



استراتيجية قطر الوطنية للأمن السيبراني 2024-2030: من حماية البنية التحتية الوطنية الحرجة إلى التعاون الدولي والدبلوماسية السيبرانية

محمد احمد محمد حسن البوعينين
كلية الدراسات العليا، أكاديمية الشرطة، قطر

الملخص

تهدف هذه الدراسة إلى تحليل استراتيجية قطر الوطنية للأمن السيبراني 2024-2030، وتتبع انتقالها من نموذج يركز على حماية البنية التحتية الوطنية الحرجة إلى نموذج شامل يدمج بين الصمود السيبراني، والحوكمة والتشريعات، وبناء القدرات البشرية، وتوظيف التقنيات الناشئة، والتعاون الدولي والدبلوماسية السيبرانية في إطار متكامل. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل مكونات الاستراتيجية وركائزها، والكشف عن العلاقات المتبادلة بينها، وتقييم مدى تكاملها في تحقيق الأهداف الوطنية. وتوصلت الدراسة إلى أن الاستراتيجية القطرية تمثل نقلة نوعية من مفهوم الحماية التقليدية إلى نموذج صمود وطني متعدد الأطراف، وأن حماية البنية التحتية الوطنية الحرجة لا يمكن فصلها عن الحوكمة والقدرات البشرية والتعاون الخارجي، كما كشفت النتائج أن التعاون الدولي في الاستراتيجية يُنظر إليه بوصفه امتداداً طبيعياً للأمن الوطني وليس مساراً منفصلاً عنه، وأظهرت أن الاستراتيجية تولى اهتماماً بالغاً ببناء القدرات البشرية والوعي المجتمعي، وبالاستثمار في التقنيات الناشئة كالذكاء الاصطناعي. وأكدت النتائج أن الاستراتيجية تمثل نموذجاً متقدماً في المنطقة العربية من حيث شموليتها وتكامل أبعادها. وخلصت الدراسة إلى مجموعة من التوصيات العملية التي يمكن أن تسهم في تعزيز فعالية الاستراتيجية الوطنية وتحقيق أهدافها على نحو أفضل، ومن أبرز هذه التوصيات: تطوير مؤشرات قياس واضحة ودقيقة لدرجة الصمود السيبراني على مستوى الدولة والقطاعات الحيوية، تمكين من التقييم الدوري للأداء وتحديد مجالات التحسين، وتوسيع نطاق تمارين الاستجابة الوطنية المشتركة وإشراك القطاعات الحيوية كافة فيها، بما يعزز التنسيق والجاهزية لمواجهة الحوادث السيبرانية الكبرى، وتعزيز آليات تبادل معلومات التهديدات بين القطاعات المختلفة وإنشاء منصات وطنية لتجميع وتحليل هذه المعلومات، ودعم البحث الجامعي والصناعة السيبرانية المحلية من خلال حوافز تشجع على الابتكار وتطوير حلول تقنية محلية، وتطوير مسار مؤسسي للدبلوماسية السيبرانية يربط الجهات التقنية والقانونية والدبلوماسية في إطار عمل موحد، وتعزيز الثقافة السيبرانية في المجتمع القطري.

الكلمات المفتاحية: الأمن السيبراني، الصمود السيبراني، البنية التحتية الوطنية الحرجة، الحوكمة السيبرانية، الدبلوماسية السيبرانية، استراتيجية قطر الوطنية للأمن السيبراني 2024-2030، الذكاء الاصطناعي.



Qatar National Cyber Security Strategy 2024–2030: From Protecting Critical National Infrastructure to International Cooperation and Cyber Diplomacy

Mohammed Ahmed Mohammed Hassan Al-Buainain

College of Graduate Studies, Police Academy, College of Graduate Studies, Qatar

ABSTRACT

This study aims to analyze Qatar's National Cybersecurity Strategy 2024–2030, tracing its transition from a model focused on protecting critical national infrastructure to a comprehensive model that integrates cyber resilience, governance and legislation, human capacity building, the deployment of emerging technologies, international cooperation, and cyber diplomacy within an integrated framework. The study employed a descriptive-analytical approach to analyze the strategy's components and pillars, reveal their interrelationships, and assess their integration in achieving national objectives. The study concluded that the Qatari strategy represents a qualitative shift from the traditional protection concept to a multi-faceted national resilience model. It also found that protecting critical national infrastructure is inseparable from governance, human capacity building, and external cooperation. Furthermore, the results revealed that international cooperation within the strategy is viewed as a natural extension of national security, not a separate track. The strategy also demonstrates a strong emphasis on human capacity building, public awareness, and investment in emerging technologies such as artificial intelligence. The findings affirmed that the strategy represents an advanced model in the Arab region in terms of its comprehensiveness and the integration of its dimensions. The study concluded with a set of practical recommendations that can contribute to enhancing the effectiveness of the national strategy and achieving its goals better. Among the most prominent of these recommendations are: developing clear and accurate indicators to measure the degree of cyber resilience at the national level and vital sectors, enabling periodic evaluation of performance and identification of areas for improvement; expanding the scope of joint national response exercises and involving all vital sectors in them, which enhances coordination and readiness to confront major cyber incidents; strengthening mechanisms for exchanging threat information between different sectors and establishing national platforms for collecting and analyzing this information.

Keywords: Cyber Security, Cyber Resilience, Critical National Infrastructure, Cyber Governance, Cyber Diplomacy, Qatar National Cyber Security Strategy 2024–2030.





المقدمة

أصبح الأمن السيبراني في العقود الأخيرة أحد المكونات الأساسية للأمن الوطني، بل لعله أصبح العمود الفقري الذي تستند إليه معظم مقومات الدولة العصرية في ظل الاعتماد المتزايد على البنية الرقمية في إدارة القطاعات الحيوية كافة، من الطاقة والاتصالات إلى المال والنقل والصحة والخدمات الحكومية، فلم يعد التهديد السيبراني مقصوراً على اختراق البيانات أو تعطيل المواقع الإلكترونية، بل أصبح قادراً على التأثير في استمرارية الخدمات الحيوية والسيادة الوطنية والثقة في الاقتصاد الرقمي، الأمر الذي جعل منه أولوية قصوى في أجندات الدول المتقدمة والناشئة على حد سواء، إذ بات واضحاً أن الفضاء السيبراني لم يعد مجرد فضاء افتراضي للتواصل وتبادل المعلومات، بل تحول إلى ساحة للصراع والتنافس بين الدول، وإلى مجال حيوي تؤثر الأحداث فيه بشكل مباشر على الأمن القومي والاستقرار الاجتماعي والازدهار الاقتصادي. وتوضح الأدبيات الحديثة أن التهديدات السيبرانية قد تحولت إلى جزء من التحديات غير التقليدية التي تواجه الدول، وأن الهجمات الرقمية قد تستهدف البنية التحتية والخدمات الوطنية الحيوية بما يهدد استقرار المجتمعات وأمنها الشامل، ولم يعد الحديث عن الأمن السيبراني مقتصرًا على دوائر المتخصصين في تقنية المعلومات، بل أصبح شأنًا وطنيًا يمس صميم السيادة والاستقرار والتنمية، ويحتل مكانة بارزة في الخطاب السياسي والاستراتيجي للدول، وفي مقدمة الأولويات الوطنية التي تستوجب التخطيط طويل المدى والتنسيق المؤسسي الراسخ (كاظم، 2023، ص 301؛ العبداني، 2024، ص 15).

وفي هذا السياق، تبنت دولة قطر مسارًا مؤسسيًا متدرجًا لتطوير قدراتها السيبرانية، بدءًا من الوعي المبكر بأهمية الفضاء الرقمي، مرورًا بإنشاء الجهات المعنية بتنظيم هذا المجال، ووصولاً إلى الاستراتيجية الوطنية للأمن السيبراني 2024-2030، التي تضع الأمن والصمود السيبراني، وحماية البنية التحتية الوطنية الحرجة، والحوكمة والتشريعات، وتنمية الاقتصاد والقدرات البشرية، والتعاون الدولي ضمن إطار وطني متكامل، ويأتي هذا البحث ليحلل هذا الانتقال النوعي من نموذج يركز على الحماية التقنية المنفردة إلى نموذج أشمل يربط الأمن السيبراني بالأمن الوطني والمرونة المؤسسية والابتكار والدبلوماسية السيبرانية، متتبعًا مسار التطور المؤسسي الذي شهدته الدولة في هذا المجال الحيوي، ومحاولاً فهم كيف يمكن لاستراتيجية وطنية أن توفق بين متطلبات الحماية التقنية من جهة، ومتطلبات التنمية الاقتصادية والاجتماعية من جهة أخرى، ومتطلبات التعاون الدولي وبناء الشراكات من جهة ثالثة، بل ومن جهة رابعة تتمثل في بناء القدرات البشرية ونشر الوعي المجتمعي، وهو ما يجعل الاستراتيجية القطرية نموذجًا متكاملًا للتعامل مع التحديات السيبرانية المعاصرة، بما يعكس إدراكًا عميقًا للطبيعة المتشابكة لهذه التحديات (الوكالة الوطنية للأمن السيبراني، 2024).

وتمثل الاستراتيجية الوطنية للأمن السيبراني 2024-2030 نقلة نوعية في التعامل مع المخاطر الرقمية، إذ لم تعد تنظر إلى الأمن السيبراني بوصفه مسألة تقنية بحتة، بل أضحت تتعامل معه باعتباره ركيزة من ركائز الأمن الوطني الشامل، ومدخلًا أساسيًا لتحقيق التنمية المستدامة والحفاظ على السيادة الوطنية في عصر التحول الرقمي المتسارع، وتتجلى أهمية هذه الاستراتيجية في كونها تُصاغ في مرحلة تنسم بتعقيد المشهد التهديدي، حيث تتداخل الهجمات السيبرانية مع الصراعات الجيوسياسية، وتستهدف البنى التحتية الحيوية بأساليب متطورة تعتمد على الذكاء الاصطناعي وتقنيات الحوسبة السحابية وإنترنت الأشياء، مما يستدعي مقاربات متجددة تتجاوز المنظور التقني الضيق إلى رؤية شاملة تدمج الأبعاد القانونية والمؤسسية والبشرية والدولية، ولم تأت هذه الاستراتيجية من فراغ، بل هي نتيج لمسيرة طويلة من التطوير المؤسسي والتشريعي، وتعكس إدراكًا عميقًا من جانب الدولة لأهمية الفضاء السيبراني في تحقيق أهدافها الوطنية، وفي مواجهة التحديات التي يفرضها هذا الفضاء على سيادتها وأمنها، كما تعكس التزامًا واضحًا ببناء قدرات وطنية مستدامة، وبالمشاركة الفاعلة في الجهود الدولية الرامية إلى تعزيز الأمن والاستقرار في الفضاء السيبراني، بما ينسجم مع رؤية قطر الوطنية 2030 التي تجعل من الإنسان والتنمية والعدالة الاجتماعية محاور أساسية للتنمية الشاملة (الوكالة الوطنية للأمن السيبراني، 2024).



مشكلة الدراسة

تتمثل مشكلة الدراسة في أن التطور السريع في البيئة الرقمية يفرض على الدول تجاوز مفهوم الحماية التقنية المنفردة نحو بناء منظومات وطنية قادرة على إدارة المخاطر العابرة للقطاعات والحدود، وهو ما يشكل تحدياً كبيراً للدول التي تسعى إلى حماية مصالحها الوطنية في فضاء سيبراني يتسم بالسيولة وعدم التمايز بين الداخلي والخارجي، ورغم التطور الواضح في المنظومة القطرية للأمن السيبراني، تظل هناك حاجة علمية ملحة إلى دراسة مدى تكامل مكونات الاستراتيجية الوطنية للأمن السيبراني 2024-2030، وبخاصة العلاقة الجدلية بين حماية البنية التحتية الوطنية الحرجة، والحوكمة القانونية والمؤسسية، وبناء القدرات البشرية، والتعاون الدولي والدبلوماسية السيبرانية، وتزداد أهمية هذه الإشكالية لأن الهجمات السيبرانية يمكن أن تمس البنية التحتية الأساسية وتثير قضايا تتعلق بالسيادة والمسؤولية الدولية وقواعد القانون الدولي، مما يجعل التعامل معها مسألة معقدة تتشابك فيها الاعتبارات التقنية مع الأبعاد السياسية والقانونية والاقتصادية، وتتطلب مقاربات متعددة التخصصات لا يمكن أن يختزلها أي نهج أحادي البعد، وهو ما يجعل دراسة الاستراتيجية الوطنية في تكاملها وأبعادها المختلفة ضرورة علمية ملحة لفهم كيفية تعامل الدولة مع هذه التعقيدات (طه، 2024، ص 55؛ الكواري، 2024، ص 300).

وتتعمق هذه الإشكالية عندما نأخذ في الاعتبار أن البنية التحتية الوطنية الحرجة في قطر، والتي تشمل قطاعات الطاقة والغاز والمالية والاتصالات والنقل والصحة والخدمات الحكومية، تمثل قلب الاقتصاد الوطني ومصدراً رئيسياً للدخل القومي، مما يجعل حمايتها من الاختراقات السيبرانية مسألة وجودية بالمعنى الدقيق للكلمة، فالهجوم السيبراني الناجح على إحدى هذه القطاعات قد يؤدي إلى تداعيات كارثية تمتد من تعطيل الإنتاج إلى شل الخدمات الأساسية، ومن فقدان الثقة في الاقتصاد الرقمي إلى التأثير على سمعة الدولة الدولية وقدرتها على جذب الاستثمارات، ومن هنا تبرز الحاجة الملحة إلى دراسة متعمقة لكيفية تعامل الاستراتيجية الوطنية مع هذه التحديات، وما إذا كانت آلياتها وأدواتها قادرة على توفير الحماية المطلوبة في مواجهة التهديدات المتطورة، وكيف يمكن لهذه الاستراتيجية أن توفق بين متطلبات الأمن من جهة ومتطلبات الانفتاح والتعاون الدولي من جهة أخرى، وهو توازن دقيق يتطلب رؤية استراتيجية واضحة وآليات تنفيذ مرنة، وقدرة على التكيف مع المتغيرات السريعة في المشهد التهديدي، فضلاً عن الإرادة السياسية والموارد المالية والبشرية اللازمة للتنفيذ الفعال (الوكالة الوطنية للأمن السيبراني، 2024؛ البدaine، 2024، ص 10).

كما تطرح الإشكالية تساؤلات أعمق حول مدى قدرة الاستراتيجية الوطنية على مواكبة التطورات التكنولوجية المتسارعة، خاصة في مجالات الذكاء الاصطناعي والتعلم الآلي وإنترنت الأشياء والحوسبة السحابية، التي تخلق أدوات هجومية جديدة وتوسع نطاق الهجمات السيبرانية لتشمل أهدافاً لم تكن في الحسبان من قبل، فالتطور التكنولوجي لا يتوقف عند حد معين، بل هو في تسارع مستمر، مما يستدعي استراتيجيات وطنية قادرة على التكيف مع هذه التغيرات، ومواكبتها، بل واستباقها في بعض الأحيان، وهذا يتطلب من الاستراتيجية أن تكون مرنة وقابلة للتحديث، وأن تتضمن آليات للتقييم الدوري والمراجعة المستمرة، وأن تستند إلى رؤية بعيدة المدى تستشرف المستقبل وتستعد له، وأن تبني قدرات بحثية وتطويرية وطنية تمكن الدولة من فهم التهديدات الناشئة وتطوير الحلول المناسبة لها، بدلاً من الاعتماد على الحلول الجاهزة المستوردة التي قد لا تتناسب مع خصوصية البيئة القطرية، بل وقد تشكل في حد ذاتها مخاطر.

السؤال الرئيس وأسئلة الدراسة

ينطلق البحث من السؤال الرئيس الآتي: إلى أي مدى تعكس استراتيجية قطر الوطنية للأمن السيبراني 2024-2030 نموذجاً متكاملًا ينتقل من حماية البنية التحتية الوطنية الحرجة إلى تعزيز الصمود السيبراني والتعاون الدولي والدبلوماسية السيبرانية؟ وهذا السؤال الرئيس يحمل في طياته إشكالية جوهرية تتعلق بقدرة الاستراتيجية على تجاوز النموذج التقليدي للأمن السيبراني الذي يركز على الحماية والدفاع إلى نموذج أشمل يدمج بين الحماية والصمود والاستجابة والتعافي، وبين الأبعاد الداخلية والخارجية للأمن السيبراني. ويتفرع عن هذا السؤال الرئيس عدد من الأسئلة الجزئية التي تسهم في معالجة جوانب الموضوع المختلفة، ونتيج تفكيك الإشكالية الكبرى إلى وحدات تحليلية قابلة للبحث والتحليل، ويمكن صياغتها على النحو التالي:



أولاً: كيف تطورت منظومة الأمن السيبراني في قطر عبر المراحل المؤسسية المختلفة ؟
ثانياً: ما الآليات التي تتبناها الاستراتيجية لحماية البنية التحتية والخدمات الحيوية ؟
ثالثاً: كيف توظف الحوكمة والتشريعات وإدارة المخاطر في تعزيز الأمن الوطني السيبراني ؟
رابعاً: ما موقع تنمية الكفاءات البشرية والابتكار والتقنيات الناشئة ضمن الاستراتيجية ؟
خامساً: كيف يمكن للدبلوماسية السيبرانية أن تصبح أداة فعالة لحماية المصالح الوطنية وتعزيز مكانة الدولة في المجتمع الدولي؟

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف العلمية والتطبيقية المترابطة، التي تتسجم مع طبيعة الموضوع وتعميقاته، وتحدد مسار البحث ومنهجيته، ويمكن إجمالها فيما يلي:

أولاً: تحليل تطور السياسة القطرية للأمن السيبراني منذ نشأتها وحتى إطلاق الاستراتيجية الوطنية 2024-2030، وتتبع المراحل المؤسسية والتشريعية التي شهدتها هذه السياسة، بهدف فهم السياق التاريخي الذي أنتج الاستراتيجية الحالية والأسس التي قامت عليها، والوقوف على الدروس المستفادة من التجارب السابقة التي شكلت منطلقاً للاستراتيجية الجديدة.

ثانياً: تفسير مرتكزات الاستراتيجية الوطنية 2024-2030 وركائزها الأساسية، من خلال قراءة متعمقة لأهدافها وغاياتها ومبادئها التوجيهية، وكشف العلاقات المتبادلة بين هذه الركائز ودور كل منها في تشكيل المنظومة السيبرانية الوطنية، مع تحليل كيف تساهم هذه الركائز في تحقيق الرؤية الوطنية الشاملة لدولة قطر.

ثالثاً: تقييم آليات حماية البنية التحتية الوطنية الحرجة المعتمدة في الاستراتيجية، ودراسة مدى قدرتها على تحقيق الصمود واستمرارية الأعمال في مواجهة الهجمات السيبرانية المتطورة، مع تحليل نقاط القوة والضعف في هذه الآليات، وتحديد الثغرات التي قد تهدد فعاليتها في مواجهة التهديدات المستقبلية.

رابعاً: تحليل منظومة الحوكمة والتشريعات وإدارة المخاطر التي تقوم عليها الاستراتيجية، ودراسة كيفية توزيع الأنوار والمسؤوليات بين الجهات المختلفة، وفعالية الأطر القانونية في دعم الأمن السيبراني وتحقيق الامتثال للمعايير الدولية، مع تقييم مدى كفاية التشريعات القائمة واقتراح مجالات للتطوير التشريعي.

خامساً: بيان دور رأس المال البشري والوعي المجتمعي والابتكار والذكاء الاصطناعي في تعزيز الأمن السيبراني، واستكشاف كيفية استثمار الاستراتيجية في هذه العناصر لبناء قدرات وطنية مستدامة قادرة على مواكبة التطورات التكنولوجية المتسارعة، وتحليل الفجوات في القدرات البشرية وسبل معالجتها.

سادساً: تحليل أبعاد التعاون الدولي القطري في المجال السيبراني، واستشراف إمكانات تطور الدبلوماسية السيبرانية باعتبارها أداة لحماية المصالح الوطنية وبناء الثقة وتبادل المعلومات والخبرات، مع دراسة الفرص والتحديات التي تواجه هذا المسار في ظل التحولات الجيوسياسية الراهنة (دعاس والصومالي، 2023؛ البابلي، 2024).

أهمية الدراسة

تتبع أهمية هذه الدراسة من اعتبارات متعددة تتعلق بالجانب العلمي والتطبيقي والإقليمي والدولي على السواء، ويمكن تفصيلها على النحو الآتي:

أولاً – الأهمية العلمية: تبرز الأهمية العلمية للدراسة من حداثة الاستراتيجية القطرية للأمن السيبراني، إذ لم يمتد على إطلاقها وقت طويل يجعل دراستها أمراً متأخراً، بل هي ما تزال في مراحلها الأولى للتطبيق، مما يجعل دراستها في هذه المرحلة أمراً بالغ الأهمية لفهم اتجاهاتها وتوجهاتها قبل أن تستقر ملامحها بشكل نهائي. كما تبرز من محدودية الدراسات العربية التي تحللها كمنظومة واحدة تجمع الأبعاد التقنية والسياسية والقانونية والدولية في إطار تحليلي متكامل، إذ إن معظم الدراسات المتاحة تتناول جوانب جزئية من الأمن السيبراني، كالجانب التقني أو القانوني أو الإداري، دون أن تقدم قراءة شاملة للاستراتيجية بوصفها وحدة متكاملة، وهو ما



تسعى هذه الدراسة إلى تجاوزه من خلال بناء نموذج تحليلي يجمع بين هذه الأبعاد المختلفة ويكشف العلاقات المتبادلة بينها.

ثانياً - الأهمية التطبيقية: تتمثل الأهمية التطبيقية في تقديم إطار تحليلي يمكن أن يفيد الجهات الحكومية والقطاعات الحيوية والباحثين عند تقييم مستوى التكامل بين الوقاية والاستجابة والتعافي والحوكمة في المنظومة السيبرانية الوطنية. كما يمكن للدراسة أن تقدم توصيات عملية قابلة للتطبيق، تعين صانعي السياسات على تحديد أولوياتهم وتحسين أدائهم في المجال السيبراني، خاصة فيما يتعلق بتطوير مؤشرات القياس وآليات التقييم الدوري للاستراتيجية، وتحديد مجالات التحسين والتطوير الممكنة.

ثالثاً - الأهمية الإقليمية: تتضح الأهمية الإقليمية في إمكانية الاستفادة من التجربة القطرية في الدراسات المقارنة لدول الخليج، خاصة مع تصاعد الارتباط بين الأمن السيبراني والسيادة والأمن الوطني في المنطقة التي تواجه تحديات سيبرانية متشابهة، وتشارك في العديد من الخصائص الاقتصادية والاجتماعية والسياسية، مما يجعل تجربة كل دولة منها ذات قيمة للدول الأخرى، وقابلة للاستفادة منها في تطوير استراتيجياتها الوطنية (كاظم، 2023؛ البداينة، 2024).

رابعاً - الأهمية الدولية: تبرز الأهمية الدولية من خلال ما تقدمه الدراسة من تحليل للبعد الدولي في الاستراتيجية القطرية، ودور الدبلوماسية السيبرانية في تعزيز مكانة قطر على الساحة الدولية، مما يسهم في فهم أوسع للدور القطري في صياغة المعايير والقواعد السيبرانية الدولية، ومشاركتها في الجهود العالمية لمواجهة التهديدات السيبرانية العابرة للحدود.

مبررات اختيار الموضوع

يرتبط اختيار هذا الموضوع بثلاثة مبررات رئيسية، يلتقي كل منها مع الآخر ليؤكد أهمية البحث وأولوته في السياق القطري والخليجي والعربي الأوسع، ويمكن تفصيلها على النحو التالي:

أولها: أن دولة قطر تعتمد بدرجة مرتفعة على البنية الرقمية في القطاعات الحكومية والاقتصادية والخدمية، وهو ما يجعل أمن هذه القطاعات واستمرارية تشغيلها قضية ذات بعد وطني بالغ الخطورة. فالاقتصاد القطري، الذي يقوم إلى حد كبير على صناعة الطاقة والغاز، يعتمد بشكل متزايد على الأنظمة الرقمية في عمليات الإنتاج والنقل والتوزيع، مما يجعله هدفاً جذاباً للهجمات السيبرانية التي قد تستهدف تعطيل هذه العمليات أو التلاعب بها أو ابتزاز الدولة من خلالها. إضافة إلى ذلك، فإن التحول الرقمي الشامل الذي تشهده الدولة في جميع القطاعات يزيد من سطح الهجوم السيبراني ويوسع نطاق التهديدات المحتملة.

وثانيها: أن الاستراتيجية الوطنية الجديدة صيغت في مرحلة تتسارع فيها مخاطر الذكاء الاصطناعي والهجمات على البنية التحتية والجرائم العابرة للحدود. فالتطورات التكنولوجية المتلاحقة، وفي مقدمتها التطبيقات المتقدمة للذكاء الاصطناعي، تخلق أدوات هجومية جديدة لم تكن معروفة من قبل، وتوسع نطاق الهجمات السيبرانية لتشمل أهدافاً لم تكن في الحسبان، مما يستدعي استراتيجيات وطنية قادرة على مواكبة هذه التطورات والتكيف معها، بل واستباقها في بعض الأحيان.

وثالثها: أن التعاون السيبراني الدولي أصبح جزءاً صريحاً من توجه الاستراتيجية القطرية، بما يبرر دراسة العلاقة بين الصمود الداخلي والدور الخارجي في المجال السيبراني. فالاستراتيجية لا تنظر إلى الأمن السيبراني بوصفه شأنًا داخلياً محضاً، بل تعتبر التعاون الدولي وبناء الشراكات الموثوقة ركيزة أساسية من ركائزها، وهو ما يثير تساؤلات حول طبيعة هذا التعاون وآلياته وأهدافه، وكيف يمكن للدبلوماسية السيبرانية أن تسهم في حماية المصالح الوطنية وتعزيز مكانة قطر على الساحة الدولية (البداينة، 2024؛ البابلي، 2024؛ الوكالة الوطنية للأمن السيبراني، 2024).

منهج الدراسة وأدواتها

تعتمد هذه الدراسة على **المنهج الوصفي التحليلي (Descriptive Analytical Approach)** بوصفه المنهج الرئيس والأداة الأساسية للبحث، وذلك لملاءمته لطبيعة الموضوع وتعقيداته، ولقدرته على توفير فهم عميق وشامل للاستراتيجية القطرية ومكوناتها. ويُستخدم هذا المنهج في هذه الدراسة لتحليل تطور البيئة



السيبرانية القطرية عبر المراحل المختلفة، ووصف مكونات الاستراتيجية الوطنية وركائزها وأهدافها، مع تقديم تفسيرات تحليلية للعلاقات بين هذه المكونات ودور كل منها في تشكيل المنظومة الكلية. وينتج هذا المنهج فهم الاستراتيجية بوصفها كياناً متكاملًا، لا مجرد تجميع لسياسات منفصلة، وهو ما يساعد في الكشف عن نقاط التكامل والتناغم بين مكوناتها، وكذلك عن مواطن الخلل أو القصور المحتملة التي قد تعيق تحقيق الأهداف المرسومة.

حدود الدراسة

تحدد حدود هذه الدراسة في ثلاثة أبعاد رئيسية، تضبط نطاق البحث وتمنع التوسع غير المبرر فيه، وتوفر إطارًا واضحًا للقارئ حول ما تتناوله الدراسة وما لا تتناوله، وهذه الحدود هي:

أولاً – الحدود الموضوعية: تتمثل في استراتيجية قطر الوطنية للأمن السيبراني وما يرتبط بها من حماية البنية التحتية الوطنية الحرجة، والحوكمة والتشريعات، وبناء القدرات البشرية والتقنية، والتعاون الدولي والدبلوماسية السيبرانية. ولا تتناول الدراسة موضوعات أخرى في مجال الأمن السيبراني لا ترتبط مباشرة بالاستراتيجية الوطنية، كالجوانب التقنية البحتة للبرمجيات الخبيثة أو آليات التشفير المتقدمة أو تفاصيل البنى التحتية التقنية، إلا بقدر ما تخدم التحليل الأساسي وتوضح السياق العام.

ثانيًا – الحدود المكانية: تقتصر الدراسة على دولة قطر، مع إشارات مرجعية محدودة إلى البيئة الدولية والإقليمية التي تتفاعل معها الدولة في المجال السيبراني. ولا تشمل الدراسة استراتيجيات دول أخرى بطريقة موسعة، وإنما تستعين بها للمقارنة المرجعية المحدودة عند الحاجة، مع التركيز على التجربة القطرية بوصفها وحدة التحليل الأساسية.

ثالثًا – الحدود الزمنية: تركز الدراسة على المرحلة الممتدة من إطلاق الاستراتيجية الوطنية الثانية 2024 حتى عام 2030، مع العودة إلى التطورات السابقة عند الحاجة لتفسير المسار المؤسسي وفهم السياق الذي نشأت فيه الاستراتيجية الحالية. ولا تتناول الدراسة مرحلة ما بعد 2030، إذ إنها خارج النطاق الزمني للاستراتيجية، كما لا تتناول بالتفصيل مرحلة ما قبل 2010 إلا بقدر ما يوضح السياق التطوري.

المبحث الأول: تطور منظومة الأمن السيبراني في قطر والإطار المؤسسي للاستراتيجية

شهدت دولة قطر خلال العقدين الماضيين تحولاً نوعياً في نهجها تجاه الأمن السيبراني، انتقلت فيه من مرحلة الوعي المبكر بأهمية الفضاء الرقمي إلى مرحلة بناء منظومة مؤسسية متكاملة قادرة على مواجهة التحديات السيبرانية المعاصرة، وقد مر هذا التطور بعدة مراحل رئيسية، يمكن تتبعها لفهم السياق الذي نشأت فيه الاستراتيجية الوطنية الحالية، والأسس التي قامت عليها، والجهات الفاعلة في المنظومة السيبرانية الوطنية، ويُعد فهم هذا التطور التاريخي أمراً ضرورياً لتقييم الاستراتيجية الحالية، إذ إنها ليست وليدة لحظة معينة، بل هي نتاج تراكمي لجهود متواصلة وتجارب متراكمة شكلت ملامحها وحددت اتجاهاتها، وقد تميزت هذه المراحل بالتدرج والتراكم، حيث بنت كل مرحلة على ما تحقق في المراحل السابقة، مما يعكس رؤية استراتيجية طويلة المدى في التعامل مع تحديات الفضاء السيبراني (الوكالة الوطنية للأمن السيبراني، 2024؛ كاظم، 2023، ص 301).

المرحلة الأولى: مرحلة الوعي والتأسيس (2000-2010)

في هذه المرحلة المبكرة، بدأت قطر تدرك أهمية الفضاء الرقمي كمجال حيوي يتطلب التنظيم والحماية، وذلك بالتزامن مع التوسع الكبير في استخدام تقنيات المعلومات والاتصالات في مختلف القطاعات، وقد تميزت هذه المرحلة بجهود محدودة نسبياً، ركزت على حماية الأنظمة الحكومية الأساسية ورفع الوعي بمخاطر الفضاء الإلكتروني، دون أن تصل إلى مستوى الاستراتيجية الوطنية المتكاملة، وقد اتسمت هذه المرحلة بطابع تقني في الغالب، حيث اقتصر الجهد على الجوانب الفنية لحماية الشبكات والأنظمة، دون اهتمام كبير بالأبعاد القانونية أو المؤسسية أو الدولية للأمن السيبراني، غير أن هذه المرحلة مثلت الأساس الذي بنيت عليه الجهود اللاحقة، إذ هيأت البيئة لظهور مؤسسات وسياسات أكثر تطوراً في المراحل التالية، ورسخت مفهوم أن الفضاء السيبراني



ليس مجرد مساحة تقنية، بل هو مجال حيوي يتطلب حماية واهتمامًا على المستوى الوطني، كما أن التحديات التي واجهتها الدولة في هذه المرحلة، كالهجمات الإلكترونية الأولية على المواقع الحكومية ومحاولات اختراق الأنظمة، كانت بمثابة جرس إنذار دفع نحو مزيد من الاهتمام بهذا المجال (كاظم، 2023، ص 302؛ العيداني، 2024، ص 15).

المرحلة الثانية: مرحلة بناء المؤسسات (2010-2020)

شهدت هذه المرحلة تطورًا نوعيًا في المنظومة القطرية للأمن السيبراني، تمثل في إنشاء هيئات ومؤسسات متخصصة في هذا المجال، ووضع أولى التشريعات المنظمة للفضاء السيبراني، ويمكن القول إن هذه المرحلة مثلت نقطة تحول حاسمة في مسار الأمن السيبراني القطري، حيث انتقلت الدولة من المقاربة التقنية المنفردة إلى مقاربة مؤسسية أكثر شمولاً، تدمج بين الجوانب التقنية والقانونية والتنظيمية، ومن أبرز ملامح هذه المرحلة إنشاء الوكالة الوطنية للأمن السيبراني، التي أصبحت المظلة المؤسسية الرئيسية للجهود الوطنية في هذا المجال، وتولت مسؤولية تنسيق الجهود بين القطاعات المختلفة ووضع السياسات والأطر التنظيمية اللازمة، وقد مثل إنشاء هذه الوكالة اعترافاً بأهمية الأمن السيبراني كمجال حيوي يتطلب مؤسسة وطنية متخصصة قادرة على تنسيق الجهود وضمان التكامل بين القطاعات المختلفة، ووضع السياسات والأطر التنظيمية اللازمة لمواكبة التطورات المتسارعة في هذا المجال (الوكالة الوطنية للأمن السيبراني، 2024؛ البداينة، 2024، ص 10). كما شهدت هذه المرحلة تطوير أولى التشريعات الوطنية المتعلقة بالجريمة الإلكترونية وحماية البيانات، مما أسهم في توفير إطار قانوني للتعامل مع التهديدات السيبرانية، وإن كان هذا الإطار بحاجة إلى تطوير مستمر لمواكبة التطورات التكنولوجية المتسارعة، وقد مثلت هذه التشريعات نقلة نوعية في التعامل مع الجرائم السيبرانية، حيث وفرت آليات للملاحقة والمحاكمة، وحددت العقوبات المناسبة للمخالفين، مما أسهم في ردع بعض الأنشطة الإجرامية في الفضاء السيبراني (العيداني، 2024، ص 18).

المرحلة الثالثة: مرحلة الاستراتيجية الوطنية الأولى (2020-2024)

في هذه المرحلة، أطلقت قطر أول استراتيجية وطنية للأمن السيبراني، والتي مثلت إطاراً شاملاً للجهود الوطنية في هذا المجال، وحددت الرؤية والأهداف والأولويات للفترة المقبلة، وقد مثلت هذه الاستراتيجية خطوة مهمة نحو تنظيم العمل السيبراني على المستوى الوطني، ووضعت الأسس للتعاون بين القطاعات المختلفة، وحددت مسؤوليات الجهات المعنية، ووضعت آليات للتنفيذ والمتابعة والتقييم، وقد بنت هذه الاستراتيجية على ما تحقق في المراحل السابقة، وسعت إلى تجاوز التحديات التي واجهت تنفيذها، مع التركيز على حماية البنية التحتية الوطنية الحرجة وبناء القدرات البشرية وتعزيز التعاون الدولي (الوكالة الوطنية للأمن السيبراني، 2024). وقد مثلت هذه الاستراتيجية نقطة انطلاق حقيقية للعمل السيبراني المنظم في قطر، ووضعت الأسس التي بنيت عليها الاستراتيجية الحالية، وقدمت دروساً مستفادة في مجالات التنفيذ والتنسيق والتقييم، أفادت في صياغة الاستراتيجية الجديدة وتطوير آلياتها وأدواتها، كما ساهمت في رفع مستوى الوعي الوطني بأهمية الأمن السيبراني، وفي بناء قدرات مؤسسية وبشرية مكنت من الانتقال إلى المرحلة التالية (كاظم، 2023، ص 305؛ البداينة، 2024، ص 15).

المرحلة الرابعة: الاستراتيجية الوطنية 2030-2024

تمثل هذه الاستراتيجية الجديدة نقلة نوعية في المسار القطري للأمن السيبراني، حيث تجاوزت المقاربات التقليدية إلى نموذج متكامل يدمج بين الصمود وحماية البنية التحتية والحوكمة وبناء القدرات والتعاون الدولي (الوكالة الوطنية للأمن السيبراني، 2024). وقد صيغت هذه الاستراتيجية في ضوء التطورات المتسارعة في المشهد التهديدي السيبراني، والتحول التكنولوجي الكبير كالدكاء الاصطناعي وإنترنت الأشياء، والاعتماد المتزايد على الفضاء الرقمي في جميع جوانب الحياة، كما استفادت من الدروس المستفادة من الاستراتيجية السابقة، ومن التطورات العالمية في مجال الأمن السيبراني، ومن أفضل الممارسات الدولية في هذا المجال (البابلي، 2024، ص 138). وتستند الاستراتيجية إلى رؤية واضحة تتمثل في بناء فضاء سيبراني قطري آمن وقادر على الصمود، يسهم في تحقيق أهداف رؤية قطر الوطنية 2030، ويعزز مكانة الدولة كمركز رقمي إقليمي وعالمي موثوق، وهذا الطموح يعكس إدراك قطر لأهمية الفضاء السيبراني في تحقيق التنمية المستدامة، وفي تعزيز مكانتها كدولة رائدة في المنطقة في مجال التحول الرقمي والأمن السيبراني (الوكالة الوطنية للأمن السيبراني، 2024).



وتتميز الاستراتيجية الجديدة بعدة خصائص نوعية تميزها عن سابقتها، من أبرزها: الشمولية، إذ تشمل الاستراتيجية جميع جوانب الأمن السيبراني، من الجانب التقني إلى القانوني إلى المؤسسي إلى البشري إلى الدولي، مما يجعلها إطاراً متكاملًا للعمل الوطني، وهذا الشمول يعكس إدراكاً عميقاً لطبيعة التحديات السيبرانية التي لا يمكن مواجهتها بمعزل عن السياقات الاجتماعية والقانونية والسياسية التي تنشأ فيها (الوكالة الوطنية للأمن السيبراني، 2024). كما تتميز بالتركيز على الصمود، إذ تتجاوز الاستراتيجية مفهوم الحماية التقليدية إلى مفهوم الصمود الذي يشمل القدرة على الاستجابة والتعافي والتكيف، مما يعكس تحولاً في الفكر الأمني من التركيز على المنع إلى التركيز على الاستمرارية، وهذا التحول يعكس تطوراً في فهم طبيعة التهديدات السيبرانية، إذ أصبح واضحاً أن منع جميع الهجمات أمر غير ممكن، وأن القدرة على الاستمرار والتعافي هي ما يحدد مدى نجاح المنظومة السيبرانية (البدائية، 2024، ص 20). وتتميز أيضاً بالتكامل المؤسسي، إذ تعمل الاستراتيجية على تعزيز التنسيق بين الجهات المختلفة، وضمان تكامل أدوارها، وتجنب الازدواجية أو الفجوات، مما يعزز كفاءة المنظومة الوطنية وفعاليتها، وهذا التكامل يتطلب آليات واضحة للتنسيق والتشاور، وقنوات اتصال فعالة بين الجهات المختلفة، وثقافة مؤسسية تشجع على التعاون وتبادل المعلومات (الوكالة الوطنية للأمن السيبراني، 2024). وتتميز أخيراً بالبعد الدولي، إذ تولي الاستراتيجية أهمية خاصة للتعاون الدولي وبناء الشراكات، وتعتبر الدبلوماسية السيبرانية أداة أساسية لتعزيز الأمن الوطني وحماية المصالح الوطنية على الساحة الدولية، وهذا البعد يعكس إدراكاً بأن التهديدات السيبرانية لا تعترف بالحدود، وأن مواجهتها تتطلب تعاوناً دولياً فعالاً، وأن الدبلوماسية السيبرانية يمكن أن تكون أداة فعالة لبناء الثقة وتبادل المعلومات وتعزيز التعاون (الوكالة الوطنية للأمن السيبراني، 2024؛ دعاس والصومالي، 2023، ص 33).

الإطار المؤسسي الحالي

تقوم المنظومة القطرية للأمن السيبراني على مجموعة من الجهات والمؤسسات التي تتكامل أدوارها لتحقيق الأهداف الوطنية، وفي مقدمتها الوكالة الوطنية للأمن السيبراني، التي تتولى مسؤولية الإشراف على تنفيذ الاستراتيجية الوطنية وتنسيق الجهود بين القطاعات المختلفة، وتعمل الوكالة بوصفها الهيئة الوطنية المختصة بشؤون الأمن السيبراني، وتضطلع بمهام متعددة تشمل وضع السياسات والأطر التنظيمية، وتقييم المخاطر، وبناء القدرات، وتعزيز التعاون الدولي، وقد أنشئت الوكالة لتكون المظلة المؤسسية للجهود الوطنية في هذا المجال، ولتضمن التنسيق بين القطاعات المختلفة، ولتكون المرجعية الوطنية في كل ما يتعلق بالأمن السيبراني (الوكالة الوطنية للأمن السيبراني، 2024). كما تشارك في المنظومة جهات أخرى كوزارة الداخلية، ووزارة الاتصالات وتكنولوجيا المعلومات، والبنك المركزي، والجهات المعنية بالقطاعات الحيوية كقطاع الطاقة والمالية والصحة والنقل، مما يشكل نسيجاً مؤسسياً متكاملًا يعمل في إطار تنسيقي موحد، وهذه الجهات تضطلع كل منها بدور محدد في المنظومة، بحسب اختصاصها وطبيعة عملها، مما يحقق التكامل المطلوب ويضمن تغطية جميع جوانب الأمن السيبراني (الوكالة الوطنية للأمن السيبراني، 2024؛ البدائية، 2024، ص 10).

وتتميز المنظومة القطرية بوجود آليات واضحة للتنسيق بين هذه الجهات، من خلال اللجان الوطنية والفرق المشتركة وقنوات التواصل المستمر، مما يساهم في تضافر الجهود وتجنب الازدواجية أو الفجوات، كما تتميز بوجود إطار وطني لإدارة الحوادث السيبرانية، يحدد إجراءات الاكتشاف والاستجابة والتعافي، ويوزع الأدوار بين الجهات المختلفة في حالات الطوارئ السيبرانية، مما يعزز الجاهزية الوطنية لمواجهة الحوادث الكبرى، وهذا الإطار يُعد أداة أساسية لضمان التنسيق في أوقات الأزمات، وتجنب الفوضى والارتباك التي قد تنجم عن وقوع حادث سيبراني كبير، كما يساهم في بناء الثقة بين الجهات المختلفة، من خلال وضوح الأدوار والمسؤوليات (الوكالة الوطنية للأمن السيبراني، د.ت.).



المبحث الثاني: حماية البنية التحتية الوطنية الحرجة والصمود وإدارة الحوادث واستمرارية الخدمات

يمثل هذا المبحث الركيزة الأساسية التي تقوم عليها الاستراتيجية القطرية، حيث تدرك الدولة أن حماية البنية التحتية الوطنية الحرجة من الهجمات السيبرانية ليست مجرد مسألة تقنية، بل هي قضية أمن وطني بامتياز، ترتبط ارتباطاً مباشراً باستقرار الدولة واستمرارية حياتها الاقتصادية والاجتماعية، وقد أولت الاستراتيجية الوطنية للأمن السيبراني 2024-2030 هذا الجانب اهتماماً بالغاً، وجعلت منه أولوية قصوى في أجندتها، وهو ما يعكس إدراكاً عميقاً للطبيعة الاستراتيجية للبنية التحتية الرقمية في عصر التحول الرقمي، حيث أصبحت هذه البنية جزءاً لا يتجزأ من السيادة الوطنية والأمن القومي، وأصبح أي تعطيل لها بمثابة تهديد مباشر للأمن الوطني بأبعاده المختلفة، وقد استندت الاستراتيجية في مقاربتها لحماية البنية التحتية إلى تقييم شامل للمخاطر التي تهدد هذه البنية، وتحديد الأولويات في تخصيص الموارد، وبناء القدرات اللازمة لمواجهة التهديدات المتطورة (الوكالة الوطنية للأمن السيبراني، 2024؛ البداينة، 2024، ص 10؛ الحرماوي، 2026؛ البائع، 2026).

وتشمل البنية التحتية الوطنية الحرجة في قطر قطاعات حيوية متعددة، يتصدرها قطاع الطاقة والغاز الذي يشكل العمود الفقري للاقتصاد الوطني، إذ تعتمد الدولة بشكل كبير على هذا القطاع في توليد الإيرادات الوطنية وتحقيق التنمية الاقتصادية والاجتماعية، وهو ما يجعله هدفاً جذاباً للهجمات السيبرانية التي قد تستهدف تعطيل عمليات الإنتاج أو النقل أو التوزيع، وتلي ذلك قطاعات المالية والاتصالات والنقل والصحة والخدمات الحكومية، التي تشكل معاً النسيج الأساسي للحياة اليومية للمواطنين والمقيمين، وتعطل أي منها قد يؤدي إلى تداعيات خطيرة تمتد إلى جميع مناحي الحياة، وقد راعت الاستراتيجية هذا التنوع في طبيعة القطاعات، ووضعت آليات حماية تتناسب مع خصوصية كل قطاع ومستوى تعرضه للتهديدات السيبرانية، مع مراعاة الترابط بين هذه القطاعات وتأثير أي اختراق في أحدها على باقي القطاعات، إذ إن البنية التحتية الوطنية ليست مجموعة من القطاعات المنعزلة، بل هي منظومة مترابطة يتأثر كل جزء منها بما يحدث في الأجزاء الأخرى (الوكالة الوطنية للأمن السيبراني، 2024؛ البداينة، 2024، ص 10؛ الحرماوي، 2026).

وتعتمد حماية البنية التحتية الوطنية الحرجة في الاستراتيجية القطرية على عدة ركائز متكاملة، يأتي في مقدمتها **تقييم المخاطر المستمر**، حيث تعمل الجهات المعنية على تحديد المخاطر السيبرانية التي تهدد كل قطاع، وتصنيفها وفق درجات الخطورة والأولوية، ووضع خطط للتعامل معها، وهذه العملية ليست ثابتة، بل هي عملية ديناميكية تتطور بتطور المشهد التهديدي، وتستفيد من المعلومات الاستخباراتية وتحليلات التهديدات لتحديث تقييم المخاطر بشكل مستمر، مع الأخذ في الاعتبار التطورات التكنولوجية المتسارعة وظهور أدوات هجومية جديدة، وقد طورت الوكالة الوطنية للأمن السيبراني منهجية متقدمة لتقييم المخاطر، تأخذ في الاعتبار الخصائص الفريدة لكل قطاع، ومستوى تعرضه للتهديدات، والأثر المحتمل لأي اختراق، مما يمكن من تخصيص الموارد بشكل يتناسب مع مستوى المخاطر (الوكالة الوطنية للأمن السيبراني، 2024؛ البابلي، 2024، ص 138؛ السائح، 2026، ص 564). كما تعتمد على تطبيق معايير الأمن السيبراني المعترف بها دولياً، كمعايير المنظمة الدولية للمعايير (ISO) ومعهد المعايير والتقنية الوطني الأمريكي (NIST)، مع تكييفها لتناسب البيئة المحلية واحتياجات القطاعات المختلفة، وضمان الامتثال لها عبر آليات رقابية فعالة، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير معايير وطنية تستند إلى المعايير الدولية، مع إضافة متطلبات إضافية تتناسب مع خصوصية البيئة القطرية واحتياجاتها الفريدة (دعاس والصومالي، 2023، ص 33).

وتولي الاستراتيجية اهتماماً خاصاً بمفهوم **الصمود السيبراني**، الذي يتجاوز مجرد الحماية إلى القدرة على الاستمرار والتعافي، ويعني ذلك أن المنظومة الوطنية لا تكفي بمنع الهجمات، بل تعد نفسها لمواجهةها عندما تحدث، وتضمن استمرار تقديم الخدمات الأساسية في أثناء الهجوم وبعده، وتستعيد الوظائف الحيوية في أقصر وقت ممكن، ويشمل هذا المفهوم عدة عناصر مترابطة، كخطط استمرارية الأعمال (Business Continuity Plans) التي تضمن استمرار تقديم الخدمات الحيوية في جميع الظروف، وخطط التعافي من الكوارث (Disaster Recovery Plans) التي تضمن استعادة الأنظمة والبيانات بعد تعرضها للاختراق أو التلف، وآليات التعلم من الحوادث التي تضمن تحسين الأداء بشكل مستمر، وقد عملت الوكالة الوطنية للأمن السيبراني



على تطوير أطر متكاملة للصمود السيبراني، تشمل الجوانب التقنية والتنظيمية والبشرية، وتضمن استمرارية الخدمات في جميع الظروف (البداية، 2024، ص 20؛ الوكالة الوطنية للأمن السيبراني، 2024). وقد أنشأت قطر إطاراً وطنياً متكاملًا لإدارة الحوادث السيبرانية، يحدد الإجراءات الواجب اتباعها عند وقوع أي حادث سيبراني، بدءاً من الاكتشاف والتبليغ، مروراً بالتحليل والاحتواء، وصولاً إلى الاستعادة والتعافي والتعلم من الحادث، ويُعد هذا الإطار أداة مهمة لضمان التنسيق بين الجهات المختلفة، وتوحيد الجهود، وتجنب الازدواجية أو الفوضى في أوقات الأزمات، حيث يوزع الأدوار والمسؤوليات بين الجهات المختلفة بوضوح، ويحدد قنوات الاتصال وآليات التنسيق في حالات الطوارئ، وقد تم تطوير هذا الإطار بالاستفادة من أفضل الممارسات الدولية، وتكييفها مع البيئة المحلية، مما يضمن فعالية الاستجابة للحوادث وسرعتها (الوكالة الوطنية للأمن السيبراني، د.ت.). ويشمل الإطار أيضاً آليات للتواصل مع الجمهور ووسائل الإعلام، لضمان نقل المعلومات الدقيقة وتجنب الذعر أو الشائعات، وآليات للتعاون مع الشركاء الدوليين عند الحاجة، خاصة في الحالات التي تتطلب معلومات استخباراتية أو خبرات فنية متخصصة، وقد أثبتت التجارب العملية فعالية هذا الإطار في التعامل مع الحوادث السيبرانية المختلفة، وساهم في بناء ثقة الجهات المعنية في قدرة المنظومة الوطنية على إدارة الأزمات السيبرانية (الوكالة الوطنية للأمن السيبراني، د.ت.). وتبرز أهمية هذا الإطار في قدرته على تقليل زمن الاستجابة للحوادث، والحد من آثارها، وضمان استعادة الخدمات بسرعة وكفاءة، وهو ما يمثل جوهر مفهوم الصمود الذي تسعى الاستراتيجية إلى تعزيزه، كما يساهم الإطار في بناء ثقافة الاستعداد والجاهزية في المؤسسات والقطاعات المختلفة، من خلال التدريبات المنتظمة وتمارين المحاكاة التي تختبر جاهزية الفرق وتحدد مجالات التحسين، وقد نظمت الوكالة الوطنية للأمن السيبراني العديد من التمارين والتدريبات التي شاركت فيها مختلف القطاعات الحيوية، مما أسهم في رفع مستوى الجاهزية الوطنية، وتحسين التنسيق بين الجهات المختلفة، وتحديد مجالات التطوير في خطط الاستجابة والتعافي (البداية، 2024، ص 20؛ الوكالة الوطنية للأمن السيبراني، 2024؛ شاهين، 2025).

المبحث الثالث: الحوكمة والتشريعات وإدارة المخاطر

يمثل هذا المبحث العمود الفقري الذي تستند إليه الاستراتيجية القطرية في تنظيم العمل السيبراني وضمان فعاليته واستدامته، إذ لا يمكن للأمن السيبراني أن يتحقق بمجرد توفر الأدوات التقنية، بل يحتاج إلى إطار حوكمة راشد يحدد الأدوار والمسؤوليات، ويضمن التنسيق بين الجهات المختلفة، ويوفر آليات للمساءلة والرقابة، وإلى تشريعات واضحة تحمي الحقوق وتحدد الالتزامات وتوفر آليات للإنفاذ، وإلى نظام متكامل لإدارة المخاطر يحدد الأولويات ويوجه الموارد نحو المجالات الأكثر خطورة، وقد أولت الاستراتيجية الوطنية لهذه الجوانب اهتماماً كبيراً، وأدركت أن نجاح المنظومة السيبرانية الوطنية يتوقف إلى حد كبير على جودة الحوكمة والتشريعات وفعالية إدارة المخاطر (الوكالة الوطنية للأمن السيبراني، 2024؛ البداية، 2024، ص 10).

أولاً: منظومة الحوكمة

تقوم منظومة الحوكمة السيبرانية في قطر على عدة مبادئ أساسية، يأتي في مقدمتها وضوح توزيع الأدوار والمسؤوليات بين الجهات المختلفة المشاركة في تنفيذ الاستراتيجية، حيث تحدد الاستراتيجية بدقة اختصاصات كل جهة، وتجنب التداخل أو الازدواجية أو الفجوات التي قد تعيق التنفيذ الفعال، وقد حرصت الوكالة الوطنية للأمن السيبراني على وضع خرائط واضحة للأدوار والمسؤوليات، وتوزيعها بين الجهات المختلفة بشكل يحقق التكامل ويتجنب التعارض، كما عملت على تطوير آليات للتشاور والتنسيق بين هذه الجهات، لضمان وحدة الرؤية والتكامل في التنفيذ (الوكالة الوطنية للأمن السيبراني، 2024). وتعمل الوكالة الوطنية للأمن السيبراني بوصفها الجهة المنسقة والمنظمة، بينما تضطلع القطاعات الحيوية بمسؤولية تنفيذ متطلبات الأمن السيبراني في مجالاتها، وتحمل مسؤولية حماية أنظمتها وبياناتها، وتلتزم بالإبلاغ عن الحوادث وتبادل المعلومات مع الجهات المعنية، وقد تم تحديد هذه المسؤوليات في وثائق رسمية واضحة، تضمن معرفة كل جهة بواجباتها وحقوقها، وتوفر أساساً للمساءلة والتقييم (الوكالة الوطنية للأمن السيبراني، 2024).

كما تقوم الحوكمة على مبدأ التكامل بين القطاعين العام والخاص، حيث تدرك الاستراتيجية أن الأمن السيبراني مسؤولية وطنية مشتركة، لا يمكن للقطاع العام وحده أن يتحملها، بل تحتاج إلى شراكة حقيقية مع القطاع الخاص الذي يمتلك خبرات تقنية متقدمة وبنى تحتية حيوية، ويعمل في مجالات حساسة كالمالية والاتصالات والطاقة،



وقد عملت الوكالة الوطنية للأمن السيبراني على بناء شراكات استراتيجية مع القطاع الخاص، من خلال آليات واضحة للتعاون وتبادل المعلومات، وحوافز تشجع على الاستثمار في الأمن السيبراني، وتوفير بيئة تنظيمية داعمة للابتكار والاستثمار في هذا المجال، وقد أثبتت هذه الشراكات فعاليتها في تحسين مستوى الأمن السيبراني في القطاعات الحيوية، وتعزيز القدرات الوطنية لمواجهة التهديدات المشتركة (دعاس والصومالي، 2023، ص 33؛ الوكالة الوطنية للأمن السيبراني، 2024). وتشمل آليات التعاون بين القطاعين العام والخاص إنشاء مجالس استشارية تضم ممثلين عن القطاع الخاص، وتنظيم ورش عمل ودورات تدريبية مشتركة، وتبادل المعلومات حول التهديدات والحوادث، والمشاركة في تمارين الاستجابة الوطنية، وقد ساهمت هذه الآليات في بناء الثقة بين القطاعين، وتحسين التنسيق في مواجهة التهديدات المشتركة (الوكالة الوطنية للأمن السيبراني، 2024؛ شاهين، 2025).

ثانياً: الإطار التشريعي

يُعد الإطار التشريعي ركيزة أساسية في منظومة الأمن السيبراني، إذ يوفر الأساس القانوني للتعامل مع التهديدات السيبرانية، ويحدد الجرائم والعقوبات، ويحمي حقوق الأفراد والمؤسسات، وينظم تبادل المعلومات والتعاون بين الجهات المختلفة، وقد شهدت قطر تطوراً تشريعياً في مجال الأمن السيبراني، تمثل في إصدار قوانين لمكافحة الجرائم الإلكترونية، وحماية البيانات الشخصية، وتنظيم الفضاء السيبراني، إلا أن هذه التشريعات ما تزال في حاجة إلى تطوير مستمر لمواكبة التطورات التكنولوجية المتسارعة، وسد الثغرات التي قد تظهر مع ظهور تقنيات جديدة وأدوات هجومية مبتكرة، وقد عملت الوكالة الوطنية للأمن السيبراني على مراجعة الإطار التشريعي بشكل دوري، وتحديد مجالات التطوير المطلوبة، واقتراح التعديلات اللازمة على القوانين القائمة (طه، 2024، ص 55؛ الكواري، 2024، ص 300؛ العيداني، 2024، ص 18؛ الحمدان وحيدري، 2025). وتولي الاستراتيجية الوطنية أهمية خاصة لتطوير الإطار التشريعي، وتعتبره أداة أساسية لتحقيق أهدافها، حيث تسعى إلى تعزيز الامتثال للمعايير الدولية، وتوفير الحماية القانونية للبنية التحتية الوطنية الحرجة، وضمان مساءلة المخالفين، وحماية حقوق الأفراد والمؤسسات في الفضاء السيبراني، وقد حددت الاستراتيجية أولويات تشريعية واضحة، تشمل تطوير قوانين حماية البيانات بما يتوافق مع المعايير الدولية، وتعزيز تشريعات مكافحة الجرائم السيبرانية، وتحديد مسؤوليات مقدمي الخدمات الرقمية، وتنظيم تبادل المعلومات بين القطاعين العام والخاص، ووضع أطر قانونية للتعاون الدولي في المجال السيبراني (الوكالة الوطنية للأمن السيبراني، 2024؛ أبو كليفة وفرج، 2024). وتشمل الأولويات التشريعية أيضاً تطوير قوانين لحماية البنية التحتية الوطنية الحرجة، وتحديد العقوبات المناسبة للهجمات السيبرانية التي تستهدف هذه البنية، وتنظيم استخدام التقنيات الناشئة كالذكاء الاصطناعي في المجال السيبراني، وضمان حماية الخصوصية في عصر التحول الرقمي (الوكالة الوطنية للأمن السيبراني، 2024؛ عطية، 2025).

ثالثاً: إدارة المخاطر

تقوم إدارة المخاطر في الاستراتيجية القطرية على عدة مبادئ أساسية، يأتي في مقدمتها **تحديد الأصول الحيوية وتقييم المخاطر التي تهددها**، حيث تعمل الجهات المعنية على تحديد الأصول الرقمية الأكثر أهمية للدولة، وتقييم المخاطر التي تتعرض لها، وتصنيفها وفق درجات الخطورة والأولوية، وتشمل هذه العملية تحليل التهديدات المحتملة، وتقييم نقاط الضعف في الأنظمة، وتحديد الآثار المحتملة للهجمات، ووضع خطط للتعامل معها، وقد طورت الوكالة الوطنية للأمن السيبراني منهجية متقدمة لتقييم المخاطر، تأخذ في الاعتبار الخصائص الفريدة لكل قطاع، ومستوى تعرضه للتهديدات، والأثر المحتمل لأي اختراق، مما يمكن من تخصيص الموارد بشكل يتناسب مع مستوى المخاطر (الوكالة الوطنية للأمن السيبراني، 2024؛ شاهين، 2025). كما تقوم إدارة المخاطر على مبدأ **التناسب بين التكلفة والفائدة**، حيث توجه الموارد نحو المجالات الأكثر خطورة، وتوازن بين تكلفة الإجراءات الأمنية وفوائدها المتوقعة، وتضمن الاستخدام الأمثل للموارد المتاحة، وتشمل هذه العملية تحديد أولويات الاستثمار في الأمن السيبراني، واختيار الإجراءات الأكثر فعالية من حيث التكلفة، وتقييم العائد على الاستثمار في التدابير الأمنية، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير نماذج لتقييم فعالية التدابير الأمنية من حيث التكلفة، تساعد الجهات المعنية على اتخاذ قرارات استثمارية رشيدة في مجال الأمن السيبراني (شاهين، 2025).



وتولي الاستراتيجية أهمية خاصة للرصد المستمر والتقييم الدوري لإدارة المخاطر، حيث تعمل الجهات المعنية على مراقبة المشهد التهديدي بشكل مستمر، وتحديث تقييم المخاطر، وتعديل الخطط والإجراءات وفقاً للتغيرات في البيئة السيبرانية، وتشمل هذه العملية جمع وتحليل المعلومات الاستخباراتية، ومشاركة المعلومات مع الشركاء، والتعلم من الحوادث السابقة، وتطوير القدرات بشكل مستمر، وقد أنشأت الوكالة الوطنية للأمن السيبراني مراكز عمليات أمنية متطورة، تقوم بمراقبة الفضاء السيبراني القطري على مدار الساعة، وتحليل التهديدات، والاستجابة للحوادث في الوقت الفعلي، مما يعزز قدرة الدولة على الاكتشاف المبكر للهجمات والاستجابة السريعة لها (الوكالة الوطنية للأمن السيبراني، 2024؛ البابلي، 2024، ص 138).

المبحث الرابع: بناء القدرات البشرية والوعي والبحث والابتكار والتقنيات الناشئة

يمثل هذا المبحث الركيزة التي تضمن استدامة المنظومة السيبرانية الوطنية وقدرتها على التكيف مع التطورات المتسارعة في المشهد التهديدي، إذ تدرك الاستراتيجية القطرية أن التقنيات وحدها لا تكفي لتحقيق الأمن السيبراني، بل تحتاج إلى كوادر بشرية مؤهلة، ووعي مجتمعي راسخ، وبحث علمي مبتكر، وتوظيف ذكي للتقنيات الناشئة، وتطوير مستمر للقدرات والمهارات، وقد أولت الاستراتيجية لهذه الجوانب اهتماماً كبيراً، واعتبرتها ركيزة أساسية لتحقيق أهدافها، وأدركت أن الاستثمار في الإنسان هو الاستثمار الأكثر استدامة في مجال الأمن السيبراني، وأن بناء القدرات الوطنية هو الضمان الأساسي لمواجهة التحديات المستقبلية (الوكالة الوطنية للأمن السيبراني، 2024؛ البابلي، 2024، ص 138؛ دعاس والصومالي، 2023، ص 33).

أولاً: بناء القدرات البشرية

تولي الاستراتيجية القطرية اهتماماً بالغاً ببناء القدرات البشرية في مجال الأمن السيبراني، وتعتبره أحد الركائز الأساسية لتحقيق أهدافها، إذ تدرك أن جودة الكوادر البشرية هي العامل الحاسم في فعالية أي منظومة سيبرانية، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير استراتيجية متكاملة لبناء القدرات البشرية، تشمل جميع المستويات، من التعليم الأساسي إلى التدريب المتخصص، ومن استقطاب المواهب إلى تطوير القيادات، وقد وضعت هذه الاستراتيجية أهدافاً واضحة ومؤشرات أداء محددة، لضمان فعالية الجهود واستدامتها (الوكالة الوطنية للأمن السيبراني، 2024). وتشمل جهود بناء القدرات عدة مسارات متكاملة، يأتي في مقدمتها تطوير التعليم والتدريب، من خلال إدراج مفاهيم الأمن السيبراني في المناهج التعليمية على مختلف المستويات، وتوفير برامج تدريبية متخصصة للمهنيين، وإقامة شراكات مع الجامعات ومراكز البحث لتطوير البرامج الأكاديمية في هذا المجال، وقد عملت الوكالة الوطنية للأمن السيبراني بالتعاون مع وزارة التعليم والتعليم العالي على إدماج مفاهيم الأمن السيبراني في المناهج الدراسية، وتطوير برامج أكاديمية متخصصة في الجامعات، وتوفير برامج تدريبية للموظفين في القطاعات الحيوية (دعاس والصومالي، 2023، ص 33؛ الطيب والهوبي والمقرن، 2025).

كما تشمل جهود بناء القدرات جذب الكفاءات والمواهب، من خلال توفير بيئة عمل جاذبة، وحوافز تنافسية، وفرص للتطوير المهني، ومسارات وظيفية واضحة، وبرامج للابتعاث والتدريب الخارجي، وتهدف هذه الجهود إلى سد الفجوة في المهارات السيبرانية التي تعاني منها معظم دول العالم، وضمان توفر الكوادر اللازمة لتنفيذ الاستراتيجية وتحقيق أهدافها، وبناء جيل من المتخصصين القادرين على مواكبة التطورات التكنولوجية والتصدي للتهديدات المتطورة، وقد أطلقت الوكالة الوطنية للأمن السيبراني مبادرات متعددة لجذب المواهب السيبرانية، كبرامج المنح الدراسية، ومسابقات الأمن السيبراني، ومعسكرات التدريب المتخصصة، مما أسهم في بناء مجتمع سيبراني واعد في قطر (البداينة، 2024، ص 20؛ الوكالة الوطنية للأمن السيبراني، 2024).

ثانياً: الوعي والثقافة السيبرانية

تدرك الاستراتيجية أن الأمن السيبراني ليس مسؤولية المؤسسات والجهات الحكومية وحدها، بل هو مسؤولية مشتركة تشمل جميع أفراد المجتمع، ولذلك تولي أهمية كبيرة لنشر الوعي والثقافة السيبرانية بين المواطنين والمقيمين، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير استراتيجية متكاملة للتوعية السيبرانية،



تستهدف جميع فئات المجتمع، من الأطفال إلى كبار السن، ومن الأفراد إلى المؤسسات، باستخدام قنوات متعددة تناسب كل فئة (الوكالة الوطنية للأمن السيبراني، 2024). وتشمل جهود التوعية عدة مسارات، كحملات التوعية العامة عبر وسائل الإعلام ومنصات التواصل الاجتماعي، وبرامج التثقيف في المدارس والجامعات، وورش العمل والندوات المتخصصة، والمواد التوعوية المنشورة على المواقع الإلكترونية والتطبيقات، وقد نفذت الوكالة الوطنية للأمن السيبراني العديد من الحملات التوعوية التي حققت انتشاراً واسعاً في المجتمع، وساهمت في رفع مستوى الوعي بمخاطر الفضاء السيبراني وسبل الحماية منه (جبار، 2025؛ الطيب والوهبي والمقرن، 2025). وتهدف جهود التوعية إلى تمكين الأفراد من حماية أنفسهم ومؤسساتهم من الهجمات السيبرانية، وتعزيز السلوكيات الآمنة في استخدام الفضاء الرقمي، وبناء مجتمع واع بمخاطر الفضاء الإلكتروني وقادر على التعامل معها، والحد من تأثير الهندسة الاجتماعية والاحتيال الإلكتروني الذي يستهدف الأفراد، كما تسهم جهود التوعية في تعزيز الثقة في الاقتصاد الرقمي والخدمات الإلكترونية، ودعم التحول الرقمي الشامل الذي تشهده الدولة، وقد أظهرت الدراسات أن المجتمعات الأكثر وعياً سيبرانياً هي الأقل تأثراً بالهجمات السيبرانية، وأن التوعية تعد أحد أكثر الإجراءات الأمنية فعالية من حيث التكلفة (جبار، 2025؛ العود ومغراف، 2024؛ الوكالة الوطنية للأمن السيبراني، 2024).

ثالثاً: البحث والابتكار

تولي الاستراتيجية أهمية كبيرة للبحث والابتكار في مجال الأمن السيبراني، وتعتبرهما محركين أساسيين لتطوير المنظومة الوطنية وقدرتها على مواكبة التطورات التكنولوجية المتسارعة، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير استراتيجية للبحث والابتكار، تشمل تحديد الأولويات البحثية، وتوفير التمويل للمشاريع البحثية، وبناء الشراكات مع المؤسسات الأكاديمية والبحثية، وتعزيز التعاون بين الأوساط الأكاديمية والصناعية (الوكالة الوطنية للأمن السيبراني، 2024). وتشمل جهود البحث والابتكار عدة مسارات، كدعم البحث العلمي في الجامعات ومراكز البحث، وتوفير التمويل للمشاريع البحثية المبتكرة، وإقامة شراكات مع المؤسسات البحثية الدولية، وتشجيع التعاون بين الأوساط الأكاديمية والصناعية، وقد أنشأت الوكالة الوطنية للأمن السيبراني برامج دعم للبحث العلمي، ومراكز تميز في مجالات الأمن السيبراني المتخصصة، مما أسهم في تطوير معرفة محلية في هذا المجال (البابلي، 2024، ص 138؛ الغامدي، 2025؛ السائح، 2026، ص 564). وتهدف جهود البحث والابتكار إلى تطوير حلول تقنية محلية تتناسب مع خصوصية البيئة القطرية، وتعزيز القدرات الوطنية في مجال اكتشاف الثغرات والتصدي للهجمات، والمساهمة في تطوير المعايير والممارسات الدولية، وبناء صناعة سيبرانية محلية قادرة على تلبية احتياجات السوق المحلي والإقليمي، وقد أسهمت هذه الجهود في تطوير عدد من الحلول التقنية المحلية، وفي بناء قدرات بحثية وطنية متخصصة، مما يعزز استدامة المنظومة السيبرانية الوطنية ويقلل الاعتماد على الحلول المستوردة (الوكالة الوطنية للأمن السيبراني، 2024؛ الصويلح، 2025).

رابعاً: توظيف التقنيات الناشئة

تولي الاستراتيجية اهتماماً خاصاً بتوظيف التقنيات الناشئة في تعزيز الأمن السيبراني، خاصة الذكاء الاصطناعي والتعلم الآلي، اللذين يقدمان إمكانيات هائلة في مجال اكتشاف التهديدات والاستجابة لها بشكل آلي وسريع، وقد عملت الوكالة الوطنية للأمن السيبراني على استكشاف تطبيقات الذكاء الاصطناعي في الأمن السيبراني، وتطوير القدرات الوطنية في هذا المجال، وبناء الشراكات مع الشركات المتخصصة (البابلي، 2024، ص 138؛ السائح، 2026، ص 564). وتشمل تطبيقات الذكاء الاصطناعي في الأمن السيبراني مجالات متعددة، كتحليل السلوك للكشف عن الأنشطة غير المعتادة، والاستجابة الآلية للحوادث، وتحليل كميات ضخمة من البيانات لتحديد الأنماط المشبوهة، والتوقع المبكر للهجمات قبل وقوعها، وتعزيز قدرات التحليل الاستخباراتي، وقد بدأت الوكالة الوطنية للأمن السيبراني في تطبيق بعض هذه التقنيات في مراكز العمليات الأمنية، مما أسهم في تحسين قدرات الاكتشاف والاستجابة، وتقليل زمن الاستجابة للحوادث (البابلي، 2024، ص 138؛ الغامدي، 2025).

كما تشمل التقنيات الناشئة الأخرى التي توليها الاستراتيجية اهتماماً، تقنيات سلسلة الكتل (Blockchain) لتأمين المعاملات والبيانات، وإنترنت الأشياء (IoT) وتحديات تأمين الأجهزة المتصلة، والحوسبة السحابية وتحديات حماية البيانات في البيئات السحابية، والتشفير المتقدم لحماية البيانات في أثناء النقل والتخزين، وتهدف



الاستراتيجية إلى توظيف هذه التقنيات في خدمة الأمن السيبراني الوطني، مع مواكبة المخاطر الجديدة التي قد تخلقها هذه التقنيات نفسها، وضمان التوازن بين الاستفادة من إمكاناتها وإدارة مخاطرها، وقد عملت الوكالة الوطنية للأمن السيبراني على تطوير أطر تنظيمية للتقنيات الناشئة، تضمن استخدامها الآمن والمسؤول، وتحمي من المخاطر المحتملة (الوكالة الوطنية للأمن السيبراني، 2024؛ البابلي، 2024، ص 138؛ البائع، 2026).

المبحث الخامس: التعاون الدولي والدبلوماسية السيبرانية وبناء الثقة والمشاركة في تطوير القواعد الدولية

يمثل هذا المبحث البعد الخارجي للاستراتيجية القطرية، ويعكس إدراك الدولة بأن الأمن السيبراني لا يمكن تحقيقه بمعزل عن البيئة الدولية، وأن التهديدات السيبرانية العابرة للحدود تتطلب تعاوناً دولياً فعالاً لمواجهتها، وأن الدبلوماسية السيبرانية يمكن أن تكون أداة فعالة لحماية المصالح الوطنية وتعزيز مكانة الدولة في المجتمع الدولي، وقد أولت الاستراتيجية الوطنية لهذه الجوانب اهتماماً كبيراً، وأدركت أن التعاون الدولي ليس مجرد خيار، بل ضرورة حتمية في مواجهة التهديدات السيبرانية التي لا تعترف بالحدود، وأن الدبلوماسية السيبرانية يمكن أن تسهم في حماية المصالح الوطنية وتعزيز مكانة الدولة في المجتمع الدولي (الوكالة الوطنية للأمن السيبراني، 2024؛ حسن، 2024، ص 292؛ راضي، 2025، ص 550).

أولاً: أهمية التعاون الدولي في المجال السيبراني

تدرك الاستراتيجية القطرية أن التهديدات السيبرانية لا تعترف بالحدود الوطنية، وأن الهجمات قد تنطلق من أي مكان في العالم وتستهدف أي دولة، مما يجعل التعاون الدولي ضرورة حتمية لمواجهتها، فالهجمات السيبرانية قد تستخدم بنى تحتية في دول مختلفة، وتستغل ثغرات في أنظمة عالمية، وتستهدف مصالح دول متعددة في آن واحد، مما يتطلب تنسيقاً دولياً للتصدي لها، وتبادلاً للمعلومات الاستخباراتية، وتعاوناً في التحقيقات، وتنسيقاً في الردود، وقد عملت قطر على بناء شراكات استراتيجية مع دول صديقة في مجال الأمن السيبراني، وتبادل المعلومات والخبرات، والمشاركة في المبادرات الإقليمية والدولية (طه، 2024، ص 55؛ الكواري، 2024، ص 300؛ الحرماوي، 2026؛ الصويلح، 2025). وتشمل مجالات التعاون الدولي في الاستراتيجية القطرية: تبادل المعلومات حول التهديدات والهجمات، والتعاون في التحقيقات الجنائية، والمشاركة في التمارين الدولية، وبناء القدرات المشتركة، وتطوير المعايير والقواعد الدولية، وقد أثبتت التجارب العملية أن التعاون الدولي الفعال يمكن أن يسهم بشكل كبير في تقليل مخاطر الهجمات السيبرانية، وفي تحسين قدرات الدول على اكتشاف التهديدات والاستجابة لها (الوكالة الوطنية للأمن السيبراني، 2024).

ثانياً: الدبلوماسية السيبرانية كأداة لحماية المصالح الوطنية

تولي الاستراتيجية القطرية أهمية خاصة للدبلوماسية السيبرانية، وتعتبرها أداة أساسية لحماية المصالح الوطنية في الفضاء السيبراني، وتعزيز مكانة الدولة في المجتمع الدولي، وقد عملت قطر على تطوير قدراتها الدبلوماسية السيبرانية، وبناء كوادر دبلوماسية متخصصة في هذا المجال، والمشاركة الفعالة في المحافل الدولية المعنية بالأمن السيبراني (الوكالة الوطنية للأمن السيبراني، 2024؛ حسن، 2024، ص 292). وتشمل الدبلوماسية السيبرانية عدة مسارات، كالمشاركة في المحافل الدولية المعنية بالأمن السيبراني، وبناء الشراكات الثنائية والإقليمية، والمشاركة في تطوير القواعد والمعايير الدولية، وتعزيز الثقة بين الدول، وحل النزاعات الناشئة عن الأنشطة السيبرانية بالوسائل السلمية، وقد شاركت قطر بنشاط في العديد من المحافل الدولية المعنية بالأمن السيبراني، كالأمم المتحدة ومنظماتها المتخصصة، والمنديات الإقليمية، ومجموعات العمل المعنية بالأمن السيبراني (راضي، 2025، ص 550؛ حسن، 2024، ص 292).

وتهدف الدبلوماسية السيبرانية القطرية إلى تحقيق عدة أهداف، من أبرزها: حماية المصالح الوطنية في الفضاء السيبراني، وتعزيز التعاون مع الشركاء الدوليين، والمشاركة في صياغة القواعد الدولية المنظمة للسلوك السيبراني، وتعزيز القدرات الوطنية من خلال الاستفادة من الخبرات الدولية، وبناء سمعة الدولة كفاعل مسؤول في المجال السيبراني، وتعمل قطر من خلال دبلوماسيتها السيبرانية على تعزيز الحوار البناء بين الدول، وبناء



الثقة من خلال الشفافية وتبادل المعلومات، وتعزيز التعاون في مواجهة التهديدات المشتركة، والمشاركة الفعالة في الأطر الإقليمية والدولية المعنية بالأمن السيبراني، وقد أسهمت هذه الجهود في تعزيز مكانة قطر كفاعل دولي مسؤول في مجال الأمن السيبراني (الوكالة الوطنية للأمن السيبراني، 2024؛ راضي، 2025، ص 550).

ثالثاً: المشاركة في تطوير القواعد والمعايير الدولية

تشارك قطر بنشاط في الجهود الدولية لتطوير القواعد والمعايير المنظمة للسلوك السيبراني، إدراكاً منها بأن الفضاء السيبراني يحتاج إلى قواعد واضحة تحكم سلوك الدول والفاعلين فيه، وتحمي السيادة الوطنية، وتحقق الاستقرار والأمن الدوليين، وقد شاركت قطر في العديد من المبادرات الدولية الرامية إلى تطوير قواعد السلوك في الفضاء السيبراني، والمساهمة في الحوارات الدولية حول هذا الموضوع (طه، 2024، ص 55؛ الكواري، 2024، ص 300). وتشمل هذه المشاركة عدة مستويات، كالمشاركة في أعمال الأمم المتحدة والمنظمات الدولية المعنية بالأمن السيبراني، والمساهمة في تطوير المعايير الفنية من خلال المنظمات المعنية، والمشاركة في المبادرات الإقليمية لتعزيز التعاون السيبراني، وبناء الشراكات مع الدول ذات الاهتمام المشترك، وقد أسهمت هذه المشاركة في تعزيز صوت قطر في المحافل الدولية، وفي التأثير في صياغة القواعد والمعايير الدولية التي تخدم مصالحها الوطنية (الوكالة الوطنية للأمن السيبراني، 2024؛ راضي، 2025، ص 550).

وتهدف هذه المشاركة إلى تحقيق عدة غايات، من أبرزها: ضمان احترام السيادة الوطنية في الفضاء السيبراني، وتعزيز الاستقرار والأمن الدوليين، ومنع تحول الفضاء السيبراني إلى ساحة للصراعات، وحماية حقوق الأفراد في الفضاء الرقمي، وتعزيز التعاون الدولي في مواجهة التهديدات المشتركة، وتسهم هذه المشاركة أيضاً في بناء سمعة قطر كدولة فاعلة ومسؤولة في المجتمع الدولي، وتعزيز قدرتها على التأثير في صياغة القواعد والمعايير الدولية التي تخدم مصالحها الوطنية، وحماية بنيتها التحتية الرقمية من التهديدات العابرة للحدود (طه، 2024، ص 55؛ الكواري، 2024، ص 300؛ الوكالة الوطنية للأمن السيبراني، 2024).

رابعاً: بناء الثقة وتبادل المعلومات

تولي الاستراتيجية أهمية خاصة لبناء الثقة بين الدول في المجال السيبراني، وتعتبره شرطاً أساسياً للتعاون الفعال، حيث تدرك أن الشك وعدم الثقة بين الدول يعيقان تبادل المعلومات والتعاون في مواجهة التهديدات المشتركة، وقد عملت قطر على بناء الثقة مع شركائها الدوليين من خلال الشفافية في السياسات والإجراءات، والالتزام بالاتفاقيات الدولية، والمشاركة الفعالة في المبادرات المشتركة (الوكالة الوطنية للأمن السيبراني، 2024؛ حسن، 2024، ص 292). وتشمل جهود بناء الثقة عدة مسارات، كالشفافية في السياسات والإجراءات، وتبادل المعلومات حول التهديدات والهجمات، والمشاركة في التمارين المشتركة، وبناء قنوات اتصال مباشرة بين الجهات المعنية، والالتزام بالقواعد والمعايير الدولية، وقد أنشأت قطر قنوات اتصال مع شركائها الدوليين لتبادل المعلومات حول التهديدات السيبرانية، والمشاركة في التمارين المشتركة لتعزيز التنسيق وبناء الثقة (راضي، 2025، ص 550).

ويهدف تبادل المعلومات إلى تعزيز قدرات الدول على اكتشاف التهديدات والاستجابة لها، وتحسين التنسيق في مواجهة الهجمات العابرة للحدود، وبناء قاعدة معرفية مشتركة حول التهديدات السيبرانية، وتعزيز الثقة بين الدول من خلال التعاون العملي، وتعمل قطر من خلال شراكاتها الدولية على تبادل المعلومات الاستخباراتية حول التهديدات الناشئة، والتعاون في تحليل الحوادث وتحديد مصادرها، والمشاركة في المبادرات الدولية لتبادل المعلومات، وبناء قدرات الدول النامية في مجال الأمن السيبراني، وقد أثبتت هذه الجهود فعاليتها في تحسين قدرات قطر على اكتشاف التهديدات والاستجابة لها، وتعزيز علاقاتها مع شركائها الدوليين (الوكالة الوطنية للأمن السيبراني، 2024؛ حسن، 2024، ص 292).

الخاتمة

في خاتمة هذا البحث الذي تناول استراتيجية قطر الوطنية للأمن السيبراني 2024-2030، وتحليل انتقالها من حماية البنية التحتية الوطنية الحرجة إلى التعاون الدولي والدبلوماسية السيبرانية، نخلص إلى جملة من النتائج والتوصيات، نرجو أن تكون إضافة علمية مفيدة، ومعيناً للباحثين والممارسين في هذا المجال الحيوي، فقد تبين من خلال التحليل الوصفي المتعمق للاستراتيجية أنها تمثل نقلة نوعية في التعامل مع التحديات السيبرانية،



وتجسد رؤية متكاملة تجمع بين الأبعاد التقنية والقانونية والمؤسسية والبشرية والدولية، مما يجعلها نموذجًا متقدمًا في المنطقة العربية، وقابلًا للاستفادة منه في الدراسات المقارنة، كما تبين أن نجاح هذه الاستراتيجية يتوقف على عوامل متعددة تتجاوز النص المكتوب، كالإرادة السياسية، والموارد المخصصة للتنفيذ، ومستوى التنسيق بين الجهات المختلفة، وقدرة الدولة على التكيف مع التغيرات السريعة في المشهد التهديدي السيبراني، وهو ما يستوجب متابعة دقيقة وتقييمًا مستمرًا لضمان تحقيق الأهداف المرسومة.

النتائج

توصلت الدراسة بعد التحليل الوصفي المتعمق للاستراتيجية الوطنية للأمن السيبراني 2024-2030 إلى مجموعة من النتائج المهمة، يمكن إجمالها على النحو التالي:

النتيجة الأولى: أثبتت الدراسة أن الاستراتيجية القطرية للأمن السيبراني تمثل انتقالًا نوعيًا من مفهوم الحماية السيبرانية التقليدية إلى نموذج صمود وطني متعدد الأطراف، يدمج بين الوقاية والاستجابة والتعافي والحوكمة وبناء القدرات والتعاون الدولي في منظومة متكاملة، وهذا الانتقال يعكس تطورًا في الفكر الأمني القطري، وتجاوزًا للنموذج التقني الضيق إلى رؤية شاملة تدمج الأبعاد المختلفة للأمن السيبراني، بما ينسجم مع التطورات العالمية في هذا المجال، ويؤكد أن الدولة قد أدركت أن الأمن السيبراني لم يعد مجرد مسألة تقنية يمكن عزلها عن باقي جوانب السياسة الوطنية، بل أصبح جزءًا لا يتجزأ من الأمن الوطني الشامل، ومن متطلبات التنمية المستدامة، ومن مقومات السيادة الوطنية في العصر الرقمي، وهذا الإدراك يعكس نضجًا في الفكر الاستراتيجي القطري، واستجابة للتحويلات العالمية في مفهوم الأمن والأمان في الفضاء السيبراني.

النتيجة الثانية: أظهرت الدراسة أن حماية البنية التحتية الوطنية الحرجة لا يمكن فصلها عن الحوكمة والقدرات البشرية والتعاون الخارجي، إذ إن هذه العناصر تشكل معًا نسيجًا مترابطًا لا يمكن فهم أحد أجزائه بمعزل عن الآخر، وتتجلى هذه التكاملية في تصميم الاستراتيجية، حيث ترتبط كل ركيزة منها بالآخرى، وتعمل جميعها في تنافس لتحقيق الهدف الوطني المنشود، وقد تبين أن نجاح الاستراتيجية يتوقف على مدى التنسيق بين هذه الركائز، وليس على قوة أي منها بمعزل عن الأخرى، إذ إن الخلل في أي ركيزة قد يؤدي إلى إضعاف المنظومة بأكملها، وجعلها عرضة للاختراقات والهجمات، وهذا ما يفسر الحرص الكبير الذي أبدته الاستراتيجية في معالجة جميع هذه الأبعاد في إطار متكامل، وفي وضع آليات واضحة للتنسيق بينها، لضمان تحقيق التكامل المنشود.

النتيجة الثالثة: كشفت الدراسة عن أن التعاون الدولي في الاستراتيجية القطرية لا يُنظر إليه بوصفه مسارًا منفصلًا عن الأمن الوطني، بل هو امتداد طبيعي له، حيث تسعى الدولة من خلاله إلى حماية مصالحها الوطنية وتعزيز مكانتها الدولية في المجال السيبراني، وهذا التصور المتكامل يمثل تطورًا مهمًا في الفكر الاستراتيجي القطري، ويعكس إدراكًا لطبيعة التهديدات العابرة للحدود التي لا يمكن لأي دولة مواجهتها بمفردها، مما يجعل التعاون الدولي ضرورة حتمية وليس خيارًا، كما يعكس إدراكًا لأهمية الدبلوماسية السيبرانية كأداة لحماية المصالح الوطنية وتعزيز مكانة الدولة في المجتمع الدولي، وقد تجلّى هذا الإدراك في تولي الاستراتيجية التعاون الدولي مكانة رفيعة بين ركائزها، وتخصيصه بآليات وأهداف واضحة، وجعله جزءًا لا يتجزأ من الرؤية الوطنية للأمن السيبراني.

النتيجة الرابعة: أظهرت الدراسة أن الاستراتيجية تولي اهتمامًا بالغًا ببناء القدرات البشرية والوعي المجتمعي، وتعتبرهما ركيزة أساسية لاستدامة المنظومة السيبرانية الوطنية، وهو ما يمثل استثمارًا طويل المدى في الأمن الوطني، ويعكس فهماً عميقاً لأهمية العنصر البشري في تحقيق الأمن السيبراني، إذ تبين أن التقنيات المتطورة وحدها لا تكفي إذا لم تتوافر الكوادر البشرية القادرة على تشغيلها وتطويرها، وأن الوعي المجتمعي هو خط الدفاع الأول في مواجهة العديد من الهجمات السيبرانية التي تستهدف العنصر البشري عبر الهندسة الاجتماعية والاحتيال الإلكتروني، وقد تجلّى هذا الاهتمام في تخصيص الاستراتيجية مساحة واسعة لبناء القدرات البشرية، وفي وضع خطط طموحة لتطوير التعليم والتدريب وجذب المواهب ونشر الوعي، مما يعكس رؤية مستقبلية تستشرف متطلبات المرحلة القادمة.

النتيجة الخامسة: أكدت الدراسة أن الحوكمة والتشريعات تشكلان العمود الفقري للمنظومة السيبرانية الوطنية، إذ لا يمكن للأمن السيبراني أن يتحقق بمجرد توفر الأدوات التقنية، بل يحتاج إلى إطار حوكمة راشد يحدد الأدوار والمسؤوليات، ويضمن التنسيق بين الجهات المختلفة، ويوفر آليات للمساءلة والرقابة، وإلى تشريعات



واضحة تحمي الحقوق وتحدد الالتزامات وتوفر آليات للإنفاذ، وقد تبين من خلال التحليل أن الاستراتيجية أولت هذه الجوانب اهتماماً كبيراً، وأدركت أن نجاح المنظومة السيبرانية الوطنية يتوقف إلى حد كبير على جودة الحوكمة وفعالية التشريعات، وهو ما انعكس في وضع أطر تنظيمية واضحة، وتوزيع دقيق للأدوار والمسؤوليات، وفي تحديد أولويات تشريعية طموحة تسعى إلى تطوير الإطار القانوني بشكل مستمر لمواكبة التطورات التكنولوجية المتسارعة.

النتيجة السادسة: بينت الدراسة أن الاستراتيجية القطرية تمثل نموذجاً متقدماً في المنطقة العربية من حيث شموليتها وتكامل أبعادها، وقدرتها على تحقيق التوازن بين متطلبات الأمن من جهة ومتطلبات التنمية والانفتاح الدولي من جهة أخرى، مما يجعلها نموذجاً يمكن الاستفادة منه في الدراسات المقارنة لدول الخليج والمنطقة العربية، وقد تبين أن الاستراتيجية استفادت من أفضل الممارسات الدولية، مع تكيفها لتناسب مع خصوصية البيئة القطرية، وهو ما يمثل توازناً دقيقاً بين الاستفادة من الخبرات العالمية والحفاظ على الخصوصية الوطنية، وقد أسهم هذا التوازن في بناء منظومة سيبرانية وطنية تستند إلى أسس علمية رصينة، مع مراعاة الظروف المحلية والخصائص الفريدة للبيئة القطرية، مما يعزز فرص نجاحها واستدامتها.

النتيجة السابعة: كشفت الدراسة أن الاستراتيجية تولي اهتماماً خاصاً بالتقنيات الناشئة، وفي مقدمتها الذكاء الاصطناعي، وتعتبره أداة محورية لتعزيز الأمن السيبراني، وقد تبين أن الاستراتيجية لا تنظر إلى هذه التقنيات بوصفها مجرد أدوات مساعدة، بل تعتبرها محركات أساسية لتطوير المنظومة الوطنية وقدرتها على مواكبة التطورات المتسارعة، وقد تجلّى هذا الاهتمام في تخصيص مساحة واسعة للحديث عن التقنيات الناشئة، وفي وضع خطط طموحة لتوظيفها في خدمة الأمن السيبراني الوطني، مع إدراك المخاطر الجديدة التي قد تخلقها هذه التقنيات نفسها، ووضع أطر تنظيمية لضمان استخدامها الآمن والمسؤول، مما يعكس رؤية متقدمة تستشرف المستقبل وتستعد له.

النتيجة الثامنة: أظهرت الدراسة أن الاستراتيجية تدرك أهمية الصمود السيبراني كهدف استراتيجي يتجاوز مجرد الحماية، وقد تجلّى هذا الإدراك في التركيز الكبير على القدرة على الاستجابة السريعة للهجمات، واستعادة الخدمات الحيوية في أقصر وقت ممكن، والتعلم من الحوادث لتحسين الأداء بشكل مستمر، وهذا التركيز يعكس تحولاً في الفكر الأمني من التركيز على المنع إلى التركيز على الاستمرارية، ومن الاعتماد على الدفاعات السلبية إلى بناء قدرات نشطة للاستجابة والتعافي، وهو ما ينسجم مع أفضل الممارسات الدولية في مجال الأمن السيبراني.

التوصيات

بناءً على النتائج التي توصلت إليها الدراسة، تقترح الباحثة مجموعة من التوصيات العملية، التي يمكن أن تسهم في تعزيز فعالية الاستراتيجية الوطنية وتحقيق أهدافها على نحو أفضل، مع الأخذ في الاعتبار التحديات والفرص التي تطرحها البيئة السيبرانية المتغيرة باستمرار:

التوصية الأولى: تطوير مؤشرات قياس واضحة ودقيقة لدرجة الصمود السيبراني على مستوى الدولة والقطاعات الحيوية، تمكن من التقييم الدوري للأداء وتحديد مجالات التحسين، وتوفير قاعدة بيانات للتعليم من التجارب وتحسين الاستجابة للحوادث المستقبلية، مع مراعاة أن تكون هذه المؤشرات قابلة للقياس والمقارنة، وتغطي جميع جوانب الصمود السيبراني، من الوقاية والاكتشاف إلى الاستجابة والتعافي، ومن الجوانب التقنية إلى التنظيمية والبشرية، كما ينبغي أن ترتبط هذه المؤشرات بأهداف الاستراتيجية بشكل مباشر، وتستخدم في تقارير الأداء الدورية التي ترفع للجهات العليا.

التوصية الثانية: توسيع نطاق تمارين الاستجابة الوطنية المشتركة، وإشراك القطاعات الحيوية كافة في هذه التمارين، بما يعزز التنسيق والجاهزية لمواجهة الحوادث السيبرانية الكبرى، ويختبر فعالية خطط الاستجابة والتعافي في ظروف تحاكي الواقع، مع التركيز على السيناريوهات المعقدة التي تتطلب تنسيقاً بين قطاعات متعددة، كما ينبغي أن تشمل هذه التمارين جميع المستويات، من المستوى التقني إلى المستوى الاستراتيجي، وأن يتم تقييمها بشكل دقيق واستخلاص الدروس المستفادة منها، وتحديث الخطط والإجراءات بناءً على هذه الدروس.

التوصية الثالثة: تعزيز آليات تبادل معلومات التهديدات بين القطاعات المختلفة، وإنشاء منصات وطنية لتجميع وتحليل هذه المعلومات واستخلاص الدروس المستفادة منها، مع ضمان سرية المعلومات وحماية مصادرها،



وتوفير آليات للتبادل الآمن والفعال مع الشركاء الدوليين، كما ينبغي تطوير قدرات تحليل المعلومات الاستخباراتية، والاستفادة من تقنيات الذكاء الاصطناعي في تحليل كميات ضخمة من البيانات، وتحديد الأنماط والاتجاهات التي قد تشير إلى تهديدات ناشئة، وتحسين القدرة على التوقع المبكر للهجمات.

التوصية الرابعة: دعم البحث الجامعي والصناعة السيبرانية المحلية، من خلال حوافز مالية ومعنوية تشجع على الابتكار في المجال السيبراني، وتطوير حلول تقنية محلية تتناسب مع خصوصية البيئة القطرية، مع إقامة مراكز تميز بحثية في مجالات الأمن السيبراني المتخصصة، وجذب الكفاءات والمواهب للعمل في هذه المراكز، كما ينبغي تعزيز التعاون بين الأوساط الأكاديمية والصناعية، وتوفير التمويل للمشاريع البحثية المبتكرة، ودعم نشر نتائج البحوث في المجالات العلمية المحكمة، والاستفادة من التجارب الدولية الناجحة في هذا المجال.

التوصية الخامسة: تطوير مسار مؤسسي للدبلوماسية السيبرانية يربط الجهات التقنية والقانونية والدبلوماسية في إطار عمل موحد، ويسهم في بناء شراكات دولية فعالة وتعزيز المشاركة في الأطر الإقليمية والدولية المعنية بالأمن السيبراني، مع بناء قدرات دبلوماسية متخصصة في هذا المجال، وتوفير التدريب المستمر للدبلوماسيين في قضايا الأمن السيبراني، كما ينبغي وضع استراتيجية واضحة للدبلوماسية السيبرانية، تحدد الأهداف والغايات والأولويات، وتوزع الأدوار والمسؤوليات بين الجهات المختلفة، وتوفر آليات للتنسيق والتشاور.

التوصية السادسة: العمل على تعزيز الثقافة السيبرانية في المجتمع القطري من خلال حملات توعية مستدامة تستهدف جميع الفئات، واستخدام وسائل الإعلام ومنصات التواصل الاجتماعي لنشر الوعي بمخاطر الفضاء السيبراني وسبل الحماية منه، وإدماج مفاهيم الأمن السيبراني في المناهج التعليمية على مختلف المستويات، مع مراعاة اختلاف الفئات العمرية والمستويات التعليمية، وتوفير مواد توعوية متنوعة تناسب كل فئة، كما ينبغي تنظيم فعاليات توعوية دورية، كالمؤتمرات والندوات وورش العمل، وإشراك المجتمع المدني والقطاع الخاص في جهود التوعية.

التوصية السابعة: تطوير الإطار التشريعي للأمن السيبراني بشكل مستمر لمواكبة التطورات التكنولوجية المتسارعة، وسد الثغرات التي قد تظهر مع ظهور تقنيات جديدة وأدوات هجومية مبتكرة، مع مراعاة التوازن بين متطلبات الأمن وحماية الحقوق والحريات، وبين حماية المصالح الوطنية ومتطلبات التعاون الدولي، كما ينبغي إجراء مراجعة دورية للتشريعات القائمة، وتحديد مجالات التطوير المطلوبة، واقتراح التعديلات اللازمة على القوانين، والمشاركة في تطوير التشريعات الدولية في هذا المجال.

التوصية الثامنة: تعزيز التعاون مع القطاع الخاص من خلال حوافز تشجع على الاستثمار في الأمن السيبراني، وتوفير بيئة تنظيمية داعمة، وبناء شراكات استراتيجية تسهم في تبادل الخبرات وتطوير الحلول، مع إنشاء مجالس استشارية تضم ممثلين عن القطاع الخاص للمشاركة في صياغة السياسات والأطر التنظيمية، كما ينبغي توفير آليات للتبادل الآمن للمعلومات بين القطاعين العام والخاص، وتنظيم فعاليات دورية تجمع الجهات من كلا القطاعين، وتعزيز ثقافة التعاون والشراكة في مواجهة التهديدات المشتركة.

التوصية التاسعة: وضع آلية وطنية للتقييم الدوري للاستراتيجية، تضمن متابعة تنفيذها بشكل مستمر، وتقييم مدى تحقيقها للأهداف المرسومة، وتحديد العوائق التي تواجه تنفيذها، واقتراح الحلول المناسبة لها، كما ينبغي أن تشمل هذه الآلية مؤشرات أداء واضحة، وتقارير دورية ترفع للجهات العليا، ومشاركة واسعة من جميع الجهات المعنية، والاستفادة من التجارب الدولية في مجال تقييم الاستراتيجيات الوطنية للأمن السيبراني.

التوصية العاشرة: العمل على تعزيز الابتكار في مجال الأمن السيبراني، من خلال إنشاء حاضنات أعمال ومسرعات متخصصة في هذا المجال، وتوفير التمويل للمشاريع الابتكارية، وتشجيع ريادة الأعمال السيبرانية، وإقامة مسابقات وجوائز تشجع على الابتكار، وبناء شراكات مع المؤسسات الدولية المتخصصة في هذا المجال، كما ينبغي توفير بيئة تنظيمية داعمة للابتكار، وإزالة العوائق التي قد تحول دون تطوير الحلول المبتكرة، وتعزيز ثقافة الابتكار في المؤسسات والقطاعات المختلفة.

ثالثاً: خاتمة البحث

في ختام هذا البحث، نؤكد على أن استراتيجية قطر الوطنية للأمن السيبراني 2024-2030 تمثل خطوة نوعية في مسار تعزيز الأمن الوطني وحماية المصالح الحيوية للدولة في الفضاء الرقمي، وقد تبين من خلال التحليل أنها استراتيجية طموحة ومتكاملة، تستند إلى رؤية واضحة وأسس علمية رصينة، وتجمع بين الأبعاد التقنية



والقانونية والمؤسسية والبشرية والدولية في إطار متكامل، مما يجعلها نموذجاً متقدماً يمكن أن يُحتذى به في المنطقة العربية، غير أن نجاح هذه الاستراتيجية لا يتوقف على النص المكتوب وحده، بل يتطلب إرادة سياسية قوية، وموارد مالية وبشرية كافية، وتنسيقاً فعالاً بين جميع الجهات المعنية، ومتابعة دقيقة وتقييماً مستمراً، وقدرة على التكيف مع المتغيرات السريعة في المشهد التهديدي السيبراني.

كما نؤكد على أن الأمن السيبراني لم يعد رفاهية أو خياراً، بل أصبح ضرورة حتمية للدول في العصر الرقمي، وأصبح جزءاً لا يتجزأ من الأمن الوطني الشامل، ومن متطلبات التنمية المستدامة، ومن مقومات السيادة الوطنية، ومن ثم فإن الاستثمار في الأمن السيبراني هو استثمار في المستقبل، وفي استقرار الدولة وأمنها وازدهارها، وفي مكانتها على الساحة الدولية، ونأمل أن تكون هذه الدراسة قد قدمت إضافة علمية مفيدة في هذا المجال، وأن تسهم في تعزيز الوعي بأهمية الأمن السيبراني، وفي تطوير السياسات والاستراتيجيات الوطنية في هذا المجال الحيوي.

وختاماً، فإن الباحثة تثنى الجهود الكبيرة التي تبذلها دولة قطر ممثلة في الوكالة الوطنية للأمن السيبراني وسائر الجهات المعنية في سبيل تعزيز الأمن السيبراني الوطني، وتؤكد على أهمية استمرار هذه الجهود وتطويرها، والاستفادة من الدروس المستفادة والتجارب الدولية الناجحة، والمشاركة الفعالة في الجهود الدولية لتعزيز الأمن والاستقرار في الفضاء السيبراني، كما تأمل أن تكون هذه الدراسة خطوة في طريق تعزيز البحث العلمي في مجال الأمن السيبراني، وأن تسهم في فتح آفاق جديدة للبحث والدراسة في هذا المجال الحيوي والمتجدد.

المصادر

1. أبو كطفية، علي عبد الستار، وفرج، ريماء. (2024). المسؤولية المدنية لمقدمي خدمات الأمن السيبراني. المجلة العربية للعلوم الإنسانية والاجتماعية، (23). <https://doi.org/10.59735/arabjhs.vi23.1264>
2. البابلي، عمار ياسر محمد زهير. (2024). دور الذكاء الاصطناعي في مواجهة الجريمة المنظمة عبر العالم الافتراضي: دراسة تحليلية. مجلة الدراسات القانونية والأمنية، 4(2)، 137-207. <https://jlss.moi.gov.qa/index.php/PAJ/article/view/130>
3. البائع، فارس محمد عبد المحسن. (2026). الحماية الدولية للبنية التحتية الرقمية الحيوية: الكابلات تحت سطح البحر والأقمار الصناعية ومراكز البيانات. مجلة العلوم التربوية والدراسات الإنسانية، (51). <https://doi.org/10.55074/hesj.vi51.1662>
4. البداينة، ذياب موسى. (2024). الإرهاب السيبراني والتقنيات الناشئة: تحديات الأمن الوطني السيبراني والسيادة الوطنية. مجلة الدراسات القانونية والأمنية، 4(1)، 7-72. <https://jlss.moi.gov.qa/index.php/PAJ/article/view/122>
5. حسن، راغب فالح. (2024). ممارسة الدبلوماسية الرقمية في ظل العصر الرقمي. مجلة المستنصرية للدراسات العربية والدولية، 21(86)، 305-305. <https://doi.org/10.35710/mjais.v21i86.454291>
6. الحمدان، سجاد صبار رزاق ساجت، وحيدري، إلهام. (2025). الإطار القانوني لحماية الأمن السيبراني في العراق: دراسة تحليلية في ضوء التشريعات الوطنية والمعايير الدولية. مجلة دراسات البصرة، 2(62)، 89-114. <https://bsj.uobasrah.edu.iq/index.php/bsj/article/view/347>
7. الحرماوي، محمد. (2026). الهجمات السيبرانية على البنية التحتية للدول. *Revue Internationale des Etudes Juridiques et Economiques* (3). <https://doi.org/10.34874/PRSM.burak-vol3iss3.87573>
8. دعاس، رانيا محمد سمير، والصومالي، صباح عبد الله. (2023). دور تطبيق معايير الأمن السيبراني على التميز التنظيمي: دراسة ميدانية على أعضاء هيئة التدريس في جامعة طيبة بالمدينة المنورة لعام 2023/2022. مجلة العلوم الاقتصادية والإدارية والقانونية، 7(10)، 33-49. <https://journals.ajsrp.com/index.php/jeals/ar/article/view/7036>



9. راضي، زينب عباس. (2025). فاعلية الأمن السيبراني في السياسة العالمية: المفهوم والتدابير الأمنية للدول. مجلة آشور للعلوم القانونية والسياسية، (1)2، 548-561. <https://doi.org/10.64184/ajlps.V2.I1.Y2025.P561-561.184>
10. السائح، سناء أحمد محمد. (2026). دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: التحديات والآليات والأفاق المستقبلية. مجلة الفاروق للعلوم، (1)2، 563-574. <https://afjs.histr.edu.ly/index.php/afjs/ar/article/view/76>
11. الصويلح، سعد مفلح حمود. (2025). المواجهة الأمنية للاختراقات الإلكترونية المستحدثة المؤثرة على الأمن القومي. المجلة العربية للدراسات الأمنية، (1)41، 17-33. <https://doi.org/10.26735/GMHF2653>
12. شاهين، منار حلمي أحمد. (2025). الإفصاح عن استراتيجيات إدارة المخاطر السيبرانية ضمن تقرير إدارة مخاطر الأمن السيبراني: دوافع وتحديات التطبيق وآليات التطوير. مجلة الإبداع المحاسبي، (1)2، 179-193. https://mbs.journals.ekb.eg/?_action=article
13. الطيب، عهد عبدالقادر، والوهبي، نجلاء تركي، والمقرن، نوره أحمد. (2025). درجة وعي طالبات الدراسات العليا في جامعة الملك سعود بالأمن السيبراني. مجلة العلوم التربوية والنفسية، 9(7)، ملحق، 1-14. <https://doi.org/10.26389/AJSRP.E16012522>
14. عطية، أحمد حاتم جبار. (2025). الأبعاد القانونية والاجتماعية للأمن السيبراني. مجلة الشرق الأوسط للدراسات القانونية والفقهية، 5(3)، 454-454. <https://doi.org/10.56961/mejljs.v5i3.1080439>
15. العيداني، محمد. (2024). التهديدات السيبرانية وجرائم المعلومات. مجلة الاجتهاد للدراسات القانونية والاقتصادية، 13(1)، 30-30. <https://doaj.org/article/12cd9e4f16ea45b18a55a2fb224f1bb315>
16. الغامدي، عبد الله سعد. (2025). الأمن السيبراني والذكاء الاصطناعي: حلول لإدارة أزمات البنية التحتية الرقمية. مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي، 45(2)، المقالة https://digitalcommons.aaru.edu.jo/jaaru_rhe/vol45/iss02/5/5
17. جبار، صفاء علي. (2025). دور الإعلام الرقمي في توعية الجمهور العراقي بمخاطر وجرائم الأمن السيبراني. مجلة واسط للعلوم الإنسانية، 21(2)، 829-849. <https://doi.org/10.31185/wjfh.Vol21.Iss2.908>
18. كاظم، إسراء عبد علي. (2023). التحديات الأمنية في قطر. مجلة حمورابي للدراسات، 12(45)، 301-312. <https://hamm-journal.org/index.php/HJS/article/view/284>
19. الكواري، خليفة أحمد. (2024). قابلية تطبيق القانون الدولي الإنساني في الفضاء السيبراني. مجلة الدراسات القانونية والأمنية، 4(2)، 299-327. <https://jlss.moi.gov.qa/index.php/PAJ/article/view/132>
20. طه، بسمة صلال. (2024). المسؤولية الدولية الناجمة عن الهجمات السيبرانية. مجلة جامعة البيان للدراسات والبحوث القانونية، 3(1)، 55-69. <https://jlssr.albayan.edu.iq/index.php/jlssr/article/view/17>
21. الوكالة الوطنية للأمن السيبراني. (2024). الاستراتيجية الوطنية للأمن السيبراني لدولة قطر 2024-2030. <https://ncsa.gov.qa/ar/national-cyber-security-strategy2030>
22. الوكالة الوطنية للأمن السيبراني. (د.ت). الإطار الوطني لإدارة الحوادث السيبرانية. <https://ncsa.gov.qa/ar/national-incident-management-framework>
23. العود، خالد ميلاد محمد، ومغراف، ميلاد سالم المختار. (2024). دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية في مؤسسات التعليم العالي: دراسة تطبيقية على طلبة كلية الاقتصاد بجامعة بني وليد. المجلة الأفروآسيوية للبحث العلمي، 2(3)، 217-230. <https://aajsr.com/index.php/aajsr/article/view/184>