دولــة قطــر

الاستراتيجية الوطنية للأمن السيبراني

مايو ٢٠١٤

المحتويات

وزارة الاتصالات وتكنولوجيا المعلومات
Ministry of Information and Communications Technology

الكلمة الافتتاحية

لقد مدت شبكة الإنترنت جسور التواصل بيننا وبين نظرائنا حول العالم على نحو لم يكن أحد ليتصوره قبل عِقد مضى، حيث نجحت في إزالة العديد من العوائق التي كانت تعرقل عملية التواصل وعززت سبل التعاون بيننا في شتى مجالات الحياة الشخصية والمهنية، بحيث أصبح الفضاء الإلكتروني جزءًا حيويًا لا يتجزأ من مجتمعنا. ويُعد الفضاء الإلكتروني عاملًا رئيسيًا لتحقيق الازدهار الاقتصادي وتحفيز الابتكار، فضلًا عن دوره في إثراء حياتنا بطرق لا حصر لها. ولا شك أن الفضاء الإلكتروني لايزال يحمل لنا في طياته الكثير من الفرص وإمكانيات التوسع في المستقبل.

ومع ذلك، نجد أن هذه الفوائد العظيمة التي يقدمها لنا الفضاء الإلكتروني محفوفة بعدد من المخاطر التي قد تهدد البنية التحتية التي تعزز من قدرتنا على الاستخدام الآمن للإنترنت، حيث تتيح طبيعة الفضاء الإلكتروني - غير المقيدة بأي حدود – لبعض الجهات المغرضة فرصًا غير مسبوقة لاختراق بيانات الأفراد والشركات وإلحاق الضرر بهم. ومن حسن الحظ أنه ليس علينا مواجهة هذا التحدي الصعب بمفردنا للحفاظ على الأمن السيبراني. ففي ظل ما يشهده العالم في العصر الحديث من زيادة في حجم الهجمات الإلكترونية بجميع أشكالها، أصبح الحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية أحد أكبر التحديات العالمية التي تواجه جميع الدول.

وسعيًا منها لمواجهة هذه التحديات، تواصل دولة قطر بذل المزيد من الجهود الرامية إلى تعزيز الأمن السيبراني، فضلًا عن تعاوننا مع نظرائنا حول العالم لخلق فضاء إلكتروني مفتوح وآمن. وفي عام ٢٠١٣، شكل معالي رئيس الوزراء «اللجنة الوطنية لأمن المعلومات» بهدف التعامل مع قضايا حماية الأمن السيبراني على المستوى الوطني وضمان تبني جميع المؤسسات العامة والخاصة لخطة العمل الصحيحة لتحقيق الأمن السيبراني. ذلك بالإضافة إلى وضع «الاستراتيجية الوطنية للأمن السيبراني لدولة قطر» التي تتناولها هذه الوثيقة.

إن أهدافنا واضحة تمامًا، وتتلخص في حماية البنية التحتية للمعلومات الحيوية الوطنية، والاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، ووضع إطار قانوني وتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني، وتعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الآمن والمناسب للفضاء الإلكتروني، وتطوير الإمكانيات الوطنية للأمن السيبراني.

وفي الوقت الذي ستقود فيه الحكومة الجهود الرامية إلى حماية الأنظمة والشبكات الحكومية، يجب أن ندرك جميعًا أن الأمن السيبراني مسؤولية مشتركة بين الجهات الحكومية والشركات والمؤسسات والأفراد، وأن التنسيق بين الأطراف المعنية هو عامل جوهري لنجاح هذه الجهود.

ومع ظهور تحديات جديدة ومعقدة في مجال الأمن السيبراني على المستوى العالمي، فطنت دولة قطر لضرورة مواجهة تلك التحديات وأخذت تبذل جهودًا حثيثة لتعزيز جاهزية ومرونة فضائنا الإلكتروني وحمايته من أجل الأجيال القادمة. وفي ضوء رؤية القيادة الحكيمة لدولة قطر، التي تجلت في «رؤية قطر الوطنية ٢٠٣٠»، سنواصل تسخير قوة تكنولوجيا المعلومات والاتصالات لضمان مستقبل مزدهر لجميع أفراد المجتمع.

الدكتورة/ حصة الجابر
وزير الاتصالات وتكنولوجيا المعلومات

الملخص التنفيذي

لقد أصبحت شبكة الإنترنت محركًا فريدًا لدفع عجلة التنمية والتقدم الاجتماعي والابتكار، بيد أنها تمثل عامل جذب للمجموعات المتخصصة في ارتكاب الجرائم الإلكترونية ومخترقي شبكة الإنترنت ونشطاء القرصنة الإلكترونية والأجهزة الاستخباراتية الأجنبية، الذين يسعون لإلحاق الضرر بنا عن طريق إضعاف بنيتنا التحتية الرقمية أو إتلافها. فقد منحهم التطور الذي شهده الفضاء الإلكتروني، غير المقيد بحدود، فرصة فريدة لاختراق بيانات الأفراد والشركات والجهات الحكومية وغيرها من المؤسسات باستخدام مجموعة من أحدث التقنيات وأكثرها ضررًا. فالحفاظ على بيئة إلكترونية آمنة، مع مواصلة التوسع في إيجاد فضاء إلكتروني يتسم بالحرية والانفتاح، هو أحد أكبر التحديات الاستراتيجية التي تواجه العالم.

"إن الاقتصاد القطري يشهد نموًا سريعًا، حيث أدى تبني تكنولوجيا المعلومات والاتصالات كمنصة انطلاق نحو الابتكار والازدهار دورًا حيويًا في تحقيق هذا النمو. وتعتبر عوامل مثل مرونة وأمن الفضاء الإلكتروني أمرًا حيويًا لتحقيق نجاح ونمو مستدامين في دولة قطر، لذلك فهي تتطلب وضع استراتيجية وطنية شاملة لمجابهة المخاطر والتهديدات الحالية والناشئة.

وفي عام ٢٠١٣، قامت دولة قطر بتشكيل اللجنة الوطنية لأمن المعلومات بهدف توفير هيكل حوكمة للتعامل مع قضايا الأمن السيبراني بشكل جماعي على أعلى المستويات الحكومية. وقد جاءت «الاستراتيجية الوطنية للأمن السيبراني لدولة قطر» تكليلًا لجهود هذه اللجنة، حيث تمثل الاستراتيجية خارطة طريق للمضي قدمًا نحو تعزيز الأمن السيبراني في دولة قطر. كما تجمع هذه الاستراتيجية بين الحوكمة الرشيدة ومجموعة من المبادرات والإجراءات وبرامج التوعية الخاصة بالأمن السيبراني، مما يجعلها استراتيجية وقائية فعالة على المدى الطويل.

لقد تم وضع الاستراتيجية في ضوء إدراكنا العميق للتهديدات والتحديات التي تواجهها دولة قطر، والتي تتضمن وجود بعض الجهات المغرضة التي تتربص بأمننا، ونقص عدد العاملين الذين يمتلكون المهارات اللازمة في مجال الأمن السيبراني من جهة ومزودي خدمات الأمن السيبراني المحليين الذين يمكن الاعتماد عليهم من جهة أخرى. تتكون الاستراتيجية من عدة فصول، يتناول الفصل الثاني منها التهديدات المحيطة بنا والإمكانيات الحالية لدى دولة قطر بشيء من التفصيل. وتشكل الإمكانيات المتاحة لدينا حاليًا، من سياسات مثل سياسة تأمين المعلومات الوطنية وقواعد الرقابة المصرفية فضلًا عن الخبرات التقنية والتشغيلية لدى مركز قطر للاستجابة لطوارئ الحاسبات (كيوسيرت) المسؤول عن تحديد الهجمات الإلكترونية وضمان إمكانية الكشف عنها ومنعها قبل تسببها بضرر كبير في مختلف المؤسسات الحكومية والقطاعات الحيوية، أساسًا قويًا لمواصلة الارتقاء بمستوى الأمن السيبراني في دولة قطر.

ويستعرض الفصل الثالث من الاستراتيجية النهج الاستراتيجي الذي تتبعه دولة قطر تجاه الأمن السيبراني على المستوى الوطني.
وتتركز رؤية دولة قطر في «خلق وتعزيز فضاء إلكتروني آمن، لحماية المصالح الوطنية لدولة قطر والحفاظ على الحقوق والقيم الأساسية لمجتمعنا».

وتسعى دولة قطر لتحقيق هذه الرؤية من خلال خمسة أهداف تحدد الإجراءات التي سيتم اتخاذها لتعزيز الأمن السيبراني في دولة قطر ولتعم الفائدة على جميع أفراد المجتمع:

- الهدف الأول: حماية البنية التحتية للمعلومات الحيوية الوطنية
- الهدف الثاني: الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة
- الهدف الثالث: وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني

- الهدف الرابع: تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الآمن والمناسب للفضاء الإلكتروني
- الهدف الخامس: تطوير وصقل الإمكانيات الوطنية للأمن السيبراني

وتشكل هذه الأهداف مجتمعة الركيزة الأساسية للحماية من الهجمات الإلكترونية والاستعداد لمواجهتها، بالإضافة إلى اكتشاف التهديدات والتحديات التي تواجه دولة قطر ومواجهتها والتعافي منها. وتستعرض الاستراتيجية المبادرات التي تدعم كل هدف من هذه الأهداف.

بالإضافة إلى ذلك، يقدم الفصل الرابع من الاستراتيجية المزيد من التفاصيل حول خطة عمل الحكومة القطرية لتحقيق رؤية دولة قطر للأمن السيبراني، وهي مرتبة وفقًا للأهداف. ومن المتوقع أن يتطلب تنفيذ هذه المشروعات المزيد من الوقت والتنسيق بين كافة الأطراف المعنية.

ولسوف يتطلب التنفيذ الناجح لهذه الاستراتيجية التزامًا مستمرًا وحوكمة وإجراءات متواصلة من قبل الأطراف المعنية الذين تربطهم رؤية مشتركة. ويرتكز نهج قطر فيما يتعلق بالأمن السيبراني على ثلاثة مبادئ توجيهية:

- ستقود الحكومة الجهود الرامية إلى الحفاظ على الأنظمة والشبكات الحكومية من خلال تنفيذ متطلبات الأمن السيبراني، مع تصميم واعتماد التقنيات المبتكرة والحديثة.
- الأمن السيبراني مسؤولية مشتركة بين جميع الجهات الحكومية والشركات والمؤسسات والأفراد.
- ستعمل دولة قطر على اتباع سياسات ومبادرات الأمن السيبراني التي تحافظ على الحقوق والقيم الأساسية لمجتمعنا بما يتفق مع القوانين واللوائح المعمول بها.

ومن الضروري توفير حوكمة قوية لتنفيذ الاستراتيجية وإدارة الأنشطة المرتبطة بها. وفي ضوء ذلك، ستقوم دولة قطر بتشكيل المكتب التنسيقي للأمن السيبراني، الذي يتبع رئيس مجلس الوزراء، ليكون جهة التنسيق والاتصال المركزية بين الأطراف المعنية على مستوى دولة قطر حول الأنشطة المتعلقة بالأمن السيبراني. كما سيعمل المكتب على: (١) تحديد الأولويات الوطنية لتحقيق أعلى مستويات الأمن السيبراني في دولة قطر، (٢) تقديم التوجيه الاستراتيجي للجهود التي تبذلها دولة قطر بشأن الأمن السيبراني، (٣) العمل في شراكة وثيقة مع الجهات التي لديها مهام واختصاصات متعلقة بالأمن السيبراني من أجل تحقيق أهداف الاستراتيجية.

ويتميز هذا النهج بكونه نهجًا متكاملًا وشاملًا من شأنه تعزيز تضافر الجهود، وتفادي بذل جهود مزدوجة، وتعظيم الاستفادة من الموارد المتاحة في إدارة البيئة الديناميكية للفضاء الإلكتروني والتهديدات الناشئة المحيطة به.

ومع ظهور تحديات جديدة ومعقدة في مجال الأمن السيبراني على المستوى العالمي، يتزايد اعتماد دولة قطر على تكنولوجيا المعلومات والاتصالات. لذا كان لزامًا على دولة قطر أن تظل متيقظة وأن تعمل على تعزيز جاهزية ومرونة فضائها الإلكتروني، وهو ما يتجلى في هذه الاستراتيجية التي تؤكد على التزام دولة قطر بالحفاظ على الفضاء الإلكتروني آمنًا من أجل الأجيال القادمة.

١. مقدمة

يتميز الاقتصاد القطري بالنمو السريع، حيث أدى تبني تكنولوجيا المعلومات والاتصالات كمنصة انطلاق نحو الابتكار والازدهار دورًا حيويًا في تحقيق هذا النمو. فتبني تكنولوجيا المعلومات والاتصالات وتطبيقها يعمل على توسيع الفضاء الإلكتروني القطري، الذي أصبح جزءًا لا يتجزأ من الحياة اليومية لأفراد المجتمع القطري. وتعتبر عوامل مثل مرونة١ وأمن الفضاء الإلكتروني أمرًا حيويًا لتحقيق نجاح ونمو مستدامين في دولة قطر، لذلك فهي تتطلب وضع استراتيجية وطنية شاملة لمجابهة المخاطر الحالية والناشئة.

في حين أن إدخال التسهيلات التي توفرها تكنولوجيا المعلومات والاتصالات الحديثة قد أسهم في تيسير التواصل بين أفراد المجتمع المترابط بشكل وثيق، إلا أن ذلك قد يؤدي إلى زيادة خطر تغيير معاييرنا الاجتماعية. كما أن الطبيعة المترابطة للفضاء الإلكتروني وأهميته الآخذة بالتزايد تعمل على زيادة تهديدات الفضاء الإلكتروني التي تدعمها مجموعة واسعة من الجهات المغرضة، حيث تتبنى هذه التهديدات مجموعات من مخترقي شبكة الإنترنت ونشطاء القرصنة الإلكترونية والمجرمون المنظمون وصولًا إلى تهديدات الحكومات الأجنبية. وتعول قطر في الوقت الراهن على مجموعة صغيرة من القوانين الجزائية التي تعنى بالتحقيق مع مرتكبي جرائم الفضاء الإلكتروني ومحاكمتهم ومعاقبتهم على جرائمهم، إلا أنه لاتزال هنالك حاجة إلى اتخاذ المزيد من التدابير لضمان الحصول على حماية أكثر شمولية ضد مخاطر وتهديدات الفضاء الإلكتروني.

لمجابهة المخاطر الحالية والناشئة، فإن الاستراتيجية الوطنية للأمن السيبراني لدولة قطر:

- تؤكد على الالتزام بحماية مصالح قطر في الفضاء الإلكتروني؛
- تؤسس لرؤية وأهداف المستقبل؛
- ترتكز على المبادئ الرئيسية للقيادة، والمسؤولية المشتركة، والقيم الأخلاقية؛
- تسترشد بالاختصاصات، والاستراتيجيات الوطنية الأخرى وأفضل الممارسات الدولية، والحقوق والقيم الخاصة بالأفراد.

٢. أهمية الأمن السيبراني لدولة قطر

تعتبر نظم تكنولوجيا المعلومات والاتصالات جزءًا لا يتجزأ من الحياة اليومية، فهي تتيح للحكومة والشركات والمؤسسات والأفراد الوصول إلى المعرفة والمعلومات الضرورية لتحويل قطر إلى دولة أكثر تقدمًا بحلول عام ٢٠٣٠١ وقد أخذت القطاعات الحيوية في دولة قطر، بما في ذلك القطاع المالي والقطاع الحكومي؛ وقطاعات الطاقة؛ والكهرباء والماء؛ والرعاية الصحية، تعتمد بشكل متزايد على التطبيقات الرقمية الحديثة، مما يمكنها من تقديم خدمات فعالة وعالية الجودة والكفاءة للعملاء في قطر وحول العالم. إن هذه التقنيات ستتيح لدولة قطر الحفاظ على نموها الاقتصادي وعملية التنمية التي تنتهجها، وتوفير مستوى مرتفع من المعيشة للأجيال القادمة، ودفع عجلة الابتكار وريادة الأعمال وتعزيز روح المبادرة، وخلق فرص عمل كثيرة.

لقد مكنت استثمارات دولة قطر الضخمة في مجال التكنولوجيا بلادنا من أن تعتلي مكانة رائدة في المنطقة، حيث تحتل دولة قطر المرتبة ٢٣ عالميًا، من بين ١٤٨ دولة، في مؤشر الجاهزية الشبكية ٢٠١٤ الذي يصدره المنتدى الاقتصادي العالمي٢. كما فاق انتشار الإنترنت في دولة قطر المتوسط العالمي بدرجة كبيرة محققًا نسبة ٣.٨٨٪ ويُعد ضمان سلامة وأمن خدمات البرودباند عاملًا رئيسيًا لزيادة حجم انتشار واستخدام الإنترنت فائق السرعة، مما يعطي المستخدمين الثقة بأن ممارسة الأنشطة الإلكترونية عبر الإنترنت لن يؤثر سلبًا على خصوصيتهم أو أمنهم.٤ وإدراكًا منها للتهديدات ونقاط الضعف المحيطة بتكنولوجيا المعلومات والاتصالات، أدرجت قيادة دولة قطر «الأمن السيبراني والسلامة على الإنترنت» كأحد ثلاثة برامج رئيسية في الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات ٢٠١٥: الأجندة الرقمية لدولة قطر. وتعد هذه الاستراتيجية ضرورية من اجل: (١) تحسين الاتصال، (٢) خلق اقتصاد قائم على الحلول والخدمات التقنية المتطورة التي من شأنها إثراء حياة جميع أفراد المجتمع في قطر، وإبراز تميز دولة قطر كأحد الدول الرائدة على المستوى الإقليمي في مجال المحتوى الرقمي العربي.

لقد استثمرت دولة قطر المليارات لتحسين البنية التحتية، بما في ذلك الجهود الرامية إلى توسيع وتحديث مطار الدوحة الدولي، وبناء ميناء جديد، وتحديث البنية التحتية للطرق، وإحداث تحول رئيسي في وسائل النقل عن طريق إنشاء نظام السكك الحديدية والمترو الجديد العالي السرعة. بالإضافة إلى ذلك، لا تدخر قطر جهدًا لتنفيذ استثمارات ضخمة في سبيل تعزيز بنيتها التحتية تمهيدًا لاستضافة بطولة كأس العالم لكرة القدم لعام ٢٠٢٢، بما في ذلك عقد استثمارات في مجال التكنولوجيا لتقديم خدمات رقمية جديدة لزوار قطر والمشاهدين الدوليين. وسوف تعتمد مشاريع البنية التحتية هذه بشكل كبير على تكنولوجيا المعلومات والاتصالات المبتكرة والمتطورة، التي توفر فرصًا كبيرةً، ليس فقط لتحقيق نمو اقتصادي وتوسع مستدامين، بل ولمعالجة قضايا الأمن السيبراني خلال الدورة الحياتية لتنفيذ هذه المشروعات.

المؤشرات الرئيسية لاستخدام تكنولوجيا المعلومات والاتصالات في قطر

- في عام ٢٠١٢، كان ٩٢٪ من الأسر من عموم السكان يمتلكون جهاز كمبيوتر، في الوقت الذي كان ٨٧٪ من عموم الأفراد يمتلكون جهاز كمبيوتر.
- في عام٢٠١٢ ، بلغت نسبة انتشار الإنترنت بين عموم الأفراد حوالي ٨٨٪.
- في عام ٢٠١٢، وصلت نسبة انتشار الهاتف النقال في قطر إلى ما يقرب من ١٠٠٪، وهي أحد أعلى المعدلات في العالم.
- في عام ٢٠١٢، استخدمت ٧٤٪ من الشركات في قطر أجهزة الكمبيوتر، بما في ذلك أجهزة الكمبيوتر المكتبية والمحمولة والأجهزة اللوحية الحديثة، حيث ارتفعت هذه النسبة من ٦٤٪ في عام ٢٠٠٨.
- وفي عام ٢٠١٢، قامت ٦٦٪ من الشركات في قطر باستخدام الإنترنت، حيث ارتفعت هذه النسبة من ٥١٪ في عام ٢٠٠٨.
- في عام ٢٠١٢، ارتفع عدد الشركات التي تنتهج سياسة أمن الاتصالات وتكنولوجيا المعلومات من ٣٧٪ في عام ٢٠١٠ لتصل إلى ٦١٪.
- في عام ٢٠١٢، مثل المحترفون في مجال تكنولوجيا المعلومات والاتصالات حوالي ٢ ٪ من مجموع القوى العاملة في دولة قطر.

المصدر: تقرير المجلس الأعلى للاتصالات، المشهد الرقمي لدولة قطر ٢٠١٣: قطاع الأعمال؛ وتقرير المجلس الأعلى للاتصالات، المشهد الرقمي لدولة قطر ٢٠١٣: الأسر والأفراد.

٢-١ التهديدات

يحقق استخدام تكنولوجيا المعلومات والاتصالات والبرودباند منافع هائلة للحكومة والشركات والمؤسسات والأفراد. ومع ذلك، كثيرًا ما تنطوي هذه التقنيات على نقاط ضعف. ونظرًا لما تتميز به دولة قطر من كونها أحد المنتجين الرئيسين للوقود النظيف، ومقرًا لشركات عالمية، ومن أوائل الدول التي تبنت التقنيات الرقمية، ودورها الرائد في الشؤون الإقليمية؛ تعد قطر مطمعًا للجهات المغرضة التي تسعى لعرقلة مسيرتها وهدم ما أحرزته من تقدم.

وقد تطورت التهديدات الإلكترونية من كونها ناتجة عن مجموعات فردية من محترفي القرصنة الإلكترونية إلى جماعات فائقة التنظيم وعصابات إجرامية متقدمة. وأصبحت الهجمات أكثر تحديدًا للأهداف وأكثر تطورًا. وقد ظهرت برمجيات ضارة جديدة وقوية، قادرة على سرقة البيانات السرية، وتعطيل البنية التحتية للشبكات. وتمثل الهجمات على البنية التحتية الحيوية وما تتضمنه من أنظمة التحكم الصناعية تهديدًا متزايدًا، لقدرتها على تعطيل الآلات الرئيسية والتسبب بعطل كارثي في المعدات، بل وخسائر في الأرواح.
ودولة قطر، مثل العديد من الدول الأخرى، يجب أن تكون مستعدةً لمجابهة الأنواع التالية من التهديدات:

- نشطاء القرصنة الإلكترونية - وهم الأفراد أو الجماعات الذين يسعون إلى تعطيل الأنظمة والشبكات بسبب مجموعة مختلفة من الدوافع، بما في ذلك التسبب في تشويه الحقائق ونشر سمعة سيئة، وتحقيق مكاسب مالية، وتنفيذ أجندات سياسية. فهم يتواصلون عبر الحدود للسيطرة على المواقع الإلكترونية المستهدفة والحصول على معلومات حيوية. وقد يسعون لإلحاق الضرر بمن يتصورونهم كأعداء لهم، إما عن طريق التشهير بهم أو عن طريق تعطيل خدماتهم. وعادةً ما يُطلق «نشطاء القرصنة الإلكترونية» هجمات موزعة لحجب الخدمة، ويقومون بتشويه محتوى مواقع الإنترنت، واختراق البيانات الحكومية الحيوية، ونشر المعلومات الشخصية لمسئولين رفيعي المستوى وكبار رجال الأعمال.

- التهديدات المستمرة المتطورة (APTs) – وهي التهديدات التي تُستخدم فيها أشكال معقدة وفريدة من البرمجيات الخبيثة للتسلل إلى المعلومات الخاصة بالجهة المستهدفة أو المعلومات الشخصية والمعلومات الحكومية الحيوية. وقد تتضمن هذه التهديدات استخدام حلول مخصصة لاستغلال شخص مطلع من داخل الجهة المستهدفة أو الهندسة الاجتماعية أو أجهزة الشبكة أو برمجيات طرف ثالث لإحداث أعطال متعددة وإتلاف البيانات وإيقاف الشبكة عن العمل.

التهديدات الإلكترونية التي تواجه دولة قطر

- كانت فيروسات حصان طروادة (Trojan)، والفيروسات المتنقلة، وغيرها من الفيروسات أكثر التهديدات الإلكترونية شيوعًا في قطر في الفترة من أبريل وحتى يونيو ٢٠١٣.
- احتلت منطقة الشرق الأوسط وشمال أفريقيا المرتبة الثالثة في استقبال أكبر كمية من الرسائل النصية غير المرغوب فيها (١٠٧ مليار رسالة نصية غير مرغوب فيها شهريًا) من نوفمبر ٢٠١٣ وحتى مارس ٢٠١٤.
- كانت دولة قطر من أحد البلدان التي تأثرت بشدة نتيجة الهجمات الإلكترونية التي وقعت في عام ٢٠١٣.

- مجموعات الجرائم الإلكترونية – تسعى المجموعات المتخصصة في ارتكاب الجرائم الإلكترونية إلى التسلل إلى معلومات الحسابات الشخصية لتتمكن من إجراء معاملات احتيالية أو سرقة الأموال الخاصة بصاحب الحساب. كما تهدف هذه المجموعات عادة إلى سرقة المعلومات، حيث تقوم بتسريبها إلى جهات وأفراد غير مصرح لهم بالاطلاع على مثل هذه المعلومات في مقابل مبلغ مالي. ويعمل مجرمو الفضاء الإلكتروني على إيجاد طرق متعددة لتحقيق أهدافهم، بما في ذلك إرسال كميات هائلة من رسائل البريد الإلكتروني منتحلين صفة أحد المصارف أو غيرها من الجهات، وذلك بهدف الحصول على المعلومات المالية للعملاء وبيانات التعرف على هويتهم. وقد يستخدمون أيضًا هجمات موزعة على نطاق واسع لحجب الخدمة، وذلك لاختراق الشركات التي تعتمد على الإنترنت. ونحن نتوقع أن تقوم مجموعات الجرائم الإلكترونية بهجمات احتيالية تتبع أسلوب الدفع مقدمًا (٤١٩ scam)، وذلك لاستهداف الأفراد غير الحذرين بهدف تحقيق ربح مالي قبل استضافة كأس العالم ٢٠٢٢ في قطر.

- أشخاص مطلعون ذوو نوايا خبيثة – وهم الأفراد الموثوق بهم والمصرح لهم بالوصول إلى المعلومات الداخلية، والذين دفعهم الكسب المادي أو الرغبة في الانتقام أو المصالح الأيديولوجية إلى تهديد سرية أو سلامة أو توافر معلومات المؤسسة ونظم المعلومات الخاصة بها. ونظرًا لأنهم مصرح لهم بالوصول إلى الأنظمة والمعلومات، فهم لا يحتاجون لاختراق دفاعات الشبكة، ويمكنهم استخدام عدة طرق للإضرار بأنظمة الحكومة والشركات أو إتلافها.

إن الهجمات الإلكترونية آخذة في الازدياد في جميع أنحاء العالم، وكذلك الحال في دولة قطر. وتتطلب هذه التهديدات اليقظة والاهتمام المستمرين. ومن جهتها تلتزم الحكومة القطرية بضمان أمن أصول ونظم المعلومات الضرورية للحكومة والشركات والمؤسسات والأفراد.

٢-٢ التحديات

إن اعتماد تقنيات جديدة مثل الحوسبة السحابية وتطبيقات الهاتف النقال الجديدة وتنفيذ تكنولوجيا الشبكة الذكية، والزيادة الكبيرة في عدد المستخدمين، توفر فرصًا مميزة للتطوير والابتكار. إلا أن هذه الفرص من شأنها أيضًا إيجاد بيئة سريعة التطور تفرض مجموعة خاصة من التحديات التي تؤثر على قدرة قطر على الابتكار والمنافسة على مستوى الاقتصاد العالمي. وتتضمن هذه التحديات:

- نقص المهارات والخدمات في مجال الأمن السيبراني – هناك نقص، على المستوى العالمي والوطني، في عدد العاملين الذين يمتلكون المعرفة والمهارات والقدرات الكافية لتسخير قوة تكنولوجيا المعلومات والاتصالات بشكل فعال مع التعامل مع قضايا الأمن السيبراني. كما أن هناك نقص في مزودي خدمات الأمن السيبراني المحليين الذين يمكن الاعتماد عليهم. ومع تزايد تعقيد منتجات وخدمات تكنولوجيا المعلومات والاتصالات، فإن نقاط النقص هذه من شأنها أن تتفاقم، وإن لم تتم معالجتها بالشكل الكافي، فستؤثر على قدرتنا على حماية البنية التحتية للمعلومات.

- مخاطر سلسلة التوريد العالمية – يتألف نظام الاتصال المشترك العالمي للفضاء الإلكتروني من عدة نظم مترابطة. وتشمل هذه النظم عدة مكونات من عدة مصادر حول العالم. وتزداد صعوبة تحديد مصدر وسلامة العناصر التي تشكل المنتجات النهائية لتكنولوجيا المعلومات والاتصالات. كما تنطوي سلسلة التوريد العالمية على نقاط ضعف يمكن أن تستغلها الجهات المغرضة لشن هجمات إلكترونية.

- ربط أنظمة التحكم الصناعية: تشهد أنظمة التحكم الصناعية ربطًا متزايدًا بشبكات الشركات والإنترنت. ومع أن هذا الربط يوفر إمكانيات تمكن من مراقبة العمليات الميكانيكية المستخدمة في إنتاج النفط والغاز الطبيعي وتوليد الكهرباء وتنقية المياه عن بعد، فإنها أيضًا تزيد من إمكانية تعرض أنظمة التحكم للتهديدات الإلكترونية.

- وضع قيود على تداول المعلومات – قد لا يرغب مالكو المعلومات أو مقدمو خدمات المعلومات في تداول المعلومات حول نقاط الضعف والحوادث وأفضل الممارسات مع الغير، وذلك خوفًا من الكشف عن نقاط الضعف التي قد يتم استغلالها. كما أن كل مؤسسة بمفردها قد لا تدرك دائمًا أن المعلومات التي في حوزتها عن تهديدات الفضاء الإلكتروني ونقاط الضعف وأفضل الممارسات الفعالة قد تكون ذات قيمة بالنسبة للآخرين.

- وعي القيادة التنفيذية –يقوم مديرو تكنولوجيا المعلومات ورؤساء أقسام نظم المعلومات ورؤساء أقسام أمن المعلومات، في جميع المؤسسات على تنوع حجمها، بالتعامل مع قضايا الأمن السيبراني، إلا أن تلك القضايا تتجاوز التشغيل الفعال للمؤسسات مؤثرة على رسالة المؤسسة وهدفها الأساسي. وللأسف، فإن التواصل بين خبراء تكنولوجيا المعلومات والقيادة العليا قد يكون محدودًا، ما ينجم عنه نقص في معرفتهم بالمخاطر الحقيقية التي تواجه المؤسسة أو الموارد الضرورية لتنفيذ المتطلبات الأمنية والتصدي للحوادث والحد من تلك المخاطر.

- تغيير التوقعات بشأن الخصوصية – نظرًا للاستخدام المتزايد للمعلومات الشخصية داخل الجهات الحكومية وخلال إدارة الأعمال الدولية، تواصل الدول سن قوانين جديدة بشأن الخصوصية وتعمل على تحديثها بهدف حماية الأفراد وبياناتهم. وتتطلب العديد من تلك الدول «مستويات كافية من الحماية» قبل السماح للمنظمات الدولية بنقل البيانات إلى وجهات خارج حدودها. فعندما لا تخضع المعلومات الشخصية لحماية كافية، تواجه المؤسسات مخاطر محتملة، وقد يعني ذلك بالنسبة لجهة حكومية فقدان الثقة في خدماتها الإلكترونية أو خسارة صفقات تجارية أمام منافسين عالميين بالنسبة لمؤسسات الأعمال.

٣-٢ الإمكانيات الحالية لمواجهة التهديدات والتحديات

لقد أدركت الحكومة القطرية أهمية الأمن السيبراني منذ عدة سنوات، وقد عملت بدأب على تطوير وتنفيذ إجراءات وتدابير وقائية في جميع أنحاء دولة قطر. ويعود الفضل لهذه الإجراءات والتدابير في تمكين الجهات الحكومية والشركات والمؤسسات والأفراد من مجابهة العديد من التهديدات والتحديات في الفضاء الإلكتروني، ما وفر أساسًا راسخًا وقويًا لتحقيق أهداف الأمن السيبراني. وفي هذا الإطار، بذلت دولة قطر العديد من الجهود، منها:

- قامت دولة قطر بوضع عدد من الاستراتيجيات وتنفيذ مجموعة من السياسات لحماية البنية التحتية لنظم المعلومات الحيوية بالنسبة للأمن الوطني والازدهار الاقتصادي، كتلك المستخدمة لتوليد الطاقة وإنتاج النفط والغاز والمعاملات المالية والرعاية الصحية والإجراءات الحكومية. وتوفر كل من سياسة تأمين المعلومات الوطنية والمعايير الوطنية لأمن أنظمة التحكم الصناعية دليلًا مهمًا لأدوات التحكم والممارسات الأمنية، وذلك لحماية معلومات البنية التحتية الحيوية وتعزيز أمن الإنترنت. وكجزء من سياسة تأمين المعلومات الوطنية، أصدرت دولة قطر في عام ٢٠١٣ المبادئ التوجيهية لمكافحة الرسائل غير المرغوب فيها بهدف تعزيز استخدام الوسائل الإلكترونية للتقليل من أثر الرسائل الإلكترونية غير المرغوب فيها على الأفراد والمؤسسات.

- ولتعزيز أمن المعاملات المالية، أصدر مصرف قطر المركزي قواعد الرقابة المصرفية، والتي تحدد أدوات رقابة الأمن السيبراني التي يجب على المصارف اتباعها، بما في ذلك إبلاغ مركز قطر للاستجابة لطوارئ الحاسبات (كيوسيرت) ومصرف قطر المركزي عند حدوث هجمات على الفضاء الإلكتروني.

- شكلت دولة قطر لجان خبراء مخاطر أمن المعلومات تضم القطاعين العام والخاص، وذلك في القطاع المالي والحكومي وقطاع الطاقة. وتتعامل هذه اللجان مع مجموعة من قضايا الأمن السيبراني، بما في ذلك الهجمات والمخاطر ونقاط الضعف والتهديدات الناشئة وأنشطة الجاهزية والاستراتيجيات التخفيفية (العلاجية). وتسهل هذه اللجان عملية تبادل المعلومات داخل كل قطاع ومع الأطراف المعنية الأخرى، وذلك بهدف تحسين مرونة البنية التحتية الحيوية.

- حققت قطر تقدمًا في وضع إطار قانوني محلي يوفر حوكمة وطنية للأمن السيبراني، ويكافح الجرائم الإلكترونية، ويحمي خصوصية الأفراد، ويعزز مرونة البنية التحتية للمعلومات الحيوية. وقد حدد المرسوم بقانون رقم (١٦) لسنة ٢٠١٠ بإصدار قانون المعاملات والتجارة الإلكترونية، الجرائم والعقوبات المتعلقة بالوصول غير القانوني لنظم المعلومات وسرقة هوية أي شخص واعتراض أو التدخل غير القانوني بأي نظام معلومات. وفي ٢٠١٣، شكلت دولة قطر اللجنة الوطنية لأمن المعلومات، الأمر الذي وفر هيكل حوكمة على أعلى المستويات الحكومية، وذلك بهدف التعامل مع الأمن السيبراني.

- وقد استثمرت دولة قطر في إثراء الخبرات الفنية والتشغيلية من خلال تشكيل مركز قطر للاستجابة لطوارئ الحاسبات (كيوسيرت)، وهي الجهة المسؤولة عن تعزيز بيئة إلكترونية قوية للحكومة ولجميع القطاعات الحيوية، وذلك للكشف عن التهديدات الإلكترونية ومنعها قبل أن تتسبب في إحداث ضرر كبير.

- في ديسمبر ٢٠١٣، نظمت قطر أول تدريب لها في مجال الأمن السيبراني على المستوى الوطني في نطاق القطاعات الحيوية، وشمل ذلك القطاع المالي والمصرفي ومنشآت وشبكات الطاقة والقطاع الحكومي والنقل، وذلك تعزيزًا لإمكانية المؤسسات على الحد من التهديدات الإلكترونية ومواجهتها.

- تواصل قطر تمكين مستخدمي الإنترنت بتوفير مجموعة من برامج التوعية بشأن الاستخدام الآمن للإنترنت والفضاء السيبراني، التي توفر للأفراد المعلومات حول التهديدات الإلكترونية والأدوات اللازمة للوقاية من تلك التهديدات وكيفية اكتشافها.

- طورت دولة قطر إمكانياتها في مجال الأدلة الجنائية الرقمية، لتعزز من قدرتها على التحقيق في الجرائم الإلكترونية. ويدعم كل من مركز مكافحة الجرائم الإلكترونية ومركز أمن المعلومات الجهود الرامية إلى حماية أفراد المجتمع واتخاذ إجراءات صارمة بحق المجرمين الذين يستخدمون الوسائل الإلكترونية المتطورة لارتكاب جرائمهم.

- شكلت دولة قطر تحالفات دولية قوية، وتشارك بفعالية في الجهود العالمية الرامية إلى وضع المعايير والأعراف الدولية المعنية بالأمن السيبراني، بما في ذلك الجهود المبذولة في الاتحاد الدولي للاتصالات ومنتدى فرق التصدي للحوادث والأمن (FIRST) ومنظومة ومؤتمر الميريديان.

إن الحكومة القطرية تستثمر بشكل فعال في الموارد البشرية ووضع السياسات والإجراءات وتطبيق التكنولوجيا، وذلك لتعزيز الأمن السيبراني للجهات الحكومية والشركات والأفراد. إلا أنه ينبغي بذل المزيد من الجهود لتلبية احتياجات المستقبل، مع ظهور التهديدات الجديدة وازدياد الاعتماد على تكنولوجيا المعلومات والاتصالات. فالجهود الحالية لا تزال موزعة بشكل موسع وتنطلق من أدنى المستويات إلى المستويات الأعلى. ونتيجة لذلك، لم يتم بعد إضفاء الطابع المؤسسي على الأمن السيبراني على المستوى الوطني، أو تنفيذه في جميع الجهات الحكومية والشركات وغيرها من المؤسسات.

وبينما تشرع الشركات في تقدير المخاطر التي تواجهها في الفضاء الإلكتروني واتخاذ الإجراءات اللازمة لتعزيز أمنها السيبراني، تتبع العديد منها سياسات مستقلة ولا تزال تواجه صعوبة في استقطاب المهارات والتقنيات الضرورية لتنفيذ الممارسات الفعالة في مجال الأمن السيبراني. وعلى الرغم من أن الأفراد يملكون إمكانية الوصول إلى المعلومات المتعلقة بالتهديدات والمخاطر في الفضاء الإلكتروني، والإجراءات البسيطة والفعالة التي يمكنهم اتخاذها عبر الإنترنت، فإنه لابد من تقديم المزيد من المساعدة للمستخدمين من أجل المحافظة على سلامة أنظمتهم وحماية معلوماتهم الشخصية. وتقدم الجهود التي تمت مناقشتها أعلاه أساسًا صلبًا للمستقبل، بيد أنه على الجهات الحكومية والشركات والأفراد العمل معًا كفريق واحد لتعزيز الأمن السيبراني لدولة قطر.

٣. نهج دولة قطر الجديد تجاه الأمن السيبراني

يـوازن نهـج دولـة قطـر الجديـد للأمـن السـيبراني بـين الحاجـة لحمايـة خدمـات تكنولوجيـا المعلومـات والاتصـالات والحاجـة لتوفـير فـرص للاسـتفادة بشـكل كامـل مـن المزايـا والكفـاءات الـتي تقدمهـا تكنولوجيـا المعلومـات والاتصـالات المتطـورة. وسـتعمل الحكومـة عـلى الدفـاع عـن مصالـح دولـة قطـر في الفضـاء الإلكـتروني مـن التهديـدات الـتي قـد تـضر بأمنهـا الوطـني، وذلـك باسـتخدام الإمكانيـات المتاحـة ابتـداء مـن الدبلوماسـية ومـرورًا بالمشـاركة في وضـع القوانـين الدوليـة ووصـولًا إلى اسـتقطاب الخـبرات العسـكرية والاسـتخباراتية والأمنيـة لإدارة عمليـات الفضـاء الإلكـتروني وحمايـة الدولـة مـن الهجمـات الإلكترونيـة واسـعة النطـاق.

تمثـل هـذه الاسـتراتيجية طريقًـا محـددًا يرمـي إلى تحقيـق الرؤيـة المسـتقبلية لدولـة قطـر بشـأن الأمـن السـيبراني. إنهـا دعـوة للحكومـة والـشركات والأفـراد لإيجـاد بيئـة إلكترونيـة أكـثر أمانًـا. ويصـف هـذا القسـم رؤيـة الأمـن السـيبراني في دولـة قطـر، ويحـدد الأهـداف والمبـادرات اللازمـة لتحقيـق تلـك الرؤيـة.

٣-١ الرؤية

خلق وتعزيز فضاء إلكتروني آمن، لحماية المصالح الوطنية لدولة قطر والحفاظ على الحقوق والقيم الأساسية لمجتمعنا.

٣-٢ الأهداف

تحقيق هذه الرؤية، تسعى دولة قطر لتحقيق الأهداف التالية:

الهدف الأول:	**الهدف الثاني:**	**الهدف الثالث:**	**الهدف الرابع:**	**الهدف الخامس:**
حماية البنية التحتية للمعلومات الحيوية الوطنية.	الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة.	وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني.	تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الآمن والمناسب للفضاء الإلكتروني.	تطوير وصقل الإمكانيات الوطنية للأمن السيبراني.

وتشـكل هـذه الأهـداف مجتمعـة الأسـاس للحمايـة مـن الهجمـات الإلكترونيـة والاسـتعداد لمواجهتهـا (نهـج اسـتباقي للأمـن السـيبراني)، بالإضافـة إلى اكتشـاف التهديـدات والتحديـات الـتي تواجـه دولـة قطـر ومواجهتهـا والتعـافي منهـا (جهـود تفاعليـة للأمـن السـيبراني).

٣-٣ المبادرات الاستراتيجية

تصف المبادرات الاستراتيجية التالية ما ستقوم به دولة قطر من إجراءات للتقدم نحو تحقيق أهداف الأمن السيبراني. وفي حين تم ترتيب المبادرات وفقًا للهدف، فإن المبادرات الخاصة بأحد الأهداف قد تقود إلى إحراز التقدم والنجاح في تحقيق أهداف أخرى.

الهدف الأول: حماية البنية التحتية للمعلومات الحيوية الوطنية

لتحقيق هذا الهدف، ستقوم دولة قطر بما يلي:

- تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية.
- تنفيذ ضوابط ومعايير الأمن السيبراني للحد من المخاطر على البنية التحتية للمعلومات الحيوية.
- تحليل اتجاهات الأمن السيبراني والمخاطر التي تهدد البنية التحتية للمعلومات الحيوية، وتقديم التقارير للأطراف المعنية في الوقت المناسب.
- تعزيز استخدام المنتجات والخدمات التكنولوجية الموثوق بها.
- المراقبة المستمرة لأمن البنية التحتية للمعلومات الحيوية.

تعد الإدارة الاستباقية لمخاطر الفضاء الإلكتروني أمرًا ضروريًا لضمان استمرار دولة قطر في تحديد وحماية الأنظمة التي تدعم تقديم الخدمات والإمكانيات الأساسية. وللحد من مخاطر الهجمات الإلكترونية المستقبلية التي قد تُشن على الأصول والأنظمة والشبكات الضرورية للحفاظ على رفاهية دولة قطر وازدهارها وأمنها، يجب على حكومة دولة قطر ومؤسسات القطاعات الحيوية والمؤسسات الأخرى تبني ضوابط أمنية وتحديد أولوية الإجراءات التي يجب اتخاذها لتحقيق هذا الهدف.

بالإضافة إلى ما تقدم، تقوم دولة قطر ببناء القدرة على جمع وتحليل الأحداث والتنبيهات والتهديدات المتعلقة بالأمن السيبراني على الشبكة الحكومية، وهي شبكة خاصة بربط الجهات الحكومية عبر منصة اتصال آمنة، مما يتيح بيئة أفضل لتبادل المعلومات وتوفير درجة أعلى من الأمان للخدمات الإلكترونية. ومن خلال تحليلات البيانات المتقدمة، تعتزم دولة قطر ربط معلومات الأمن السيبراني لتحديد الاتجاهات المتعلقة بالالتزام بالمتطلبات الأمنية والتهديدات التي تستهدف الشبكة . وستتيح هذه المراقبة المستمرة للشبكات الحيوية لدولة قطر إدراك المخاطر التي تستهدف الشبكات والكشف عن الهجمات والتهديدات في أقرب وقت ممكن واتخاذ الإجراءات الفورية للحد من آثارها.

الهدف الثاني: الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، من خلال مشاركة المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة

لتحقيق هذا الهدف، ستقوم دولة قطر بما يلي:

- تعزيز إمكانيات الإلمام والتحديث لوضع الأمن السيبراني.
- بناء قدرات الاستجابة للهجمات الإلكترونية وتحسينها باستمرار.
- الحد من إمكانية تعرض البنية التحتية للمعلومات الحيوية لهجمات إلكترونية.
- وضع الآليات والإجراءات التي من شأنها تسهيل اتخاذ الإجراءات اللازمة وتداول المعلومات مع الأطراف المعنية في الوقت المناسب.
- ضمان الجاهزية من خلال إجراء تدريبات المحافظة على الأمن السيبراني.

ويعد الإلمام بالوضع أمرًا ضروريًا لبناء الوعي اللازم للكشف عن الحوادث والهجمات الإلكترونية والتعامل معها بشكل فعال والتعافي منها. وينبغي أن يكون لدى الجهات المنظمة لكل قطاع ومؤسسات القطاعات الحيوية إمكانية مراقبة أنشطة الشبكات وأن يكونوا دائمًا ملمين بالوضع الأمني. وسيعزز تبادل البيانات والمعلومات بين القطاعات الحيوية من زيادة الوعي بالحالة الراهنة للتهديدات، فضلًا عن توفير نظام إنذار مبكر للتمكن من منع الهجمات والحوادث الإلكترونية واكتشافها والتصدي لها. كما ستقوم دولة قطر بتأسيس المكتب التنسيقي للأمن السيبراني، الذي يتبع رئيس مجلس الوزراء، ليكون جهة التنسيق والاتصال المركزية بين الأطراف المعنية حول الوظائف الرئيسية للأمن السيبراني، بما في ذلك إدارة الهجمات الإلكترونية على المستوى الوطني. فتضافر الجهود وإقامة شراكات بين الأطراف المعنية المتعددة بهدف تبادل المعلومات والإلمام بوضع التهديدات والحوادث والهجمات الإلكترونية، سيعزز من قدرة دولة قطر على توقع مثل هذه الحوادث والهجمات، والتعامل معها والتعافي منها بأقل الأضرار التي قد تصيب الجهات الحكومية والشركات وأفراد المجتمع. وسيتم تنظيم تدريبات منتظمة حول الأمن السيبراني على المستوى الوطني وعلى مستوى كل قطاع، لزيادة التعاون وتبادل المعلومات والتنسيق بين الأطراف المعنية بهدف تحديد المخاطر وإجراء التحسينات اللازمة.

الهدف الثالث: وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني

لتحقيق هذا الهدف، ستقوم دولة قطر بما يلي:

- تعزيز قدرات دولة قطر على مكافحة الجريمة الإلكترونية.
- وضع وتنفيذ القوانين واللوائح والسياسات الوطنية للتعامل مع قضايا الأمن السيبراني والجريمة الإلكترونية.
- مراقبة وتعزيز الالتزام بالقوانين واللوائح والسياسات الوطنية المتعلقة بالأمن السيبراني والجريمة الإلكترونية.
- بناء شراكات دولية متينة والحفاظ عليها لوضع معايير وقواعد الأمن السيبراني.

تعمل دولة قطر على إيجاد إطار قانوني ديناميكي قادر على مواكبة تطور التهديدات الإلكترونية والتقنيات الحديثة في ظل اكتساب الجهات الحكومية والشركات والمجتمع بأكمله لمزيد من الخبرات ذات الصلة. إن تطوير وسن مجموعة شاملة من القوانين المتعلقة بالأمن السيبراني والجريمة الإلكترونية ووضعها موضع التنفيذ سيرتقي بالمؤسسات من خلال تحديد الأدوار والمسؤوليات. وستعمل دولة قطر بالتعاون مع الجهات الحكومية المعنية وغيرها من المؤسسات لوضع القوانين واللوائح والسياسات الوطنية عن طريق مشاركة وجهات النظر والآراء.

إن الحكومة القطرية حريصة على اتخاذ التدابير اللازمة لحماية المواطنين والمقيمين من الجرائم الإلكترونية. وستعمل دولة قطر على تحييد الهجمات والحد منها باستخدام تقنيات إنفاذ القوانين المتطورة في جمع الأدلة الجنائية والتحقيق بشأن الأنشطة الإجرامية.

وتتطلب مكافحة الجريمة الإلكترونية وغيرها من التهديدات الإلكترونية التعاون بين دول العالم. ومن جهتها، ستقوم الحكومة القطرية بالتنسيق مع المجتمع الدولي لتعزيز الإمكانيات داخل دولة قطر وحول العالم بهدف مكافحة الجريمة الإلكترونية. فضلًا عن ذلك، ستنشئ دولة قطر كيانات متخصصة وتحصل على الإمكانيات اللازمة لزيادة قدرتها على منع الجريمة الإلكترونية ومكافحتها. كما أن المشاركة في الجهود الدولية لوضع معايير وقواعد الأمن السيبراني العالمي وتحديد وتعزيز أفضل الممارسات وتحديث وزيادة وسائل حماية الخصوصية والحفاظ على حوكمة مستقرة وفعالة للإنترنت ستدعم دولة قطر في الوفاء بالتزاماتها المتعلقة بالفضاء الإلكتروني.

الهدف الرابع: تعزيز ثقافة الأمن السيبراني التي من شانها دعم الاستخدام الآمن والمناسب للفضاء الإلكتروني

لتحقيق هذا الهدف، ستقوم دولة قطر بما يلي:

- تعزيز وعي المجتمع بالأمن السيبراني باستخدام وسائل وقنوات متعددة.
- تشجيع الأفراد على استخدام أدوات وحلول السلامة على الإنترنت للوقاية من الهجمات الإلكترونية.
- تطوير مناهج تثقيفية حول الأمن السيبراني وإتاحتها في المدارس والكليات والجامعات.

إن الحفاظ على بيئة آمنة للأنشطة على الإنترنت أمر ضروري لتعزيز الثقة الرقمية. ولتشجيع اقتصاد مزدهر عبر الإنترنت، يجب أن يثق العملاء بأن تعاملاتهم آمنة وأن معلوماتهم الشخصية في أمان. ويُعد تعزيز الوعي والتشجيع على تبادل المعلومات بين الجهات الحكومية والشركات والمؤسسات من أهم الوسائل الفعالة في تحسين الأمن السيبراني. بالإضافة إلى ذلك، يجب أن تقوم المؤسسات بجمع المعلومات الشخصية واستخدامها وحمايتها بصورة مناسبة، الأمر الذي سيمكّن المستخدمين من حماية أنفسهم ضد سرقة هوياتهم.

لقد حققت دولة قطر تقدمًا في بناء ثقافة الأمن السيبراني من خلال حملات السلامة على الإنترنت، ومنها اليوم العالمي لإنترنت أكثر أمانًا لعام ٢٠١٣، وإعلانات تستهدف مجموعات بعينها للتحذير من عمليات الاحتيال وغيرها من التهديدات عبر الإنترنت من خلال مواد مطبوعة وعبر شبكات التواصل الاجتماعي. ويتطلب تحقيق هذا الهدف تعاونًا كبيرًا بين الأطراف المعنية من الحكومة وجهات إنفاذ القانون وقادة الصناعة والمؤسسات الأكاديمية لتطوير وتطبيق حلول للسلامة على الإنترنت ولتثقيف جميع فئات المجتمع حول أهمية الأمن السيبراني والمتطلبات القانونية ذات الصلة.

الهدف الخامس: تطوير وصقل الإمكانيات الوطنية للأمن السيبراني

لتحقيق هذا الهدف، ستقوم دولة قطر بما يلي:

- تطوير قوى عاملة مهنية في مجال الأمن السيبراني والحفاظ عليها.
- تعزيز فرص تأسيس الشركات وتنافسية كل من القطاعين العام والخاص بدولة قطر في مجال الأمن السيبراني.
- الاستثمار في الأبحاث الرامية إلى تطوير وتسويق التقنيات والحلول المبتكرة في مجال الأمن السيبراني.

يجب أن تتصدر دولة قطر المبادرات التثقيفية التي تعمل على تطوير وصون قوى عاملة قطرية في مجال الفضاء الإلكتروني تكون قادرة على الدفاع عن الفضاء الإلكتروني وحمايته من الحوادث والهجمات الإلكترونية. ولمواكبة بيئة المخاطر المتطورة، فإن دولة قطر تحتاج لموظفين في الجهات الحكومية وقطاعات الصناعة لديهم إدراك عميق للتطورات الجديدة في الفضاء الإلكتروني ومدى تأثيرها على العمليات الإلكترونية.

وفي الوقت ذاته، ينبغي أن تواصل دولة قطر دفع عجلة الابتكار المحلية اللازمة لتحديد وتنفيذ الحلول الجديدة لمواجهة التحديات المستقبلية المعقدة التي تقف أمام الأمن السيبراني. كما يجب توفير بيئة تسمح لشركات الأمن السيبراني المحلية بأن تزدهر حتى تتمكن من تزويد القطاعات الحكومية والحيوية بالمنتجات والخدمات التي تحتاجها في مجال الأمن السيبراني.

إن تطوير وتنفيذ خطة عمل وطنية لإجراء أبحاث وتطويرات في مجال الأمن السيبراني تركز على الحلول التي من شأنها توقع الهجمات الإلكترونية ومكافحتها ومنع وصولها إلى البنية التحتية للمعلومات الحيوية، سيسهم في ضمان جاهزية دولة قطر لمواجهة التهديدات الإلكترونية الناشئة. واستنادًا لنقاط القوة الأساسية الحالية في تحليلات البيانات والحوسبة الاجتماعية، ستكون دولة قطر قادرة على اتباع خطة عمل وطنية تدعم تطبيق تحليلات بيانات الوقت الحقيقي للكشف عن الهجمات الإلكترونية والقيام بإجراءات الكشف عن الأدلة الجنائية والتخفيف من عواقب الحوادث الإلكترونية، وتوقع الهجمات الإلكترونية التي تستهدف البنية التحتية في قطر ومكافحتها وهزيمتها في نهاية الأمر.

٤. خطة العمل للأعوام ٢٠١٤-٢٠١٨

تستعرض خطة العمل المزيد من التفاصيل حول خطة الحكومة لتحقيق رؤية دولة قطر للأمن السيبراني، وهي مرتبة وفقًا للأهداف. وينبغي على الأطراف المعنية من الجهات والمؤسسات الحكومية، مثل وزارة الدفاع ووزارة الاتصالات وتكنولوجيا المعلومات ووزارة الداخلية والنيابة العامة ومؤسسة قطر والجهات المنظمة للقطاعات ومؤسسات القطاعات الحيوية والمجلس الأعلى للتعليم وغيرها من المؤسسات، العمل معًا لتنفيذ هذه الإجراءات بما يحقق مصالح دولة قطر.

الهدف الأول: حماية البنية التحتية للمعلومات الحيوية الوطنية

المبادرة	الإجراء
تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية	▪ وضع إطار وطني لإدارة المخاطر على البنية التحتية للمعلومات الحيوية، وذلك لتوجيه جهود تحديد أصول ومؤسسات البنية التحتية للمعلومات الحيوية وتقييم التهديدات ونقاط الضعف والعواقب وتطوير ملفات المخاطر ▪ إجراء تقييمات منتظمة للمخاطر التي تواجه مؤسسات القطاعات الحيوية وغيرها من المؤسسات فيما يتعلق بالبنية التحتية للمعلومات الحيوية ▪ إجراء تقييمات حول مدى الترابط والاعتماد المتبادل بين مؤسسات القطاعات الحيوية لتحديد المخاطر المنهجية التي تواجهها
تنفيذ ضوابط ومعايير الأمن السيبراني للحد من الخطر على البنية التحتية للمعلومات الحيوية	▪ وضع نموذج ومعايير خاصة بالأمن السيبراني للبنية التحتية للمعلومات الحيوية، يتضمن ضوابط محددة للأمن السيبراني ▪ إجراء عمليات تقييم وتدقيق منتظمة لمؤسسات القطاعات الحيوية، وذلك لقياس وتقييم فعالية برامج وضوابط الأمن السيبراني ▪ وضع استراتيجيات إدارة المخاطر لحماية الخدمات والأنظمة والمؤسسات الأكثر حيوية، ومتابعة تنفيذ تلك الاستراتيجيات ▪ تبادل المعلومات حول المخاطر واستراتيجيات إدارة المخاطر بين مختلف القطاعات، لتحديد أولويات إجراءات التخفيف من حدة تلك المخاطر واستثمار الموارد المتاحة
تحليل اتجاهات الأمن السيبراني والمخاطر التي تهدد البنية التحتية للمعلومات الحيوية، وتقديم التقارير للأطراف المعنية في الوقت المناسب	▪ إنشاء مراكز عمليات أمنية خاصة بقطاعات أو مؤسسات بعينها أو مراكز معلومات للكشف عن التهديدات
تعزيز استخدام المنتجات والخدمات التكنولوجية الموثوق بها	▪ تطوير الإمكانيات الحالية لتقييم منتجات وأنظمة تكنولوجيا المعلومات والاتصالات واعتماد استخدامها في القطاعات الحيوية ▪ وضع مبادئ توجيهية لتحديد المتطلبات الأمنية لمزودي خدمات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
المراقبة المستمرة لأمن البنية التحتية للمعلومات الحيوية	▪ وضع آلية لإجراء عمليات تشخيص ومراقبة مستمرة للشبكات من أجل تشكيل وعي أكبر بالمخاطر وتعزيز الإجراءات الوقائية والكشف عن الأجهزة المتضررة ومعالجتها، وإبلاغ المستخدمين المتضررين

الهدف الثاني: الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة	
المبادرة	**الإجراء**
تعزيز إمكانيات الإلمام والتحديث لوضع الأمن السيبراني	▪ تطوير إمكانيات التنسيق على المستوى الوطني لتعزيز الإدراك العام لوضع التهديدات والحوادث المتعلقة بالأمن السيبراني، والمساعدة في التعامل مع الحوادث الإلكترونية التي قد تتعرض لها دولة قطر ▪ تأسيس نظام وطني لتسجيل ومراقبة التهديدات والحوادث والهجمات الإلكترونية
بناء قدرات الاستجابة للهجمات الإلكترونية وتحسينها باستمرار	▪ وضع آلية للتنسيق وإدارة التعامل مع الحوادث الإلكترونية ▪ إنشاء شبكة لتبادل المعلومات بين مراكز عمليات الفضاء الإلكتروني، وذلك لتيسير التعامل مع الحوادث وتبادل المعلومات وتوفير فرص التدريب
الحد من إمكانية تعرض البنية التحتية للمعلومات الحيوية لهجمات إلكترونية	▪ إجراء تقييمات منتظمة للشبكات لتحديد الرموز والمصادر الضارة وإزالتها من البنية التحتية للشبكات ▪ تطوير أدوات الكشف عن التهديدات المستمرة المتطورة على البنية التحتية للمعلومات ووضعها موضع التنفيذ
وضع الآليات والإجراءات التي من شأنها تسهيل اتخاذ الإجراءات اللازمة وتداول المعلومات مع الأطراف المعنية في الوقت المناسب	▪ تطوير وتشغيل أنظمة وأدوات لمشاركة المعلومات ذات الصلة بالتهديدات ونقاط الضعف الإلكترونية بين الأطراف المعنية الموثوق بهم ▪ عقد مزيد من الشراكات بين القطاعات المختلفة لتضافر جهود الأطراف المعنية لمواجهة التهديدات الإلكترونية وتعزيز جاهزية ومرونة ومتانة البنية التحتية للمعلومات الحيوية ▪ إنشاء منتدى يجمع العاملين في المجال الأمني من جميع القطاعات الحيوية لمواجهة المخاطر النظامية
ضمان الجاهزية من خلال إجراء تدريبات المحافظة على الأمن السيبراني.	▪ تنظيم التدريبات الخاصة بالأمن السيبراني على المستوى الوطني ودمج الدروس المستفادة في السياسات والإجراءات والآليات التشغيلية ▪ إجراء تدريبات خاصة بالأمن السيبراني على مستوى القطاع لتقييم واختبار إمكانيات التعامل مع الحوادث في مؤسسات القطاعات الحيوية ▪ المشاركة في التدريبات الدولية الخاصة بالفضاء الإلكتروني أو استضافتها بهدف بناء علاقات دولية قوية واختبار آليات التنسيق للتعامل مع الحوادث

الهدف الثالث: وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني	
المبادرة	**الإجراء**
تعزيز قدرات دولة قطر على مكافحة الجريمة الإلكترونية	▪ تطوير قدرات جديدة للتحقيق في الأنشطة الإجرامية من خلال التدريب وتقنيات الأدلة الجنائية الحديثة واستخدام التكنولوجيا ▪ سن قانون مكافحة الجريمة الإلكترونية لمنح القائمين على إنفاذ القانون سلطات جديدة ولتحديد الأفعال الإجرامية ▪ جمع الإحصائيات المتعلقة باتجاهات الجرائم الإلكترونية وطرق ارتكابها
وضع وتنفيذ القوانين واللوائح والسياسات الوطنية للتعامل مع قضايا الأمن السيبراني والجريمة الإلكترونية	▪ إجراء مراجعات منتظمة للقوانين والسياسات الأخرى لضمان استمرار قدرتها على التعامل مع الاحتياجات الناشئة في مجال الأمن السيبراني ▪ تمرير قوانين مقترحة (مثل قوانين حماية الخصوصية والبيانات، وقانون حماية البنية التحتية للمعلومات الحيوية) لمنع سوء استخدام المعلومات الشخصية وحماية البنية التحتية للمعلومات الحيوية
مراقبة وتعزيز الالتزام بالقوانين واللوائح والسياسات الوطنية المتعلقة بالأمن السيبراني والجريمة الإلكترونية	▪ وضع منهجية وآلية لتحديد مدى التزام مؤسسات القطاعات الحيوية بالقوانين واللوائح وتنفيذها للسياسات الوطنية ▪ وضع مبادئ توجيهية وتوفير الموارد اللازمة لمؤسسات القطاعات الحيوية، مثل التدريب والأدوات وورش عمل للتدقيق، وذلك لتشجيع اعتماد أفضل ممارسات الأمن السيبراني ولتسهيل الالتزام بالمتطلبات ذات الصلة ▪ تقييم الاستراتيجية الوطنية للأمن السيبراني لدولة قطر ورفع تقارير سنوية حول الجهود التي بذلتها الحكومة ومؤسسات القطاعات الحيوية لتنفيذ الاستراتيجية وتعزيز الأمن السيبراني
بناء شراكات دولية متينة والحفاظ عليها لوضع معايير وقواعد الأمن السيبراني	▪ التعاون مع الشركاء الدوليين بشكل منتظم بشأن السياسات والعمليات التشغيلية لزيادة الوعي بالأمن السيبراني، وتحديد التهديدات والتعامل معها، وتنسيق الإجراءات الهادفة لتعزيز الأمن السيبراني في جميع أنحاء العالم ▪ تعزيز الاتفاقيات الثنائية ومتعددة الأطراف الحالية وإبرام اتفاقيات جديدة لحث الجهات المختلفة على تبادل المعلومات حول قضايا الفضاء الإلكتروني والارتقاء بالتحقيقات الجنائية ودعم عمليات الفضاء الإلكتروني

الهدف الرابع: تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الآمن والمناسب للفضاء الإلكتروني	
المبادرة	**الإجراء**
تعزيز وعي المجتمع بالأمن السيبراني باستخدام وسائل وقنوات متعددة	▪ تعزيز الوعي الوطني بالأمن السيبراني والحفاظ عليه لدى مختلف فئات المجتمع (مثل الأطفال والطلبة وأولياء الأمور وكبار السن وموظفي الحكومة والشركات الصغيرة والمتوسطة والمسؤولين التنفيذيين وغيرهم) ▪ إنشاء برنامج للمنح والمكافآت، وذلك لتكريم التميز في مجال الأمن السيبراني بتقديم إسهامات رئيسية في هذا المجال، مثل تقديم الحلول أو الخدمات المبتكرة أو تنفيذ ضوابط الأمن السيبراني واتباع أفضل الممارسات
تشجيع الأفراد على استخدام أدوات وحلول السلامة على الإنترنت للوقاية من الهجمات الإلكترونية	▪ العمل مع مزودي خدمات الإنترنت وغيرها من الجهات لمساعدة المستخدمين من الأفراد لتحديد سلامة أجهزتهم
تطوير مناهج تثقيفية حول الأمن السيبراني وإتاحتها في المدارس والكليات والجامعات	▪ العمل مع الجامعات والكليات على تطوير وتنفيذ مناهج وبرامج تثقيفية تتناول الأمن السيبراني على مستوى التعليم العالي والدراسات العليا ▪ العمل مع المدارس على وضع برامج تعليمية حول السلامة على الإنترنت، وتزويد المدرسين والإداريين بالمواد التي تدعمهم في تنفيذ مهمتهم

الهدف الخامس: تطوير وصقل الإمكانيات الوطنية للأمن السيبراني	
المبادرة	**الإجراء**
تطوير قوى عاملة مهنية في مجال الأمن السيبراني والحفاظ عليها	▪ تطوير نموذج كفاءة القوى العاملة في مجال الأمن السيبراني ▪ تنظيم مسابقات في مجال الأمن السيبراني على الصعيدين المحلي والوطني لمختلف الفئات العمرية لاختيار أفضل المهارات القطرية وصقل مهاراتهم وتشجيعهم على متابعة مسيرتهم في مجال الأمن السيبراني
تعزيز فرص تأسيس الشركات وتنافسية كل من القطاعين العام والخاص بدولة قطر في مجال الأمن السيبراني	▪ رعاية مسابقات تعزز الابتكار في مجال الأمن السيبراني وتشجيع الشركات الصغيرة والمتوسطة على توفير الحلول والخدمات المبتكرة في هذا المجال
الاستثمار في الأبحاث الرامية إلى تطوير وتسويق التقنيات والحلول المبتكرة في مجال الأمن السيبراني	▪ وضع خطة عمل وطنية لإجراء الأبحاث وإحداث تطوير في مجال الأمن السيبراني، وذلك لتعزيز الاستثمار في الحلول التي يمكن تحويلها بسرعة من مرحلة التطوير إلى مرحلة التنفيذ ▪ تأسيس شراكات استراتيجية مع الجامعات والمعاهد والمؤسسات البحثية داخل دولة قطر وفي الخارج فيما يتعلق بمشاريع الأبحاث والتطوير في مجال الفضاء الإلكتروني

٥. نهج التنفيذ

يتطلب تنفيذ هذه الاستراتيجية التزامًا متواصلًا وحوكمة وإجراءات مستمرة من قبل العديد من الأطراف المعنية الذين يتشاركون مسؤولية الالتزام بنهج الدولة ككل تجاه الأمن السيبراني. ويرتبط الأطراف المعنية بعضهم ببعض من خلال مجموعة من المبادئ التوجيهية المشتركة التي تدعم رؤية مستقبل الأمن السيبراني في دولة قطر.

٥-١ المبادئ التوجيهية

يرتكز نهج دولة قطر للأمن السيبراني على ثلاثة مبادئ:

قيادة الحكومة لجهود الأمن السيبراني – تتولى الحكومة مسؤولية حماية معلومات وأنظمة وشبكات الحكومة وضمان سريتها وسلامتها وتوفرها. وستقود الحكومة الجهود المبذولة وستقدم القدوة للمؤسسات الأخرى من خلال تنفيذ متطلبات الأمن السيبراني مع تصميم واعتماد التقنيات المبتكرة والحديثة التي تشكل أساس الاقتصاد.

الأمن السيبراني مسؤولية مشتركة – تقع مسؤولية الأمن السيبراني على عاتق جميع الجهات الحكومية والشركات والمؤسسات والأفراد.

تتمثل مسؤولية الحكومة القطرية في حماية معلوماتها وأنظمتها وشبكاتها، والاستثمار في الأشخاص والإجراءات والتقنيات اللازمة لحماية الخدمات التي يعتمد عليها المجتمع القطري، وتحديد اتجاه النمو والتطور المستمرين لدولة قطر.

وتتمثل مسؤولية الشركات في حماية معلوماتها وأنظمتها وشبكاتها الحيوية من التهديدات الإلكترونية، وتبادل المعلومات، والتعامل مع أي حادث أو هجمة إلكترونية تتعرض لها.

يتعين على الأفراد الإلمام بالتهديدات الإلكترونية ومعرفة من يقوم بجمع معلوماتهم الشخصية، واتخاذ الإجراءات الضرورية لتأمين معلوماتهم وأنظمتهم وشبكاتهم.

الحفاظ على الحقوق والقيم الأساسية – في الفضاء الإلكتروني، يرتبط الأمن والخصوصية بشكل وثيق. فالمعلومات الشخصية أو الخاصة تتم حمايتها بالشكل الأمثل من خلال الإجراءات الأمنية الحازمة وتطبيق أفضل الممارسات لمنع الوصول غير المصرح إليها أو سوء استغلالها. وستعمل دولة قطر على اتباع سياسات ومبادرات الأمن السيبراني التي تحافظ على الحقوق والقيم الأساسية لمجتمعنا بما ينسجم مع قوانين وتطلعات أفراد المجتمع.

قيم الأمن السيبراني
▪ حماية الحكومة والشركات والمؤسسات والأفراد من المحتوى والسلوكيات غير المقبولة عبر الإنترنت التحلي بالتسامح والاحترام ▪ الابتكار وتبادل الأفكار والمعلومات ▪ دعم الجهود الجماعية والتعاونية لمواجهة التحديات المعقدة للأمن السيبراني ▪ توفير بيئة تشجع الاستثمارات في مجال الأمن وا لتكنو لو جيا

٥-٢ الحوكمة

ولتنفيذ هذه الاستراتيجية وإدارة الأنشطة المرتبطة بها، من الضروري تطبيق معايير حوكمة قوية. وفي ضوء ذلك، ستقوم دولة قطر بتشكيل المكتب التنسيقي للأمن السيبراني، الذي يتبع رئيس مجلس الوزراء، ليكون جهة التنسيق والاتصال المركزية بين الأطراف المعنية على مستوى دولة قطر حول الأنشطة المتعلقة بالأمن السيبراني. كما سيعمل المكتب على: (١) تحديد الأولويات الوطنية لتحقيق أعلى مستويات الأمن السيبراني في دولة قطر، (٢) تقديم التوجيه الاستراتيجي للجهود التي تبذلها دولة قطر بشأن الأمن السيبراني، (٣) العمل في شراكة وثيقة مع الجهات التي لديها مهام واختصاصات متعلقة بالأمن السيبراني من أجل تحقيق أهداف الاستراتيجية.

ومن الضروري أن تلتزم الأطراف المعنية بالتنفيذ الناجح للاستراتيجية. فالأطراف المعنية ستكون مسؤولة عن وضع خططها التنفيذية التفصيلية فيما يتعلق بالإجراءات التي تحتاج لتنفيذها. وستحتاج كل من الجهات الحكومية ومؤسسات القطاعات الحيوية وغيرها من المؤسسات إلى متابعة الإنجازات والتقدم الذي تم إحرازه، وأن تكون على استعداد لتقديم تحديثات منتظمة إلى المكتب. كما يجب على الأطراف المعنية مواصلة التنسيق مع الجهات الأخرى بفعالية على جميع المستويات في المجتمع لتعزيز الأمن السيبراني.

٥-٣ قياس الأداء

من الضروري التنسيق بين الأطراف المعنية وتكامل عملية اتخاذ القرار والمتابعة الدائمة لسير العمل، لإنجاز المبادرات والإجراءات المحددة في هذه الاستراتيجية والوثائق المؤيدة لها. وسوف يحدد المكتب التنسيقي آليات المتابعة لتقييم التقدم، والعمل مع اللجنة الوطنية لأمن المعلومات والأطراف المعنية لاتخاذ القرارات اللازمة فيما يتعلق بتحديد الأولويات وإجراء التعديلات على خطة العمل، ورصد الجهود الرامية إلى إحراز تقدم نحو إنجاز أهداف الاستراتيجية باستخدام مجموعة من أدوات القياس. كما سيقوم المكتب التنسيقي بإعداد تقرير سنوي حول التقدم في إنجاز الأهداف، مضيفًا بذلك رؤية مستمرة لجهود تأمين الفضاء الإلكتروني لدولة قطر.

٦. المضي قدمًا نحو المستقبل

ستقوم دولة قطر بمراجعة الاستراتيجية كل أربع سنوات، أو عند الحاجة، وإجراء التعديلات والتحسينات التي يتم الاتفاق عليها وذلك لمواكبة التطورات القانونية والتشغيلية والتكنولوجية التي تطرأ على المستويين المحلي والدولي. وسيكون الهدف من هذه المراجعة أن تكون الاستراتيجية منسجمة مع أي وثيقة استراتيجية جديدة (مثل استراتيجيات التنمية) على المستوى الوطني واستقبال آراء جميع الجهات المعنية.

ومع ظهور تحديات عالمية جديدة ومعقدة في مجال الأمن السيبراني، يتزايد اعتماد دولة قطر على تكنولوجيا المعلومات والاتصالات. لذا يجب علينا أن نتحلى باليقظة وأن نعمل معًا وبشكل مستمر على تعزيز جاهزية ومرونة فضائها الإلكتروني وفقًا لهذه الاستراتيجية، حيث تتميز الاستراتيجية الوطنية للأمن السيبراني لدولة قطر بتأكيدها على التزام دولة قطر بحماية الفضاء الإلكتروني من أجل الأجيال لقادمة

شكر وتقدير

نود أن نتوجه بالشكر لأعضاء اللجنة الوطنية لأمن المعلومات برئاسة الدكتورة حصة الجابر، وزيرة الاتصالات وتكنولوجيا المعلومات، لمشاركتهم وإسهاماتهم الفاعلة لوضع الاستراتيجية الوطنية للأمن السيبراني لدولة قطر.

العميد/ **صالح خميس الكبيسي**
نائب رئيس اللجنة الوطنية لأمن المعلومات
مدير إدارة نظم المعلومات
وزارة الداخلية

المقدم/ **نواف أحمد الرميحي**
مدير نظم معلومات الشركات
جهاز أمن الدولة

الدكتور/ **سيف محمد الكواري**
مدير إدارة نظم وتقنية المعلومات
وزارة الخارجية

السيد/ **على عبد الله الصديقي العمادي**
مدير نظم المعلومات
قطر للبترول

السيد/ **أحمد سلطان الملا**
مدير إدارة نظم المعلومات
وزارة العدل

العميد المهندس/ **عبد العزيز فلاح الدوسري**
مدير إدارة الشؤون الفنية
القوات المسلحة القطرية

السيد/ **عبد الله محمد النعيمي**
رئيس العمليات
مركز قطر للمعلومات الائتمانية

السيد/ **مصطفى هونيد**
مدير أول أمن معلومات الشركات
شركة Ooredoo

السيدة/ **مريم حاجي عبدالله**
مدير إدارة نظم المعلومات
النيابة العامة

السيد/ **خالد صادق الهاشمي**
المدير التنفيذي لقطاع الأمن السيبراني
وزارة الاتصالات وتكنولوجيا المعلومات

ونود أيضًا أن نتوجه بالشكر للسيد راشد زايد النعيمي، أخصائي الأمن السيبراني بوزارة الاتصالات وتكنولوجيا المعلومات،والدكتورة هدى بركة، مستشار وزير الاتصالات وتكنولوجيا المعلومات لإسهاماتهما في وضع الاستراتيجية الوطنية للأمن السيبراني.

الملحق «أ»: التعريفات

حملات التوعية
وهي أنشطة الاتصالات والتوعية المعدة لتعزيز الوعي ودعم الأمن السيبراني وترسيخ المعرفة بالتهديدات الإلكترونية والممارسات الأمنية، والتي تقود في النهاية إلى اعتماد التغييرات الضرورية في السلوك على الإنترنت.

الإمكانيات
الأشخاص والإجراءات والتكنولوجيا التي تدعم أهداف الأمن السيبراني.

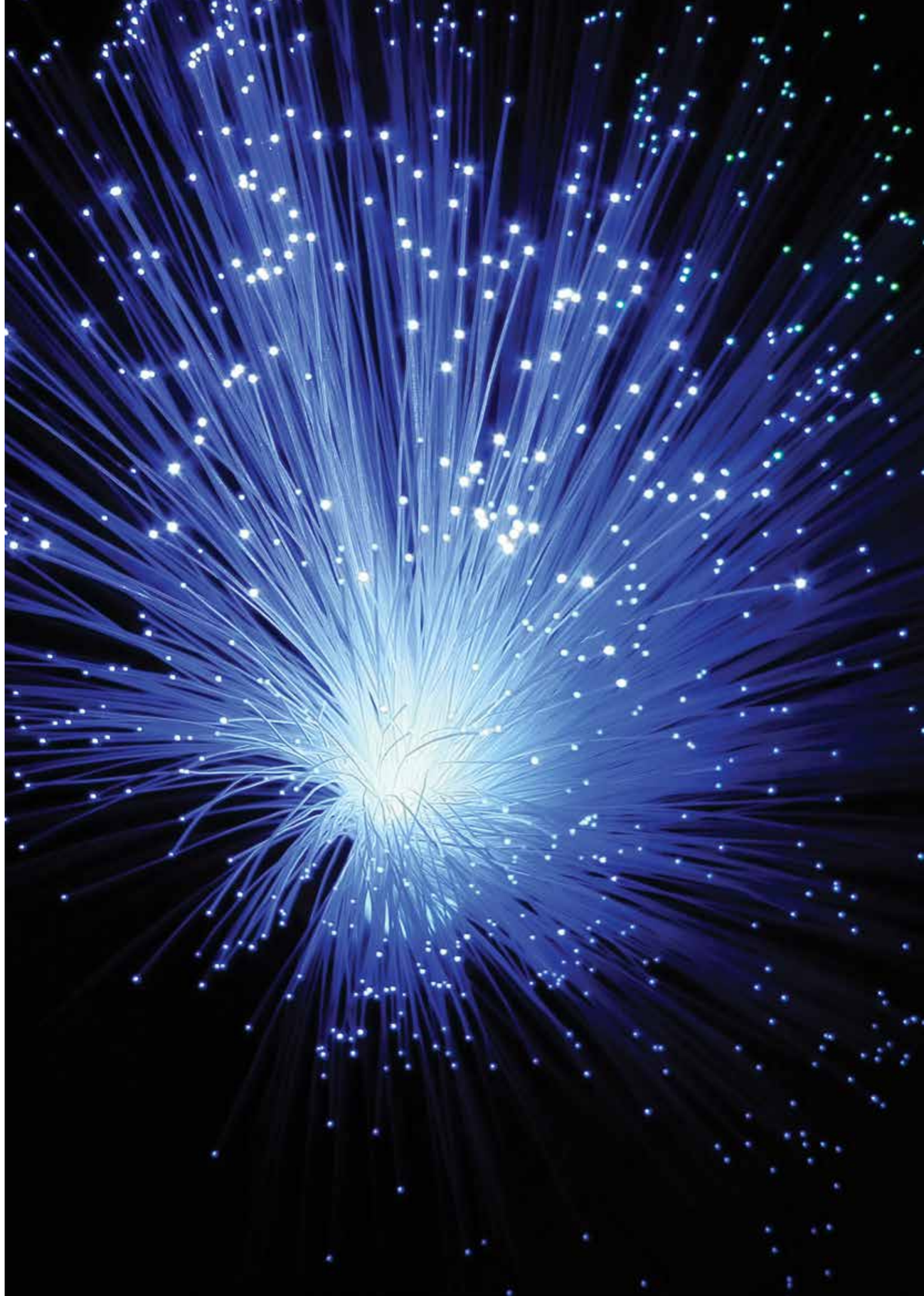
البنية التحتية الحيوية
هي الأصول المادية أو الأنظمة أو الأجهزة، التي قد يكون لتدميرها أو إتلافها أثر خطير على صحة أو سلامة أو أمن دولة قطر أو وضعها الاقتصادي أو على عمل الحكومة بشكل فعال.

البنية التحتية للمعلومات الحيوية
تقنيات تكنولوجيا المعلومات والاتصالات وأنظمتها وخدماتها وأصول البيانات الخاصة بها التي تُعد حيوية لدولة قطر وفقًا لمعايير التصنيف التالية:

١. تحديد إجراءات العمل الرئيسية للمؤسسة واعتمادها على الأصول التي تمتلكها وتديرها المؤسسة (مثل: محطة توليد الطاقة، معمل التكرير، دفتر الأستاذ العام وغيرها).
٢. استخدام جدول شدة التأثير، وذلك لتحديد عامل التأثير بالنسبة لفقدان/ تعطل كل أصل من الأصول الرئيسية.
٣. تصنيف كافة الأصول بأنها حيوية عندما تكون درجة التأثير أكبر من عشرين (٢٠)

جدول شدة التأثير

عامل/ درجة التأثير	منخفض (١)	متوسط (٣)	مرتفع (٥)	شديد (١٥)
تعزيز وعي المجتمع بالأمن السيبراني باستخدام وسائل وقنوات متعددة	أقل من ١٠	١٠-١٠٠	١٠٠-٥٠٠	أكبر من ٥٠٠
	أقل من ٢٠ مليون	٢٠-٢٠٠ مليون	٢٠٠ مليون – ١ مليار	أكثر من ١ مليار
التأثير المتبادل بين القطاعات (على القطاعات الأخرى)	بسيط	متوسط / انقطاع	كبير/ انقطاع	إضعاف شامل
نطاق التأثير	محلي	محلي على نطاق واسع أو في عدة قطاعات (جزئي)	على المستوى الوطني أو في قطاع واحد (بالكامل)	دولي أو في عدة قطاعات (بالكامل)
التأثير على الخدمة	أقل من ١	١-٣٠	٣٠-١٨٠	أكثر من ١٨٠
التأثير على ثقة الجمهور	الجمهور يدرك الخطورة المنخفضة على الدولة والقدرة الكبيرة على السيطرة عليها	الجمهور يدرك الخطورة متوسطة الحجم على الدولة والقدرة المتوسطة للسيطرة عليها	الجمهور يدرك الخطورة الكبيرة على الدولة والقدرة المنخفضة على السيطرة عليها	الجمهور يدرك شدة الخطورة على مستوى الدولة وعدم التيقن من السيطرة عليها



القطاع الحيوي

يشمل القطاعات الحيوية في دولة قطر، على سبيل المثال لا الحصر:

- قطاع الطاقة والكهرباء والماء
- القطاع المالي
- القطاع الحكومي
- قطاع الرعاية الصحية
- قطاع تكنولوجيا المعلومات والاتصالات
- قطاع النقل والمواصلات

مؤسسات القطاعات الحيوية

وهي المؤسسات التي تمتلك جزءًا أساسيًا من البنية التحتية للمعلومات الحيوية داخل دولة قطر أو تقوم بتشغيله أو تقوم بالأمرين معًا.

الجريمة الإلكترونية

سوء السلوك أو الجريمة المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات. على سبيل المثال، الوصول غير القانوني للأنظمة أو المعلومات أو الاحتيال أو سرقة الهوية أو الهجمات المتعلقة بالمحتوى.

الأمن السيبراني

مجموعة الأدوات والسياسات والمفاهيم والإجراءات الأمنية والمبادئ التوجيهية ومنهجيات إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل التأمين والتقنيات التي يمكن استخدامها لحماية بيئة الفضاء الإلكتروني وأصول الشركات والمستخدمين. وتتضمن أصول الشركات والمستخدمين أجهزة الكمبيوتر المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وانظمة الاتصالات وكافة المعلومات التي تم نقلها أو تخزينها عبر الفضاء الإلكتروني. ويسعى الأمن السيبراني لتوفير الخصائص الأمنية لأصول الشركات والمستخدمين والمحافظة عليها من المخاطر الأمنية ذات الصلة في بيئة الفضاء الإلكتروني. وتشمل الأهداف العامة للأمن السيبراني السرية والسلامة (التي قد تتضمن التصديق وعدم إنكار المسؤولية) والإتاحة. ١

ضوابط الأمن السيبراني

الإجراءات الوقائية أو المضادة لضمان سرية وسلامة وتوفر أصول أو أنظمة أو شبكات المعلومات، والحد من المخاطر التي تتعرض إليها تلك الأصول والأنظمة والشبكات.

الفضاء الإلكتروني

البيئة الافتراضية أو الإلكترونية التي تنتج عن شبكة مرتبطة بتكنولوجيا المعلومات والاتصالات (مثل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات وأدوات التحكم المدمجة) التي تربط الناس بالخدمات والمعلومات.
نظام الاتصال المشترك – مجموعة من المؤسسات والأنظمة والأجهزة المتصلة والمرتبطة فيما بينها والتي تتفاعل لتحقيق عدة أغراض باستخدام آليات وإجراءات مختلفة.

التدريبات

المشاركة التفاعلية (من نصف يوم إلى ٥ أيام أو أكثر) والتي تمكن المشاركين من التعامل مع سيناريو معين في بيئة خالية من المخاطر. تتيح هذه التدريبات أدوات فعالة لاختبار خطط التعامل مع الحوادث والتحقق من صحة السياسات والخطط والإجراءات، وتحديد نقاط الضعف ومتطلبات التقارير وتقييم المخاطر والجاهزية، واكتشاف نقاط الارتباط وفجوات الاستجابة، وإيجاد تصور مشترك بين مختلف الأطراف المعنية، وتعزيز إدراك مشترك للأدوار والمسؤوليات. ويمكن الإشارة إلى التدريبات أيضًا على أنها المحاكاة للواقع أو حلقات دراسية أو تمارين أو مناورات.

المعلومات الشخصية

وهي المعلومات المسجلة عن شخص معين، والتي تشمل على سبيل المثال لا الحصر، الاسم والعنوان والبريد الإلكتروني ورقم الهاتف والوضع العائلي والرعاية الصحية أو البيانات المالية والتاريخ الوظيفي والمؤسسات المرتبط بها.
السياسة – وهي مجموعة من الأدوات، مثل الاستراتيجيات أو المعايير أو الأطر العامة أو المبادئ التوجيهية أو غيرها من الوثائق الأخرى التي تحدد المسؤوليات والصلاحيات والإجراءات والعمليات المؤسسية وكيفية تطبيقها وتقدم شرحًا ووصفًا لها.

المرونة

وهي القدرة على الاستعداد والتكيف مع الظروف المتغيرة والصمود والتعافي بسرعة من الاضطرابات التي تنتج عن الهجمات أو الحوادث المتعمدة أو تلك التي قد تحدث لأسباب طبيعية.

أشخاص مطلعون لا يتعمدون إحداث ضرر

هم الأشخاص المصرح لهم بالدخول إلى شبكة المؤسسة أو نظامها أو معلوماتها، والذين قد يشكلون تحديًا، وذلك نتيجة قيامهم بإجراء غير متعمد (دون نية للتسبب بضرر) قد يتسبب في ضرر أو يؤثر على سرية أو سلامة أو إتاحة الشبكات أو الأنظمة أو المعلومات.