

الأمن السيبراني



أهداف الأمن السيبراني

- ▶ تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالدولة والمواطنين.
- ▶ حماية شبكة المعلومات والاتصالات من التخريب والتدمير والاختراق، والذي قد يؤثر على سير العمل.
- ▶ وضع آلية لتشفير كافة التعاملات الالكترونية.
- ▶ تطوير الخبرات ومواكبة آخر المستجدات في هذا المجال لحماية شبكات المعلومات من أي اختراقات.



الأمن السيبراني

"يعرف الأمن السيبراني (Cyber security) بأنه الأمن الذي يعنى بتطبيق التقنيات، والعمليات، والضوابط، بهدف حماية الأنظمة، وشبكات الحواسيب، والبرامج، والأجهزة، والبيانات من التعرض للهجمات الإلكترونية، والذي يعتبر فعل غير مشروع، ويقرر له القانون عقوبة أو تدبيراً احترازياً." ⁽¹⁾

كما يعرف أيضا بمجموعة الأدوات والسياسات ومفاهيم الأمن والضوابط والمبادئ التوجيهية ومنهجيات إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية بيئة الفضاء الإلكتروني وأصول المؤسسات والمستخدمين، وتقليل المخاطر السيبرانية من التهديدات الداخلية والخارجية للجهة وحمايتها.

"والأمن السيبراني يتعلق بتأمين شامل للبيانات المعرضة للخطر من خلال رفع مستوى تطوير تكنولوجيا المعلومات والاتصالات، وحماية مواقع تخزين المعلومات والبيانات والتقنيات المستخدمة لتأمينها، وحمايته من الفضاء السيبراني، وحماية نظم المعلومات، وأصبحت ظاهرة إلكترونية خطيرة تهدد أمن البلدان، وأنشطة إجرامية عابرة للحدود ومختربة ومتحدية لكل القوانين." ⁽²⁾

مخاطر الأمن السيبراني

اضطرابات الأعمال: توقف الخدمات التجارية بسبب أعمال التخريب.

الخسارة المالية: متمثلة في خسائر في الإيرادات، وفقدان السرية، والشفافية والنزاهة، وإتاحة المعلومات لأفراد غير مسموح لهم بالاطلاع على البيانات.

اختراق الأمن السيبراني: بسبب فيروسات الكمبيوتر أو توقف الخدمة.

فقدان السمعة: نتيجة لفقد ثقة العملاء في المؤسسة.

الآثار القانونية: ومنها العقوبات الإدارية والعقوبات المالية والقوانين المنظمة لذلك بسبب إفشاء المعلومات.

فقدان البيانات أو سرقتها: والتي أصبحت متاحة بسبب اختراقات الفيروسات أو الهاكرز. ⁽³⁾



أنواع الجرائم الالكترونية عبر الفضاء السيبراني ⁽⁴⁾

الدخول غير المشروع، أو الاستيلاء على بيانات الحاسوب: خرق أجهزة الكمبيوتر بهدف السيطرة والتحكم بالمعلومات والبيانات.

الأفعال ذات الصلة بالحاسوب التي تنطوي على خطاب الكراهية: السيطرة على الأجهزة وإرسال وتخريض المجتمع على خطاب الكراهية.

خرق حقوق الطبع والنشر: بمعنى سرقة الأبحاث والدراسات والتقارير.

جرائم العلامة التجارية ذات الصلة بالحاسوب: سرقة العلامات التجارية المخصصة بالأجهزة الكمبيوترية.

السيطرة على إرسال البريد: بمعنى التحكم بالتراسل البريدي والاطلاع على خصوصية الموظفين.

امتلاك أدوات إساءة استعمال جهاز الحاسوب: السيطرة على الأنظمة في جهاز الكمبيوتر بهدف الإساءة للغير.

التزوير والاحتيال الالكتروني: السيطرة والهيمنة بتزوير المحاضر والعقود التي تبرم بواسطة التراسل الإلكتروني.

الفرق بين الأمن السيبراني وأمن المعلومات ⁵

أوجه المقارنة	الأمن السيبراني	أمن المعلومات
التعريف	مجموعة من الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به	حماية المعلومات ونظم المعلومات من الوصول لغير المصرح لهم، والاستخدام، والإفصاح، والتعديل واحداث الخلل أو التدمير
الهدف العام	يسعى إلى حماية البيانات، ومصادر التخزين، والأجهزة من مخاطر الهجمات الإلكترونية في الفضاء السيبراني.	يسعى إلى حماية البيانات من أي نوع من أنواع التهديدات.
نطاق التعامل	يتعامل مع الجرائم الإلكترونية، والاحتيال الإلكتروني، وتنفيذ القانون.	يتعامل مع عملية الوصول غير المصرح به للمعلومات، والكشف عن أي تعديل أو خلل.
مهارات التطبيق	يعتمد تطبيق الأمن السيبراني على وجود أشخاص محترفين ومدربين على التعامل مع التهديدات	يوفر أمن المعلومات قاعدة أساس لأمن البيانات، ويتم من خلاله تدريب الأشخاص على تحديد أولويات الموارد قبل مواجهة التهديدات أو الهجمات.

العلاقة بين الأمن السيبراني ومكافحة الفساد

تسعى الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت لعام 2020/2017، لضمان فضاء إلكتروني آمن ومرن لحماية المصالح الوطنية لدولة الكويت، واتخاذ كافة التدابير الأمنية لتعزيز القدرة على الإدارة والاستجابة لأي طارئ، وحماية البنى التحتية والفضاء الإلكتروني لممارسة الجرائم مثل غسيل الأموال، والرشوة، والابتزاز، والتهديد، وتهريب المخدرات والأسلحة، والاتجار بالبشر، والتلاعب المالي، وتعزيز أمن المعلومات بكافة أشكاله للتأكد من تسخير كافة الإمكانيات واتخاذ كافة التدابير اللازمة لذلك، والسعي إلى مكافحة الجرائم الإلكترونية وتعزيز أفضل الممارسات في مجال التوعية بمستجدات الأمن السيبراني واتخاذ التدابير الوقائية والاستجابة للأزمات.

واتساق مع تلك الأهداف الاستراتيجية تأتي أهداف الهيئة العامة لمكافحة الفساد لتتلاقى مع منع جرائم الفساد في كل صورها وأشكالها ومواكبة طرق حدوثها سواء بالطرق التقليدية أو الحديثة المتطورة.

ومن هذا أيضاً تبذل الهيئة الجهود لتوعية المجتمع بتلك الجرائم ووسائل حدوثها ومخاطرها. ⑥ ⑦



عقوبة الجرائم الإلكترونية

وفقا للقانون الكويتي في شأن مكافحة جرائم تقنية المعلومات، بأنه يعاقب بالحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تتجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولا غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية.

"فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تتجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين." ⑨



المركز الوطني للأمن السيبراني

صدر مرسوم رقم (37) لسنة 2022 بإنشاء المركز الوطني للأمن السيبراني، لتأمين وحماية الشبكات المعلوماتية، وشبكة الاتصالات، ونظم المعلومات، وعمليات جمع وتبادل المعلومات باستخدام أي وسيلة إلكترونية، ويهدف المركز إلى تحقيق الأهداف المنبثقة من الاستراتيجية وعلى الأخص ما يلي:

▶ بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية الدولة من تهديدات الفضاء السيبراني الوطني.

▶ حماية المصالح الحيوية في الفضاء الإلكتروني، والاشراف على بناء القدرات الوطنية المتخصصة في مجال الأمن السيبراني.

▶ تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الإلكتروني.

▶ حماية ومراقبة الأصول والبنية التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية في دولة الكويت.

▶ إتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني. ⑧

نبذه عن نتائج مؤشر الأمن السيبراني (GCI) لعام 2020

على الصعيد العالمي يلاحظ من درجات مؤشر الأمن السيبراني لدول العالم أن جميع الدول تحسنت درجاتها في عام 2020 عن العام 2018.

وعلى الصعيد العربي حصلت المملكة العربية السعودية على المركز الأول من بين الدول العربية بدرجة (99.54)، فيما حصلت دولة الإمارات على المركز الثاني بدرجة (98.06)، وحلت دولة الكويت في المركز التاسع بدرجة (75.07)، أما خليجياً فقد حلت دولة الكويت في المركز السادس.

Global Cybersecurity Index



مؤشر الأمن السيبراني

يصدر المؤشر العالمي للأمن السيبراني جي سي آي (GSI) من الاتحاد الدولي للاتصالات التابع للأمم المتحدة، ويشير بأن الأمن السيبراني يتطور باستمرار، وستكون هناك حاجة إلى نهج مستدام ومطور من قبل الدول لضمان بأن كافة البرامج والطلول الرقمية آمنة، وموثوقة وجديرة بالثقة، والحفاظ على متطلبات الأمن السيبراني.

ومعايير القياس والتقييم التي يقوم عليها المؤشر هي على النحو التالي:

▶ السياسات التنظيمية والتشريعات: تهدف التشريعات إلى تعزيز الأمن السيبراني ولحماية مصالح الحيوية للدولة وأمنها.

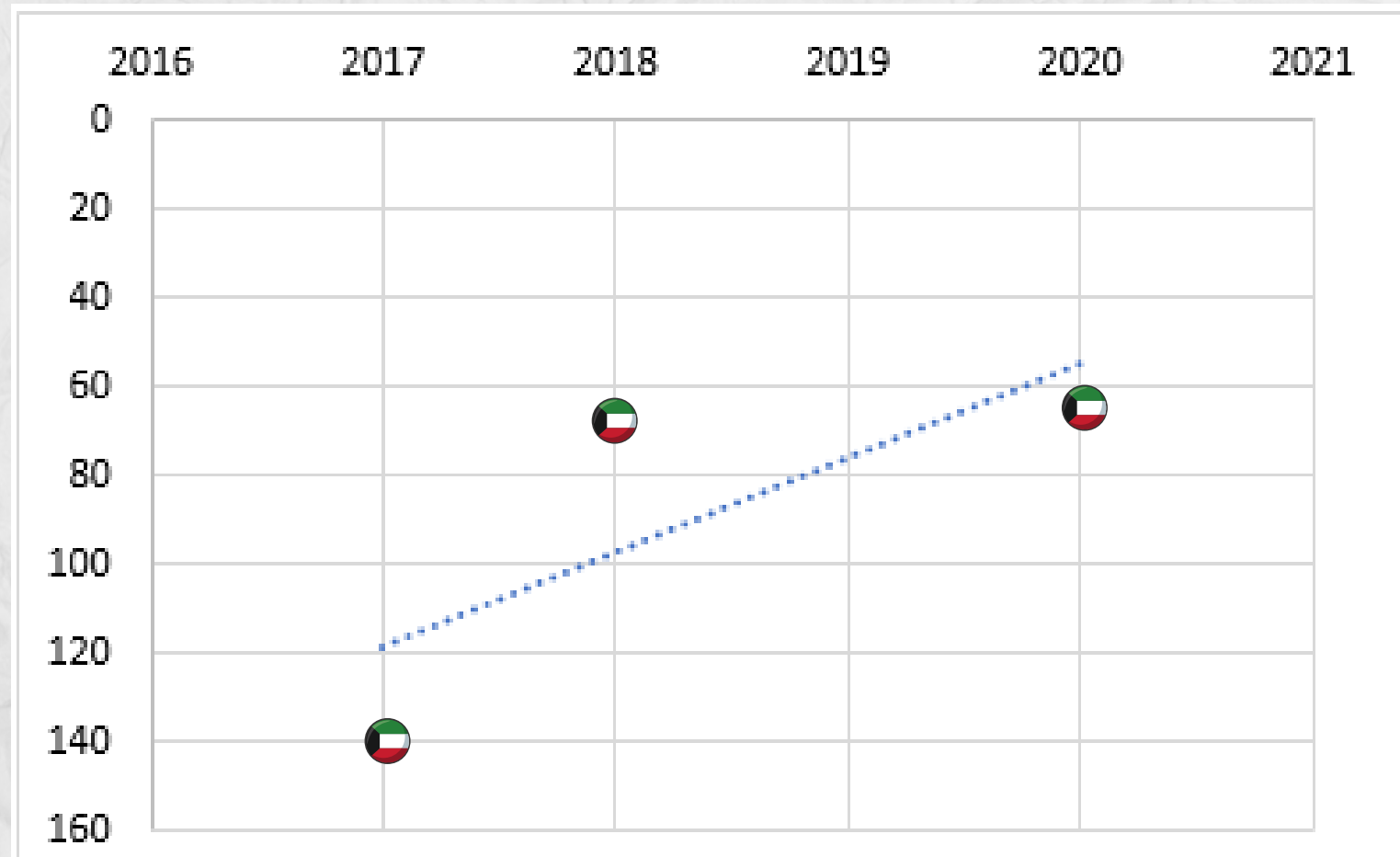
▶ الإطار المؤسسي: تعزيز قيم المحافظة على الأمن المؤسسي.

▶ بناء القدرات البشرية: رفع مستوى الوعي بالأمن السيبراني، وبناء ثقافة سيبرانية عالية المستوى لدى الموظفين.

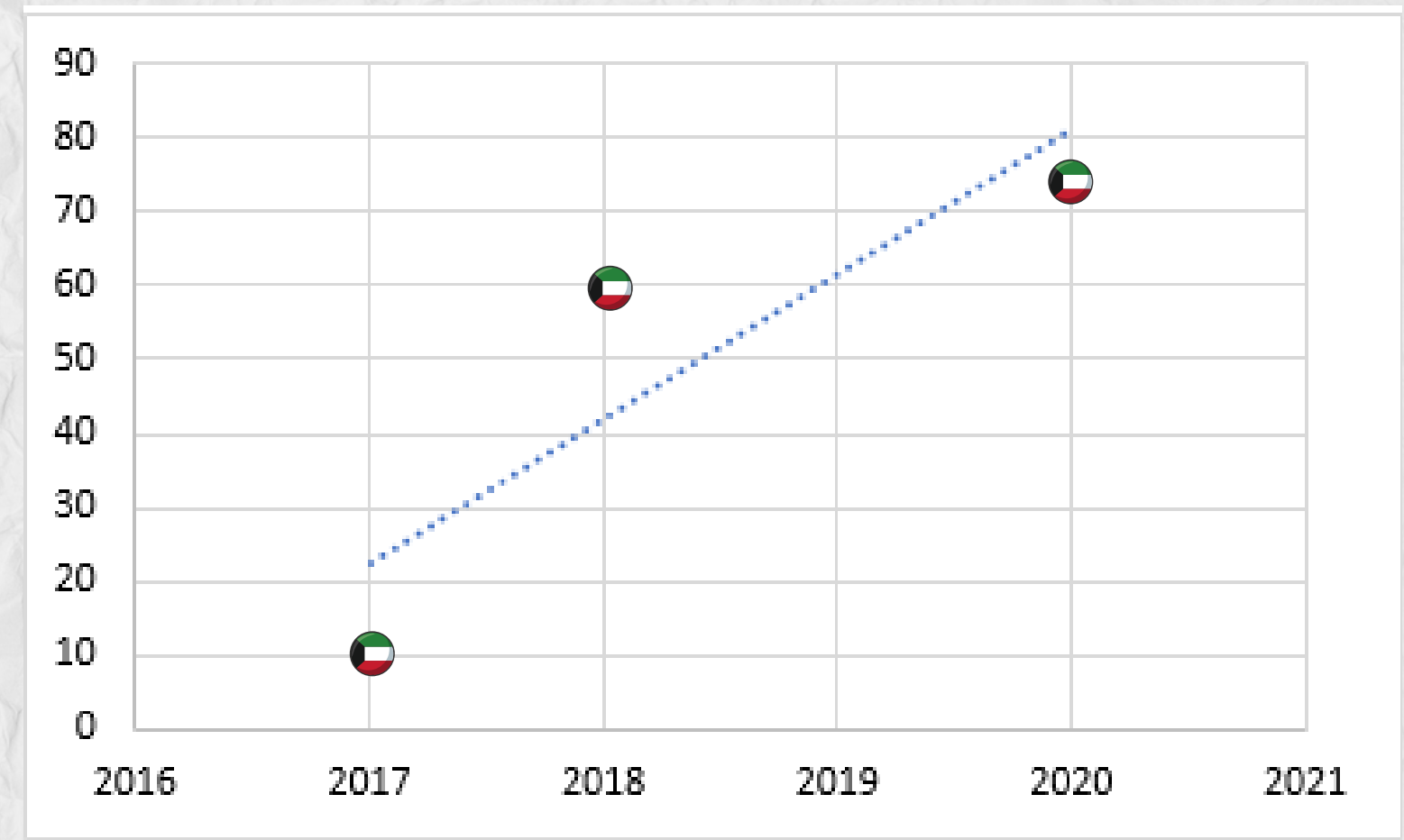
▶ توافر القدرات التقنية والفنية اللازمة: الحد من التهديدات السيبرانية الداخلية والخارجية.

نتيجة دولة الكويت في مؤشر الأمن السيبراني

في آخر بيانات صادرة عن الاتحاد الدولي للاتصالات (ITU)، حصلت دولة الكويت على درجة (100/75.07) في مؤشر الأمن السيبراني وعليه احتلت الترتيب (194/65) في عام 2020، مرتفعة عن العام السابق 2018 مركزين، بينما كانت في المركز (194/67). كما أنها قفزت 72 مركزاً في عام 2018 عن العام 2017 عندما كانت في الترتيب (193/139) ما يعني أن هناك تطوراً تدريجياً ملحوظاً في هذا المجال.



الشكل (2) ترتيب دولة الكويت في مؤشر الأمن السيبراني 2020-2017



الشكل (1) درجات دولة الكويت في مؤشر الأمن السيبراني 2020-2017

المصادر

توصيات عامة 10

- 1 الرجباني، عبيد (2020). الجرائم الالكترونية ومخاطرها. الأردن: دار الثقافة للنشر والتوزيع. ص 20-26.
- 2 الرجباني، عبيد (2020). الجرائم الالكترونية ومخاطرها. الأردن: دار الثقافة للنشر والتوزيع. ص 31.
- 3 البحيصي، عهام (2013). واقع إدارة أمن إدارة نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها. جامعة الإسلامية- غزة. ص 50-60.
- 4 يوسف، أمير (2015). جرائم تقنية المعلومات بدول الخليج العربي، والجهود الدولية والمحلية لمكافحته، جرائم الانترنت والحاسوب الالكترونية في دول الخليج العربي. مصر: دار الكتب العربية. ص 68-74.
- 5 مواش، ضرغام (2017). جريمة التجسس المعلوماتي. الأردن: مكتبة دار السلام القانونية. ص 43-129.
- 6 استراتيجية الكويت لتعزيز النزاهة ومكافحة الفساد 2019-2024.
- 7 قانون رقم (2) لسنة 2016 في شأن إنشاء الهيئة العامة لمكافحة الفساد والأحكام الخاصة بالكشف عن الذمة المالية ولوائحته التنفيذية.. مادة (22) أي جرائم أخرى ينص عليها قانون آخر باعتبارها جرائم فساد.
- 8 الكويت اليوم العدد 1572 الأحد 5 رجب 1443 هـ الموافق 6 فبراير 2022 السنة الثامنة والستون، ص 9-11.
- 9 قانون رقم (63) لسنة 2015، في شأن مكافحة جرائم تقنية المعلومات الفصل الثاني الجرائم والعقوبات المادة (2).
- 10 الرجباني، عبيد (2020). الجرائم الالكترونية ومخاطرها. الأردن: دار الثقافة للنشر والتوزيع. ص 442-456.

- ▶ ترسيخ استخدام مبادئ ومعايير حوكمة أمن المعلومات، وتسخير تكنولوجيا المعلومات والاتصالات لأغراض التنمية والانسانية.
- ▶ إعداد الدورات التدريبية بتكنولوجيا المعلومات لمعرفة التطورات الحديثة، والتعرف على الجرائم المحتملة وكيفية معالجتها وفق المعايير الدولية.
- ▶ تطوير عمل الجهات الرقابية الداخلية والخارجية لتشمل التقليل من مخاطر الجرائم الالكترونية.
- ▶ تطوير الأجهزة المعلوماتية في القطاع العام والخاص حتى يكون هناك أمن سيبراني متكامل.
- ▶ نشر ثقافة السيبرانية ومعالجة ظاهرة الفجوة الرقمية ومحو أمية تكنولوجيا المعلومات لدى غير المتخصصين.
- ▶ ترسيخ ثقافة مكافحة الفساد على تقنيات حماية التكنولوجيا المتقدمة والبنية التحتية الوطنية الحيوية.
- ▶ دراسة وتطوير القوانين والتشريعات لوقف الاستخدامات السيئة في التكنولوجيا وحماية أمن المعلومات وتشريع ضوابط للأمن السيبراني.
- ▶ دعم البحوث والدراسات العلمية الوطنية لتحسين أمن المعلومات الوطني وتشجيع الابتكار والتطوير في هذا الخصوص.