الاستراتيجية الوطنية
للأمـن السيبـــــراني

الاستراتيجية الوطنية للأمـن السيبـــــراني

2030 - 2024

دولـة قـطـر

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

كلمة افتتاحيَّة
لمعالي رئيس مجلس الوزراء

" إن الأمـن السـيبراني بـات يُشـكّل ضـرورة مُلحّـة فـي حياتنـا للحفـاظ علـى أمـن اقتصادنـا وبنيتنـا التحتيـة والمعلومـات الشـخصية لشـعبنا فـي ظـل التطـور السـريع الـذي نشـهده، وبالنظـر إلـى الـرؤى الطموحـة لدولـة قطـر، فإننـا بحاجـة إلـى اسـتراتيجية تمكّننـا مـن إدارة المخاطـر والتصـدي للتهديـدات السـيبرانية وتعزيـز ازدهـار دولـة قطـر فـي ظـل تطـور وتقـدم التقنيـات الحديثـة.

إن إطلاق الاسـتراتيجية الوطنيـة للأمـن السـيبراني يأتـي مـن بـاب سـعينا إلـى دعـم مجتمعنـا الطمـوح فـي مواكبـة التطـور التكنولوجـي الـذي يشـهده عالمنـا مـن خلال مبادئهـا وأهدافهـا، ولا شـكّ فـي أنّ هـذه الاسـتراتيجية سـتكون ركيـزة أساسـية لتحقيـق رؤيـة قطـر 2030.

لقـد تـم وضـع هـذه الاسـتراتيجية وتصميمهـا بشـكل يضـع الابتـكار والقـدرة علـى التكيّـف أساسـاً لهـا وذلـك إدراكًا منّـا بـأنّ التهديـدات السـيبرانية تتطـوّر وتـزداد وتيـرة تعقيداتهـا يومـاً بعـد يـوم. ومـن منطلـق حرصنـا علـى حمايـة الأصـول الرقميـة والسـيادية لدولـة قطـر مـن خلال توظيـف أفضـل الخبـرات والكفـاءات والتقنيـات المتوفـرة، شـدّدت الاسـتراتيجية علـى ضـرورة إقامـة شـراكات فعّالـة لتبـادل المعلومـات والخبـرات مـع الجهـات العامـة والخاصـة المحليـة والدوليـة، إلـى جانـب توفيـر البيئـة المناسـبة لاسـتقطاب أفضـل الكـوادر المتخصصـة بالأمـن السـيبراني وتدريبهـا وتطويرهـا.

إننـا نؤكـد علـى ضـرورة تعـاون وتكاتـف كافـة المقيميـن علـى أرض دولـة قطـر باخـتلاف جنسـياتهم وثقافاتهـم للنهـوض بدولـة قطـر وتعزيـز ازدهارهـا ، وهـذه مكانـة ستسـعى الاسـتراتيجية الجديـدة للأمـن السـيبراني إلـى ترسـيخها بمـا يحفـظ أمـن أصولنـا الرقميـة ويضـع دولـة قطـر فـي طليعـة المسـاهمين فـي تطويـر الأمـن السـيبراني علـى السـاحة الدوليـة."

معالي الشيخ/ محمد بن عبد الرحمن بن جاسم آل ثاني

رئيس مجلس الوزراء ووزير الخارجية

كلمة افتتاحيَّة
لسعادة رئيس الوكالة الوطنية للأمن السيبراني

"يشرّفني أن أضع بين أيديكم الاستراتيجية الوطنية الجديدة للأمن السيبراني لدولة قطر، والتي نطمح من خلالها أن تكون دولتنا في طليعة الدول الساعية إلى ضمان الاستخدام الآمن للتقنيات الحالية والناشئة، وبالتالي إرساء أسس متينة لمجتمع المستقبل.

يشهد عالمنا تحوّلًا رقميًّا سريع الخُطى جعل من الأمن السيبراني أحد أكبر التحديات التي تواجهها الدول في الوقت الراهن. ولأنّ الخدمات المترابطة تزداد عددًا والقنوات الرقمية تحظى بأهمية غير مسبوقة، أصبح للفضاء الإلكتروني تأثيرات مباشرة على واقع الأمن الوطني والحياة اليومية للأفراد، فكان لابد من تبنّي استراتيجية وطنية للأمن السيبراني تتسم بالشمول والصمود والنظرة المستقبلية.

صُمّمت هذه الاستراتيجية لمجابهة هذه التحديات والتصدي للتهديدات الناشئة، ليس ذلك فحسب، فهي تهدف أيضًا إلى تمكين دولتنا من الازدهار والاستفادة من أحدث الابتكارات التكنولوجية. وإذ تقرّ هذه الاستراتيجية الحاجة إلى حماية الأنظمة والبنى التحتية الحيوية من الهجمات السيبرانية باستخدام منهجيات متقدمة تدرك التحول من المخاطر الإلكترونية إلى المخاطر الرقمية ومن الأمن السيبراني إلى الصمود السيبراني.

وبالإضافة إلى التصدي للتهديدات الناشئة، تشدد الاستراتيجية على أهمية الابتكار والبحث والتطوير واستقطاب الكوادر المتخصصة التي لا غنى عنها لضمان فعالية الأمن السيبراني. ومن هذا المنطلق، فهي تسعى إلى إعداد نخبة متنوعة من الكوادر ذات الكفاءة في المجال.

كما تولي الاستراتيجية أهمية بارزة لتشجيع الابتكار في قطاع الأمن السيبراني من خلال إيجاد بيئة يستطيع فيها أصحاب المشاريع والشركات الناشئة تصميم حلول مبتكرة لتحديات الأمن السيبراني.

تطرح الاستراتيجية الجديدة للأمن السيبراني نهجًا شاملًا وعصريًا لتعزيز الأمن السيبراني، وهو نهج يهيئ دولة قطر للتعامل مع تحديات المستقبل، وفي الوقت نفسه، يشجّع الابتكار والبحث والتطوير وإعداد واستقطاب الكوادر المتخصصة حتى تصبح قطر مساهمًا فاعلًا في منظومة الأمن السيبراني العالمية."

سعادة المهندس عبد الرحمن علي الفراهيد المالكي

رئيس الوكالة الوطنية للأمن السيبراني

جدول المحتويـــات

قائمة الجـــداول

قائمة الأشكـــال

شكر وتقدير

ساهمت المدخلات البناءة الثرية من الأطراف المعنية داخل الوكالة الوطنية للأمن السيبراني والمؤسسات والجهات المختلفة في الدولة في تطوير الاستراتيجية الوطنية للأمن السيبراني. حيث اشتملت رحلة تطوير الاستراتيجية على العمل المشترك وعقد ورش عمل عديدة مع قطاعات مختلفة لدراسة المشهد السيبراني في دولة قطر، ودراسة نقاط القوة، والمخاطر الحالية والمستقبلية وكذلك التحديات والفرص.

وتنتهز الوكالة الوطنية للأمن السيبراني هذه الفرصة لتوجيه الشكر والتقدير لكافة المؤسسات والجهات التي شاركت في تطوير الاستراتيجية الوطنية للأمن السيبراني ومراجعتها واعتمادها.


National Cyber Security Agency
الوكالة الوطنية للامن السيبراني

المقدمة

ساهم التطور التكنولوجي في السنوات الأخيرة في إعادة تشكيل أساليب الحياة والعمل والتواصل الاجتماعي في قطر والعالم، ومع أن التوجه العالمي للتحول الرقمي قد أطلق العنان لآفاق جديدة، إلا أنه قدم لنا أيضاً تحديات جديدة. لذلك من الضروري العمل على الاستفادة من التطور التكنولوجي وضمان الأمن والسلامة في الفضاء السيبراني وتعزيز القدرات الوطنية بشكل عام في مجال الأمن السيبراني وبشكل استباقي يواكب التطور العالمي. ففي عالم شديد الترابط، تشهد التهديدات التي يطرحها الفضاء السيبراني تطوّرًا مستمرًّا، مما يتطلّب من القطاعَين العام والخاص والأفراد توحيد جهودهم لتهيئة بيئة سيبرانية آمنة تضمن لدولة قطر المزيد من الازدهار.

لطالما اعتبرت دولة قطر أن الأمن السيبراني يهدف إلى تحقيق توازن بين حماية المؤسسات والأفراد من ناحية، والاستفادة من فرص التحول الرقمي من ناحية أخرى. وقد نجح هذا النهج القطري الذي يتميز بالثبات والاستباقية والشمول، إذ إنه أدى إلى إنشاء الفريق القطري للاستجابة لطوارئ الحاسب الآلي عام 2005 ونشر أول استراتيجية وطنية للأمن السيبراني عام 2014، بالإضافة إلى وضع قوانين وتنظيمات لتأمين الفضاء السيبراني، وإنشاء مركز الأمن السيبراني في وزارة الداخلية كما عملت دولة قطر على زيادة الاستثمارات في التكنولوجيا الناشئة والبحوث والابتكار، وتنفيذ مبادرات لزيادة الوعي والمعرفة بشأن الأمن السيبراني، وإبرام العديد من الشراكات الإقليمية والدولية بهدف رفع مستوى جاهزية الأمن السيبراني في الدولة.

مع تطور التكنولوجيا وزيادة التواصل، تطوّرت طبيعة التهديدات السيبرانية، فهي تحديات نشِطة تشهد تزايدًا مستمرًا في درجة تعقيدها ووتيرة حدوثها وحجم أثرها. وتستلزم هذه البيئة دائمة التغيّر تحديث الاستراتيجية لضمان تلبيتها للاحتياجات الوطنية الحالية للأمن السيبراني مع إتاحة المجال في الوقت نفسه للابتكار الرقمي. وقد كان إنشاء الوكالة الوطنية للأمن السيبراني عام 2021 والتي تشمل مسؤولياتها تنسيق مبادرات الأمن السيبراني عاملاً إضافياً دفع إلى تطوير نظام وطني جديد للأمن السيبراني. وبما أن الأمن السيبراني مسؤولية مشتركة، فإن الاستراتيجية في نسختها الثانية (2024-2030) تدعو لتوحيد الجهود من قبل المؤسسات والأفراد في دولة قطر. وقد اعتمدت الاستراتيجية الجديدة على الجهود والنجاحات السابقة، مُستندةً إلى مدخلات قدمتها أكثر من 30 مؤسسة من الهيئات الحكومية والشركات والأوساط الأكاديمية، بالإضافة إلى أنها تتوافق مع رؤية قطر الوطنية 2030 وتساهم في تحقيقها، وقد حرصت عملية إعدادها على المواءمة مع استراتيجية التنمية لدولة قطر.

من المقرر أن توجّه الاستراتيجية الجديدة الجهود التي تبذلها دولة قطر لتعزيز وترسيخ ثقافة الأمن السيبراني لدى جميع شرائح المجتمع والدفع بمشاريع البحث والابتكار والاستثمار في قطاع الأمن السيبراني. وستقود أيضًا المساعي الرامية إلى زيادة الإمكانيات والقدرات في مجال الأمن السيبراني، وستتيح فرصًا جديدة لدولة قطر لعصر رقمي آمن ومزدهر.

01

السياق الحالي
للأمن السيبراني

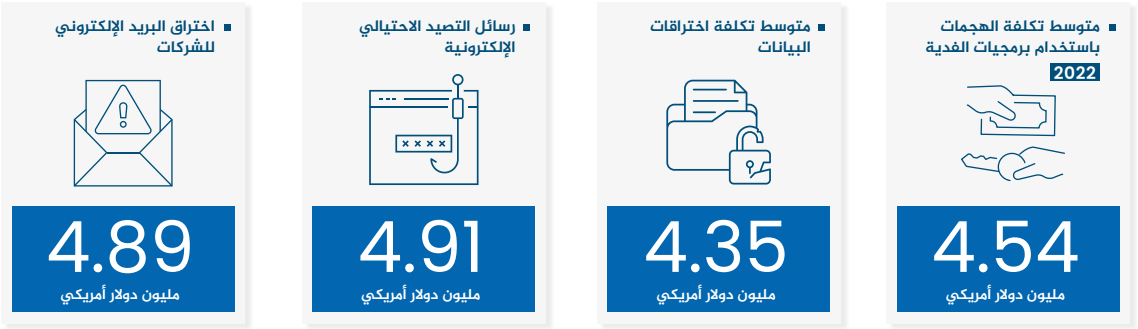
1. السياق الحالي للأمن السيبراني

تعتبر قطر في رحلة مستمرة من التحسين في مجال الأمن السيبراني، حيث حققت إنجازات كبيرة في هذا المجال خلال السنوات الماضية. ومع ذلك، يستمر المشهد العام العالمي للتهديدات السيبرانية في التطور وتستمر التهديدات السيبرانية الجديدة في الظهور فهناك تحديات سيبرانية جديدة تستدعي المعالجه، وستساعد هذه الاستراتيجية دولة قطر على تعزيز إمكانياتها السيبرانية العامة فيما يخص الاستجابة لهذه التحديات العالمية.

1.1 - المشهد العام للتهديدات السيبرانية

يزداد عدد وتنوع الهجمات السيبرانية التي يشنها المهاجمون عبر السنين، حيث يستخدمون أدوات متطورة ويوسعون نطاق أهدافهم. إذاً، فإنهم مصممون بشكل أكبر على استهداف ليس فقط بيئات تكنولوجيا المعلومات، بل بيئات التكنولوجيا التشغيلية أيضًا، ويستخدمون طرق هجوم يصعب الكشف عنها. وهذا يجعل من إمكانية التنبؤ بالمشهد العام العالمي للتهديدات السيبرانية أمرًا صعبًا[1]. فعلى المستوى العالمي، قُدِّرَ متوسط تكلفة الهجمات باستخدام برمجيات الفدية بنحو (4.54 مليون دولار أمريكي[2]) في عام 2022، بينما قُدِّرَ متوسط تكلفة اختراقات البيانات بما يعادل (4.35 مليون دولار أمريكي[2])

وعلى وجه التحديد، فقد بلغ متوسط تكلفة اختراقات البيانات التي تسببت فيها تقنيات الهندسة الاجتماعية ما يعادل (4.10 مليون دولار أمريكي[3]) في عام 2022 ، لكن تبقى رسائل التصيد الاحتيالي الإلكترونية من أكثر وسائل الهجوم تكلفة (4.91 مليون دولار أمريكي[2]) يليها اختراق البريد الإلكتروني للشركات (4.89 مليون دولار أمريكي[2])



يكمن التحدي الأكبر الذي يواجه الدول والاقتصاد العالمي في الهجمات السيبرانية التي تستهدف قطاع الطاقة، لا سيما الغاز، إذ إن الإمدادات التي توفرها الدولة منه ذات أهمية قصوى للعديد من شركائها الدوليين. وتحتل قطر مكانة بارزة على الصعيد الدولي فهي شريك عالمي أساسي بفضل موقعها الجغرافي، وما تمتلكه من احتياطيات الطاقة، ورؤوس أموالها، وشعبها، وثقافتها. ومع ذلك، فإن الأهمية المتزايدة لدولة قطر على الساحة العالمية جعلت منها هدفًا أساسيًا للتهديدات السيبرانية. لذلك، فمن المهم الاستمرار في تعزيز الإمكانيات الوطنية في مجال الأمن السيبراني لمواجهة المخاطر السيبرانية المتطورة والحد من تعرض الدولة للهجمات السيبرانية أو التحديات.

2.1 - مساعي دولة قطر وإنجازاتها حتى بداية عام 2024

كانت قطر أول دولة في المنطقة تحدد الهجمات الإلكترونية على المستوى الوطني، مما أدى إلى إنشاء الفريق القطري للاستجابة لطوارىء الحاسب الآلي في عام 2005، والذي تم توجيه جهوده نحو أربعة أنشطة رئيسية:

- توفير معلومات دقيقة وفي الوقت المناسب عن التهديدات والثغرات الحالية والناشئة في مجال أمن المعلومات.
- الاستجابة للتهديدات والثغرات ذات الصلة بالجهات الوطنية.
- تعزيز تبني معايير أمن المعلومات و المنهجيات والأساليب وأفضل الممارسات والأدوات ذات الصلة.
- بناء القدرات والإمكانيات المحلية لإدارة المخاطر السيبرانية عن طريق توفير التوعية والتدريب بخصان الأمن السيبراني.

لقد تجلى التزام الدولة بالأمن السيبراني في تنفيذها الناجح لاستراتيجية عام 2014. ومنذ ذلك الحين، لقد اتخذت قطر خطوات لتوحيد حوكمة الأمن السيبراني وتنسيق الجهود الوطنية، وقد كانت نقطة التحول الحاسمة على هذا الصعيد هي إنشاء الوكالة الوطنية للأمن السيبراني[4] عام 2021.

كما كانت استضافة دولة قطر لكأس العالم لكرة القدم 2022 من ضمن الأحداث الكبرى التي استعدت لها دولة قطر سيبرانياً فتحضيرًا لكأس العالم لكرة القدم 2022، أصدرت قطر "إطار الأمن السيبراني 2022"[5] . حدد هذا الإطار الشامل القدرات المتعلقة بالأمن السيبراني اللازمة لحماية الخدمات الوطنية الحيوية والمنصات الرقمية التي تدعم كأس العالم. وتم متابعة خطط العمل ورفع القدرات داخل عدد كبير من المؤسسات للتأكد من مستوى الجاهزية السيبرانية للحدث. كما تم تنفيذ المناورات السيبرانية الوطنية لتوفر سيناريوهات خاصة بالجاهزية السيبرانية خلال استضافة الأحداث الكبرى، وإعطاء الفرص للمؤسسات لمراجعة وتحسين خطط الجاهزية لديها. وقد نجحت دولة قطر في استضافة كأس العالم لكرة القدم لعام 2022، وبذلك أظهرت قدرا عالياً من الصمود لمواجهة التهديدات السيبرانية.

قطاع الأمن السيبراني والابتكار فيه

تشجع قطر بنشاط تطوير صناعة الأمن السيبراني المحلية والبحوث الرقمية وبرامج الابتكار السيبراني، وقد قدر سوق الأمن السيبراني الخاص بها بمبلغ مليار دولار أمريكي في عام 2022 ومن المتوقع أن يصل إلى 1.6 مليار دولار أمريكي بحلول عام 2026 (بزيادة سنوية قدرها 12.7)[6].

أنشأت الحكومة مراكز بحوث متخصصة في الأمن السيبراني، وتوفر التمويل لدعم الابتكار والبحث في مجال الأمن السيبراني في الصناعة. على سبيل المثال، توفر واحة قطر للعلوم والتكنولوجيا أحدث المرافق ووخدمات الدعم للشركات الناشئة والمشاريع التكنولوجية وشركات التكنولوجيا العالمة، ومختبر قطر الوطني للبحوث يدعم تطوير خطط وبرامج وطنية متعلقة بالأمن السيبراني.

الشراكة مع الصناعة المحلية والدولية والأوساط الأكاديمية والمؤسسات البحثية، ومعهد قطر لبحوث الحوسبة مركزاً بحثيًا آخر يعمل على تحديد ناقلات التهديدات الجديدة، وتطوير حلول الأمن السيبراني المصممة خصيصاً لتلبية الاحتياجات الوطنية. بالإضافة إلى ذلك، تساهم هذه المراكز في تدريب المتخصصين في مجال الأمن السيبراني، وتعزيز القدرات الوطنية و القدرة على إدارة الهجمات السيبرانية.

وضع القوانين والأدوات التنظيمية لتأمين الفضاء السيبراني

اعتمدت قطر قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، والذي يتناول الجرائم التي تنطوي على اختراق نُظم الحاسب الآلي وبرامج المعلومات والشبكات والمواقع الإلكترونية[7] . ومنذ ذلك الحين، أصدرت الدولة تشريعات أخرى مهمة تتعلق بالفضاء السيبراني، مثل قانون حماية خصوصية البيانات الشخصية رقم (13) لسنة 2016[8] والذي ينظم خصوصية البيانات في دولة قطر.

بالإضافة إلى ذلك، اعتمدت دولة قطر مجموعة من السياسات والأطر، مثل سياسة تصنيف البيانات الوطنية ومعيار تأمين المعلومات الوطنية والتي تقدم توجيهات بشأن كيفية تنفيذ نظام متكامل لإدارة أمن المعلومات. كما وضعت الدولة سياسات ومعايير تغطي مستجدات الأمن السيبراني في مجالات مثل الأمن السحابي ونظم التحكم الصناعي ومعايير دورة حياة تطوير البرمجيات الآمنة، من بين جملة موضوعات أخرى.

بذلت دولة قطر جهودًا كبيرة لمعالجة مخاطر سلسلة التوريد. طورت قطر المعلومات الوطنية إطار الامتثال الأمني، الذي يقدم خدمات الاعتماد للمؤسسات وخدمات الاعتماد لمقدمي الخدمات. وهو يكمل الإطار الوطني لضمان المعلومات في قطر من أجل إنشاء فضاء سيبراني آمن وحيوي. بالإضافة إلى ذلك، تم تفويض دولة قطر من قبل لجنة إدارة المعايير المشتركة لترتيبات الاعتراف بالمعايير المشتركة، لإصدار شهادات أمن المعلومات لمنتجات وأنظمة تكنولوجيا المعلومات.

إرساء قواعد متينة لتعزيز رفع القدرات والوعي السيبراني

كان لدولة قطر جهود حيثية في رفع القدرات وبناء الكفاءات في الأمن السيبراني، وإطلاق برامج وطنية متعددة لنشر الثقافة السيبرانية والوعي السيبراني للتصدي للمخاطر والتهديدات لكافة فئات المجتمع. إطار المبادرة الرئيسي هو (سايبر إيكو)، وهو مشروع مناهج الأمن السيبراني بالشراكة بين الوكالة الوطنية للأمن السيبراني ووزارة التربية والتعليم العالي.

المساهمات العالمية والالتزامات الدولية

على الصعيد الدولي، أقرت دولة قطر وتابعت تنفيذ مبادرات مهمة للمساهمة في تعزيز صمود الأمن السيبراني العالمي، كما عززت تبادل الملعلومات والتعاون، مع زيادة مشاركتها في الهيئات السيبرانية الإقليمية والدولية. ومن الأمثلة الرئيسية على ذلك "مشروع ستاديا" (Project Stadia) [9]، الذي يمثل مبادرة تابعة لمنظمة الشرطة الجنائية الدولية (الإنتربول) تهدف إلى تعزيز التعاون الدولي بشأن الترتيبات الأمنية، بما في ذلك السيبرانية منها، في الفعاليات الرياضية الكبرى، والفريق العامل المفتوح العضوية ، الذي أنشئ بموجب قرار الجمعية العامة 73/27 لتصدي تحديات الأمن السيبراني العالمي الملحة من خلال تعزيز الحوار و التعاون بين الدول الأعضاء في الأمم المتحدة وأصحاب المصلحة في الصناعة والمنظمات غير الحكومية والأوساط الأكاديمية، وترتيب الاعتراف بالمعايير المشتركة.

على الرغم من اتخاذ دولة قطر لعدة خطوات لتعزيز مرونتها السيبرانية، فمن الضروري لها مواصلة التكيف والتقدم لمواجهة التحديات الناشئة ذات الصلة. ويصف القسم التالي عددًا من التحديات الملحة على صعيد الأمن السيبراني والتي تواجهها الدول في كل أنحاء العالم، بما في ذلك دولة قطر، وكذلك الفرص المحتملة التي يحملها الفضاء السيبراني في طياته.

3.1 - التحديات والفرص

أصبحت الهجمات السيبرانية أكثر تكرارًا وتطورًا وشدةً. ويواجه العالم، بما في ذلك قطر، مجموعة متزايدة من التحديات التي يجب أن تتناولها الاستراتيجية الجديدة. ومع ذلك، يمكن أن تحمل هذه التحديات أيضًا فرصًا جديدة لتعزيز قدرات الأمن السيبراني وإمكانياته.

- **إدارة الأزمات والمخاطر السيبرانية على الصعيد الوطني للتعامل بفعالية مع المشهد العام المتغير للتهديدات السيبرانية**

يعتبر ارتفاع وتيرة الهجمات السيبرانية الموجهة ضد البنية التحتية الوطنية الحيوية باعثًا للقلق على الصعيد العالمي حيث أن الدراسات الدولية أظهرت بأن المؤسسات التي تواجه تعطلات سيبرانية تتكبد خسائر مالية تُقَدَّرُ في المتوسط بنحو 2.8 مليون دولار أمريكي لكل حادثة، وأن قطاع النفط والغاز هما الأكثر تأثرًا من بين سائر القطاعات[10]. وبالإضافة إلى الخسائر المالية، يمكن أن تؤدي المخاطر المحتملة للتعطل الشديد في البنية التحتية الوطنية الحيوية إلى أزمة على الصعيدين الوطني والعالمي.

الأكثر تأثراً

يعتبر قطاع النفط والغاز هما الأكثر تأثرًا من بين سائر القطاعات في الهجمات السيبرانية الموجهة ضد البنية التحتية الوطنية الحيوية

2.8 مليون دولار أمريكي

متوسط الخسائر التي تتكبدها المؤسسات التي تواجه تعطلات سيبرانية على الصعيد العالمي

يمكن للدول التعامل مع هذا التهديد من خلال تطوير منهجيات مُتّسقة فيما يخص ممارسات إدارة الأزمات والمخاطر السيبرانية على الصعيد الوطني. ويمكن أن تُشكّل هذه المنهجيات فرصة للسلطات لتعزيز الإمكانيات الوطنية والاستعداد للتهديدات السيبرانية المحتملة من حيث الحماية منها والكشف عنها والاستجابة لها . بالإضافة إلى ذلك، يمكن لهذه الممارسات أن تساعد في الحد من الآثار طويلة الأجل، مثل زيادة التعرض للهجمات المستقبلية والإضرار بالسمعة وفقدان الثقة العامة في الفضاء السيبراني.

- **تبادل المعلومات المتعلقة بالتهديدات السيبرانية وإمكانيات الاستجابة للحوادث السيبرانية من أجل مجابهة الهجمات السيبرانية شديدة التطور**

تواصل مجموعات ضارة العمل على تحسين أدواتها وتقنياتها، ما يؤدي إلى زيادة تطور ووتيرة الهجمات السيبرانية. لذلك، تحتاج المؤسسات إلى اتباع ممارسات متينة وفعالة في مشاركة المعلومات المتعلقة بالتهديدات.

يمكن أن يكون تبادل الخبرات والمعلومات بشأن التهديدات والحوادث والثغرات وإجراءات التخفيف وأفضل الممارسات في مجال الأمن السيبراني فرصة لتحسين التنسيق والتعاون على المستوى الوطني والاستراتيجي بين الأطراف المعنية ولتعزيز قدرات إدارة الحوادث السيبرانية. تساهم مشاركة المعلومات بشأن التهديدات السيبرانية، إلى جانب توافر قدرات أعلى في مجال إدارة الحوادث السيبرانية، في زيادة القدرة الإجمالية للحماية من التهديدات السيبرانية.

- **التنسيق والتعاون على مستوى البنية التحتية الوطنية الحيوية لتحسين صمود الأمن السيبراني**

تعد الهجمات السيبرانية ضد البنية التحتية الوطنية الحيوية مصدر قلق على المستوى العالمي بشكل عام وفي دولة قطر بشكل خاص. قد يؤدي نجاح الهجمات السيبرانية التي تستهدف منشآت وطنية حيوية مثل قطاع الطاقة إلى تعطل أنشطة الاقتصاد الوطني والأقليمي والعالمي. إذ تمثل قطاعات البنية التحتية الوطنية الحيوية، وخاصة تلك التي تعتمد بشكل كبير على التكنولوجيا التشغيلية، أهدافاً رفيعة المستوى، مما يجعل من الضروري الاحتفاظ بسجل للأزمات والمخاطر السيبرانية على الصعيد الوطني والأصول الحيوية ومخاطرها المحتملة على البلد.

يمكن للتعاون الأكثر حيوية بين السلطات الحكومية ومنظمي القطاع ومشغلي الأزمات والمخاطر السيبرانية على الصعيد الوطني تعزيز مرونة الأمن السيبراني في الأزمات والمخاطر السيبرانية على الصعيد الوطني. من خلال العمل معا، يمكن لأصحاب المصلحة تبادل المعلومات حول تهديدات الأمن السيبراني المحتملة وتقنيات التقليل من المخاطر. ينبغي تبادل الملعومات عبر مختلف قطاعات الأزمات والمخاطر السيبرانية على الصعيد الوطني لضمان إمكانية استخدام الخبرة المستفادة في صناعة واحدة لحماية قطاعات الأزمات والمخاطر السيبرانية على الصعيد الوطني الأخرى.

- **تعزيز أمن سلاسل التوريد لحماية البيئة السيبرانية العامة**

تعتمد العديد من المؤسسات على الموردين لتزويدها بالمنتجات والنظم والخدمات. نظرا لأن الصناعة وقطاع الخدمات يتغيران مع تطور التكنولوجيا، فإن التهديدات السيبرانية تتغير أيضا. يعد تأمين سلاسل التوريد فرصة لتعزيز صمود الفضاء السيبراني، إذ تستهدف المجموعات الضارة الموردين بهدف الوصول إلى الجهة الرئيسية التي ينوون اختراقها، أو يستهدفون منصات تشغيلية حيوية تستخدمها مختلف القطاعات.

أطر قانونية ورقابية ملائمة للتعامل مع المخاطر السيبرانية الناشئة

يترافق التطور التكنولوجي مع تطور في المخاطر السيبرانية. لذلك لا بدّ من صياغة الأطر القانونية والرقابية المناسبة وتحديثها بانتظام وإلّا سيؤدي التطور المتسارع للتقنيات الناشئة وظهور منتجات وخدمات جديدة إلى ثغرات جديدة في ظل غياب معايير أمنية واضحة. ويرجع ذلك في الأساس إلى أن سرعة تطوير وتبني التقنيات الناشئة تفوق بكثير قدرة النظام القانوني على فرض تدابير أمنية تواكب هذه التطورات[11] . على سبيل المثال، عملت المؤسسات في الأعوام القليلة الماضية على تبني مجموعة من الحلول التي تشمل الذكاء الاصطناعي والتعلم الآلي وإنترنت الأشياء، والتي يُمكن أن تشكل تحديات مختلفة في غياب فهم واضح وحوكمة محددة لها.

علاوةً على ذلك، خَلصت دراسات دولية حديثة إلى أن المديرين التنفيذيين للشركات يُدركون قيمة قوانين الأمن السيبراني والأدوات التنظيمية المرتبطة كوسيلة للحد من المخاطر السيبرانية [12]. كما تُشير أفضل الممارسات الدولية على نحو متزايد إلى أن الإنفاذ الصحيح لتنظيمات الأمن السيبراني من شأنه أن يسهم في تعزيز الصمود السيبراني في كل القطاعات والحد من المخاطر الناجمة عن سلاسل التوريد ونقاط الارتباط بين القطاعات[12].

لذلك، فهذه فرصة ثمينة لتعزيز عملية تطوير الأطر القانونية والرقابية المناسبة التي تراعي المشهد المتغير للتهديدات وتتكيف مع التكنولوجيا المتطورة وتحقق التوازن الأمثل بين الأمن والابتكار.

قدرات وإمكانيات إجراء التحقيقات والملاحقات القضائية المتعلقة بالجرائم السيبرانية للتعامل الفوري مع الأشكال الجديدة للجرائم السيبرانية

صُنفت الجرائم السيبرانية ضمن أكبر عشرة مخاطر عالمية للعقد القادم[12]، وتشهد تطورًا ملحوظًا نتيجة لظهور الجرائم السيبرانية كخدمة في كل أنحاء العالم، في حين تُعتبر جودة معايير الحماية للجهات منخفضة مما يسمح بتسلل المجرمين المحتملين[13].

وفي هذا السياق، يتمثل أحد التحديات الرئيسية في قدرات وخبرات سلطات إنفاذ القانون والسلطات القضائية فيما يخص إجراء تحقيقات عن الجرائم السيبرانية وملاحقتها. وتتطلب مواكبة هذه الجرائم الاستمرار في تعلم التقنيات والمهارات الجديدة، وهذا أمر يفرض على الدول، بما فيها قطر، تقديم البرامج التدريبية والتوعوية في المواضيع المتعلقة بالجرائم السيبرانية، وتزويد سلطات إنفاذ القانون والسلطات القضائية بالمعرفة والأدوات والمهارات اللازمة لأداء أدوارهم على أكمل وجه.

كما تتطلب مكافحة الجرائم السيبرانية تعزيز التعاون على المستويين الوطني والدولي. وتُشير الأهمية المتزايدة للأدلة الرقمية والجنائية (خصوصًا فيما يتعلق بالملاحقة القضائية) إلى ضرورة تعزيز وتوطيد التعاون بين سلطات إنفاذ القانون والأطراف المعنية الأخرى. يلزم أيضًا استخدام آلية فعالة لجمع الأدلة الرقمية ومشاركتها وحفظها والاستفادة منها، وكذلك تبادل بيانات الجرائم السيبرانية وأفضل الممارسات لمكافحتها. سيمثل التعزيز المستمر لقدرات وإمكانيات السلطات المعنية بإنفاذ القانون والملاحقات القضائية، وتزويدها بالمعرفة والمهارات والأدوات المناسبة، فرصة للتصدي بفعالية لأشكال جديدة من الجرائم السيبرانية في الوقت المناسب.

تنسيق ذو فاعلية لتعزيز الابتكار في مجال الأمن السيبراني

يُعدّ تسريع وتيرة الابتكار في مجال الأمن السيبراني عنصرًا أساسيًا لتحسين تكنولوجيا الأمن السيبراني في أي دولة في العالم. ويجب أن يواكب الابتكار في مجال الأمن السيبراني التقنيات الناشئة الأخرى بهدف تحديد المخاطر السيبرانية المحتملة وإدارتها، مما يعزز حماية الأفراد والمؤسسات. على سبيل المثال، يُمكن لتكنولوجيا مثل الحوسبة الكمية أن تحل مشكلات معقدة بشكل أسرع بكثير من أجهزة الحاسب التقليدية، وأن تُحقق التقدم في العديد من القطاعات، لكنها قد تشكل تهديدًا لنظم التشفير التي تدعم البنية التحتية الرقمية في العالم[14]. وينطوي الاستثمار في الابتكار في مجال الأمن السيبراني على أهمية كبيرة لضمان أمن التكنولوجيا الجديدة المستحدثة في السوق.

لا تقتصر مزايا الابتكار في مجال الأمن السيبراني على توفير الحماية من المخاطر المحتملة والمستقبلية فحسب، بل إنها تمثل أيضًا فرصة لتطوير قطاع الأمن السيبراني المحلي والصادرات المحتملة. وحتى يتحول الابتكار في مجال الأمن السيبراني إلى عامل تمكين اقتصادي رئيسي، هناك حاجة إلى مزيد من التنسيق بين الهيئات الأكاديمية والمؤسسات التي تركز على البحوث من جهة والشركات من جهة أخرى. فمن شأن تحسين التعاون بين الأطراف المعنية تسهيل التحول من إجراء بحوث الأمن السيبراني إلى تبني إجراءات الأمن السيبراني في السوق من خلال معالجة أية أوجه عدم مواءمة قد تظهر بين نتائج البحوث وممارسات الأعمال.

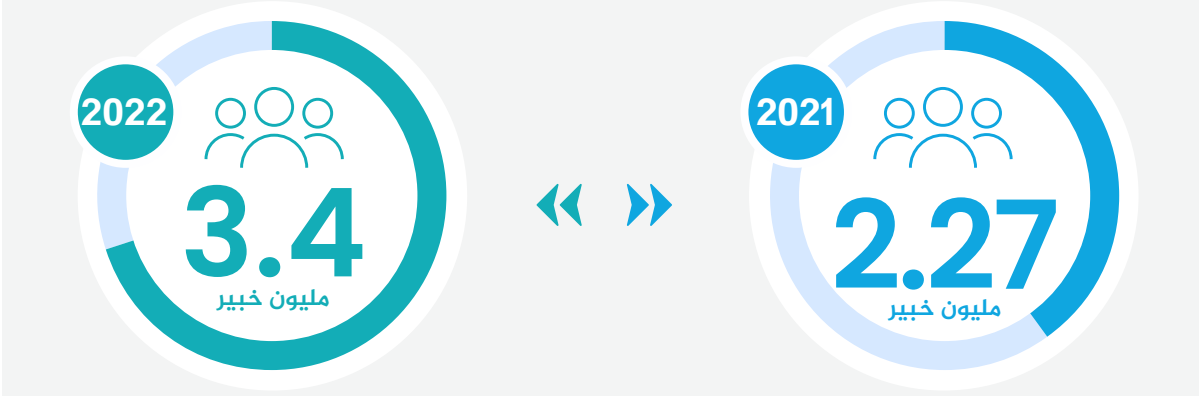
■ زيادة الاستثمارات لتشجيع تطوير قطاع لصناعة للأمن السيبراني

يُمكن أن يساعد الوصول إلى آليات التمويل المناسبة على دعم مشاريع البحث والابتكار في مجال الأمن السيبراني، وتسريع ترجمة البحوث والنماذج الأولية في الشركات الناشئة، على سبيل المثال، إلى منتجات الأمن السيبراني التي يتم تسويقها في السوق.

يعد تقديم حوافز لتعزيز قطاع الأمن السيبراني المحلي ودعم الشركات الناشئة والناضجة في مجال الأمن السيبراني فرصة لتنويع الاقتصاد القطري والدفع بعجلة الابتكار في مجال الأمن السيبراني، وينبغي أن تقترن هذه الجهود بتدابير تشجع الاستثمارات بهدف تعزيز الأعمال التجارية القائمة وإنشاء أعمال تجارية جديدة.

■ تعزيز الحوافز لتمكين الأفراد من العمل في مجال الأمن السيبراني

ليس هناك مجال للشك بأن النقص في الكوادر المتخصصة في الأمن السيبراني، والناجمة عن عدم التطابق بين العرض والطلب على المختصين في مجال الأمن السيبراني، تُشَكِّلُ إحدى تحديات القطاع الأكثر صعوبة وإلحاحًا على مستوى العالم[15] ، وهي السبب الرئيسي الذي يجعل المؤسسات تواجه تحديات في تحقيق الصمود السيبراني. وقد قُدِّر الفرق بين العرض والطلب على أخصائيي الأمن السيبراني بما يقارب من 2.27 مليون خبير في عام 2021[16] و3.4 مليون خبير حتى نهاية عام 2022 حول العالم[16].



الفرق بين العرض والطلب على أخصائيي الأمن السيبراني بين عامي 2021 و 2022 حول العالم

بالنظر إلى الفجوة الكبيرة في الكوادر المتخصصة في مجال الأمن السيبراني على مستوى العالم، من المهم تشجيع الأفراد على العمل في مجال الأمن السيبراني من مرحلة مبكرة. وقد يشكل إشراك الطلاب والشباب في مجال الأمن السيبراني تحديًا للعديد من البلدان، بما فيها قطر. لذلك يجب تطوير مبادرات في المدارس لإظهار فوائد مهن الأمن السيبراني للطلاب، إذ ستكون فرصة لتطوير الكوادر المحلية والقوى العاملة ذات المهارات العالية في مجال الأمن السيبراني في الدولة.

■ استقطاب الكوادر والكفاءات في مجال الأمن السيبراني والاحتفاظ بها

تتفاقم الفجوة في القوى العاملة المتخصصة في مجال الأمن السيبراني على الصعيدين المحلي والعالمي نتيجة عدم قدرة المؤسسات في الاحتفاظ بالكوادر والكفاءات المتخصصة في هذا المجال لمدة طويلة. وتواجه الدول في كل أنحاء العالم تحديات مرتبطة باستقطاب خبراء الأمن السيبراني المؤهلين والاحتفاظ بهم. وتُبيّن الدراسات الدولية أن خبراء الأمن السيبراني يغادرون مناصبهم غالبًا بسبب عدم كفاية المكافآت المالية، ومحدودية فرص التطور الوظيفي، وارتفاع مستويات الإجهاد في العمل، وغياب الدعم من القيادات. ويُمكن للمبادرات التي تشجع التطوير المهني المستمر ضمن المسار الوظيفي للأمن السيبراني، بما في ذلك الحوافز وآليات الترقية، أن تمثل فرصة لاستقطاب المهنيين الأكثر مهارة وموهبة في مجال الأمن السيبراني واستبقائهم.

المخاطر السيبرانية المتعلقة بالأخطاء البشرية التي يجب معالجتها

غالبًا ما يكون السلوك البشري سببًا أساسيًا وراء نجاح الهجمات السيبرانية، إذ يُمكن لأي مستخدم أن يتحول إلى ثغرة محتملة بسبب غياب الوعي للتهديدات السيبرانية والتدريب غير الكافي المتعلق بالأمن السيبراني والافتقار إلى الوعي الأساسي بالأمن السيبراني. وتنظر معظم المؤسسات إلى الأخطاء البشرية كأحد الأسباب الأكثر شيوعًا لحالات الاختراق الناجحة[17].

تواجه كل دول العالم هذا التحدي، بما فيها دولة قطر. وهناك حاجة إلى بذل مزيد من الجهود على المستويين الوطني والدولي لتحسين التدريبات المقدمة وتعزيز الوعي على نطاق واسع. علاوة على ذلك، يمكن تصميم مبادرات تستهدف فئات محددة من المجتمع، وتخصيصها لتلبية احتياجات تلك الفئات. وتمثل التوعية بمخاطر الأمن السيبراني فرصة لتقليل الأخطاء البشرية في الفضاء السيبراني.

تعزيز التعاون الدولي للتعامل مع المخاطر السيبرانية العالمية

تُعدّ المخاطر والتهديدات السيبرانية غير مُقيدة بالحدود الوطنية على عكس التهديدات التقليدية، وذلك بسبب الطبيعة المترابطة للفضاء السيبراني وتقدم الرقمنة والعولمة. وغالبًا ما يمتد تأثير الهجمات السيبرانية إلى دول أخرى من العالم، مما يزيد من صعوبة الاستجابة الحكومية. ويجب أن تعمل الدول مع المجتمع الدولي لضمان فضاء سيبراني آمن وتطوير حلول دولية وضمان سلامة الأفراد.

تتطلب المشاركة في الجهود العالمية حول الأمن السيبراني، لا سيما في المنتديات متعددة الأطراف مثل الأمم المتحدة، أن يمتلك المسؤولون المعنيون خبرات واسعة وكفاءة كبيرة في السياسات السيبرانية لتسليط الضوء على الإمكانيات السيبرانية للدولة على المسرح الدولي وإبرام أطر تعاون وشراكات مع وكالات أمن سيبرانية أخرى.

يمكن أن تشكل المبادرات التي تشجع الشراكات والتعاون الدولي فرصة لتعزيز مكانة الدول في المشهد السيبراني الدولي. وبالمثل، فإن دعم تطوير معايير إقليمية ودولية، مع التركيز على تسخير التكنولوجيا الحديثة لأغراض سلمية، قد يساهم أيضًا في تعزيز دور الدول في الساحة الدولية.

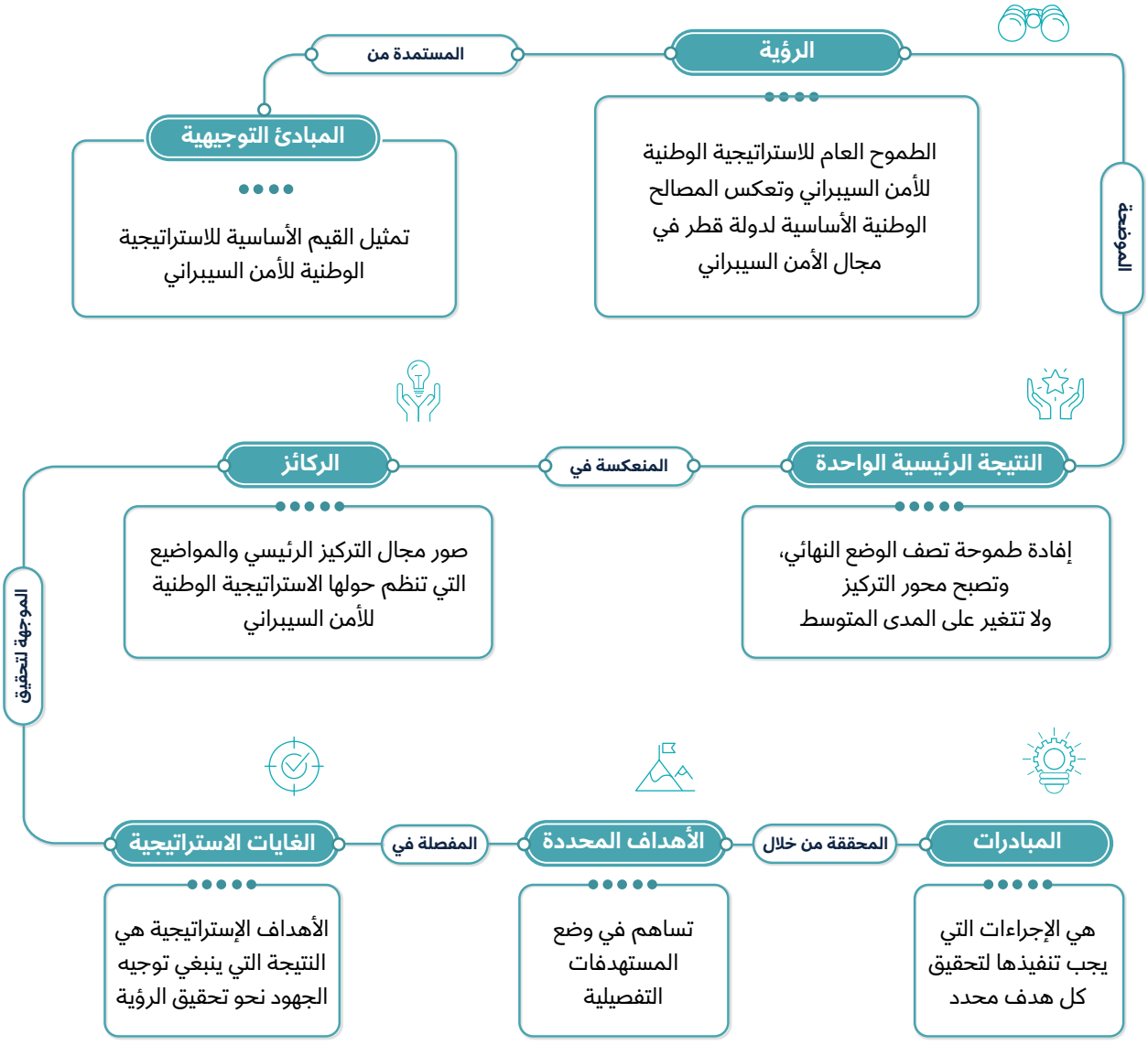
ستتناول مكونات هذه الاستراتيجية (2024-2030) الرؤية - المبادئ التوجيهية - الغايات الاستراتيجية - الركائز - الأهداف المُحددة - المبادرات والتحديات والفرص ذات الصلة بالأمن السيبراني، كما هو مفصل في الأقسام التالية.

02

المكونات الأساسية للاستراتيجية

المكونات الأساسية للاستراتيجية

تشمل هذه الاستراتيجية ستة مكونات أساسية، وهي تُحدد مجتمعةً التوجه العام للدولة في مجال الأمن السيبراني:



الشكل 1: الاستراتيجية للأعوام 2024-2030: المكونات الأساسية ونقاط ارتباطها

1.2 - الرؤية والنتيجة الرئيسية الواحدة

تتبنى الرؤية الخاصة بالاستراتيجية للأعوام 2024-2030 التزام الأطراف المعنية بالتعاون لتحقيق هدف مشترك، وهو توفير فضاء سيبراني آمن للأفراد والمؤسسات. ويُعد تعزيز الأمن والصمود السيبراني من العوامل التمكينية الرئيسية.

الشكل 2: الرؤية والنتيجة الرئيسية الواحدة

النتيجة الرئيسية الواحدة

إن النتيجة الرئيسية الواحدة للاستراتيجية الوطنية للأمن السيبراني في دولة قطر 2024-2030 هي بمثابة علامة طموحة تلخص جوهر البرنامج الوطني للإحصاء في قطر. وهي نقطة مرجعية ثابتة توجه قطر نحو فضاء سيبراني آمن ومرن. إنه يمثل التزاما أساسيا بتأمين المجال الرقمي لصالح الأفراد والمنظمات على حدٍ سواء. وباعتبارها نقطة مركزية مستقرة وغير متغيرة، تضمن النتيجة الرئيسية الواحدة أن كل جهد ومبادرة يتم القيام بها ضمن الاستراتيجية الوطنية للأمن السيبراني تساهم في تحقيق رؤية الاستراتيجية الوطنية للأمن السيبراني. إن الفضاء السيبراني الأكثر أمانا وصمود لن يؤدي فقط إلى تعزيز تنمية الدولة، بل سيدعم أيضاً نموها، الازدهار المستمر في العصر الرقمي.

2.2 - المبادئ التوجيهية

تـم تحديـد سـته مبـادئ توجيهيـة، والتـي تمثـل القواعـد الرئيسـية فـي تحقيـق الأمـن السـيبراني الوطنـي. تسـاعد هـذه المبـادئ فـي التوجيـه والإرشـاد لتنفيـذ الاسـتراتيجية الوطنيـة للأمـن السـيبراني وتوجيـه أصحـاب المصلحـة فـي تنفيـذ المبـادرات. إذ تـم اتبـاع المبـادئ التوجيهيـة وتطبيقهـا طـوال دورة حيـاة الاسـتراتيجية بأكملهـا (مـن التطويـر إلـى التنفيـذ إلـى المراقبـة)، فإنهـا سـتدعم تحقيـق كل مـن الرؤيـة والغايـات الاسـتراتيجية.

المسؤولية المشتركة

تحفيـز كل جهـة فـي المنظومة السـيبرانية علـى أداء دور فعـال، وتحمـل مسـؤولية ممارسـات الأمـن السـيبراني الخاصـة بهـا، والمسـاهمة فـي تعزيـز الإمكانيـات الوطنيـة السـيبرانية.

نهج قائم على إدارة المخاطر

تقليـل المخاطـر السـيبرانية إلـى مسـتوى مقبـول، مـع مراعـاة السـياق والأهـداف المحـددة.

التركيز على النتائج

التركيـز علـى الغايـات الفعالـة القابلـة للتحقيـق والتـي مـن شـأنها تحقيـق رؤيـة الاسـتراتيجية.

حقوق الأفراد الشخصية

تعزيـز حقـوق الأفـراد ومسـؤولياتهم فـي البيئـة الرقميـة.

الازدهار الاقتصادي

تعزيـز الأمـن والصمـود السـيبراني لتكـون بمثابـة ضمانـات رئيسـية للنمـو والازدهـار الاقتصـادي.

التنسيق والتعاون

تنسـيق الجهـود الوطنيـة وتوحيدهـا ومواءمتها لتحسـين الأمـن السـيبراني الوطني.

الشكل 3: المبادئ التوجيهية للاستراتيجية

3.2 - الركائز | الغايات الاستراتيجية | الأهداف المحددة

1 - ركائز الاستراتيجية الوطنية للأمن السيبراني والغايات الاستراتيجية المرتبطة بها

تم تحديد ركائز الاستراتيجية الوطنية للأمن السيبراني من خلال تحديد مجموعة من الدوافع، مما ساعد في تحديد اتجاه التطلعات في قطر في مجال الأمن السيبراني للمستقبل. تم تحديد هذه الدوافع أو المحركات بناءً على التحديات العالمية المتزايدة للأمن السيبراني، والإنجازات الرئيسية في مجال الأمن السيبراني في الدولة، والنتائج المستقبلية المرغوبة، بما في ذلك الفرص والطموحات الوطنية الشاملة للتحول التي عبرت عنها رؤية قطر الوطنية 2030 والمبادئ التوجيهية الستة التي تقع في قلب الاستراتيجية الوطنية للأمن السيبراني.

الركيزة الأولى: الأمن والصمود السيبراني في النظام البيئي القطري

- التبني الفعال والسريع لأحدث التوجهات في مجال الأمن السيبراني، للتصدي للمشهد العام المتغير للتهديدات السيبرانية، وإنشاء منظومة يؤدي فيها كل طرف معني دورًا في تعزيز إمكانيات الأمن السيبراني على الصعيد الوطني.
- التنسيق الوطني لتعزيز الأمن والصمود السيبراني والثقة في البيئة السيبرانية.
- تمكين الأفراد والمؤسسات لإدارة المخاطر السيبرانية والشعور بالحماية والأمان في الفضاء السيبراني.
- تحسين موقف الأمن السيبراني في الدولة وحماية قطاعات البنية التحتية الحيوية ضد التهديدات السيبرانية.

الركيزة الثانية: التشريعات والتنظيم وإنفاذ القانون من أجل فضاء سيبراني آمن

- توسيع نطاق الأدوات التشريعية والتنظيمية لمواكبة تحديات الأمن السيبراني التي تنشأ مع التطور التكنولوجي.
- تنظيم الفضاء السيبراني لحماية حقوق الأفراد ومصالحهم مع تمكين الازدهار والنمو في الوقت نفسه.
- تعزيز قدرات وإمكانيات إجراء التحقيقات والملاحقات القضائية المتعلقة بالجرائم السيبرانية للتعامل الفوري مع الأشكال الجديدة للجرائم السيبرانية.

الركيزة الثالثة: اقتصاد مزدهر ومبتكر يعتمد على البيانات

- تطوير إمكانيات الابتكار في مجال الأمن السيبراني للمساهمة في تنويع أنشطة الاقتصاد القطري.
- تعزيز الإبداع والابتكار فيما يخص التطورات التكنولوجية المتقدمة.
- تأسيس قطاع وطني للابتكار في مجال الأمن السيبراني.

الركيزة الرابعة: الثقافة السيبرانية وتنمية مواهب القوى العاملة

- تمكين نظام تعليمي بمعايير عالمية يزود الأفراد بالمعارف والمهارات والكفاءات المناسبة في مجال الأمن السيبراني.
- تطوير قوى عاملة على درجة عالية من المهارة في مجال الأمن السيبراني والاحتفاظ بها.
- نشر ثقافة متينة فيما يخص الأمن السيبراني بين الأفراد والمؤسسات.

الركيزة الخامسة: التعاون الدولي والشراكة الموثوقة

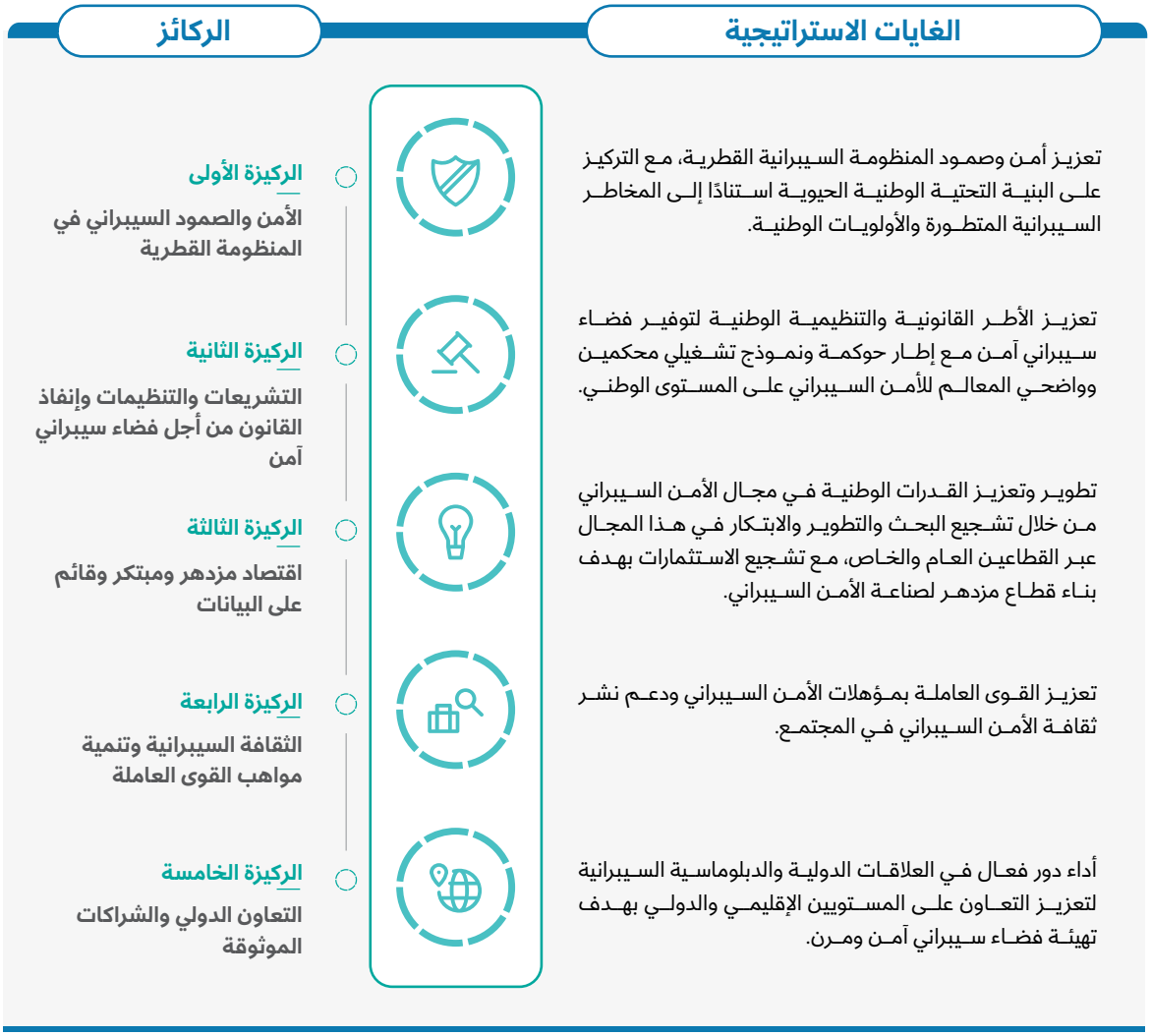
- تعزيز التعاون الإقليمي والدولي في التعامل مع المخاطر السيبرانية على الصعيد العالمي.
- تعزيز دور دولة قطر و مساهمتها في مجال الأمن السيبراني على الساحة الدولية.

الجدول 1: ربط الدوافع بركائز الاستراتيجية

تم تحديد خمس ركائز تمثل اللبنات الأساسية التي تقوم عليها هيكلة وتنظيم الاستراتيجية الوطنية للأمن السيبراني، وتتكون من المحاور الأساسية المتعلقة بالأمن السيبراني والتي ستتناولها الاستراتيجية الوطنية للأمن السيبراني لتحقيق رؤيتها.

يكمن الهدف من هذه الركائز هو توفير تغطية شاملة لجميع مجالات تركيز الاستراتيجية الوطنية للأمن السيبراني. على الرغم من أن كل مجال يتناول مجالاً محدداً، إلا أن الركائز مترابطة وتدعم بعضها البعض. يوفر التقدم في أحد الركائز أساسًا عامًا للأمن السيبراني يدعم نتائج الركائز الأخرى وعندما يجتمع يفي بالرؤية الاستراتيجية الوطنية للأمن السيبراني.

من أجل ضمان إدارة الاستراتيجية الوطنية للأمن السيبراني والتركيز عليها بشكل جيد وصيانتها بشكل صحيح بالإضافة إلى تحقيق النتائج المرجوة لكل ركيزة، تمت صياغة غاية استراتيجية لكل ركيزة. ولهذه الغايات الاستراتيجية دور فعال في تحديد اتجاه الجهود الجماعية نحو تحقيق النتائج المقصودة.



الشكل 4: أوجه الترابط بين الغايات الاستراتيجية والركائز

2 - تحقيق الغايات الاستراتيجية من خلال الأهداف المحددة

تم تحديد مجموعة الغايات الاستراتيجية على أنها النتائج المرجوة التي توجه إليها الجهود ضمن كل ركيزة، وعندما يتم دمجها تكون بمثابة نقطة انطلاق نحو تحقيق الرؤية الاستراتيجية الوطنية للأمن السيبراني. ولضمان إمكانية تحقيقها، يتم دعم كل غاية استراتيجي من خلال تحديد أهداف محددة لكل ركيزة استراتيجية وطنية للأمن السيبراني.

الركيزة الأولى ◇ الأمن والصمود السيبراني في النظام البيئي في قطر.

الغاية الاستراتيجية

تعزيز الأمن والصمود السيبراني في قطر مع التركيز على البنية التحتية الوطنية الحيوية بناءً على المخاطر السيبرانية المتطورة والأولويات الوطنية

الأهداف المحددة

1. تحقيق التقدم الفعال في فهم الظروف المتعلقة بالمخاطر والتهديدات السيبرانية على الصعيد الوطني لضمان تعزيز أمن وصمود الفضاء السيبراني في دولة قطر.
2. تعزيز الإمكانيات التقنية الوطنية والمؤسسية في قطر للحماية من التهديدات السيبرانية والكشف عنها والاستجابة لها والحد منها في الوقت المناسب.
3. إدارة الأزمات السيبرانية الوطنية بشكل فعال من خلال التنسيق مع الجهات المعنية على المستوى الوطني، مع ضمان الاستجابة والتعافي السريعين من الأزمات السيبرانية واستمرارية الخدمات الحيوية.
4. تعزيز صمود البنية التحتية الوطنية الحيوية واستمرارية الخدمات الحيوية بالتنسيق مع الجهات التنظيمية للقطاع ومشغلي البنية التحتية الوطنية الحيوية.

الجدول 2: الركيزة الأولى وأهدافها المحددة

الركيزة الثانية: التشريعات والتنظيمات وإنفاذ القانون من أجل فضاء سيبراني آمن.

الغاية الاستراتيجية

تعزيز الأطر القانونية والتنظيمية الوطنية لتوفير فضاء سيبراني آمن من خلال إطار حوكمة ونموذج تشغيلي محكمين وواضحي المعالم للأمن السيبراني على المستوى الوطني.

الأهداف المحددة

1. وضع الأطر القانونية والتنظيمية المناسبة التي تراعي المشهد العام المتغير للتهديدات وتحقق التوازن الصحيح بين الأمن والابتكار.
2. وضع لوائح تنظيمية للقطاعين العام والخاص لتعزيز الضمان السيبراني والامتثال والمشاركة في آليات الإشراف.
3. الاستمرار في تعزيز قدرات وإمكانيات سلطات إنفاذ القانون على الصعيد الوطني للتحقيق في كافة أشكال الجرائم السيبرانية وملاحقتها قضائيًا ومكافحتها بفعالية.

الجدول 3: الركيزة الثانية وأهدافها المحددة

الركيزة الثالثة: اقتصاد مزدهر ومبتكر وقائم على البيانات

الغاية الاستراتيجية

تطوير وتعزيز القدرات الوطنية في مجال الأمن السيبراني من خلال تشجيع البحث والتطوير والابتكار في هذا المجال عبر القطاعين العام والخاص، مع تشجيع الاستثمارات بهدف بناء قطاع مزدهر لصناعة الأمن السيبراني.

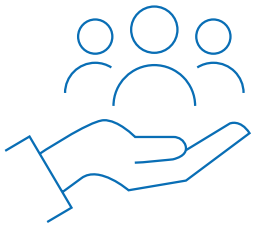
الأهداف المحددة

1. بذل جهود منسقة في مجال البحث والتطوير والابتكار فيما يخص الأمن السيبراني بما يواكب احتياجات السوق وأولويات الأمن الوطني.
2. تشجيع الاستثمارات المستدامة لجعل قطر مركزًا للابتكار في مجال الأمن السيبراني وراعية للأفكار، مع طرحها لتكنولوجيات وحلول ومنتجات مبتكره في سوق الأمن السيبراني على المستويات الوطنية والإقليمية والدولية.
3. تشجيع الاستثمارات لتحقيق الاستدامة على صعيد تطوير قطاع الأمن السيبراني الوطني والمساهمة في الناتج المحلي الإجمالي للبلاد.

الجدول 4: الركيزة الثالثة وأهدافها المحددة

الركيزة الرابعة: تطوير الثقافة السيبرانية وتنمية مواهب القوى العاملة.

الغاية الاستراتيجية



تعزيز القوى العاملة بمؤهلات الأمن السيبراني ودعم نشر ثقافة الأمن السيبراني في المجتمع

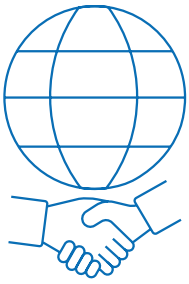
الأهداف المحددة

1. مواءمة المعرفة والمهارات المدرَّسة في البرامج التعليمية والتدريبية مع الاحتياجات السيبرانية لكل من القطاعين الحكومي والخاص.
2. تمكين الأفراد من جميع فئات المجتمع من خلال توفير المعرفة والمهارات ذات الصلة للتحفيز على العمل في مجال الأمن السيبراني.
3. رعاية المواهب الكامنة وتحفيزها وإشراكها من أجل تشجيعها على العمل في مجال الأمن السيبراني.
4. استقطاب المهنيين الأكفاء واستبقائهم في قطاع الأمن السيبراني لسد الفجوة في القدرات اللازمة في مجال الأمن السيبراني داخل الدولة.
5. تمكين الأفراد في قطر لفهم مخاطر الأمن السيبراني وتعزيز ثقافتهم السيبرانية ليصبحوا قادرين على اتخاذ الخطوات المناسبة لحماية مؤسساتهم وأنفسهم.

الجدول 5: الركيزة الرابعة وأهدافها المحددة

الركيزة الخامسة: التعاون الدولي والشراكات الموثوقة

الغاية الاستراتيجية



أداء دور فعال في العلاقات الدولية والدبلوماسية السيبرانية لتعزيز التعاون على المستويين الإقليمي والدولي بهدف تهيئة فضاء سيبراني آمن ومرن.

الأهداف المحددة

1. عقد وتعزيز شراكات موثوقة على المستويين الإقليمي والدولي لتعزيز التعاون وبناء القدرات والإمكانيات السيبرانية المتبادلة وفهم التهديدات المشتركة.
2. تعزيز قدرات الدبلوماسية السيبرانية لدولة قطر لتعزيز دورها في المناقشات والأحداث والمبادرات الدولية والإقليمية المتعلقة بالسيبرانية.
3. تعزيز مساهمة قطر في الحوار العالمي بشأن الأمن السيبراني لبناء فضاء سيبراني دولي يتسم بالأمن والأمان والاستقرار ويعزز تطوير معايير سيبرانية دولية إيجابية.
4. تعزيز التوعية حول الجهود التي تبذلها قطر على المستوى الإقليمي والدولي لتعزيز مكانتها في مجال الأمن السيبراني.

الجدول 6: الركيزة الخامسة وأهدافها المحددة

03

تنفيذ الاستراتيجية

3. تنفيذ الاستراتيجية

من أجل جعل الاستراتيجية الوطنية للأمن السيبراني 2024-2030 فعالة، يجب على الجهات المعنية بالتنفيذ العمل بشكل مشترك لتنفيذ المبادرات، التي ستساعد بشكل مجتمعي على تحقيق الأهداف المحددة لكل ركيزة. وستساعد هذه الأهداف المحددة في تحقيق الغايات الاستراتيجية وفي النهاية تحقيق الرؤية للاستراتيجية الوطنية للأمن السيبراني.

الرؤية | "جهود موحدة لتعزيز الثقة في الفضاء السيبراني لتقدم وازدهار قطر"

النتيجة الرئيسية الواحدة: فضاء سيبراني بمستوى عالي من الأمن والصمود يساهم في ازدهار دولة قطر

المبادئ التوجيهية

- المسؤولية المشتركة
- التركيز على النتائج
- نهج قائم على إدارة المخاطر
- الازدهار الإقتصادي
- حقوق الأفراد الشخصية
- التنسيق والتعاون

الركائز

الركيزة الأولى	الركيزة الثانية	الركيزة الثالثة	الركيزة الرابعة	الركيزة الخامسة
الأمن والصمود السيبراني في المنظومة القطرية	التشريعات والتنظيمات وإنفاذ القانون من أجل فضاء سيبراني آمن	اقتصاد مزدهر ومبتكر وقائم على البيانات	الثقافة السيبرانية وتنمية مواهب القوى العاملة	التعاون الدولي والشراكات الموثوقة

الغايات الاستراتيجية

1. تعزيز أمن وصمود المنظومة السيبرانية القطرية، مع التركيز على البنية التحتية الوطنية الحيوية استنادًا إلى المخاطر السيبرانية المتطورة والأولويات الوطنية.
2. تعزيز الأطر القانونية والتنظيمية الوطنية لتوفير فضاء سيبراني آمن مع إطار حوكمة ونموذج تشغيلي محكمين وواضحي المعالم للأمن السيبراني على المستوى الوطني.
3. تطوير وتعزيز القدرات الوطنية في مجال الأمن السيبراني من خلال تشجيع البحث والتطوير والابتكار في هذا المجال عبر القطاعين العام والخاص، مع تشجيع الاستثمارات بهدف بناء قطاع مزدهر لصناعة الأمن السيبراني.
4. تعزيز القوى العاملة بمؤهلات الأمن السيبراني ودعم نشر ثقافة الأمن السيبراني في المجتمع.
5. أداء دور فعال في العلاقات الدولية والدبلوماسية السيبرانية لتعزيز التعاون على المستويين الإقليمي والدولي بهدف تهيئة فضاء سيبراني آمن ومرن.

الشكل 5: نظرة شاملة حول مكونات الاستراتيجية الوطنية للأمن السيبراني

1.3 - الركيزة الأولى - الأمن والصمود السيبراني في المنظومة القطرية

الهدف المحدد الأول

تعزيز فهم الظروف المحيطة بالمخاطر والتهديدات الإلكترونية على الصعيد الوطني لضمان حماية صمود الفضاء السيبراني في قطر.

المبادرات - الهدف المحدد الأول

1.1.1 توفير نهج وطني لإدارة المخاطر السيبرانية بهدف مراقبتها وتقييمها ومعالجتها على المستوى الوطني بالتنسيق مع المؤسسات العامة والخاصة.

2.1.1 وضع إطار عمل وبروتوكولات وقنوات آمنة مخصصة لتبادل المعلومات للمؤسسات العامة والخاصة في قطر، لتمكينها من تبادل المعلومات بشأن التهديدات والثغرات والمخاطر والحوادث السيبرانية.

3.1.1 تعزيز إمكانيات الوعي العام بشأن المخاطر السيبرانية وتوقع التهديدات السيبرانية المستقبلية في القطاع العام والخاص

الهدف المحدد الثاني

تعزيز الإمكانيات التقنية الوطنية والمؤسسية في قطر للحماية من التهديدات السيبرانية والكشف عنها والاستجابة لها والحد منها في الوقت المناسب.

المبادرات - الهدف المحدد الثاني

1.2.1 وضع متطلبات محددة للأمن السيبراني للمؤسسات العامة والخاصة، مع مراعاة اختلاف أحجامها وطبيعتها، من أجل إدارة المخاطر السيبرانية بفاعلية وتعزيز نضج إدارة الحوادث السيبرانية.

2.2.1 تمكين المؤسسات العامة والخاصة لتقييم وتحسين نضج الأمن السيبراني لديها.

3.2.1 تشجيع المؤسسات العامة والخاصة على تقييم الأثر المالي للمخاطر السيبرانية، والتأمين ضد الحوادث السيبرانية للحد من التكاليف الناجمة عنها.

4.2.1 دعم وتسهيل تشكيل فرق الاستجابة لحوادث الأمن السيبراني القطاعية.

الهدف المحدد الثالث

إدارة الأزمات السيبرانية الوطنية بشكل فعال، مع ضمان الاستجابة والتعافي السريعين من الأزمات السيبرانية واستمرارية الخدمات الحيوية.

المبادرات - الهدف المحدد الثالث

1.3.1 إنشاء هيكل حوكمة مركزي لإدارة الأزمات والتعافي من الكوارث في مجال الأمن السيبراني على المستوى الوطني، مع تحديد أدوار ومسؤوليات واضحة للسلطات الوطنية ذات الصلة بمشاركة ممثلين من مختلف القطاعات.

2.3.1 تطوير آليات لإدارة الأزمات السيبرانية الوطنية وتنفيذها، وتمكين الاستجابة الفعالة للأزمات من خلال التنسيق المناسب بين الجهات الحكومية والمؤسسات الأخرى.

3.3.1 إعداد برامج محاكاة لصمود الأمن السيبراني بهدف إجراء تدريبات لاختبار الإمكانيات الوطنية فيما يتعلق بالجاهزية السيبرانية ومراقبتها باستمرار.

الهدف المحدد الرابع

تعزيز صمود البنية التحتية الوطنية الحيوية واستمرارية الخدمات الحيوية بالتنسيق مع الجهات التنظيمية للقطاع ومشغلي البنية التحتية الوطنية الحيوية.

المبادرات - الهدف المحدد الرابع

1.4.1 تعريف المتطلبات اللازمة لتحديد وتصنيف البنية التحتية الوطنية الحيوية والأصول الحيوية داخل كل قطاع، بالتنسيق مع الجهات التنظيمية للقطاع ومشغليه، ووضع خطط الصمود السيبرانية للقطاعات الحيوية.

2.4.1 وضع إطار محدد لإدارة المخاطر السيبرانية، بالتنسيق مع الجهات التنظيمية والمشغلين في القطاع، بما في ذلك إدارة مخاطر الأطراف الخارجية وأمن سلاسل التوريد، لتمكين البنية التحتية الوطنية الحيوية من تقييم هذه المخاطر واتخاذ الإجراءات المناسبة للحد منها.

3.4.1 إنشاء آليات وطنية للإبلاغ عن الحوادث السيبرانية، تكون مصممة خصيصًا للبنية التحتية الوطنية الحيوية، لتنسيق إمكانيات الوقاية من هذه الحوادث والكشف عنها والاستجابة لها.

4.4.1 إنشاء آليات لتبادل معلومات الكشف عن التهديدات السيبرانية داخل البنية التحتية الوطنية الحيوية وعبر قطاعاتها لتسهيل تبادل المعلومات وتعزيز الإلمام بوضع المخاطر السيبرانية.

2.3 - الركيزة الثانية - التشريعات والتنظيمات وإنفاذ القانون من أجل فضاء سيبراني آمن

3.3 - الركيزة الثالثة - اقتصاد مزدهر ومبتكر وقائم على البيانات

الهدف المحدد الأول

بذل جهود منسقة في مجال البحث والتطوير والابتكار فيما يخص الأمن السيبراني بما يساير احتياجات السوق وأولويات الأمن الوطني.

المبادرات - الهدف المحدد الأول

1.1.3 إنشاء هيكل حوكمة على المستوى الوطني لتنسيق الجهود بين الحكومة والقطاع الخاص والأوساط الأكاديمية في مجال البحث والتطوير والابتكار.

2.1.3 وضع استراتيجية وطنية متماسكة للابتكار في مجال الأمن السيبراني، مع تحديد الأولويات الوطنية الرئيسية بناءً على تحليلات السوق القائمة على البيانات بالشراكة مع القطاع الخاص والأوساط الأكاديمية.

الهدف المحدد الثاني

تشجيع الاستثمارات المستدامة لجعل قطر مركزًا للابتكار في مجال الأمن السيبراني وراعية للأفكار، مع طرحها لتكنولوجيات وحلول ومنتجات مبتكره في سوق الأمن السيبراني على المستويات الوطنية والإقليمية والدولية.

المبادرات - الهدف المحدد الثاني

1.2.3 إعداد برامج تحفز على الابتكار في مجال الأمن السيبراني لدعم مساهمة المؤسسات والأفراد في إنشاء أفكار جديدة، وجمع نخبة من الباحثين والمهنيين المنكبين على البحث والتطوير كمصدر للابتكار.

2.2.3 بناء وتوسيع برامج إمكانيات تطوير الأمن السيبراني لمواجهة التحديات الناشئة في مجال الأمن السيبراني وأولوياته الوطنية والتقليل من الاعتماد على الإمكانيات والحلول الخارجية فقط.

المبادرات - الهدف المحدد الثالث

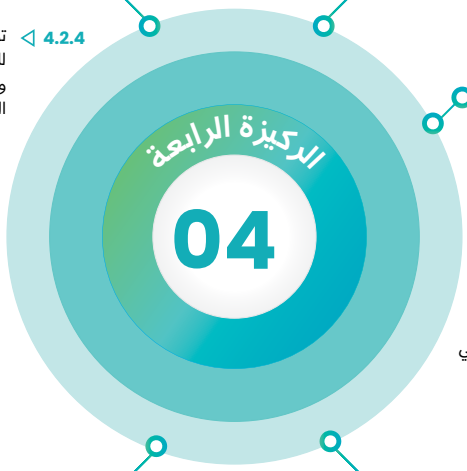
1.3.3 دعم الشركات الناشئة والشركات الأخرى لتطوير وتقديم خدمات ومنتجات مبتكرة في مجال الأمن السيبراني.

2.3.3 تسهيل ودعم إنشاء مسرّعات للأمن السيبراني لدعم الاستثمارات في مشاريع هذا القطاع من خلال ربط المستثمرين المحتملين بالمبتكرين.

الهدف المحدد الثالث

تشجيع الاستثمارات لتحقيق الاستدامة على صعيد تطوير قطاع الأمن السيبراني الوطني والمساهمة في الناتج المحلي الإجمالي للبلاد.

4.3 - الركيزة الرابعة - الثقافة السيبرانية وتنمية كوادر القوى العاملة



الهدف المحدد الأول

مواءمة المعرفة والمهارات التي يتم تدريسها في برامج التعليم والتدريب مع الاحتياجات السيبرانية لكل من الحكومة والقطاع الخاص.

المبادرات - الهدف المحدد الأول

1.1.4 فهم وتحديد متطلبات القوى العاملة الحالية والمستقبلية في مجال الأمن السيبراني من حيث الحجم والمعارف والمهارات والكفاءات، بالإضافة إلى تحديد التحديات المحتملة الماثلة أمام تطوير قوى عاملة عالية المهارة في هذا المجال.

2.1.4 وضع إطار وطني للقوى العاملة في مجال الأمن السيبراني يوفر لغة مشتركة ويحدد المعارف والمهارات والكفاءات المطلوبة لمختلف الأدوار الوظيفية في المجال للقطاعين العام والخاص.

الهدف المحدد الثاني

تمكين الأفراد من جميع فئات المجتمع من خلال توفير المعرفة والمهارات ذات الصلة للتحفيز على العمل في مجال الأمن السيبراني.

المبادرات - الهدف المحدد الثاني

1.2.4 إنشاء برامج تعليمية محددة في مجال الأمن السيبراني على كافة مستويات التعليم (الابتدائي والثانوي والجامعي) بهدف تشجيع الأفراد على العمل في هذا المجال.

2.2.4 إنشاء برنامج اعتماد وطني للدرجات العلمية والمهنية في مجال الأمن السيبراني.

3.2.4 تنسيق الجهود بين الجامعات ومراكز البحوث لمواءمة وتعزيز عمل معامل الأمن السيبراني، من أجل استكمال المعارف النظرية للطلاب بمهارات عملية وتوفير فرص تدريبات مهنية لهم.

4.2.4 توفير دورات تدريبية معتمدة في مجال الأمن السيبراني للارتقاء بمهارات المهنيين والممارسين في القطاع وتمكينهم من خلال تزويدهم بالمعارف والمهارات المناسبة.

الهدف المحدد الثالث

رعاية المواهب الكامنة وتحفيزها وإشراكها من أجل تشجيعها على العمل في مجال الأمن السيبراني.

المبادرات - الهدف المحدد الثالث

1.3.4 وضع برامج لتوعية الطلاب وأولياء الأمور بالفرص المهنية المتاحة في مجال الأمن السيبراني.

2.3.4 تعزيز ودعم برامج المنح الدراسية الوطنية في مجال الأمن السيبراني.

الهدف المحدد الرابع

استقطاب المهنيين الأكفاء واستبقائهم في قطاع الأمن السيبراني لسد الفجوة في القدرات اللازمة مجال الأمن السيبراني داخل الدولة.

المبادرات - الهدف المحدد الرابع

1.4.4 فهم وتحديد التحديات المتعلقة باستقطاب القوى العاملة في مجال الأمن السيبراني واستبقائها في قطر، وستُستخدم نتائج هذه المبادرة في صياغة وتنفيذ مبادرات لتعزيز القوى العاملة في هذا المجال في قطر.

2.4.4 اعتماد تعريف موحد للمناصب الوظيفية في مجال الأمن السيبراني في كل من القطاع العام و الخاص.

3.4.4 تطوير المسارات الوظيفية للمهنيين في مجال الأمن السيبراني في القطاعين العام والخاص، مع تقديم حوافز الاستبقاء من أجل تشجيعهم على التطور الوظيفي طويل الأمد في المهنة.

4.4.4 تمكين المرأة في قطر تولي أدوار قيادية في مجال الأمن السيبراني من خلال تطوير برامج التوجيه والإرشاد وتوفير فرص الارتقاء الوظيفي.

الهدف المحدد الخامس

تمكين الأفراد في قطر لفهم مخاطر الأمن السيبراني وتعزيز ثقافتهم السيبرانية ليصبحوا قادرين على اتخاذ الخطوات المناسبة لحماية مؤسساتهم وأنفسهم.

المبادرات - الهدف المحدد الخامس

1.5.4 إعداد برامج وطنية للتوعية السيبرانية للجمهور العام، بما في ذلك الأطفال وكبار السن، لتعزيز المعرفة والمهارات المتعلقة بالسلامة السيبرانية.

2.5.4 إبرام شراكات بين الهيئات الحكومية والقطاع الخاص لتعزيز الوعي بالأمن السيبراني في صفوف موظفيهم.

3.5.4 إعداد برامج وطنية تشجع على تبني الأخلاقيات السيبرانية وثقافة السلامة السيبرانية.

5 .3 - الركيزة الخامسة - التعاون الدولي والشراكات الموثوقة

الهدف المحدد الأول

عقد وتعزيز شراكات موثوقة على المستويين الإقليمي والدولي لتعزيز التعاون وبناء القدرات والإمكانيات السيبرانية المتبادلة وفهم التهديدات المشتركة.

المبادرات - الهدف المحدد الأول

1.1.5 تطوير شراكات سيبرانية دولية لتشجيع تبادل المعلومات حول التهديدات السيبرانية.

2.1.5 تعزيز العلاقات الثنائية ومتعددة الأطراف القائمة مع الدول والمؤسسات، وإبرام شراكات جديدة على المستويين الإقليمي والدولي، لتطوير مبادرات بناء القدرات والإمكانيات في مجال الأمن السيبراني.

3.1.5 وضع آليات للشراكات والتعاون بهدف مواجهة التهديدات السيبرانية العابرة للحدود الوطنية والكشف عن الجرائم السيبرانية ومكافحتها وملاحقتها.

الهدف المحدد الثاني

تعزيز قدرات الدبلوماسية السيبرانية لدولة قطر لتعزيز دورها في المناقشات والأحداث والمبادرات الدولية والإقليمية المتعلقة بالسيبرانية.

المبادرات - الهدف المحدد الثاني

1.2.5 تمكين الموظفين الدبلوماسيين وغيرهم من المسؤولين المعنيين من إيصال رسالة مشتركة حول الأمن السيبراني في المناقشات والفعاليات والمنتديات الإقليمية والدولية ذات الصلة بالمجال بما يتوافق مع المصالح الوطنية لدولة قطر.

2.2.5 إعداد الموظفين الدبلوماسيين وغيرهم من المسؤولين المعنيين للمشاركة بفاعلية في مناقشات وفعاليات ومنتديات الأمن السيبراني الإقليمية والدولية.

الهدف المحدد الثالث

تعزيز مساهمة قطر في الحوار العالمي بشأن الأمن السيبراني لبناء فضاء سيبراني دولي يتسم بالأمن والأمان والاستقرار ويعزز تطوير معايير سيبرانية دولية إيجابية.

المبادرات - الهدف المحدد الثالث

1.3.5 المساهمة في تطوير القانون الدولي ووضع قواعد الفضاء السيبراني من خلال المشاركة الفعالة في مبادرات الأمم المتحدة وغيرها من المبادرات الإقليمية والدولية.

2.3.5 المساهمة في تطوير معايير مشتركة للأمن السيبراني على المستويين الإقليمي والدولي.

الهدف المحدد الرابع

تعزيز جهود التوعية التي تبذلها قطر على المستوى الدولي لتعزيز مكانتها في مجال الأمن السيبراني

المبادرات - الهدف المحدد الرابع

1.4.5 تنظيم واستضافة فعاليات الأمن السيبراني الوطنية والدولية لتعزيز حضور قطر في المشهد العالمي لهذا المجال.

2.4.5 دعم الهيئات الحكومية والقطاع الخاص والمؤسسات الأكاديمية للترويج لمبادراتها المتعلقة بالأمن السيبراني أمام المجتمع الدولي.

04

التنفيذ، المتابعة والمراجعة

4. التنفيذ، المتابعة والمراجعة

ومن خلال المتابعة والمراجعة، ستعمل الوكالة الوطنية للأمن السيبراني على تقييم أنشطة وإنجازات هذه الاستراتيجية بشكل دوري مع الأطراف المعنية ذات الصلة، بالإضافة إلى تقييم مدى كفاية الغايات والمقاييس ذات الصلة. وستُستَخدم مجموعة من مؤشرات الأداء الرئيسية لتتبع التقدم الفعال على صعيد هذه الاستراتيجية وقياس نجاح تنفيذ الأهداف المحددة.

ستستفيد الوكالة الوطنية للأمن السيبراني بشكل كبير من هذه العملية، فالمتابعة والمراجعة سيمكنان من رصد التقدم الفعال في تنفيذ المبادرات، مما يساهم في صياغة سياسات فعالة في مجال الأمن السيبراني، إضافة إلى زيادة الصمود لدى الأطراف المعنية عند استعراض التقدم الفعال في المبادرات المُسندة إليها.

تُعَدُّ القدرة على تعديل المسار عند الضرورة أمراً هاما لضمان استمرار توافق التنفيذ مع احتياجات دولة قطر. ولابد من إجراء تقييمات دورية لبيئة المخاطر السيبرانية خلال السنوات المشمولة في هذه الاستراتيجية، مع مراعاة التطور السريع للتكنولوجيات وزيادة تطور التهديدات السيبرانية.

أما على مستوى التنفيذ والمتابعة التشغيلية، فيجب على الأطراف المعنية المسؤولة عن تنفيذ مبادرات هذه الاستراتيجية متابعة تقدمها وفعاليتها، يجب عليهم تقديم تقارير دورية عن نتائجهم إلى مكتب مراقبة الإستراتيجية الذي تم إنشاؤه داخل الوكالة الوطنية للأمن السيبراني، من خلال عملية رسمية لتمكين الفهم الشامل لكيفية تنفيذ الإستراتيجية الوطنية للأمن السيبراني، يمكن نتائج المتابعة والمراجعة الكشف عن أي انحرافات عن خطة التنفيذ الأصلية، مثل الانحراف عن الجدول الزمني أو عدم كفاية الموارد أو التغيرات على صعيد الأولويات، ومعالجتها بسرعة، وسيضمن ذلك عدم التأثير على تحقيق الأهداف المحددة والغايات الاستراتيجية.

أخيرًا، سيتم إعداد تقارير سنوية تصف حالة تنفيذ هذه الاستراتيجية والدروس المستفادة، مع رسم صورة كاملة المعالم للكيفية التي تجري بها تنفيذ الاستراتيجية.


01
التطوير
02
التنفيذ
03
المتابعة
04
المراجعة
05
التقييم
الإستراتيجية الوطنية للأمن السيبراني

05
الخـاتمة

5. الخـاتمة

تشـجع هـذه الاسـتراتيجية علـى بـذل جهـود تعاونيـة لتعزيـز الصمـود والإمكانيـات السـيبرانية لكافـة الأطـراف المعنية، ولقـد اتخـذت قطـر خطـوات لتوحيـد الحوكمـة الأمنيـة السـيبرانية مـن مؤسسـات وأفـراد، لمواجهـة المخاطـر السـيبرانية القائمـة والمسـتقبلية، إذ تُعَـدُّ "المسـؤولية المشـتركة" بالغـة الأهميـة لنجـاح تنفيـذ الاسـتراتيجية بالاعتمـاد علـى التعـاون الوثيـق بيـن الحكومـة والقطـاع الخـاص والأوسـاط الأكاديميـة والمجتمـع.

هـذه الاسـتراتيجية عبـارة عـن دعـوة للعمـل. ومـن هـذا المنطلـق، تكمـن غايتهـا فـي تحويـل الأهـداف إلـى إجـراءات فعليـة تنعكـس بشـكل إيجابـي علـى الوضـع الحالـي والمسـتقبلي للأمـن السـيبراني، وقـد صُمّمـت للتركيـز علـى النتائج، بحيـث تتضافـر مكوناتهـا الأساسـية، مـن غايـات اسـتراتيجية وأهـداف محـددة ومبـادرات، لدعـم الرؤيـة الشـاملة. ولضمـان إحـداث أثـر إيجابـي، سـتكون المتابعـة نشـاطًا مسـتمرًا طـوال المـدة التـي تغطيهـا الاسـتراتيجية، وسـيتم إعـداد تقاريـر سـنوية لاسـتعراض التقـدم الفعـال.

اسـتنادًا إلـى الجهـود الوطنيـة السـابقة علـى صعيـد الأمـن السـيبراني، مـع النظـر إلـى المسـتقبل، تعمـل هـذه الاسـتراتيجية إلـى تهيئـة بيئـة سـيبرانية حيويـة وموثوقـة وآمنـة، لأنهـا تسـاعد فـي تحقيـق غايـات رؤيـة قطـر الوطنيـة 2030، كمـا أنهـا تسـاهم فـي وضـع الدولـة بمكانـة بـارزة علـى رأس سـلم الابتـكار، فـضلًا عـن تأمينهـا لمسـتقبل ينبـض حيـاةً وازدهـارًا.

06

الملحقات

6. الملحقات

الملحق (أ): مسرد مصطلحات الأمن السيبراني الرئيسية

المصطلح	التعريف
البُنى التحتية الحيوية	الأصول المادية أو الأنظمة أو الأجهزة، التي يكون لتعطلها أو اختراقها أو إتلافها أثر خطير على صحة أو سلامة أو أمن دولة قطر أو وضعها الاقتصادي أو على عمل الحكومة بشكل فعال.
الأزمات السيبرانية (أو التعطل)	حدث سيبراني غير مخطط له يتسبب في جعل الأصول غير قابلة للتشغيل لفترة زمنية معينة (على سبيل المثال، انقطاع الطاقة البسيط أو الممتد، أو عدم توفر الشبكة لفترة طويلة، أو تلف أو تدمير معدات أو مرافق).
المنظومة السيبرانية	تجمُّع وتفاعلات مجموعة متنوعة من المشاركين (مثل الشركات الخاصة والمؤسسات غير الربحية والحكومات والأفراد والمبادرات) والأجهزة السيبرانية (الحواسيب الآلية والبرمجيات وتكنولوجيات الاتصالات).
حدث سيبراني	تغيير في الأمن السيبراني قد يؤثر على مبادرات المؤسسة، بما في ذلك الرسالة، القدرات، والسمعة. يتم تسجيل وتحديد هذا التغيير في نقطة زمنية معينة وقد يتطلب تقييمًا إضافيًا.
الحادث السيبراني	حدث ضار يؤثر على سرية أو سلامة أو توافر أي نوع من الأصول المعلوماتية، وقد تم التحقق منه كتهديد محتمل.
الصمود السيبراني	القدرة على الاستعداد للتعطلات الناجمة عن الهجمات أو الحوادث المتعمدة أو الحوادث أو التهديدات التي تحدث بشكل طبيعي، والتكيف معها ومجابهتها والتعافي السريع منها.
المخاطر السيبرانية	مقياس لمدى تعرض الكيان للخطر الناجم عن ظروف أو أحداث محتملة، وعادة ما يتم حسابه بناءً على احتمالية حدوث الأحداث أو الحوادث السيبرانية، و التأثيرات السلبية التي قد تنشأ إذا حدثت هذه الأحداث أو الحوادث. يمكن للمخاطر السيبرانية أن تؤدي إلى خسارة مالية، وتعطل تشغيلي، أو أضرار بسبب فشل التقنيات الرقمية المستخدمة في الوظائف المعلوماتية و/أو التشغيلية التي يتم إدخالها في نظام للتصنيع عبر وسائل إلكترونية نتيجة للوصول غير المصرح به، أو الاستخدام غير المصرح به، أو الكشف، أو التعطيل، أو التعديل، أو الإتلاف لنظام التصني.
الأمن السيبراني	مجموعة الأدوات والسياسات والمفاهيم والضمانات الأمنية والمبادئ التوجيهية ومنهجيات إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات وسبل الضمان والتكنولوجيا التي يمكن استخدامها لحماية البيئة السيبرانية وأصول الشركات والمستخدمين. وتتضمن أصول الشركات والمستخدمين أجهزة الحواسيب المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات وكافة المعلومات التي يتم نقلها أو تخزينها عبر البيئة السيبرانية. ويسعى الأمن السيبراني إلى توفير الخصائص الأمنية لأصول الشركات والمستخدمين والمحافظة عليها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتشمل الأهداف العامة للأمن السيبراني السرية والسلامة (والتي قد تتضمن المصادقة وعدم إنكار المسؤولية) والإتاحة.

المصطلح	التعريف
التهديدات السيبرانية	أي ظرف أو حدث يمكن أن يؤثر سلبًا على المبادرات المؤسسية (بما في ذلك المهام أو الوظائف أو المكانة أو السمعة)، أو الأصول المؤسسية، أو الأفراد من خلال نظام معلومات مصدره وصول غير مصرح به إلى المعلومات و/أو إتلافها و/أو الإفصاح عنها و/أو تعديلها و/أو حجب الخدمة، بالإضافة إلى إمكانية وجود مصدر تهديد لاستغلال ثغرة معينة في نظام المعلومات.
الهجمات السيبرانية	أي نوع من الأنشطة الإجرامية التي تحاول جمع موارد نظام المعلومات أو المعلومات نفسها أو تعطيلها أو إنكارها أو تقليلها أو إتلافها.
الجرائم السيبرانية	سوء السلوك أو الجريمة المرتكبة باستخدام التكنولوجيا، مثل الوصول غير القانوني إلى الأنظمة أو المعلومات أو الاحتيال أو سرقة الهوية أو الهجمات المتعلقة بالمحتوى مثل البريد المزعج.
الفضاء السيبراني	البيئة الافتراضية أو الإلكترونية التي تنتج عن شبكة مترابطة لتكنولوجيات المعلومات والاتصالات (مثل الإنترنت وشبكات الاتصالات وأنظمة الحواسيب والمعالجات وأجهزة التحكم المدمجة) التي تربط الأفراد بالخدمات والمعلومات.
التكنولوجيا الناشئة	مجموعة من الابتكارات التكنولوجية الواعدة التي أحدثت أثرًا ملموسًا على الحياة اليومية على الرغم من أنها لا تزال في المراحل الأولى من التطوير والتطبيق.
الاستجابة للحوادث	الحد من انتهاكات السياسات الأمنية والممارسات الموصى بها.
الابتكار	يعمل الابتكار على تسخير البحث والتطوير لإنشاء منتجات أو خدمات يمكن أن تكون جديدة للمؤسسة أو السوق أو العالم، ويمكن أن يتضمن تطوير معارف أو تكنولوجيات جديدة، أو تكييف التكنولوجيا القائمة بطرق جديدة بهدف تحقيق أثر اقتصادي ومجتمعي إيجابي.
معلومات الكشف عن التهديدات	معلومات التهديدات التي تم تجميعها أو تحويلها أو تحليلها أو تفسيرها أو إثرائها لتوفير السياق اللازم لمبادرات صنع القرار.
الثغرات	مواطن الضعف في نظام المعلومات أو إجراءات أمن النظام أو الضوابط الداخلية أو التنفيذ والتي يمكن استغلالها أو تفعيلها من قبل مصدر للتهديد.

الجدول 7 : مسرد مصطلحات الأمن السيبراني الرئيسية

الملحق (ب): المراجع

1 World Economic Forum (2022). (2023, January 18). Global Cybersecurity Outlook 2022. (المنتدى الاقتصادي العالمي. (2023). توقعات الأمن السيبراني على الصعيد العالمي لعام 2022.) متوفر على: https://www.weforum.org/reports/global-cybersecurity-outlook-2023 06

2 IBM. (2022). Cost of a data breach 2022. (آي بي إم. (2022). تكلفة خرق البيانات لعام 2022.) متوفر على: https://www.ibm.com/reports/data-breach 06

3 CrowdStrike. (2022). 2022 Global Threat Report. (كراودستراياك. (2022). تقرير التهديدات العالمية لعام 2022) متوفر على: "https://www.crowdstrike.com/global-threat-report/ 06

4 National Cyber Security Agency. (n. d.) National Cyber Security Agency (الوكالة الوطنية للأمن السيبراني. (بلا تاريخ). الوكالة الوطنية للأمن السيبراني.) متوفر على: تم الدخول إليه يوم 2 فبراير 2023 على الرابط: https://ncsa.gov.qa/ 07

5 Supreme Committee for Delivery & Legacy (2018). Qatar 2022 Cybersecurity Framework اللجنة العليا للمشاريع والإرث (2018). إطار أمن المعلومات لعام 2022 متوفر على: https://www.qatar2022.qa/sites/default/files/Qatar2022Framework.pdf. 07

6 Trescon CyberSec. (2022, July 22). Spearheading The Security Infrastructure in Digitalized Qatar. World Cyber Security Summit. (تريسكون سايبرسيك. (22 يوليو 2022). قيادة البنية التحتية الأمنية في قطر الرقمية. القمة العالمية للأمن السيبراني.) متوفر على: https://tresconglobal.com/conferences/cyber-sec/qatar/ 07

7 Al Meezan. (2014, February 10). Cybercrime Prevention Law No. 14 of 2014. Al Meezan Qatar Legal Portal. (الميزان. (10 فبراير 2014). قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014. بوابة الميزان القطرية القانونية الإلكترونية.) متوفر على: https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar 07

8 Al Meezan. (2016, December 29). Personal Data Privacy Protection Law No.13 of 2016. Al Meezan Qatar Legal Portal. (الميزان. (29 ديسمبر 2016). قانون حماية البيانات الشخصية رقم (13) لسنة 2016. بوابة الميزان القطرية القانونية الإلكترونية.) متوفر على: https://www.almeezan.qa/LawPage.aspx?id=7121&language=ar 07

9 INTERPOL. (n.d.). Stadia activities. (الإنتربول. (بلا تاريخ). أنشطة مشروع ستاديا.) متوفر على: https://www.interpol.int/en/How-we-work/Project-Stadia/Stadia-activities 08

09 Trend Micro. (2022). The State of Industrial Cybersecurity 2022. (ترينـد ميركـو. (2022). حالـة الأمـن السـيبراني الصناعـي.) متوفـر علـى:
https://resources.trendmicro.com/IoT-survey-report.html

11 World Economic Forum. (2023). Global Risks Report 2023. (المنتـدى الاقتصـادي العالمـي. (2023). تقريـر المخاطـر العالميـة لعـام 2023.) متوفـر علـى:
https://www.weforum.org/reports/global-risks-report-2023

11 World Economic Forum. (2023). Global Cybersecurity Outlook 2023. (المنتـدى الاقتصـادي العالمـي. (2023). توقعـات الأمـن السـيبراني علـى الصعيـد العالمـي لعـام 2023) متوفـر علـى:
https://www.weforum.org/reports/global-cybersecurity-outlook-2023

12 Sophos. (2022). Sophos 2023 Threat Report- Maturing criminal marketplaces present new challenges to defenders. (سـوفوس. (2022). تقريـر سـوفوس عـن التهديـدات لعـام 2023 - الأسـواق الإجراميـة الآخـذة فـي النضـج تمثـل تحديـات جديـدة أمـام المدافعيـن.) متوفـر علـى:
https://www.sophos.com/en-us/content/security-threat-report

12 World Economic Forum (2022). Organizations should make these 3 changes now to protect against the quantum computing threat. (المنتـدى الاقتصـادي العالمـي. (2022). ينبغـي للمؤسسـات القيـام بهـذه التغييـرات الثلاثـة الآن لحمايـة أنفسـها مـن تهديـد الحوسـبة الكميـة). متوفـر علـى:
https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/

13 World Economic Forum. (2023). Global Cybersecurity Outlook 2022. (المنتـدى الاقتصـادي العالمـي. (2023). توقعـات الأمـن السـيبراني علـى الصعيـد العالمـي لعـام 2022.) متوفـر علـى:
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022

13 International Information System Security Certification Consortium. (2022). (ISC)2 Cybersecurity Workforce Study. (اتحـاد شـهادات أمـن نظـم المعلومـات الدوليـة. (2022). (ISC) 2 دراسـة القـوى العاملـة فـي مجـال الأمـن السـيبراني.) متوفـر علـى:
https://www.isc2.org/Research/Workforce-Study?wpisrc=nl_cybersecurity202&wpmm=1

15 World Economic Forum. (2023). Global Cybersecurity Outlook 2023. (المنتـدى الاقتصـادي العالمـي. (2023). توقعـات الأمـن السـيبراني علـى الصعيـد العالمـي لعـام 2023) متوفـر علـى:
https://www.weforum.org/reports/global-cybersecurity-outlook-2023