت تقارير المسح الأمني الصادرة عن مركز أمن المعلومات في الهيئة الوطنية لخدمات تقانة المعلومات وجود ثغرات أمنية في أغلب المواقع والخدمات الإلكترونية تنوعت في مستوى خطورتها، وبالرغم من تسجيل تحسن ملحوظ خلال السنوات الأخيرة إلا أن المؤشرات التالية بينت ما يلي:

1- ما زالت الثغرات عالية الخطورة تشكل 20 % من الثغرات المكتشفة.
2- حوالي 21 % فقط من المواقع الحكومية التي خضعت للمسح الأمني عام 2021 خالية من الثغرات الأمنية.

واقع الشراكات والتعاون الإقليمي والدولي

بينت الدراسة أن واقع الشراكات والتعاون الإقليمي والدولي في مجال أمن المعلومات محدود، وخصوصاً خلال سنوات الحرب والحصار الاقتصادي، ونظراً لعدم وجود مركز استجابة للطوارئ المعلوماتية متخصص بإقامة شراكات وتعاون إقليمي ودولي، فإن الواقع اقتصر على بعض الشراكات بين الشركات الخاصة المحلية والأجنبية وخصوصاً في القطاع المصرفي.

واقع التعليم العالي والبحث العلمي

تتنوع تسميات المقررات الجامعية السورية التي ترتبط بمفاهيم الأمن السبراني، ولكن يمكن تصنيفها في ثلاثة أنماط وفق أهداف المقرر واختصاصات الطلاب التي تنتمي عموماً إلى الهندسات والتقانات والرياضيات، وتركزت بالآتي:

1- أمن نظم المعلومات. 2- أمن الشبكات.

3- نظم التشفير.

وتركز هذه المقررات على معارف في حلول الأمن السبراني، في حين يحتاج مختصو الأمن السبراني في المؤسسات المختلفة إلى معارف في إدارة نظم الأمن السبراني، وأيضاً إلى معارف في تقييم وتدقيق أمن نظم المعلومات، ولم تتوجه الجامعات السورية، ولا سيما كليات الهندسة المعلوماتية وهندسة الاتصالات، إلى إضافة اختصاص في الأمن السبراني يغطي كافة المعارف المذكورة.

أما فيما يتعلق بالدراسات العليا، فلا يوجد في المؤسسات الأكاديمية السورية برامج ماجستير أو دكتوراه في الأمن السبراني تحديداً، ولكن بالمقابل يوجد العديد من مشاريع ورسائل الماجستير والدكتوراه التي تدمج بين الأمن السبراني ومجال الاختصاص الأساسي.

البرامج والمشاريع والمبادرات

البرنامج الأول أمن البنى التحتية

يهدف هذا البرنامج إلى دعم الشبكة والنظم المعلوماتية الوطنية بالحلول الأمنية العتادية والبرمجية والتصميمية لزيادة مناعتها في مواجهة الهجمات الإلكترونية وفق ما يلي:

أ. إنشاء وتطوير المركز الوطني للاستجابة للطوارئ المعلوماتية.

حيث يعتبر المركز أو وحدات الكشف المبكر عن الهجمات السبرانية هو خط الدفاع الأول من خلال تعاون حكومي – حكومي لبناء المركز الذي يؤمن كشف مصادر الهجمات السبرانية، وتحليل أساليب عملها، والثغرات المستخدمة.

ب. تأهيل فريق الاستجابة للطوارئ المعلوماتية بحيث يكون مختصاً بتكنولوجيا المعلومات وأمنها، مهمته مساعدة الجهات العامة والخاصة والشركات والأفراد على الاستجابة والحد والوقاية من الحوادث السبرانية وتقديم الدعم اللازم بهذا المجال من خلال:

- اكتشاف الهجمات السبرانية.
- الاستجابة للحوادث السبرانية.
- الحماية والتأمين ومعالجة الحوادث السبرانية.

ج. تشكيل فرق عمل للاستجابة للطوارئ المعلوماتية في المؤسسات التي لديها منظومات معلوماتية ذات بيانات وخدمات حرجة.

د. استكمال بناء منظومة التوقيع الرقمي بهدف التحقق من هوية الموقع وسلامة تبادل البيانات المرسلة وعدم الإنكار وتقديم خدمات الختم الزمني.

ه. تعزيز البنية التحتية المعلوماتية للمؤسسات التي لديها منظومات معلوماتية ذات بيانات وخدمات حرجة لمواجهة أخطار أمن المعلومات.

البرنامج الثاني تطوير الإطار القانوني والتنظيمي

يهدف البرنامج إلى مراجعة الجوانب القانونية والتنظيمية المتعلقة بالأمن السبراني من قوانين وسياسات وضوابط وفق ما يلي:

أ . إصدار تشريع للأمن السبراني بعد مراجعة شاملة لكافة القوانين ذات الصلة بالأمن السبراني.

ب. إصدار قانون حماية البيانات الشخصية.

ت. تطوير وتحديث السياسات في مجال الأمن السبراني.

البرنامج الثالث نشر ثقافة الوعي السبراني

يهدف هذا البرنامج إلى تنمية "ثقافة الوعي السبراني"، والتي تهدف بشكل رئيسي إلى تعزيز الوعي العام للمستخدمين بالقضايا الأساسية المتعلقة بالأمن السبراني، ويمكن تحديد خمسة مسارات رئيسية لعمل البرنامج:

أ . تعزيز الوعي بقضايا الأمن السبراني: ويقصد بذلك تضمين مفاهيم الأمن السبراني في القيم والسلوكيات والممارسات الخاصة بالحكومة والقطاع الخاص والمستخدمين بشكل عام، وذلك بهدف تعظيم قدرة المستخدمين على حماية أنفسهم من المخاطر الناتجة عن نشاطهم على الشبكة.

ب. تعزيز الثقة لدى المستخدمين تجاه الخدمات المقدمة على الشبكة: ويتم ذلك من خلال زيادة قدرة المستخدمين على تقييم المعلومات المقدمة لهم عبر الشبكة، وتمكينهم من تقييم مصداقية مواقع الوب ونتائج البحث المقدمة لهم، ومدى إتاحة الخدمات التي تسمح للمستخدمين بالتمييز بين المعلومات الصحيحة والمضللة، واتخاذ الإجراءات الكفيلة بزيادة ثقة المستخدمين بالخدمات الإلكترونية.

ت. تعزيز فهم المستخدمين لأهمية حماية بياناتهم على الشبكة: ويتم ذلك من خلال رفع سوية الوعي لدى المستخدمين لأهمية حماية بياناتهم الشخصية، وتمكينهم من اتخاذ الإجرائيات الكفيلة بحماية تلك البيانات.

ث. وضع آلية لإدارة ومعالجة الشكاوى تسمح للمستخدمين بتقديم الشكاوى بخصوص الاستخدامات المسيئة على شبكة الإنترنت، ومنها النصب والاحتيال عن طريق الشبكة، والابتزاز وانتحال الشخصية.

ج. الاعتماد على وسائل الإعلام والمنصات الإعلامية الرقمية في تغطية القضايا المتعلقة بالأمن السبراني، ولفت النظر إلى أهمية تلك القضايا، والإسهام في وضع السلوكيات والممارسات المذكورة في البند الأول.

البرنامج الرابع بناء القدرات والمعرفة

يهدف هذا البرنامج إلى تنمية القدرات في مجال الأمن السبراني لدى الحكومة والقطاع الخاص والمواطنين بشكل عام، وذلك على مختلف المستويات: مستوى رفع الوعي الأبسط، والمناهج التعليمية، والتدريب الاحترافي في مجالات الأمن السبراني.

ويمكن أن ينفذ هذا البرنامج وفق أربعة مسارات رئيسية هي:

أ. التعليم في مجالات الأمن السبراني: توفير مواد تعليمية من سوية جيدة في مجالات الأمن السبراني مع عدد كاف من المعلمين والمحاضرين، ويقتضي ذلك وجود تكامل بين القطاع التعليمي وقطاع الأعمال للتأكد من ربط مخرجات التعليم باحتياجات سوق العمل.

ب. التدريب الاحترافي في مجالات الأمن السبراني: توفير برامج تدريب احترافية تساعد في بناء الكوادر البشرية المتخصصة في مجالات الأمن السبراني، وتوطين المعرفة في هذا المجال ضمن المؤسسات ونقلها وتبادلها.

ت. البحث والابتكار في مجالات الأمن السبراني: من خلال العمل على امتلاك القدرات العالية المستوى الكفيلة بإنتاج الابتكارات والقيام بالأبحاث العلمية المتطورة في مجالات الأمن السبراني، وذلك بما يسمح بمواجهة التحديات التي تواجه القطاعات المختلفة التي تعتمد على تقانة المعلومات والاتصالات، مع ضرورة تفعيل التشاركية بين القطاعين العام والخاص بهدف تعزيز الاستثمارات مما يؤدي إلى تحقيق الأهداف المطلوبة.

البرنامج الخامس الشراكات والتعاون الإقليمي والدولي

يهدف البرنامج إلى تطوير الشراكات والتعاون على المستويين الإقليمي والدولي وفق ما يلي:

أ. تعزيز التعاون الدولي وخصوصاً مع الدول الصديقة في مجال الأمن السبراني، بما يسمح بتباد الخبرات والإنذار المبكر حول الأخطار المحتملة والحوادث الأمنية الشائعة، ووضع آليات للتصدي لهذه الحوادث وخطة لمعالجتها من خلال مراكز الاستجابة للطوارئ المعلوماتية، وصولاً لإيجاد اتفاقات دولية وعربية في مجال مكافحة الجرائم الإلكترونية بما يضمن المشاركة بالمعلومات التقنية كناتج لهذا التعاون ويعزز من قدرة سورية على التصدي للهجمات السبرانية.

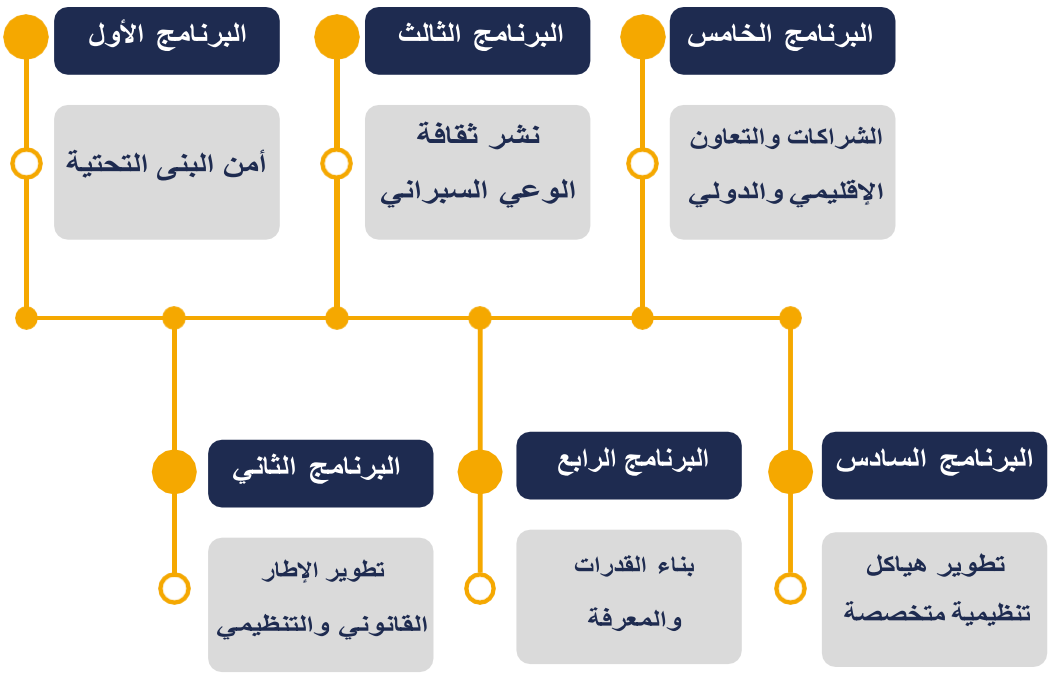
ب. تعزيز دور القطاع الخاص المحلي في مجال الأمن السبراني، بما يساهم فيدعم الجهود الوطنية الرامية إلى رفع مستوى أمن المعلومات في القطاعين العام والخاص، وخلق شراكات وتعاون مشترك يكون فيها القطاع الخاص شريك في الاستجابة للطوارئ والتصدي للحوادث على الشبكة.

البرنامج السادس تطوير هياكل تنظيمية متخصصة

من أهم المشكلات والتحديات التي تعترض نشر مفهوم الأمن السبراني هو تحديد المسؤوليات والمهام للعاملين في المؤسسة أو الوزارة، لذلك يعتبر إنشاء وحدات تنظيمية متخصصة تُعنى بالأمن السبراني في كل جهة عامة ضرورة ملحة، مع تأمين المستلزمات الفنية والكوادر البشرية المؤهلة والمدربة والتي تسهم في تنفيذ الاستراتيجية المقرة من الحكومة.

قائمة المشاريع والمبادرات

يبين الجدول أدناه قائمة البرامج والجهات المسؤولة عن التخطيط ومتابعة التنفيذ بما يضمن تحقيق البرنامج لأهدافه المحددة، والجهات المشاركة في تنفيذ البرنامج، والمشاريع والمبادرات المقترحة ضمن كل برنامج والتي تضم ثمانية مشاريع وثلاث عشر مبادرة، تشكل قائمة المشاريع لمدة عامين فقط من تاريخ إقرار الاستراتيجية، حيث قد تشكل بعض المبادرات لبنة أساسية لمشاريع مستقبلية، بما يتوافق مع الاستراتيجية ومع التطورات التكنولوجية عالمياً والاحتياجات والتهديدات المحتملة:



البرنامج الأول : أمن البنى التحتية

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
أمن البنى التحتية	وزارة الاتصالات والتقانة	كافة الجهات العامة

المشاريع المقترحة للبرنامج الأول

اسم المشروع	وصف المشروع	الجهة المسؤولة
مشروع مركز الاستجابة للطوارئ المعلوماتية	- إنشاء مركز تنسيق على المستوى الوطني و/أو على المستوى الإقليمي بشكل مركزي، بهدف التنسيق للتعامل مع الحوادث المعلوماتية الطارئة، ويوفر إمكانية الربط مستقبلاً مع مراكز استجابة للطوارئ المعلوماتية في الجمهورية العربية السورية. - بناء فريق استجابة للطوارئ المعلوماتية يتمتع بالمؤهلات والخبرات المناسبة ومتابعة تدريب وتأهيل أعضاء الفريق بشكل مستمر، وتتبع التطورات في مجال أمن المعلومات.	الهيئة الوطنية لخدمات تقانة المعلومات
مركز التصديق الإلكتروني	تأمين منظومة مبنية بأفضل الممارسات لإدارة دورة حياة الشهادات الرقمية للعاملين بالقطاع العام والخاص. - اعتماد شهادة جذر وطنية يمكنها توقيع واعتماد شهادات مزودي خدمات تصديق فرعية	الهيئة الوطنية لخدمات تقانة المعلومات
المنصة الوطنية لمؤشرات الأمن السبراني	إنشاء منصة وطنية لتقييم الأمن السبراني من خلال مجموعة من التقارير الإحصائية الدورية	الهيئة الوطنية لخدمات تقانة المعلومات
مراكز استجابة قطاعية للأمن السبراني لدى بعض جهات القطاع العام	إنشاء فرق وطنية قطاعية للاستجابة للطوارئ المعلوماتية	الجهات الحكومية المعنية

المبادرات / الإجراءات للبرنامج الأول

المبادرة	الهدف	الجهة المسؤولة
مبادرة حماية المنظومات المعلوماتية في الجهات العامة	تهدف هذه المبادرة إلى تطبيق آليات حماية على المنظومات المعلوماتية في كافة الجهات الحكومية وفق معايير معتمدة من قبل الهيئة الوطنية لخدمات تقانة المعلومات وبما يتوافق مع المعايير العالمية	الهيئة الوطنية لخدمات تقانة المعلومات

ملاحظة: تعتبر المشاريع 1، 2 مشاريع متقاطعة ومتكاملة مع استراتيجية التحول الرقمي للخدمات الحكومية

البرنامج الثاني : تطوير الإطار القانوني والتنظيمي

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
يهدف هذا البرنامج إلى دراسة ومراجعة القوانين في الفضاء السبراني، ووضع الضوابط والسياسات اللازمة لحماية الفضاء السبراني	وزارة الاتصالات والتقانة	وزارة العدل وزارة الداخلية وزارة الدفاع

المبادرات / الإجراءات للبرنامج الثاني

المبادرة	الهدف	الجهة المسؤولة
إصدار قانون حماية البيانات الشخصية	حماية خصوصية أفراد المجتمع عبر توفير الحوكمة السليمة لإدارة البيانات.	وزارة الاتصالات والتقانة
تحديث السياسة الوطنية لأمن المعلومات	تحديث وثيقة السياسة الوطنية لأمن المعلومات، وفق أحدث المعايير العالمية، بحيث تشكل المعيار الوطني لسياسات امن المعلومات	الهيئة الوطنية لخدمات تقانة المعلومات
مبادرة سياسة أمن معلومات لكل وزارة، متوافقة مع السياسة الوطنية لأمن المعلومات	اختبار بعض الجهات الحكومية التي لديها منظومات معلوماتية ذات حساسية عالية وتطبيق سياسات أمن المعلومات لديها بالتعاون مع الهيئة الوطنية لخدمات تقانة المعلومات، ليتم تعميم التجربة لاحقاً	كافة الوزارات

البرنامج الثالث : نشر ثقافة الوعي السبراني

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
يهدف هذا البرنامج بشكل رئيسي إلى تعزيز الوعي العام للمستخدمين بالقضايا الأساسية المتعلقة بالأمن السبراني	وزارة الاتصالات والتقانة	وزارة الإعلام وزارة التربية

المشاريع المقترحة للبرنامج الثالث

اسم المشروع	وصف المشروع	الجهة المسؤولة
تعزيز ثقافة الأمن السبراني لمدراء القطاع الحكومي	يهدف المشروع إلى إقامة ورشات تعريفية وتدريبية لمدراء القطاع الحكومي من مستوى معاوني وزراء ومدراء عامين بهدف تعزيز ثقافة الأمن السبراني ودعم الجهود الرامية إلى تطبيق سياسات وإجراءات الأمن السبراني على مستوى نظم المعلومات في المؤسسات	الهيئة الوطنية لخدمات تقانة المعلومات

المبادرات / الإجراءات للبرنامج الثالث

المبادرة	الهدف	الجهة المسؤولة
مبادرة إدخال مفاهيم أمن المعلومات في المناهج التعليمية	إدخال مفاهيم الأمن السبراني في بعض المدارس الحكومية والخاصة بحيث يتم ذلك من خلال اختيار مدارس محددة وقياس النتائج بهدف تعميم التجربة لاحقاً	وزارة التربية
مبادرة حملة توعوية على القنوات التلفزيونية المحلية	نشر إعلانات تلفزيونية توعوية في مجال الأمن السبراني على القنوات التلفزيونية	وزارة الإعلام وزارة الاتصالات والتقانة
مبادرة نشرات توعوية للعاملين بالقطاع العام حول مفاهيم أمن المعلومات	إصدار نشرات توعوية دورية من قبل مركز أمن المعلومات لدى الهيئة موجهة للعاملين بالقطاع العام	الهيئة الوطنية لخدمات تقانة المعلومات
مبادرة بناء الوعي في مجال الأمن السبراني	إطلاق حملات توعية للعموم في قضايا الأمن السبراني مع التركيز على المخاطر وطريقة معالجتها	الهيئة الوطنية لخدمات تقانة المعلومات

البرنامج الرابع : بناء القدرات المعرفية

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
يهدف هذا البرنامج إلى تنمية القدرات التخصصية في مجال الأمن السبراني لدى القطاع العام والقطاع الخاص	الهيئة الوطنية لخدمات تقانة المعلومات	جميع الجهات الحكومية

المشاريع المقترحة للبرنامج الرابع

اسم المشروع	وصف المشروع	الجهة المسؤولة
مشروع تدريب الكوادر التخصصية على سياسات أمن المعلومات	يهدف هذا المشروع إلى تدريب الكوادر التخصصية لدى الوزارات على إعداد سياسة أمن معلومات لدى كل وزارة متوافقة مع السياسة الوطنية لأمن المعلومات	الهيئة الوطنية لخدمات تقانة المعلومات
مشروع تدريب تخصصي في مجال أمن المعلومات	يهدف هذا المشروع إلى إطلاق تدريب تخصصي احترافي لمسؤولي أمن المعلومات لدى الجهات العامة والخاصة	وزارة الاتصالات والتقانة

المبادرات / الإجراءات للبرنامج الرابع

المبادرة	الهدف	الجهة المسؤولة
رعاية المواهب الشابة في مجالات الأمن السبراني	تشجيع واستقطاب المواهب الشابة الواعدة من خلال إقامة العديد من الأنشطة كالمسابقات وبرامج الاحتضان	الهيئة الوطنية لخدمات تقانة المعلومات
مبادرة إعداد مناهج تخصصية في مجال الأمن السبراني	توافر مواد تعليمية ذات سوية جيدة في مجالات الأمن السبراني مع عدد كافٍ من المدرسين والمحاضرين، بحيث تشمل التعليم الجامعي التخصصي والمعاهد التقانية التخصصية	وزارة التعليم العالي والبحث العلمي
مبادرة إطلاق مشاريع بحثية في مجال الأمن السبراني	العمل على امتلاك القدرات العالية المستوى الكفيلة بإنتاج الابتكارات والقيام بالأبحاث العلمية المتطورة في مجالات الأمن السبراني	وزارة الاتصالات والتقانة الهيئة الوطنية لخدمات تقانة المعلومات وزارة التعليم العالي والبحث العلمي

البرنامج الخامس : الشراكات والتعاون الدولي

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
يهدف البرنامج إلى تطوير الشراكات على المستوى الدولي والمحلي في مجال الأمن السيبراني	وزارة الاتصالات والتقانة	وزارة الخارجية والمغتربين وزارة الداخلية

المبادرات / الإجراءات للبرنامج الخامس

المبادرة	الهدف	الجهة المسؤولة
مبادرة تعزيز التعاون الدولي مع الدول الصديقة في مجال الأمن السيبراني	تبادل الخبرات والإنذار المبكر حول الأخطار المحتملة والحوادث الأمنية الشائعة، ووضع آليات للتصدي لهذه الحوادث وخطة لمعالجتها من خلال مراكز الاستجابة للطوارئ المعلوماتية	الهيئة الوطنية لخدمات تقانة المعلومات
مبادرة تعزيز دور القطاع الخاص المحلي في مجال الأمن السيبراني	دعم الجهود الوطنية الرامية إلى رفع مستوى أمن المعلومات في القطاعين العام والخاص	الهيئة الوطنية لخدمات تقانة المعلومات

البرنامج السادس : تطوير هياكل تنظيمية متخصصة

وصف البرنامج	الجهة المسؤولة	الجهات المشاركة
إنشاء وحدات تنظيمية متخصصة تُعنى بالأمن السيبراني في كل جهة عامة، مع تأمين المستلزمات الفنية والكوادر البشرية المؤهلة والمدربة والتي تنفذ الاستراتيجية المقرة من الحكومة	رئاسة مجلس الوزراء	وزارة الاتصالات والتقانة وزارة التنمية الإدارية

المشاريع المقترحة للبرنامج السادس

اسم المشروع	وصف المشروع	الجهة المسؤولة
مشروع إحداث وحدات تنظيمية متخصصة بالأمن السيبراني	إنشاء وحدات تنظيمية متخصصة تُعنى بالأمن السيبراني في كل جهة عامة، مع تحديد المسؤوليات والمهام للعاملين في المؤسسة أو الوزارة، وتوفير الكوادر البشرية اللازمة	رئاسة مجلس الوزراء وزارة التنمية الإدارية

حوكمة الاستراتيجية

تعتبر حوكمة الاستراتيجية من أهم العوامل التي تضمن نجاح تنفيذ الاستراتيجية واستمرارية العمل بها، لذلك يجب الاهتمام بتوصيف البنى التنظيمية المسؤولة عن عمليات الحوكمة بما فيها التخطيط ومراجعة الأولويات وتوفير التمويل وآليات التنفيذ والمتابعة وخلق الثقافة والمناخ اللازم لضمان نجاح التنفيذ .
يبين الإطار أدناه مقترحاً حموكمة الاستراتيجية وضمان تنفيذها عن طريق توزيع الأدوار والمسؤوليات التي تتطلبها عملية احموكمة وفق الآتي:

1. **اللجنة العليا للتحول الرقمي:** اللجنة الوطنية العليا برئاسة السيد رئيس مجلس الوزراء وعضوية الوزارات التي يختارها السيد رئيس المجلس، والتي تشكل المرجعية العليا في تنفيذ استراتيجية التحول الرقمي للخدمات الحكومية، ويقع على عاتقها في إطار حوكمة هذه الاستراتيجية المهام الآتية:
   - إقرار الأولويات الوطنية المقترحة من اللجنة الوطنية للأمن السبراني.
   - تأمين التمويل اللازم لتنفيذ المشاريع والمبادرات المتعلقة بالاستراتيجية وفق الأولويات.
   - متابعة التقدم في تنفيذ الاستراتيجية بناء على تقارير اللجنة الوطنية للأمن السبراني.

2. **اللجنة الوطنية للأمن السبراني:** وهي لجنة إشراف ومتابعة وتنسيق برئاسة السيد وزير الاتصالات والتقانة، وعضوية ممثلين من مرتبة معاون وزير أو مدير عام أو مدير إدارة من الجهات التالية: (وزارة الداخلية، وزارة الإعلام، وزارة الاتصالات والتقانة، وزارة الدفاع، مركز الدراسات والبحوث العلمية)، ويمكن أن تستعين اللجنة بمن تراه مناسباً حسب الحاجة، وتقع عليها المسؤوليات التالية:
   - اقتراح الأولويات الوطنية في مجال الأمن السبراني.
   - وضع الخطط اللازمة لتنفيذ برامج الاستراتيجية.
   - التنسيق بين مختلف الجهات المعنية في مجال الأمن السبراني.
   - متابعة تنفيذ الخطط الوطنية ورفع التقارير الخاصة بها إلى اللجنة العليا للتحول الرقمي.
   - المراجعة الدورية لمهام الوحدات التنظيمية لأمن المعلومات وإقرار ما يلزم بشأنها، وفق متطلبات تنفيذ الاستراتيجية.

3. **وحدة تنظيمية لأمن المعلومات** ضمن الوزارات والجهات المعنية لتنفيذ المشاريع والمبادرات وفق الخطط التي تضعها اللجنة الوطنية للأمن السبراني.

تقوم وزارة الاتصالات والتقانة من خلال البنى التنظيمية المتوفرة لديها، أو من خلال فرق عمل تخصصية لمهام محددة، بما يلي:

   - تدقيق وثائق المشاريع والمبادرات لضمان اتساقها مع أهداف هذه الاستراتيجية.
   - إعداد مؤشرات الأداء المتعلقة بالمشاريع وقياسها، ورفع تقارير دورية بهذا الخصوص إلى اللجنة الوطنية للأمن السبراني.

الخاتمـــــة

تتمثل رؤية الجمهورية العربية السورية في ضمان تنفيذ برامج ومبادرات الاستراتيجية الوطنية للأمن السبراني باعتبارها أحد أساسيات التحول الرقمي في سورية، بالإضافة إلى دورها في تعزيز الانتقال إلى الاقتصاد الرقمي كأحد أهم الفرص المتاحة لسورية.

وتشكل هذه الاستراتيجية الإطار العام لترسيخ أفضل الممارسات اللازمة في مجالات الأمن السبراني بهدف حماية المصالح الوطنية مع الإشارة إلى أنه ستتم مراجعتها بشكل دوري بناء على تغيّر المتطلبات والأولويات، وذلك لأن مواجهة المخاطر والجرائم المعلوماتية تحتاج لتنسيق وشراكة مجتمعية واسعة تشمل الجهات الحكومية والخاصة والمؤسسات البحثية لتعظيم الاستفادة من الفرص المتميزة التي تتيحها تقانات الاتصالات والمعلومات الحديثة في شتى مجالات التنمية الاقتصادية والاجتماعية والثقافية، مع حماية مجتمعنا من مخاطر وأضرار الجرائم والهجمات السبرانية.

الملحق رقم / 1 /

قام فريق إعداد الاستراتيجية بإعداد استبيان حول السياسة الوطنية لأمن المعلومات للقطاع الحكومي، واستبيان عبر منصة إلكترونية للعموم بهدف تقييم واقع الأمن السبراني، وكانت النتائج:

- أغلب المتجاوبين مع الاستبيان هي فئة الشباب بنسبة 51%.
- أغلب أنظمة التشغيل المستخدمة يومياً، هي أنظمة Windows و Android بنسبة 65%.
- يوجد وعي مقبول لضرورة استخدام برمجيات مكافحة البرمجيات الخبيثة بنسبة 59%، وانخفاض الوعي بمفهوم الهندسة الاجتماعية بنسبة 36%.
- انخفاض بمستوى التدريب بمجال أمن المعلومات عموماً حيث بلغت نسبة من تلقوا تدريبات بهذا المجال 35%.
- تفاوت ردة الفعل اتجاه الاختراق، حيث كانت نسبة رد الفعل الأصح 42%.
- ضعف في ثقافة إعلام الجهات المختصة عند حدوث اختراق حيث بلغت نسبة الإبلاغ 10% من الحالات.
- بلغت نسبة اتباع إجراءات الحمايات الأمنية عند استخدام وسائل التواصل الاجتماعي 64%.
- تفاوت تفعيل الحمايات الأمنية على المستوى الشخصي حيث كانت نسبة من يقومون بتفعيل جدار النار على مستوى نظام التشغيل هي 37 %.
- انخفاض نسبة متابعة الأهل للأولاد عند استخدام الهواتف أو الحواسب على الشبكة، حيث كانت نسبة المتابعة 18%.

تحليل الفجوات

بناءً على نتائج تقييم مستوى الالتزام بتطبيق الضوابط الأساسية للأمن السبراني، وتقييم مخاطر الأمن السبراني، وتحليل تأثير الأعمال، وتقييم نضج الأمن السبراني، تم إجراء التحليل الرباعي (SWOT)، ويوضح هذا التحليل مواضع القوة والضعف، ومواضع الفرص والتهديدات في مجال أمن المعلومات.

الداخلية

نقاط القوة

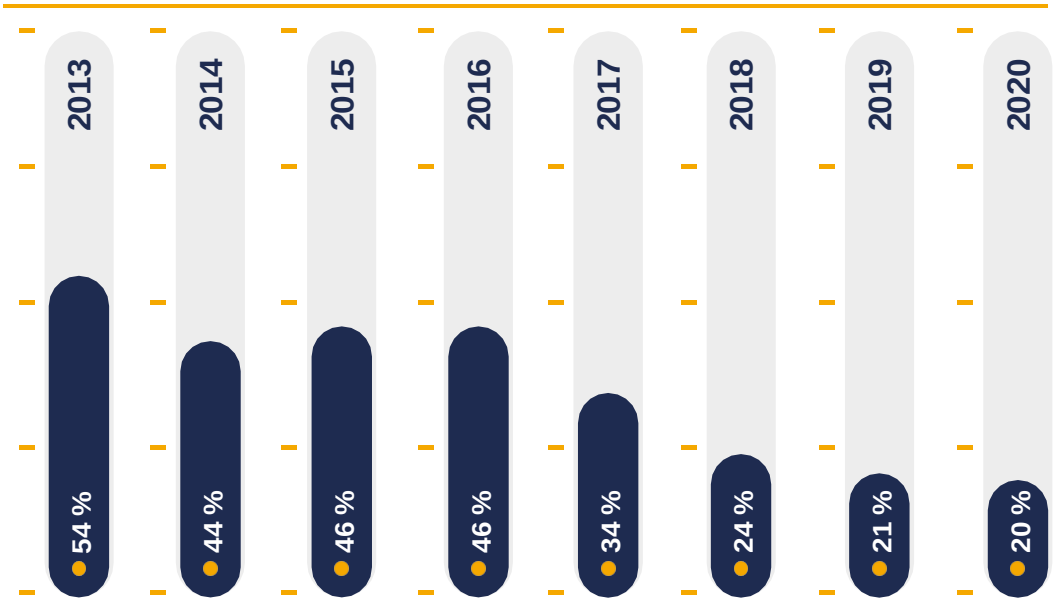
- إصدار معظم قوانين الفضاء السبراني. إصدار السياسات الوطنية.
- توفر شبكة حكومية آمنة.
- إحداث فرع مكافحة الجريمة المعلوماتية. إحداث مخبر أمن المعلومات الوطني.
- وجود كليات متخصصة في مجال الهندسة المعلوماتية.
- وجود البنية التحتية لإصدار المفتاح العام (التوقيع الرقمي).
- تنظيم انتشار التطبيقات الإلكترونية الخاصة بالهواتف الذكية وفق ضوابط خاصة بأمن المعلومات وحماية البيانات الشخصية.
- توفر خريجين موهوبين في مجال الأمن السبراني.
- إطلاق الاستراتيجية الوطنية للتحول الرقمي متضمنة برنامج أمن المعلومات.
- مبادرة ومسابقات اكتشاف المهارات في مجال الأمن السبراني، مثل: CTF-Syria.
- عضوية الاتحاد الدولي للاتصالات والمركز الإقليمي للأمن السبراني.

نقاط الضعف

- عدم توفر الموارد البشرية المؤهلة في مجال أمن المعلومات من حيث الكم والتخصص والتسرّب المستمر في الكوادر خارج القطاع العام.
- عدم وجود دائرة/قسم متخصص بأمن المعلومات لدى الجهات العامة والخاصة ما عدا القطاع المصرفي.
- عدم وجود الوعي الكافي بتهديدات الأمن السبراني لدى العاملين أو المواطنين بشكل عام.
- عدم إنشاء المركز الوطني للاستجابة للطوارئ المعلوماتية.
- عدم توفر حلول الحماية من التهديدات المتقدمة والمستمرة لدى معظم المؤسسات.
- عدم وجود تقنيات أمن أسماء النطاقات.
- عدم توفر اختصاص أمن معلومات في كليات الهندسة المعلوماتية.
- ضعف التمويل ورصد موازنات الأمن السبراني باعتباره خارج نطاق الأولويات.
- ضعف التحفيز الجاذب والمحافظ على الكوادر البشرية الموهوبة والمتخصصة في مجالات الأمن السبراني لدى القطاع العام.
- عدم وجود آليات دور رقابي أو إشرافي فعال على
- تطبيق معايير الأمن السبراني الوطنية أو العالمية في كافة القطاعات العامة أو الخاصة.
- الاعتماد على برمجيات مقرصنة أو قديمة في تشغيل النظم المعلوماتية
- غياب التعاون مع الهيئات الإقليمية والدولية لإخماد الهجمات السبرانية الخارجية من مصدرها.
- عدم مراعاة جانب الأمن السبراني عند توريد أو تطوير أو تشغيل أغلب المنظومات المعلوماتية في القطاع العام أو الخاص.
- التكتم على حوادث الأمن السبراني في الجهات العامة والخاصة وعدم وجود آليات فعالة لرصدها.

	الفرص	التهديدات
الخارجية	• مبادرات من دول حليفة للتعاون في مجال الأمن السبراني.	• تغيّر الأنظمة التقنية بصورة متكرّرة و/أو قلّة الأنظمة المتعلّقة بالأمن السبراني. • انتشار الهجمات السبرانية بشكل عام، وعلى بعض الجهات العامة والخاصة. • التقدم السريع والمستمر في مجال تقانة المعلومات. • الحظر التكنولوجي وخصوصاً في مجالات تجهيزات وبرمجيات الأمن السبراني وعدم وجود بدائل محلية. • الظروف الاقتصادية والسياسية الصعبة.

مقارنة نسب الثغرات الأمنية عالية الخطورة لعام 2020 مع الأعوام السابقة



نسب استخدام أنواع بيئات التطوير لمواقع ويب