التهديدات الرقمية وأثرها على الأمن القومي القطري (دراسة تحليلية للإرهاب الإلكتروني)

Digital Threats and Their Impact on Qatari National Security (An Analytical Study of Cyber Terrorism)

أ. **حسن خلف حسن الكعبى:** باحث في مرحلة الدكتوراه، تخصص القانون، جامعة لوسيل، قطر

Mr. Hassan Khalaf Hassan Al-Kaabi: PhD Researcher in Legal, College of Law, Lusail University, Qatar.

Doi: https://doi.org/10.56989/benkj.v6i3.1800

تاريخ الاستلام: 2026-01-10 تاريخ القبول: 2026-02-10 تاريخ النشر 2026-03-01

المستخلص:

هدفت الدراسة إلى تحليل مفهوم التهديدات الرقمية والإرهاب الإلكتروني، وبيان أثرهما في الأمن الوطني والسياسي والاقتصادي في دولة قطر، وتقييم فعالية الاستراتيجيات الحكومية المعتمدة لمكافحتهما، مع تقديم مقترحات عملية لتعزيز منظومة الأمن السيبراني. وتنطلق الدراسة من عدة فرضيات، أبرزها أن التهديدات الرقمية تشكّل خطرًا حقيقيًا ومتناميًا على الأمن القومي القطري، وأن فعالية المواجهة ترتبط بمدى التكامل بين الأطر التشريعية والقدرات التقنية والتعاون المؤسسي على المستويين المحلي والدولي. وقد اعتمدت الدراسة على المنهج التحليلي لدراسة طبيعة التهديدات الرقمية، والمنهج الوصفي لبيان آثارها في القطاعات الحيوية، إضافة إلى المنهج المقارن لاستعراض بعض التجارب الدولية، والمنهج الاستكشافي لتشخيص التحديات العملية المرتبطة بمكافحة الإرهاب الإلكتروني. وتوصلت إلى عدة نتائج، من أبرزها أن الإرهاب الإلكتروني يمثل تهديدًا مباشرًا للأمن القومي القطري لما له من قدرة على تعطيل البنية التحتية الحيوية وزعزعة الاستقرار الاقتصادي والسياسي، وأن الاستراتيجيات الوطنية القطرية في مجال الأمن السيبراني حققت تقدمًا ملحوظًا، لكنها لا تزال بحاجة إلى تطوير مستمر لمواكبة تطور الهجمات الرقمية، وأوصت بضرورة تعزيز بناء القدرات البشرية المتخصصة في مجال الأمن السيبراني، وتوسيع نطاق التعاون الإقليمي والدولي لمواجهة التهديدات الرقمية العابرة للحدود بصورة أكثر فاعلية.

الكلمات المفتاحية: التهديدات الرقمية، الإرهاب الإلكتروني، الأمن القومي القطري، الأمن السيبراني، حماية البنية التحتية الحيوية.

Abstract:

The study aimed to analyze the concept of digital threats and cyberterrorism, examine their impact on national, political, and economic security in the State of Qatar, and evaluate the effectiveness of the government strategies adopted to combat them, while proposing practical recommendations to strengthen the cybersecurity framework. The study is based on several hypotheses, most notably that digital threats constitute a real and growing danger to Qatari national security, and that the effectiveness of countermeasures depends on the level of integration between legislative frameworks, technical capabilities, and institutional cooperation at both the domestic and international levels. The study employed the analytical approach to examine the nature of digital threats, the descriptive approach to clarify their effects on vital sectors, in addition to the comparative approach to review selected international experiences, and the exploratory approach to diagnose practical challenges related to combating cyberterrorism. The findings indicate that cyberterrorism represents a direct threat to Qatari national security due to its ability to disrupt critical infrastructure and destabilize economic and political stability, and that although Qatar's national cybersecurity strategies have achieved notable progress, they still require continuous development to keep pace with the evolution of digital attacks. The study recommends strengthening the development of specialized human capacities in cybersecurity and expanding regional and international cooperation to more effectively address cross-border digital threats.

Keywords: Digital Threats, Cyberterrorism, Qatari National Security, Cybersecurity, Critical Infrastructure Protection

المقدمة:

تُعدّ التهديدات الرقمية في العصر الحديث أحد أبرز مظاهر التحوّل في طبيعة المخاطر التي تواجه الدول؛ إذ لم تعد التهديدات مقتصرة على الأبعاد العسكرية التقليدية، بل امتدت لتشمل الفضاء السيبراني بما ينطوي عليه من مخاطر اختراق الأنظمة، وتعطيل البنى التحتية الحيوية، وسرقة البيانات، والتجسس الإلكتروني، ونشر المعلومات المضللة، بل وحتى استخدام التقنيات الرقمية في دعم التنظيمات الإرهابية وتمويلها وتنسيق عملياتها. وقد أدى الانتشار الواسع للتقنيات الحديثة، كالذكاء الاصطناعي، والحوسبة السحابية، وإنترنت الأشياء، وسلاسل الكتل (Blockchain)، إلى تعقيد البيئة الأمنية، بحيث أصبح الفضاء الرقمي ميدانًا مفتوحًا للصراعات غير المتماثلة، التي قد تُمارَس فيها أفعال عدائية من قِبل دول، أو جماعات منظمة، أو حتى أفراد يمتلكون مهارات تقنية متقدمة.

ويُقصد بالأمن القومي، في مفهومه المعاصر، قدرةُ الدولة على حماية كيانها السياسي والدستوري، وصون وحدتها الإقليمية، والحفاظ على استقرارها الاقتصادي والاجتماعي، وضمان سلامة مؤسساتها الحيوية من أي تهديد داخلي أو خارجي. ولم يعد الأمن القومي مفهومًا عسكريًا صرفًا، بل أصبح مفهومًا مركبًا يشمل الأمن الاقتصادي، والأمن المعلوماتي، والأمن الصحي، والأمن البيئي، وغيرها من الأبعاد التي تتكامل لضمان استدامة الدولة. ومن هذا المنطلق، بات الأمن السيبراني يُعدّ ركيزة أساسية ضمن منظومة الأمن القومي، نظرًا لاعتماد الدول المتزايد على الأنظمة الرقمية في إدارة قطاعات الطاقة، والمياه، والنقل، والمصارف، والاتصالات، والخدمات الحكومية.

أما في السياق القطري، فإن الأمن القومي يرتبط ارتباطًا وثيقًا بمشروع الدولة في التحول الرقمي وتحقيق رؤية قطر الوطنية 2030، التي تقوم على اقتصاد المعرفة، والحوكمة الرشيدة، وتطوير البنية التحتية الذكية. وقد استثمرت دولة قطر بصورة مكثفة في بناء شبكات اتصالات متقدمة، وأنظمة حكومية إلكترونية، ومنصات مالية رقمية، ومرافق حيوية تعتمد على التقنيات الحديثة. غير أن هذا التقدم التقني يواكبه، بالضرورة، ارتفاع في مستوى المخاطر السيبرانية، سواء في صورة هجمات تستهدف المنشآت الحيوية، أو محاولات لاختراق البيانات السيادية، أو حملات تضليل إعلامي رقمي قد تمسّ السلم الاجتماعي والثقة في المؤسسات.

ومن ثمّ، تأتي هذه الورقة البحثية لتتناول، بالتحليل العلمي، التهديدات الرقمية والإرهاب الإلكتروني بوصفهما تحديين مركزيين للأمن القومي القطري، مع دراسة أبعادهما القانونية والاستراتيجية، وبيان انعكاساتهما على الاستقرار الوطني، وصولًا إلى اقتراح آليات متكاملة تجمع بين التطوير التشريعي، وبناء القدرات التقنية، وتعزيز التعاون الدولي، بما يضمن تحصين الفضاء الرقمي القطري وحماية مقومات الدولة الحديثة في ظل بيئة أمنية عالمية متغيرة ومتسارعة.

مشكلة الدراسة:

السؤال الرئيس الذي تسعى هذه الدراسة للإجابة عليه هو:

ما هو تأثير التهديدات الرقمية والإرهاب الإلكتروني على الأمن القومي القطري، وما هي الاستراتيجيات المتبعة لمكافحة هذه التهديدات؟

فرضيات الدراسة:

إن التهديدات الرقمية والإرهاب الإلكتروني يشكّلان تهديدًا حقيقيًا للأمن القومي القطري، وأن ثمة حاجة إلى تعزيز التعاون بين القطاعين العام والخاص لمكافحة هذه التهديدات. كما تفترض الدراسة أن السياسات الحكومية القطرية في هذا المجال بحاجة إلى تطوير مستمر لمواكبة التحديات المتزايدة.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق عدة أهداف رئيسية؛ من أبرزها:

1. دراسة وتحليل التهديدات الرقمية التي قد تؤثر على الأمن القومي القطري.
2. فهم أثر الإرهاب الإلكتروني على القطاعات الحيوية في دولة قطر.
3. تقييم استراتيجيات الحكومة القطرية لمكافحة الإرهاب الإلكتروني والتهديدات الرقمية.
4. تقديم توصيات لتحسين الإجراءات الأمنية الرقمية وتعزيز التنسيق المحلي والدولي لمكافحة الإرهاب الإلكتروني.

أهمية الدراسة:

تكتسب هذه الدراسة أهمية كبيرة نظرًا لأن التهديدات الرقمية تُشكّل تحديًا حقيقيًا للأمن الوطني، إذ إن الهجمات الإلكترونية يمكن أن تؤثر بصورة مباشرة في استقرار النظامين الاقتصادي والسياسي. وعليه، فمن المهم أن تكون هذه الورقة مرجعًا للمختصين وصنّاع القرار في قطر لفهم آليات التصدي لهذا النوع من الإرهاب، فضلًا عن الإسهام في تطوير استراتيجيات فعّالة لمواجهته.

منهج الدراسة:

اعتمدت الدراسة على المنهج التحليلي الذي يركّز على تحليل البيانات ذات الصلة بالتهديدات الرقمية والإرهاب الإلكتروني في قطر، والمنهج المقارن الذي يسلّط الضوء على تجارب الدول الأخرى في هذا المجال، بالإضافة إلى المنهج الوصفي لدراسة تأثير هذه التهديدات في القطاعات الحيوية. كما سيُستخدم المنهج الاستكشافي لاستكشاف التحديات التي تواجهها قطر في التصدي لهذه

التهديدات وتقديم حلول عملية، إلى جانب المراجعة الأدبية لتسليط الضوء على الدراسات السابقة ذات الصلة بالموضوع.

المطلب الأول: التهديدات الرقمية وأثرها على الأمن القومي القطري

تُعدّ التهديدات الرقمية من أبرز التحديات التي تواجه الأمن القومي القطري في العصر الحديث، وذلك بالنظر إلى التطور السريع في البنية التحتية الرقمية وتزايد الاعتماد على التقنيات الحديثة في مختلف القطاعات الحيوية. وتتراوح هذه التهديدات بين الهجمات الإلكترونية التي تستهدف المؤسسات الحكومية والخاصة، والفيروسات والبرمجيات الخبيثة التي قد تؤدي إلى تعطيل الأنظمة الرقمية وتدمير البيانات الحساسة. ولا يقتصر تأثير هذه التهديدات على القطاع التقني، بل يمتد ليطال جوانب حيوية مثل الطاقة، والاتصالات، والنقل، مما يعكس أهمية تعزيز الأمن السيبراني في قطر.

وتواجه دولة قطر تحديات متعددة في التصدي لهذه التهديدات، تشمل نقص التنسيق بين المؤسسات الرقابية، وتزايد تعقيد أساليب الهجمات، فضلًا عن ضعف بعض الأنظمة الرقابية الداخلية في بعض المؤسسات. وعلى الرغم من الجهود المبذولة لتحسين الأمن السيبراني، فإن التهديدات الرقمية لا تزال في تزايد، مما يتطلب تبنّي استراتيجيات شاملة ومتكاملة لمكافحتها.

الفرع الأول: مفهوم التهديدات الرقمية

تشير التهديدات الرقمية إلى الأنشطة العدائية التي تستهدف النظم المعلوماتية بهدف إحداث ضرر، أو الوصول غير المصرّح به إلى بيانات ومعلومات حساسة، أو تعطيل الخدمات. وتتخذ هذه التهديدات أشكالًا متعددة، وتستهدف مختلف الأصول الرقمية مثل الخوادم، وقواعد البيانات، وشبكات الاتصال، مما يؤدي إلى اختراق البيانات أو إيقاف النظام بشكل كامل. ومع الاعتماد المتزايد على التكنولوجيا في القطاعات الحكومية والخاصة، أصبحت هذه التهديدات تُشكّل خطرًا حقيقيًا على الأمن القومي، لا سيما في دولة مثل قطر، التي تشهد تطورًا كبيرًا في بنيتها التحتية الرقمية[1].

أنواع التهديدات الرقمية:

1. الهجمات السيبرانية هي أحد أبرز أنواع التهديدات الرقمية. يتم تنفيذ هذه الهجمات باستخدام أساليب متعددة مثل الفيروسات، البرمجيات الخبيثة، وبرامج التجسس، التي تؤدي إلى تعطيل الأنظمة أو اختراقها. من بين أبرز هذه الهجمات، تأتي هجمات الفدية حيث يقوم المهاجمون بتشفير البيانات في النظام ويطالبون بدفع فدية لفك التشفير. أيضًا تعد هجمات التصيد الاحتيالي

[1] بني حمد، يحيى محمد (2021)، الأمن السيبراني: التهديدات والتحديات وطرق الحماية، ط1، (عمان: دار الخليج للنشر والتوزيع)، ص 45.

من الأنواع الشائعة التي تهدف إلى سرقة البيانات الشخصية من خلال رسائل إلكترونية تحتوي على روابط ضارة.

2. الهجمات على البنية التحتية الحيوية جانب آخر من التهديدات الرقمية يتعلق بالهجمات التي تستهدف البنية التحتية الحيوية مثل القطاعات المتعلقة بالطاقة، المياه، والاتصالات. هذه الهجمات قد تؤدي إلى تعطيل الخدمات الأساسية، مما يشكل خطرًا على استقرار المجتمع. من بين هذه الهجمات، تبرز (هجمات الحرمان من الخدمة الموزعة)، التي تهدف إلى تعطيل الشبكات من خلال إغراق الأنظمة بالكثير من البيانات التي لا يمكن التعامل معها[1].

إضافة إلى الهجمات الخارجية، توجد بعض **التهديدات الداخلية**، التي تأتي من داخل المؤسسات نفسها. في هذه الحالة، قد يقوم بعض الموظفين أو الأفراد الذين لديهم وصول مشروع إلى الأنظمة المعلوماتية باستخدام هذا الوصول لأغراض ضارة مثل سرقة البيانات أو إلحاق الضرر بالنظام. يعد هذا النوع من التهديدات خطيرًا للغاية نظرًا لأن المهاجمين يتمتعون بالثقة والوصول إلى المعلومات الحساسة.

الجهات الفاعلة في التهديدات الرقمية:

تتعدد الجهات الفاعلة في الهجمات الرقمية، حيث يشمل ذلك القراصنة الفرديين الذين قد يقومون بالهجمات بهدف اختبار مهاراتهم أو تحقيق مكاسب مالية. كما يمكن أن تكون هناك مجموعات منظمة تعمل بشكل متناسق مع أهداف سياسية أو اقتصادية. في بعض الحالات، تقوم الدول المعادية بتنفيذ هجمات سيبرانية كجزء من الحروب السيبرانية، بهدف التأثير على استقرار الدول الأخرى. كما أن التهديدات الداخلية تشكل خطرًا إضافيًا، حيث قد يسعى موظفون داخل المؤسسات إلى إحداث الضرر أو سرقة البيانات.

أهداف التهديدات الرقمية:

إن من أبرزه أهداف هذه التهديدات الرقمية سرقة البيانات التي قد تشمل البيانات المالية أو الشخصية. يمكن أن تؤدي الهجمات إلى تعطيل الأنظمة بشكل مؤقت أو دائم، مما يتسبب في توقف الخدمات أو تدمير الأنظمة. في بعض الحالات، يسعى المهاجمون إلى التخريب السياسي، مثل التأثير على الانتخابات أو إحداث الاضطرابات في النظام السياسي. كما تتضمن الأهداف الأخرى الابتزاز المالي، مثل تلك التي تحدث في هجمات الفدية.

[1] جاسم، إبراهيم محمد (2020)، الأمن السيبراني: الحماية من التهديدات الرقمية في العصر الحديث، الطبعة الأولى، (عمان: دار دجلة للنشر والتوزيع)، ص 88-92.

آثار التهديدات الرقمية على الأمن القومي:

تتجسد آثار هذه التهديدات على الأمن القومي في عدة جوانب. الضرر الاقتصادي من أبرز هذه الآثار، حيث تؤدي الهجمات الرقمية إلى تكاليف مالية ضخمة بسبب تعطيل الأنظمة أو سرقة البيانات. كما أن تهديد النظام السياسي يصبح أمرًا حيويًا، إذ يمكن أن تؤثر الهجمات الإلكترونية على الانتخابات أو تؤدي إلى فقدان الثقة في المؤسسات الحكومية. بالإضافة إلى ذلك، فإن تضرر الثقة العامة في المؤسسات قد يؤدي إلى فقدان الأمن الاجتماعي والسياسي في الدولة[1].

تعد التهديدات الرقمية مشكلةً معقدةً ومتزايدةً، تتطلب اتخاذ تدابير وقائية فعالة من جميع الجهات المعنية في الدولة. لتفادي هذه المخاطر، يجب على قطر تعزيز قدراتها في مجال الأمن السيبراني، والعمل على تقوية التعاون بين الحكومة والقطاع الخاص، وتطوير التشريعات المتعلقة بالأمن الرقمي.

الفرع الثاني: تأثير التهديدات الرقمية على القطاعات الحيوية في قطر

يعد الاعتماد المتزايد على التكنولوجيا الرقمية في إدارة القطاعات الحيوية من أبرز مظاهر التطور في دولة قطر، حيث أصبحت الشبكات الرقمية وأنظمة المعلومات جوهرية في تشغيل المؤسسات الحيوية مثل الطاقة، الاتصالات، الخدمات المالية، والمرافق الأساسية. ومع هذا الاعتماد، تتعرض هذه القطاعات إلى مخاطر جسيمة في حال تعرضها لهجمات رقمية، مما ينعكس بصورة مباشرة على أداء الخدمات الوطنية واستقرار المجتمع والنظام الاقتصادي للدولة. تؤكد الاستراتيجية الوطنية للأمن السيبراني أهمية حماية **البنية التحتية الوطنية الحيوية** من المخاطر السيبرانية المتطورة، وذلك لضمان استمرارية الخدمات الأساسية وعدم تأثرها بالهجمات .

تشكل الهجمات الرقمية تهديدًا مباشرًا لعمل المؤسسات المنتجة للطاقة والمياه والكهرباء، حيث يمكن أن تتسبب في تعطل أنظمة التحكم الصناعي، مما يؤدي إلى توقف العمليات التشغيلية أو حتى إلحاق أضرار مادية جسيمة بالبنية التحتية. ولهذا السبب، تضع الجهات المعنية مثل الوكالة الوطنية للأمن السيبراني(NCSA) توصيات لمعايير أمان خاصة بقطاع الطاقة والمياه تتضمن تطبيق **معايير ISA/IEC 62443** لتعزيز حماية أنظمة التحكم التشغيلي في هذه المرافق الحيوية، وذلك بالتعاون مع شركات مثل "كهرماء" لضمان قدرة هذه القطاعات على مواجهة الهجمات

[1] خليفة، إيهاب (2017): حروب الجيل الخامس: الأشكال الجديدة للصراعات في العصر الرقمي، (القاهرة: مركز المستقبل للأبحاث والدراسات المتقدمة)، ص 142-145.

الرقمية[1]. بالإضافة إلى ذلك، هناك تأثير واضح للتهديدات الرقمية على القطاع المالي والمصرفي في قطر، حيث تعتمد البنوك والمؤسسات المالية بشكل كبير على الأنظمة الرقمية لإدارة الحسابات والمعاملات. إن اختراق هذه الأنظمة أو **تسريب البيانات** من شأنه أن يهدد ثقة الجمهور في الخدمات المالية، ويؤدي إلى خسائر مالية كبيرة وتأثيرات سلبية على الاستقرار الاقتصادي. وقد أظهرت تقارير عن تزايد محاولات التسريبات الرقمية والجرائم السيبرانية في الدولة الحاجة إلى رفع مستوى حماية البيانات، وتعزيز الإجراءات القانونية والتنظيمية للتصدي لهذه الهجمات قبل أن تتسبب في أضرار لا يمكن تعويضها [2].

من جانب آخر، يتعرض قطاع الاتصالات أيضًا لضغط التهديدات الرقمية، خاصة مع انتشار شبكات الجيل الخامس 5G وتوسع الخدمات الرقمية، إذ إنَّ أي اختراق في هذا القطاع يمكن أن يؤدي إلى **تدهور جودة الخدمات** أو تعطلها، ما يؤثر على التواصل بين الأفراد والقطاعات المختلفة في الدولة ويعطل سير الأعمال اليومية. وتعد مبادرات مثل تعزيز الاستجابة لحوادث الأمن السيبراني وممارسة التدريبات الدورية من قبل الجهات المختصة جزءًا من جهود قطر لبناء قدرات مرنة تمنع توقف هذه الخدمات الحيوية وتأمينها ضد المخاطر المستقبلية، إن تأثير التهديدات الرقمية على هذه القطاعات الحيوية لا يقتصر على الخسائر الاقتصادية المباشرة، بل يمتد أيضًا ليشمل **تراجع الثقة** في قدرة الدولة على حماية أصولها الرقمية، ما يجعل الأمن السيبراني أولوية استراتيجية في الحفاظ على استقرار المجتمع والاقتصاد الوطني. ولهذا تتطلب الجهود الوطنية استمرار تطوير الأطر التنظيمية، وتعزيز التعاون بين الجهات الحكومية والقطاع الخاص لضمان حماية فعالة للبنى التحتية الحساسة، والحفاظ على قدرة قطر في مواجهة التهديدات الرقمية المتزايدة .

الفرع الثالث: التحديات التي تواجه قطر في التصدي للتهديدات الرقمية

تواجه دولة قطر مجموعة من التحديات المتزايدة التي تعيق جهودها في التصدي للتهديدات الرقمية التي تهدد أمنها السيبراني. مع التوسع الكبير في استخدام التكنولوجيا الرقمية في كافة المجالات، لا سيما في القطاعات الحيوية مثل الطاقة، النقل، والمالية، فإن مواجهة هذه التهديدات أصبحت ضرورة استراتيجية. وعلى الرغم من الإجراءات المتخذة على المستويات الحكومية والمؤسسية، إلا أن هناك العديد من المعوقات التي يجب معالجتها لضمان حماية فعالة للبنية التحتية

[1] وكالة الأمن السيبراني الوطنية (2024)، إطار الامتثال للأمن السيبراني الوطني: قطاع الطاقة والخدمات الحيوية، (الدوحة: وكالة الأمن السيبراني الوطنية)، ص 22–25.

[2] مصرف قطر المركزي (2022): استراتيجية أمن المعلومات للقطاع المالي في دولة قطر، النسخة الثانية، (الدوحة: إدارة نظم المعلومات)، ص 18–21.

الرقمية في قطر. تتراوح هذه التحديات بين الجانب التقني، البشري، التنظيمي، والتشريعي، مما يعكس تعقيد البيئة السيبرانية التي يجب أن يتم التعامل معها بحذر واحترافية.

أولا: التحديات التقنية والتطور المستمر للهجمات الرقمية

إنَّ من أبرز التحديات التي تواجه قطر في التصدي للتهديدات الرقمية هي التطور المستمر للهجمات الرقمية وارتفاع مستوى تعقيدها. تعد الهجمات الرقمية اليوم أكثر تطورًا، حيث يتم استخدام تقنيات جديدة تشمل البرمجيات الخبيثة المتقدمة، هجمات الفدية التي تقوم بتشفير البيانات والمطالبة بفدية لفك التشفير، إضافة إلى الهجمات ذات الهدف السياسي مثل الحروب السيبرانية التي قد تهدد الاستقرار السياسي والاقتصادي للدولة. في ظل هذا التطور السريع، تجد المؤسسات القطرية نفسها أمام تحديات كبيرة في تحديث أنظمتها الدفاعية لمواكبة هذه الهجمات المتجددة.[1]

تتمثل التحديات التقنية في ضرورة تحديث أنظمة الحماية بشكل دوري، واستخدام أدوات وتقنيات متطورة مثل الذكاء الاصطناعي وتعلم الآلة للكشف عن التهديدات الجديدة بسرعة وفعالية. ولكن هذا يحتاج إلى استثمار مكثف في البنية التحتية التقنية من أجل ضمان أن الأنظمة تعمل بكفاءة وتستطيع التصدي للهجمات المعقدة التي تتطور بشكل مستمر[2].

ثانيا: نقص الكفاءات البشرية في مجال الأمن السيبراني

نقص الكفاءات البشرية في مجال الأمن السيبراني يمثل أحد التحديات الكبرى التي تواجه قطر في التصدي للتهديدات الرقمية. يعاني قطاع الأمن السيبراني في الدولة من نقص في المهارات المتخصصة اللازمة لمواكبة التطورات التقنية السريعة. على الرغم من الجهود التي تبذلها قطر في تدريب وتأهيل كوادرها في هذا المجال، فإن الطلب على المتخصصين في الأمن السيبراني يفوق العرض بكثير. ولا تقتصر هذه المشكلة على قطر فقط، بل تشمل معظم دول المنطقة التي تواجه تحديات مماثلة في هذا المجال، في هذا السياق، الاستثمار في التعليم والتدريب في مجال الأمن السيبراني يعد أمرًا بالغ الأهمية. ومن المتوقع أن تزداد الحاجة إلى الخبراء في هذا المجال بشكل كبير مع تزايد الاعتماد على التكنولوجيا الحديثة في كافة القطاعات. ولهذا فإن قطر بحاجة إلى

[1] السدحان، عبد الرحمن (2023)، الأمن السيبراني والذكاء الاصطناعي: التحولات الكبرى في حروب المعلومات، الطبعة الثانية، (الرياض: دار الكتاب الجامعي)، ص 158-161.

[2] خليل، محمد السعيد (2024)، الأمن السيبراني في عصر الذكاء الاصطناعي: الفرص والتهديدات، الطبعة الأولى، (القاهرة: دار النهضة العربية)، ص 112-115.

برامج تعليمية متخصصة، بالتوازي مع المبادرات الحكومية والشراكات مع الجامعات والمؤسسات الأكاديمية لتعزيز مستوى التأهيل في هذا المجال[1].

ثالثا: تحديات التشريعات والأنظمة القانونية

من أبرز التحديات القانونية التي تواجهها قطر هو توفير إطار قانوني مرن يتعامل مع الجرائم الرقمية العابرة للحدود. على الرغم من الجهود المبذولة في محاربة الجرائم السيبرانية، فإن الأنظمة القانونية بحاجة إلى مزيد من التنسيق بين الدول لضمان التعاون الفعال في ملاحقة المهاجمين، خاصة أن الهجمات السيبرانية غالبًا ما تكون عالمية ولا تقتصر على حدود دولة معينة. كما أن قطر بحاجة إلى تعزيز الوعي القانوني حول حماية البيانات الرقمية والخصوصية في إطار المعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR) الخاصة بالاتحاد الأوروبي[2].

رابعا: ضعف التنسيق بين القطاعين العام والخاص

يعد ضعف التنسيق بين القطاعين العام والخاص من أبرز التحديات التي تواجه قطر في حماية بنيتها التحتية الرقمية، على الرغم من الجهود التي تبذلها الحكومة لتعزيز قدرات الأمن السيبراني في المؤسسات الحكومية، تتمثل إحدى العقبات في هذا السياق في الاختلافات التنظيمية بين المؤسسات الحكومية والخاصة في طريقة تعاملها مع البيانات وحمايتها. فبينما يتمتع القطاع الحكومي بضوابط تنظيمية قوية، تواجه الشركات الخاصة تحديات في التوافق مع المعايير الحكومية بسبب اختلاف ممارسات الأمان السيبراني التي قد تفتقر إلى التنسيق والتكامل المطلوب[3].

خامسا: القصور في الوعي المجتمعي بالتهديدات الرقمية

الوعي المجتمعي بأهمية الأمن السيبراني يشكل تحديًا آخر في قطر. مع أن الكثير من المؤسسات الحكومية والخاصة تركز على تطبيق أفضل الممارسات الأمنية داخل منظوماتها، فإن الأفراد في المجتمع قد لا يدركون دائمًا خطورة التهديدات الرقمية التي قد يتعرضون لها، مثل التصيد الاحتيالي أو الهجمات على الأجهزة الشخصية. عدم الوعي الكافي يمكن أن يؤدي إلى ثغرات أمنية بسبب أخطاء بشرية، مثل فتح روابط مشبوهة أو مشاركة معلومات حساسة.

---

[1] الجابر، حصة بنت سلطان (2022)، التحول الرقمي والأمن السيبراني في قطر: رؤية استراتيجية، (الدوحة: جامعة حمد بن خليفة للنشر)، ص 74-77.

[2] السيد، حسن (2021)، النظام القانوني القطري في مواجهة الجرائم السيبرانية: دراسة تحليلية، الطبعة الثانية، (الدوحة: دار نشر جامعة قطر)، ص 189-192.

[3] المنصوري، ريم محمد (2023)، حوكمة التحول الرقمي: الموازنة بين الابتكار والأمن المعلوماتي، (الدوحة: وزارة الاتصالات وتكنولوجيا المعلومات)، ص 142-145.

إن التثقيف المستمر للمواطنين في مجال الأمن السيبراني أصبح أمرًا بالغ الأهمية، خاصة في ضوء النمو الهائل في استخدام الأجهزة الرقمية على مستوى الأفراد. يجب أن تشمل برامج التوعية تعليم المواطنين كيفية حماية بياناتهم وتجنب المخاطر المحتملة عند التفاعل مع الإنترنت أو التطبيقات الإلكترونية[1].

سادسا: تحديات التعاون الإقليمي والدولي

تُعَدُّ التحدياتُ المتعلقةُ بالتعاون الإقليمي والدولي من أبرز التحديات التي تواجه قطر في التصدي للتهديدات الرقمية؛ إذ إنَّ الهجمات السيبرانية لا تتقيد بالحدود الوطنية، مما يجعل التعاون بين الدول في هذا المجال أمرًا ضروريًا لمواجهة المهاجمين السيبرانيين، ولا سيما أولئك الذين يتخذون من دول أخرى مقراتٍ لهم. ومع وجود اختلافات في قوانين الأمن السيبراني بين الدول، يواجه هذا التعاون صعوباتٍ في التنفيذ على أرض الواقع، مما يجعل التعامل مع المهاجمين عبر الحدود أمرًا معقدًا.

المطلب الثاني: الإرهاب الإلكتروني وأثره على الأمن القومي القطري

يشهد العالم في العصر الحالي تطورًا مستمرًا في أساليب الإرهاب، إذ لم يعد يقتصر على الهجمات التقليدية عبر الحدود الجغرافية، بل امتد إلى الفضاء الرقمي في صورة الإرهاب الإلكتروني. ويشمل هذا النوع من الإرهاب أي نشاط إلكتروني يستهدف إلحاق الضرر بالمؤسسات أو الأفراد عبر الأنظمة الرقمية، سواء تمثل ذلك في تعطيل الخدمات، أو سرقة المعلومات، أو التأثير في النظم السياسية والاقتصادية. وبالنسبة لدولة قطر، التي تعتمد بدرجة كبيرة على البنية التحتية الرقمية في تسيير العديد من قطاعاتها الحيوية مثل الطاقة والاتصالات والخدمات المالية، فإن الإرهاب الإلكتروني يمثل تهديدًا حقيقيًا يتطلب استجابة استراتيجية شاملة.

تتنوع أساليب الإرهاب الإلكتروني وتتطور باستمرار؛ فمن هجمات الفدية التي تسعى إلى تعطيل الأنظمة الرقمية وطلب مبالغ مالية مقابل إعادة تشغيلها، إلى هجمات التصيد الاحتيالي التي تستهدف الأفراد للحصول على بيانات حساسة، مرورًا بالهجمات الموجهة ضد البنية التحتية الحيوية مثل قطاعي الطاقة والنقل. وقد تؤدي هذه الأنواع من الهجمات إلى تعطيل الخدمات الأساسية، مما يؤثر بصورة مباشرة في استقرار الدولة وأمنها الداخلي. وفي هذا السياق، من الضروري النظر في

[1] كمال، جاسم محمد (2024)، الوعي الرقمي والمواطنة المسؤولة في مجتمع المعرفة، ط1، (الدوحة: دار الثقافة للنشر والتوزيع)، ص215–218.

تأثير الإرهاب الإلكتروني على الأمن القومي القطري، وكيف تنعكس هذه الهجمات على استقرار النظامين السياسي والاقتصادي في البلاد[1].

تستهدف الهجمات الإلكترونية في قطر، بشكل أساسي، القطاعات التي تعتمد اعتمادًا كبيرًا على الأنظمة الرقمية، مثل قطاعي الطاقة والاتصالات، إذ يمكن أن يؤدي تعرض هذه القطاعات لهجمات سيبرانية إلى تعطيل عمليات حيوية، مما يتسبب في أضرار اقتصادية جسيمة وفقدان الثقة في قدرة الدولة على حماية بنيتها التحتية. وفي حال استهداف البنوك أو النظام المالي، على سبيل المثال، قد تنشأ أزمات مالية تؤثر في الاقتصاد الوطني بوجه عام، وتُضعف الثقة في النظام المالي. ولا تقتصر تهديدات الإرهاب الإلكتروني على الجوانب الاقتصادية، بل تمتد إلى الأمنين السياسي والاجتماعي؛ إذ قد تؤدي الهجمات السيبرانية إلى نشر الشائعات والتأثير في الرأي العام من خلال التحكم في وسائل الإعلام الرقمية أو اختراق الحسابات الرسمية لشخصيات سياسية بارزة. كما يمكن توظيف هذه الهجمات للضغط على القرارات السياسية، مما يجعل من الضروري مواجهة هذا النوع من الإرهاب بحذر شديد. لذلك، تُعَدّ مكافحة الإرهاب الإلكتروني من الأولويات الأمنية في قطر، ويتطلب ذلك تطوير استراتيجيات فعالة على المستويين الوطني والدولي للتصدي لهذه الهجمات، وتشمل هذه الاستراتيجيات تعزيز القدرات الدفاعية السيبرانية للدولة، وتحسين التعاون بين القطاعات المختلفة، وتطوير التشريعات التي تعزز قدرة الدولة على مكافحة هذا النوع من الإرهاب.

الفرع الأول: تعريف الإرهاب الإلكتروني وأهدافه

تعريف الإرهاب الإلكتروني

الإرهاب الإلكتروني هو «نوع من أنواع الإرهاب الحديث الذي يُنفَّذ من خلال استخدام الإنترنت أو الوسائل الرقمية لتحقيق أهداف تخريبية، سواء كانت سياسية أو اقتصادية أو اجتماعية، ويستهدف عادةً البنية التحتية الرقمية أو الأنظمة الإلكترونية الحساسة. وتُنفَّذ الهجمات الإرهابية الرقمية باستخدام أساليب وتقنيات تكنولوجية متقدمة، مثل البرمجيات الخبيثة، والهجمات الموزعة عبر الإنترنت، وبرمجيات الفدية، وغيرها من الأدوات الرقمية التي تهدف إلى إلحاق الأذى أو السيطرة على الأنظمة المعلوماتية للمؤسسات أو الدول»[2].

[1] الشاوي، علي محمد (2023)، الإرهاب السيبراني: حروب القرن الحادي والعشرين والأمن القومي العربي، ط1، (الدوحة: دار جامعة حمد بن خليفة للنشر)، ص 112–115.

[2] بشير، محمد الفاتح محمود (2022)، الإرهاب الإلكتروني: دراسة في المفاهيم والآليات والمواجهة القانونية، ط1، (عمان: دار الخليج للنشر والتوزيع)، ص56–59.

يمكن تعريف الإرهاب الإلكتروني بأنه «أي هجوم منظم على الأنظمة المعلوماتية والمرافق الحيوية باستخدام تكنولوجيا المعلومات بغرض التسبب في الخراب أو الضرر المادي أو الاضطراب السياسي والاجتماعي». وتكمن خطورة هذا النوع من الإرهاب في أنه لا يتطلب وجودًا جسديًا في موقع الهجوم؛ إذ يمكن تنفيذه عن بُعد عبر الإنترنت، مما يُعقّد مهمة كشف هذه الهجمات أو إيقافها[1].

أصبح الإرهاب الإلكتروني جزءًا أساسيًا من الحروب السيبرانية التي يُستَخدم فيها الفضاء الإلكتروني أداةً لتهديد الأمن القومي للدول. ولا يقتصر هذا النوع من الهجمات على الأفراد المتطرفين أو الجماعات الإرهابية التقليدية، بل قد يكون مصدره دولٌ معادية أو جماعاتٌ منظمة تسعى إلى تحقيق أهداف سياسية أو اقتصادية على حساب الأمن الوطني أو الاستقرار الدولي.

أهداف الإرهاب الإلكتروني:

يهدف الإرهاب الإلكتروني إلى تحقيق مجموعة من الأهداف التي تتراوح بين التأثير على الأنظمة السياسية إلى إلحاق الضرر بالبنية التحتية الاقتصادية، ويمكن تلخيص هذه الأهداف في النقاط التالية:[2]

1. التأثير على الأمن القومي والسيادة الوطنية:

الهدف الرئيس من الإرهاب الإلكتروني هو تهديد الأمن القومي لدولةٍ معينة، ويتم ذلك من خلال استهداف البنية التحتية الوطنية مثل شبكات الكهرباء، ومحطات المياه، أو أنظمة النقل. ومن خلال تعطيل هذه الأنظمة، يمكن للجماعات الإرهابية إحداث أزمات تؤدي إلى شلّ الحياة اليومية للمواطنين، مما يفضي إلى تراجع الثقة في الحكومة وقدرتها على حماية مصالح الدولة.

وعلى سبيل المثال، قد يؤدي هجوم سيبراني على الأنظمة العسكرية أو أجهزة الاستخبارات إلى إرباك التنسيق بين الأجهزة الأمنية الوطنية. وفي حالة قطر، قد يشمل الهجوم الإلكتروني استهداف شبكات الاتصالات، مما يُعطّل الاستجابة السريعة للأزمات ويُعرّض المعلومات الحكومية والخاصة للخطر.

[1]. كمال، جاسم محمد (2023)، الأمن السيبراني في الاستراتيجية القطرية: الوقاية والمواجهة، (الدوحة: دار لوسيل للنشر والتوزيع)، ص 158–160.

[2] خليفة، إيهاب (2023)، حروب الجيل الخامس: الأسلحة السيبرانية وتأثيرها على استقرار الدول، الطبعة الثانية، (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية)، ص 210–215.

2. تحقيق أهداف سياسية:

قد يسعى الإرهابيون الإلكترونيون إلى التأثير في الأنظمة السياسية أو في السياسات الخارجية لدولةٍ معينة؛ فعلى سبيل المثال، قد يشنّون هجمات تستهدف البنية التحتية للانتخابات أو وسائل الإعلام بقصد تشويه صورة الحكومة في نظر الرأي العام الداخلي أو الدولي.

وقد شهدنا في الماضي أمثلة على هذا النوع من الهجمات؛ ومن أبرز الأمثلة الواقعية على خطورة التهديدات الرقمية على الأمن القومي ما تعرّضت له شركة أرامكو السعودية في أغسطس 2012 من هجوم إلكتروني واسع النطاق عُرف باسم «Shamoon»، إذ أدى الهجوم إلى مسح بيانات ما يقارب 30 ألف جهاز حاسوب داخل الشركة، وتعطيل الأنظمة الإدارية واللوجستية لفترة مؤقتة. وقد استهدف الهجوم البنية الرقمية للشركة بوصفها أحد أهم أعمدة الاقتصاد الوطني السعودي، مما كشف عن قدرة الهجمات السيبرانية على المساس بالأمن الاقتصادي والاستقرار الوطني دون استخدام القوة العسكرية التقليدية. وفي حالة قطر، يمكن أن يؤثر هذا النوع من الإرهاب الإلكتروني في الثقة العامة ويُضعف الشرعية السياسية للمؤسسات الوطنية[1].

3. الإضرار بالاقتصاد الوطني:

يستهدف الإرهاب الإلكتروني القطاع الاقتصادي في الدولة من خلال تعطيل المعاملات المالية أو استهداف الأنظمة البنكية أو حتى الأسواق المالية. الهجمات الإلكترونية التي تستهدف الأنظمة المصرفية أو أنظمة الدفع يمكن أن تؤدي إلى خسائر مالية ضخمة، وكذلك إضعاف الثقة في الاستقرار الاقتصادي للدولة.

تعتمد القطاعات المالية في دولة قطر بشكل كبير على الأنظمة الرقمية، ولذلك فإنَّ أي هجوم إلكتروني على البنوك أو المؤسسات المالية قد يعطل قدرة القطاع المالي على العمل بشكل طبيعي. كما يمكن أن يسبب الهجوم فقدان البيانات الحساسة التي قد تكون عرضة للاستخدام غير المشروع، مما قد يؤدي إلى ضرر طويل الأمد على اقتصاد الدولة.

4. تخريب البنية التحتية الحيوية:

يعد التخريب الموجه ضد البنية التحتية الحيوية أحد الأهداف الرئيسية للإرهاب الإلكتروني. تستهدف الهجمات عادةً الأنظمة الصناعية الحيوية مثل أنظمة الطاقة، النقل، المياه، وحتى المستشفيات. في قطر، يعد قطاع الطاقة والمرافق الخدمية مثل محطات الكهرباء ومرافق المياه أهدافًا

[1] Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. Survival, 55(2), p. 82.

محتملة، حيث أن تعطيل هذه الأنظمة يمكن أن يتسبب في أزمات كبيرة تؤثر على حياة المواطنين بشكل مباشر.

على سبيل المثال، يمكن لهجوم إلكتروني على مرافق الطاقة أن يؤدي إلى انقطاع الكهرباء على مستوى واسع، ما يؤدي إلى تعطل الأعمال ونقص الخدمات الأساسية التي يعتمد عليها المواطنون يوميًا.

5. الهجوم على الأفراد وحقوقهم:

يمكن للإرهاب الإلكتروني أن يستهدف الأفراد بشكل مباشر من خلال التهديدات الرقمية مثل الابتزاز الرقمي أو التصيد الاحتيالي للحصول على معلومات حساسة. يمكن للجماعات الإرهابية استخدام هذه الأساليب لسرقة البيانات الشخصية أو المالية للأفراد بغرض الضغط عليهم لتحقيق أهداف معينة. كما قد يسعى الإرهابيون إلى نشر الفوضى في المجتمع عبر الإشاعات التي يتم نشرها من خلال شبكات التواصل الاجتماعي، مما يؤدي إلى إثارة الذعر بين المواطنين.

6. تأثيرات على العلاقات الدولية:

قد تكون للهجمات الإلكترونية تأثيرات سلبية على العلاقات الدولية، حيث يمكن أن تؤدي إلى التصعيد في الصراعات الدولية أو تدخل القوى العالمية في شؤون الدول المستهدفة. قد يستخدم الفاعلون في الإرهاب الإلكتروني الهجمات كوسيلة لتهديد الأمن الإقليمي والدولي، ويؤدي ذلك إلى زيادة التوترات بين الدول المتضررة. على سبيل المثال، قد تسعى بعض الدول إلى استخدام الهجمات السيبرانية ضد دول أخرى كوسيلة للضغط السياسي.

استراتيجيات الإرهاب الإلكتروني

يختلف أسلوب تنفيذ الهجمات الإرهابية الرقمية بشكل كبير حسب الهدف الرئيسي للمهاجمين. يمكن أن يكون الأسلوب المستخدم متنوعًا، يشمل:[1]

1. **الهجمات الموجهة:** حيث يهاجم الإرهابيون **منشأة أو قطاعًا محددًا** مثل قطاع الطاقة أو البنية التحتية الوطنية.
2. **الهجمات الشاملة:** وهي الهجمات التي تستهدف **أنظمة متعددة** داخل الدولة أو المؤسسات ذات العلاقة بهدف التسبب في **أكبر قدر من الفوضى والضرر**.

يُعَدّ الإرهاب الإلكتروني من أخطر التهديدات التي تواجه الأمن القومي في العصر الرقمي؛ فمن خلال استهداف القطاعات الحيوية مثل الطاقة والاتصالات والخدمات المالية، يسعى الإرهابيون

[1]. الشاوي، مصدر سابق، ص142-145.

إلى تحقيق أهداف استراتيجية متعددة، تبدأ بالتأثير في الأمن السياسي ولا تنتهي بتقويض البنية التحتية الاقتصادية. وفي دولة قطر، ينبغي التعامل مع هذه التهديدات بصورة شاملة عبر استراتيجيات أمنية متطورة تواكب التطورات التكنولوجية وتأخذ في الحسبان الأبعاد السياسية والاقتصادية لهذه الهجمات، الأمر الذي يتطلب بناء بيئة أمنية قوية، فضلًا عن تعزيز التعاون الإقليمي والدولي في هذا المجال.

الفرع الثاني: تأثير الإرهاب الإلكتروني على الأمن الوطني والسياسي والاقتصادي

أدى الانتشار المتسارع للتكنولوجيا الرقمية إلى تعزيز العديد من جوانب الحياة اليومية، إلا أن هذا التقدم التكنولوجي رافقه أيضًا ظهور تهديدات جديدة تستهدف الأمن القومي. من بين هذه التهديدات، يعد الإرهاب الإلكتروني أحد أخطر التحديات التي تواجه الدول في العصر الحديث. الإرهاب الإلكتروني هو استخدام الإنترنت والوسائل الرقمية الأخرى لتنفيذ هجمات تهدف إلى إلحاق الضرر بالبنية التحتية الحيوية للدولة، وبالتالي التأثير على الأمن الوطني والسياسي والاقتصادي. تستهدف هذه الهجمات عادةً الأنظمة الحكومية، القطاعات الحيوية مثل الطاقة والاتصالات، بالإضافة إلى البنوك والمؤسسات المالية، ما يؤدي إلى أضرار كبيرة تؤثر على استقرار الدولة في مجالات متعددة. في هذه الفقرة، سيتم التطرق إلى تأثير الإرهاب الإلكتروني على الأمن الوطني، السياسي والاقتصادي في دولة قطر باعتبارها نموذجًا لدراسة كيفية تأثير هذه الهجمات على الدول الحديثة ذات البنية الرقمية المتطورة [1].

أولا: تأثير الإرهاب الإلكتروني على الأمن الوطني

يعد الأمن الوطني المسؤول عن حماية الدولة ومؤسساتها من أي تهديدات خارجية أو داخلية قد تهدد استقرارها، وقد يكون الإرهاب الإلكتروني أحد أكبر التهديدات التي تواجه الدول في الحفاظ على أمنها القومي. في دولة قطر، حيث تعتمد معظم القطاعات الحيوية على الأنظمة الرقمية المتقدمة، قد تؤدي الهجمات السيبرانية إلى تعطيل خدمات حيوية مثل الطاقة، المياه، والنقل، ما يشكل تهديدًا مباشرًا للأمن الوطني.

1. تعطيل البنية التحتية الحيوية

تستهدف الهجمات الإلكترونية، بشكل رئيس، البنية التحتية الحيوية التي تُعَدّ عماد الأمن الوطني، مثل محطات توليد الكهرباء، وأنظمة النقل، والمرافق الصحية. وفي قطر، يُعَدّ قطاع الطاقة من القطاعات الأساسية التي تعتمد على الأنظمة الرقمية في تنظيم العمليات وضمان استمراريتها؛ إذ يمكن أن يتسبب هجوم سيبراني على هذه الأنظمة في توقف الإنتاج أو تعطل الإمدادات الأساسية،

[1] كمال، مصدر سابق، ص 42-45.

مما يخلق أزمة وطنية تؤثر في ملايين المواطنين. وقد شهدت بعض الدول، مثل أوكرانيا، هجمات إلكترونية استهدفت شبكات الطاقة، مما أدى إلى انقطاع الكهرباء على نطاق واسع وترك المواطنين في الظلام لفترات طويلة. كما أن الهجمات على أنظمة النقل، التي قد تؤدي إلى توقف حركة الطيران أو النقل البري، تشكل تهديدًا للأمن الداخلي من حيث حركة التنقل الجماعي أو إمدادات الإغاثة في حالات الطوارئ. إن استمرار قطر في الاعتماد على التكنولوجيا الرقمية في إدارة هذه القطاعات يجعلها عرضةً لمثل هذه الهجمات التي قد تُفضي، في حال وقوعها، إلى حالة من الفوضى[1].

2. التهديدات السياسية من خلال الهجمات الإلكترونية

تتمثل بعض الهجمات السيبرانية في استهداف الأنظمة السياسية للدولة، حيث يمكن التلاعب في الانتخابات أو نشر الشائعات عبر وسائل الإعلام الرقمية. الهجمات التي تستهدف الأنظمة الانتخابية والمعلومات الحكومية يمكن أن تؤدي إلى فقدان الثقة العامة في الحكومة وتفكيك الإجماع السياسي داخل الدولة. في قطر، على الرغم من أن النظام السياسي يتسم بالاستقرار، فإن الهجمات الإلكترونية التي تستهدف الأنظمة الحكومية قد تؤدي إلى إضعاف قدرة الحكومة على اتخاذ قرارات استراتيجية سريعة أو قد تضر بمصداقية الدولة داخليًا وخارجيًا.

ثانيا: تأثير الإرهاب الإلكتروني على الأمن السياسي

لا يقتصر تأثير الإرهاب الإلكتروني على القطاعات الحيوية والاقتصادية فقط، بل يمتد أيضًا إلى الأمن السياسي، حيث يمكن أن تكون الهجمات الرقمية أداة فعالة لإحداث الاضطرابات السياسية. تلعب الفضاء الرقمي وشبكات التواصل الاجتماعي دورًا كبيرًا في تشكيل الرأي العام، ما يجعلها هدفًا رئيسيًا للمهاجمين الذين يسعون إلى التأثير على النظام السياسي في الدولة.

3. التأثير على الاستقرار السياسي

تستهدف الهجمات الإلكترونية الأنظمة السياسية في الدولة بهدف التأثير على استقرار الحكومة وتقويض شرعية النظام الحاكم. من خلال الاختراقات الرقمية والتلاعب بالمعلومات، يمكن للجماعات الإرهابية أو القوى المعادية نشر الأخبار الكاذبة أو التلاعب بالبيانات الحكومية لنشر الشائعات وتفكيك الثقة بين المواطنين والحكومة. في قطر، حيث يتوقع أن تلعب المعلومات الرقمية دورًا متزايدًا

[1] خليفة، إيهاب (2024)، أمن البنية التحتية الحرجة في العصر الرقمي: حماية المرافق الاستراتيجية من التخريب السيبراني، (القاهرة: المركز العربي للبحوث والدراسات)، ص 175–178.

في المشاركة السياسية واتخاذ القرارات، فإن مثل هذه الهجمات يمكن أن تؤدي إلى إحداث زعزعة في العلاقة بين القيادة والمواطنين[1].

4. التلاعب بالانتخابات والآراء العامة

قد تستهدف الهجمات السيبرانية الأنظمة الانتخابية بهدف التلاعب بالنتائج أو تحريف عمليات التصويت، أو حتى إثارة أزمات اجتماعية من خلال تشويه الحقائق ونشر الأكاذيب عبر الإنترنت. كما يمكن أن تطال هذه الهجمات منصات التواصل الاجتماعي والمنتديات العامة لترويج دعاية سياسية أو أيديولوجيات متطرفة. وقد كشفت بعض الدراسات في مجال الأمن السيبراني عن أساليب متنوعة يستخدمها المهاجمون في هذا السياق، مثل التصيد الاحتيالي والهجمات على قواعد البيانات الانتخابية.

ثالثًا: تأثير الإرهاب الإلكتروني على الأمن الاقتصادي

يشمل الأمن الاقتصادي حماية الاقتصاد الوطني من المخاطر التي تهدد الاستقرار المالي والنمو الاقتصادي، ويُعَدّ الإرهاب الإلكتروني من أبرز التهديدات التي تستهدف هذا النوع من الأمن. إذ يمكن للهجمات الرقمية أن تتسبب في تعطيل العمليات المالية وسرقة البيانات الاقتصادية، مما يؤدي إلى خسائر مالية فادحة وتراجع الثقة العامة في الأسواق.

5. تأثير الهجمات على البنوك والمؤسسات المالية

تُعَدّ البنوك والمؤسسات المالية أهدافًا رئيسية للهجمات الإلكترونية نظرًا لاعتمادها الكبير على الأنظمة الرقمية في إجراء المعاملات المالية. وقد تؤدي الهجمات السيبرانية على النظام المالي إلى تعطيل التحويلات المالية أو الصفقات الاستثمارية، مما يفضي إلى آثار اقتصادية جسيمة على المدى القصير. وفي قطر، حيث يُعَدّ القطاع المالي من أكثر القطاعات حساسية، فإن استهداف المؤسسات المالية قد يؤدي إلى تراجع الثقة في العملة الوطنية والتأثير في الاستثمارات الدولية. كما أن تعطيل الأنظمة المصرفية قد يُربك الاقتصاد الوطني من حيث تدفق الأموال وتسجيل المعاملات المالية، مما يضر بمصداقية قطر بوصفها مركزًا ماليًا في المنطقة[2].

---

[1] آل ثاني، ناصر بن حمد (2022)، السيادة الرقمية وتحديات الأمن القومي في القرن الحادي والعشرين، (الدوحة: دار لوسيل للنشر والتوزيع)، ص 182–185.

[2] مصرف قطر المركزي (2023)، إطار مرونة القطاع المالي السيبراني: الاستراتيجية واللوائح التنظيمية، الطبعة الثانية، (الدوحة: قسم الإشراف والرقابة)، ص 88–91.

6. الآثار على الأسواق المالية

تستهدف الهجمات السيبرانية أيضًا الأسواق المالية، حيث يمكن أن تؤدي الهجمات على بورصة قطر أو البنوك الكبرى إلى خسائر مالية ضخمة نتيجة توقف الأنظمة لفترات طويلة. إن استهداف هذه القطاعات الحيوية يضعف من ثقة المستثمرين ويؤثر سلبًا على الاستثمارات الأجنبية التي تعد ضرورية لدعم الاقتصاد القطري. في حال تعرض القطاع المالي أو بورصة الأسهم القطرية للهجوم، فقد ينشأ ركود اقتصادي، ويؤدي ذلك إلى ارتفاع تكلفة الدين للدولة.

7. التأثير على التجارة والقطاع الصناعي

يمكن أن تتأثر القطاعات الصناعية والتجارية أيضًا بهجمات الإرهاب الإلكتروني، حيث تعتمد هذه القطاعات بشكل متزايد على الأنظمة الرقمية في إدارة سلاسل التوريد والمعاملات التجارية. يمكن أن تؤدي الهجمات الإلكترونية على شبكات الإمداد إلى تعطيل العمليات التجارية والإنتاج الصناعي، ما يتسبب في انخفاض الإنتاج وزيادة التكاليف. كما أن الهجمات على التجارة الإلكترونية يمكن أن تضر ب القطاع التجاري، وتؤدي إلى خسائر مالية هائلة نتيجة إغلاق المواقع التجارية أو تعطيل أنظمة الدفع.[1]

للإرهاب الإلكتروني تأثيرات عميقة على الأمن الوطني والسياسي والاقتصادي في دولة قطر. من خلال استهداف القطاعات الحيوية مثل الطاقة، النقل، والخدمات المالية، يمكن أن تؤدي الهجمات السيبرانية إلى خسائر كبيرة في جميع المجالات، بدءًا من تعطيل الحياة اليومية للمواطنين وصولًا إلى تدهور الثقة في النظام السياسي والاقتصادي. وعلى الرغم من الجهود الكبيرة التي تبذلها الدولة لتعزيز أمنها السيبراني، فإن الإرهاب الإلكتروني يظل تهديدًا مستمرًا يتطلب استراتيجيات وقائية واستجابة سريعة لتجنب الأضرار الكبيرة التي قد تنجم عنه.

الفرع الثالث: استراتيجيات الحكومة القطرية لمكافحة الإرهاب الإلكتروني

تمثل استراتيجيات الحكومة القطرية في مواجهة الإرهاب الإلكتروني جزءًا أساسيًا من الجهود الوطنية لتعزيز الأمن السيبراني وحماية الأمن القومي من مخاطر الفضاء الرقمي. ومع التوسع الكبير في استخدام التكنولوجيا الرقمية في مؤسسات الدولة والقطاع الخاص، أدركت الحكومة القطرية منذ وقت مبكر أهمية وضع إطار استراتيجي متكامل يساهم في مواجهة التهديدات الرقمية، لا سيما تلك التي تنطوي على نوايا إرهابية تستهدف البنى التحتية الحيوية أو التأثير على الاستقرار الوطني. تتمحور الاستراتيجيات الوطنية حالياً حول تعزيز الحماية، تطوير التشريعات، بناء القدرات البشرية،

[1] خليفة، مرجع سابق، ص198-201.

وزيادة التعاون الدولي، وذلك في إطار رؤية قطر الوطنية 2030 لضمان مجتمع آمن ومزدهر في الفضاء الرقمي .

الاستراتيجية الوطنية للأمن السيبراني 2024–2030

في سبتمبر 2024، أطلقت الحكومة القطرية الاستراتيجية الوطنية للأمن السيبراني 2024–2030، التي تمثل حجر الأساس في جهودها لمكافحة التهديدات الرقمية والإرهاب الإلكتروني، وتأتي الاستراتيجية في سياق تكامل السياسات الوطنية مع هدف تحقيق رؤية قطر الوطنية 2030[1].

ترتكز هذه الاستراتيجية على خمس ركائز رئيسية تشمل:[2]

1. تعزيز الأمن والصمود السيبراني في نظام الدولة الرقمي، وبالأخص حماية البنية التحتية الوطنية الحيوية. يهدف ذلك إلى ضمان قدرة الشبكات الحساسة مثل الطاقة والاتصالات والنقل على الصمود أمام الهجمات الرقمية المتقدمة وفورية الاستجابة للحوادث.
2. التشريعات والتنظيمات وإنفاذ القانون لتوفير إطار قانوني متماسك يتعامل مع الجرائم الإلكترونية بكافة أشكالها، بما في ذلك الإرهاب الإلكتروني وتعزيز آليات التعاون بين الجهات الوطنية المختلفة.
3. نمو اقتصاد مبتكر قائم على البيانات، حيث تم إدراج بناء القدرات الوطنية في المجالات التقنية والبحث والتطوير في صميم الاستراتيجية لتعزيز الاستقلالية التقنية.
4. تعزيز الثقافة السيبرانية وتنمية القوى العاملة، عبر برامج توعية وطنية وتدريب متخصصين في مجال الأمن السيبراني، لضمان وجود خبرات وطنية متقدمة للتصدي للهجمات الرقمية.
5. التعاون الدولي والشراكات الموثوقة لمواجهة التهديدات العابرة للحدود بتنسيق دولي فعال، مما يعكس إدراك قطر لأهمية الشراكات الإقليمية والدولية في مكافحة الإرهاب الإلكتروني.

تسعى هذه الركائز مجتمعة إلى بناء منظومة وطنية شاملة وعادلة تتعامل مع الأخطار الرقمية بكفاءة أعلى، وتضمن حماية المصالح الحيوية للدولة والمجتمع .

[1] وكالة الأمن السيبراني الوطنية (2024)، الاستراتيجية الوطنية للأمن السيبراني بدولة قطر 2024–2030: نحو فضاء سيبراني آمن ومرن، (الدوحة: وكالة الأمن السيبراني الوطنية)، ص 12–15.

[2] المرجع السابق، ص18–22.

إنشاء وتعزيز دور الوكالة الوطنية للأمن السيبراني(NCSA)

أُنشئت الوكالةُ الوطنيةُ للأمن السيبراني في قطر عام 2021 بوصفها جهةً مركزيةً موحدةً مسؤولةً عن تنسيق جهود الأمن السيبراني على مستوى الدولة، بما في ذلك مكافحة الإرهاب الإلكتروني وإدارة الاستراتيجية الوطنية ذات الصلة[1].

تقوم الوكالة بعدة أدوار استراتيجية، من أبرزها:[2]

1. تطوير السياسات والأطر التنظيمية للأمن السيبراني القومي، بما يتوافق مع أفضل الممارسات الدولية .
2. إعداد وتنفيذ برامج التوعية الوطنية، التي تستهدف رفع مستوى الوعي الأمني بين المؤسسات لحكومية، الشركات، والأفراد بشأن أساليب الهجمات الرقمية وطرق الوقاية منها .
3. دفع جهود التعاون الدولي مع الجهات المماثلة، والمساهمة في تبادل المعلومات الأمنية، وتنظيم المبادرات المشتركة التي تعزز الاستجابة للتهديدات الرقمية .

توضح هذه المبادرات التزام قطر بتعزيز حضورها في منتديات الأمن السيبراني العالمية، وتأهيلها كجهة فاعلة في تطوير **المعايير الدولية** لممارسة الأمن الرقمي.

الخاتمة:

في ختام هذه الدراسة، يتضح أن التهديدات الرقمية، ولا سيما الإرهاب الإلكتروني، باتت تمثل تحديًا جوهريًا للأمن القومي القطري بأبعاده الأمنية والسياسية والاقتصادية، في ظل الاعتماد المتزايد على البنية الرقمية في إدارة القطاعات الحيوية. وقد أظهرت الدراسة أن استهداف البنية التحتية الحيوية، والتأثير في الأنظمة السياسية، وتهديد القطاع المالي، يُشكّل مخاطر مباشرة على استقرار الدولة وثقة المجتمع في مؤسساتها.

كما بيّنت الدراسة أن دولة قطر حققت تقدمًا ملحوظًا في مواجهة هذه التهديدات من خلال تبنّي الاستراتيجية الوطنية للأمن السيبراني، وإنشاء الوكالة الوطنية للأمن السيبراني، وتطوير الإطار التشريعي المنظّم للجرائم الإلكترونية، إلا أن هذه الجهود لا تزال بحاجة إلى دعم مستمر عبر تنمية القدرات البشرية المتخصصة، وتعزيز التعاون الإقليمي والدولي، ومواكبة التطورات التقنية المتسارعة.

---

[1] القرار الأميري رقم (1) لسنة 2021 بإنشاء وكالة الأمن السيبراني الوطنية، الجريدة الرسمية لدولة قطر، العدد (4)، ص5–8.

[2] وكالة الأمن السيبراني الوطنية (2025)، مرجع سابق، ص24–27.

وفي هذا السياق، تبرز أهمية ترسيخ ثقافة سيبرانية وطنية قائمة على التوعية والوقاية، إلى جانب تعزيز الشراكة بين القطاعين العام والخاص. ويظل الحفاظ على الأمن السيبراني ركيزة أساسية لحماية المستقبل الرقمي لدولة قطر وضمان استقرارها وأمنها في ظل التحديات الرقمية المتنامية.

النتائج:

1. التهديدات الرقمية تمثل تهديدًا حقيقيًا للأمن القومي القطري: الدراسة أظهرت أن التهديدات الرقمية، وخاصة الإرهاب الإلكتروني، تشكل تهديدًا فعليًا للبنية التحتية الحيوية في قطر، مثل قطاعات الطاقة والنقل والاتصالات، مما يؤثر بشكل كبير على الأمن الوطني.
2. تعطيل البنية التحتية الرقمية يؤثر بشكل مباشر على حياة المواطنين: استهداف البنية التحتية الحيوية في قطر يمكن أن يتسبب في انقطاع الخدمات الأساسية مثل الكهرباء والمياه والنقل، مما يؤدي إلى أزمات اجتماعية واقتصادية.
3. الأمن السياسي يتأثر بتلاعب المعلومات والهجمات على الأنظمة الحكومية: الهجمات الرقمية على الأنظمة السياسية أو الانتخابات يمكن أن تؤدي إلى زعزعة الثقة بين المواطنين والحكومة، وبالتالي إضعاف الاستقرار السياسي.
4. الاقتصاد القطري عرضة للهجمات الرقمية: الهجمات على القطاع المالي والأنظمة الاقتصادية يمكن أن تعرض قطر لخسائر مالية ضخمة، بما في ذلك تعطيل المعاملات المالية والتجارة الإلكترونية.
5. الاستراتيجيات الوطنية تعد فعالة لكن لا تزال بحاجة لتطوير مستمر: على الرغم من أن قطر قد وضعت استراتيجيات فعالة لمكافحة الإرهاب الإلكتروني، إلا أن التطورات السريعة في التكنولوجيا والهجمات السيبرانية تتطلب تحديثًا مستمرًا لهذه الاستراتيجيات.
6. التعاون الدولي والإقليمي أساسي لمكافحة التهديدات الرقمية العابرة للحدود: التعاون بين الدول والمنظمات الدولية يعد أداة فعالة في مكافحة الإرهاب الإلكتروني، حيث أن التهديدات الرقمية لا تقتصر على حدود الدول بل تمتد إلى كافة الأنحاء.
7. نقص الكفاءات المتخصصة في الأمن السيبراني يشكل عائقًا كبيرًا: من أبرز التحديات التي تواجه قطر في التصدي للإرهاب الإلكتروني هو نقص الخبرات المتخصصة في الأمن السيبراني، مما يعرقل قدرة المؤسسات على التصدي للهجمات المتطورة.

التوصيات:

1. تحديث الاستراتيجيات الوطنية للأمن السيبراني: يوصى بتطوير استراتيجيات جديدة للأمن السيبراني بما يتناسب مع التطورات التقنية السريعة، والتركيز على تحديث أنظمة الحماية بما يواكب الابتكارات الحديثة في مجال الهجمات الرقمية.
2. تعزيز بناء القدرات البشرية في مجال الأمن السيبراني: يوصى بالاستثمار بشكل أكبر في التدريب والتطوير للكوادر المتخصصة في الأمن السيبراني، من خلال تقديم برامج تدريبية على أعلى مستوى وتعزيز التعاون مع الجامعات والمؤسسات التعليمية لتوفير الكفاءات اللازمة.
3. توسيع التعاون الإقليمي والدولي في مجال مكافحة الإرهاب الإلكتروني: يجب تعزيز التعاون بين قطر والدول الأخرى في مجال الأمن السيبراني لمكافحة التهديدات العابرة للحدود، وتبادل المعلومات والخبرات من خلال المشاركة في اتفاقيات دولية مثل اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.
4. تحسين التشريعات وتطوير الأطر القانونية لمكافحة الجرائم الإلكترونية: يوصى بتحديث القوانين المحلية المتعلقة بالأمن السيبراني لضمان معاقبة الجرائم الرقمية بشكل أكثر فعالية، مع مراعاة تكنولوجيا الجريمة الحديثة، وتعزيز التنسيق بين الجهات القانونية والأمنية.
5. تطوير برامج توعية شاملة للمجتمع والمؤسسات: يجب تكثيف البرامج التوعوية التي تركز على تعليم المواطنين والمؤسسات حول أهمية الأمن الرقمي وكيفية الحماية من الهجمات الإلكترونية، خاصة من خلال وسائل الإعلام الاجتماعية والورش التدريبية.

قائمة المصادر والمراجع:

أولا: الكتب

1. آل ثاني، ناصر بن حمد. (2022). السيادة الرقمية وتحديات الأمن القومي في القرن الحادي والعشرين (ط. 1). الدوحة: دار لوسيل للنشر والتوزيع.
2. بشير، محمد الفاتح محمود. (2022). الإرهاب الإلكتروني: المفاهيم والمواجهة القانونية والتقنية (ط. 1). عمّان: دار الخليج.
3. خليفة، إيهاب. (2023). حروب الجيل الخامس: الأسلحة السيبرانية وتأثيرها على استقرار الدول (ط. 2). القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية.
4. خليفة، إيهاب. (2024). أمن البنية التحتية الحرجة في العصر الرقمي: حماية المرافق الاستراتيجية من التخريب السيبراني (ط. 1). القاهرة: المركز العربي للبحوث والدراسات.
5. الشاوي، علي محمد. (2023). الإرهاب السيبراني: حروب القرن الحادي والعشرين والأمن القومي العربي (ط. 1). الدوحة: دار جامعة حمد بن خليفة للنشر.

6. شرعان، عمار. (2021). الأمن السيبراني والعملية السياسية: حماية الديمقراطية الرقمية من الاختراقات (ط. 1). بيروت: المركز العربي للأبحاث ودراسة السياسات.
7. كمال، جاسم محمد. (2023). الأمن السيبراني في الاستراتيجية القطرية: الوقاية والمواجهة (ط. 1). الدوحة: دار لوسيل للنشر والتوزيع.
8. كمال، جاسم محمد. (2024). الوعي الرقمي والمواطنة المسؤولة في مجتمع المعرفة (ط. 1). الدوحة: دار الثقافة للنشر والتوزيع.

ثانيا: التشريعات والقوانين

1. القرار الأميري رقم (1) لسنة 2021 بإنشاء وكالة الأمن السيبراني الوطنية، الجريدة الرسمية لدولة قطر، العدد (4).
2. قانون حماية خصوصية البيانات الشخصية رقم (13) لسنة 2016، الجريدة الرسمية لدولة قطر.
3. قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، الجريدة الرسمية لدولة قطر.
4. مصرف قطر المركزي (2023)، إطار مرونة القطاع المالي السيبراني: الاستراتيجية واللوائح التنظيمية، الدوحة: قسم الإشراف والرقابة.
5. وكالة الأمن السيبراني الوطنية (2024)، الاستراتيجية الوطنية للأمن السيبراني بدولة قطر 2024–2030: نحو فضاء سيبراني آمن ومرن، الدوحة.
6. وكالة الأمن السيبراني الوطنية (2025)، التقرير السنوي لحالة الأمن السيبراني في دولة قطر، الدوحة.
7. وكالة الأمن السيبراني الوطنية (2024)، تقرير كفاءة الكوادر الوطنية: استراتيجية بناء القدرات البشرية في الفضاء السيبراني، الدوحة.
8. وزارة الخارجية القطرية (2025)، التقرير السنوي حول التعاون الدولي والدبلوماسية الرقمية، الدوحة: إدارة الشؤون الأوروبية والأمريكية.

ثالثاً: التقارير

1. تقارير الاتحاد الدولي للاتصالات (ITU) (2024)، مؤشر الأمن السيبراني العالمي (GCI): تقرير حالة الدول العربية، جنيف.
2. دراسات مركز "إنترناشيونال كرايسس جروب" (2023)، الأمن السيبراني في منطقة الخليج العربي: آفاق التعاون والمواجهة.

رابعا: المراجع الأجنبية

1. Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. Survival, 55(2).