الإرهاب الالكتروني: المخاطر والمبادرات الإستراتيجية: قراءة في التجربة القَطَرية

Cyber Terrorism: Risks and Strategic Initiatives A reading in The Qatari Experience

عبد العالي هبال

جامعة باتنة، الجزائر ، abdoupolitic@gmail.com

تاريخ الإرسال: 2021/01/14 **تاريخ القبول:** 2021/04/07 **تاريخ النشر:** 2021/07/10

ملخص:

يناقش هذا المقال عدة موضوعات، منها: التعرف على ظاهرة الإرهاب الالكتروني والوسائل المستعملة في القيام بالأعمال التخريبية الالكترونية، مع التطرق إلى استراتيجيات مكافحة هذه الجريمة الالكترونية التي شكلت هاجسا كبيرا للكثير من الدول، ومن بينها دولة قطر التي أدركت أهمية الأمن السيبراني، منذ عدة سنوات، وقد عملت بدأب على تطوير وتنفيذ عدة إجراءات وتدابير لمجابهة تهديدات الفضاء الالكتروني.

***الكلمات المفتاحية** الإرهاب، الإرهاب الالكتروني، الأمن السيبراني، تكنولوجيا المعلومات والاتصال، دولة قطر*

Abstract:

The article discusses several topics, including; Knowing the electronic terrorism phenomenon and its means, the strategies of combat the electronic crimes, which concidered as a great concern for all countries, including the State of Qatar, which understood the importance of cybersecurity early, and has worked diligently to develop and implement several Procedures and measures to confront the threats and challenges related to cyberspace

***keywords:** Terrorism, E- Terrorism, Cybersecurity, Information and Communication Technology, The State of Qatar*

* **المؤلف المرسل: عبد العالي هبال abdoupolitic@gmail.com**

مقدمة:

أدى التطور التكنولوجي لوسائل الاتصال الحديثة إلى تحول جذري في مفهوم الظاهرة الإرهابية، من خلال إعادة تشكيل أشكالها الحالية؛ بحيث لم تعد تحتفظ بشكلها التقليدي القادر على الاستهداف والهجوم؛ بل أصبحت عابرة للحدود، مما يصعب السيطرة عليها سواء بإغلاق الحدود أو تأمينها؛ فالجماعات الإرهابية، الآن، معنية بانتشار الفكرة وتجنيد العناصر عبر الانترنت، كما انتقلت المعسكرات التدريبية، الآن من العالم الحقيقي إلى العالم الافتراضي؛ حيث لم يعد من الضروري تدريب الأفراد في معسكر مختبئ في كهف أو على قمة جبل، ولكن العنصر الجديد يحتاج فقط إلى الحصول على التدريب من خلال الدخول إلى مواقع الجماعات الإرهابية.

أصبح الإرهاب الالكتروني خطراً يهدد العالم بأسره، بسبب سهولة الاستخدامات السيئة للتقنيات الحديثة مع شدة أثرها وضررها، فيقوم المستخدم بعمله الإرهابي وهو في منزله أو في مكتبه، أو في مقهى أو حتى من غرفة في احد الفنادق، بهدف ترويع الناس وإيذائهم وتعريض حياتهم للخطر.

لقد أضحت هذه الجريمة الالكترونية هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الانترنت والذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم يوم بعد يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية والتي سببت أضرارا جسيمة على الأفراد والمنظمات والدول.

قطر من الدول الرائدة في مجال الاتصالات الرقمية، وتطورها يعتمد على قدرتها في ضمان أمن تقنياتها وبياناتها وشبكاتها في مواجهة الكثير من التهديدات والتحديات، إلا أن وتيرة الهجمات باتت متزايدة وأكثر تطورا، وتتسبب في أضرار أكثر حالة نجاحها؛ وبالتالي لابد من أخذ إجراءات حاسمة لحماية الاقتصاد وخصوصيات المواطنين. من خلال وضع إستراتيجية وطنية لمحاربة الإرهاب الالكتروني وحماية الأمن المعلوماتي، مما يجعلها قادرة وصامدة في عالم رقمي سريع تطور.

وعليه، يهدف هذا المقال إلى تناول موضوع مخاطر الإرهاب الالكتروني والتدابير والاحترازات الرامية لمجابهته وذلك، باستعراض التجربة القطرية في مواجهة الإرهاب الالكتروني، مع التطرق في بداية المقال إلى المرتكزات النظرية والمفاهيمية للإرهاب الالكتروني مع التعريف بوسائل هذه الجريمة الخطيرة، والتي تتطلب وضع استراتيجيات عديدة؛ فنية، قانونية، سياسية، وأمنية للتصدي إليها ومجابتها.

وتتلخص مشكلة الموضوع في البحث عن مفهوم الإرهاب الالكتروني، والوسائل التي يستعملها الإرهابيون في تنفيذ أعمالهم المروعة، مع عرض الآليات المختلفة لمواجهة هذا السلوك الإجرامي، الذي شكل هماً يؤرق، اليوم، الكثير من الدول، ومنها دولة قطر التي بذلت جهوداً كبيرة من أجل تحقيق أمنها السيبراني، لذلك؛ فإن المقال يتناول الإجابة عن الإشكالية من خلال السؤال التالي:

- ماهي أهم المبادرات الإستراتيجية لدولة قطر في مواجهة تهديدات الإرهاب الالكتروني؟

ويندرج تحت هذا السؤال التساؤلات التالية:

- ماهي المرتكزات النظرية والمفاهيمية للإرهاب الالكتروني؟

- ماهي وسائل التي يستخدمها الإرهابيون في القيام بأعمالهم المروعة؟
- ما سبل مواجهة العمل الإرهابي الالكتروني؟
- ما محاور الإستراتيجية القطرية في التصدي لظاهرة الإرهاب الالكتروني؟

1. الإرهاب الالكتروني: رؤية معرفيــة

الإرهاب في اللغات الأجنبية القديمة مثل اليونانية؛ حركة من الجسد تفزع الآخرين، وقد أطلق معجم اللغة العربية في معجمه الوسيط على الإرهابيين وصفاً يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم؛ فكلمة إرهاب تستخدم للرعب أو الخوف الذي يسببه فرد أو جماعة أو تنظيم سواء أكان لأغراض سياسية أو شخصية أو غير ذلك؛ فتتطور ظاهرة الإرهاب جعلها لا تقتصر على الناحية السياسية فقط؛ بل شملت نواحي قانونية، عسكرية، اقتصادية، تاريخية واجتماعية.

وقد وضع وزراء الداخلية والعدل العرب في الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998م تعريفا للإرهاب بأنه:" كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم أو تعريض حياتهم أو أمنهم أو حريتهم للخطر أو إلحاق الضرر بالبيئة أو أحد المرافق أو الأملاك العامة أو الخاصة أو اختلاسها أو الاستيلاء عليها أو تعريض أحد الموارد الطبيعية للخطر". (السند 1430هـ، ص. 34)

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوما بعد يوم سواء في المؤسسات المالية أو المرافق العامة أو المجال التعليمي أو الأمني وغير ذلك؛ و لكن بالرغم من الفوائد التي لا حصر لها للوسائل الإلكترونية؛ فإنه هناك الوجه الأخر لها المتمثل في استخدامات السيئة و الضارة لهذه التقنيات الحديثة، ومنها الإرهاب الإلكتروني.

إن الإرهاب الإلكتروني ما هو إلا نسخة الكترونية عن الإرهاب التقليدي، والذي نشأ و ترعرع في أحضان بيئة تقنية المعلومات والاتصالات وشبكة الانترنت، تم خطف هذه التقنية من قبل مجرمي الإرهاب وتم تسخيرها لأهدافهم الإجرامية، كما تم استقطاب العديد ممن لهم خبرة و علم في هذه التقنيات فوجدوا ضالتهم في هذه البيئة الجذابة، وتم التركيز عليها في العديد من عملياتهم للأسباب التالية: (السند 1430هـ، ص. 35)

- بيئة تقنية المعلومات و الاتصالات والانترنت أسرع وارخص وأدق من الطرق التقليدية للإرهاب؛
- استطاعتهم التخفي من أعين جهات المواجهة؛
- لا يوجد حواجز مادية في طريقهم و لا يوجد حدود دولية أو جغرافية تحول دونهم و ارتكاب جرائمهم في أي بقعة من بقاع الدنيا؛
- ترتكب الجريمة الإلكترونية عن بعد؛
- تأثيرها مروع و مدمر و عنيف و الخسائر كثيرة.

ووفقا للتعريف الذي قدمته دوروثي دينينج، أحد أبرز الباحثين في مجال الأمن الإلكتروني، يجمع مصطلح الإرهاب الإلكتروني Cyber Terrorism ما بين مفهوم" الإرهاب" و"الفضاء الإلكتروني"، ومن ثم؛ فهو يشير إلى الاعتداءات والتهديدات الموجهة لأجهزة الحاسب الآلي والشبكات الإلكترونية والمعلومات الموجودة

عليها بهدف إجبار الحكومات والمجتمعات على أفعال معينة لإغراض سياسية أو اجتماعية (الشهري 2015، ص. 35)

هناك عدد من المصطلحات التي تستخدم وتتداخل في معانيها مع الإرهاب الالكتروني منها؛ الحرب الفضائية (CYBER WAR)، وحرب الشبكات (Net War). وحرب المعلومات (IWF)، والإرهاب الفضائي (Cyber Terrorism) والإرهاب التخيلي ((Virtual Terrorism).

ويُعرف الإرهاب التخيلي على أنه:" التقاء للإرهاب مع الفضاء التخيلي، وهو يعني التهديدات غير القانونية ضد الحاسبات والشبكات والمعلومات المخزنة، وذلك لإخافة أو إجبار الحكومات أو الناس لتعزيز أهداف سياسية أو اجتماعية، وهو العنف ضد الأفراد أو الممتلكات أو أنه مؤذ لدرجة كافية لخلق الخوف، والتعديات المفضية للموت أو الإصابة أو الانفجارات أو الخسارة الاقتصادية ماهي إلا أمثلة للتعديات على الإرهاب التخيلي، ويمكن تصنيف الجمهور المستهدف في ثلاث فئات هي: الأفراد، الممتلكات، والحكومات. (البداينة 2008، ص. ص. 12-13)

نظرًا لعدم وجود تعريف دقيق ومتفق عليه لمفهوم الإرهاب السيبراني، تتداخل فئتان مختلفتان من الإرهاب؛ الإرهاب السيبراني الخالص والإرهاب السيبراني الهجين.

النوع الأول: الإرهاب الالكتروني الخالص، ويتعلق بالهجمات المباشرة على البنية التحتية الالكترونية للضحية، مثل أجهزة الكمبيوتر، والشبكات والمعلومات، المخزنة، لتحقيق أهداف مختلفة مثل تدهور وظائف أنظمة المعلومات، وتدمير الأصول الافتراضية والمادية وحجب المواقع وتعطيل الحياة اليومية من خلال استهداف البنى التحتية التي تعتمد على البرامج مثل المنشآت الطبية، والمنح الدراسية، وأنظمة النقل والمالية..الخ

أما النوع الثاني: الإرهاب الالكتروني الهجين، ويتعامل مع استخدام الإرهابيين للفضاء الالكتروني في أنشطتهم المختلفة ومن أهم نماذجه:

- الدعاية والحرب النفسية، كان لتنظيم داعش سبع وكالات صحفية، بالإضافة إلى 37 مكتبا في دول مختلفة، كما لتنظيم القاعدة فرع أعلامي يسمى "سحاب"؛
- الاتصال والأمن: والهدف من ذلك إرسال رسائل مشفرة وإخفاء محتوى المناقشات السرية، أو التخطيط لهجمات وتنسيقها، مثل مقتل القس الفرنسي في نورماندي في يوليو 2016 حيث تلقى القتلة تعليماتهم عبر الشبكة؛
- تجنيد أعضاء جدد فالويب أصبح الأداة الأكثر استخداماً لتجنيد ودعم المنظمات الإرهابية؛
- التدريب: نشر كتيبات تدريبية على مواقع المنظمات حول كيفية وتصنيع المتفجرات؛
- جمع التبرعات؛
- جمع المعلومات عن الأهداف البشـــرية المحتملة.(https://bit.ly/39fVJSQ)

2. وسائل الإرهاب الالكتروني

للإرهاب الإلكتروني وسائل متعددة نذكر منها، ما يلي:

1- **الفيروسات:** الفيروسات الإلكترونية هي برامج تصمم لإحداث تدمير أو تعطيل في برمجيات الحواسيب بدون علم من أصحاب تلك الأجهزة، وهناك عدة أنواع من هذه الفيروسات الحاسوبية منها ما هو صعب التحديد و الأخر سهل التحديد ومنها ما هو سريع الانتشار مؤذ، والآخر بطيء الانتشار و يحتاج إلى أيام أو أسابيع أو أشهر و بعضها غير مؤذ ويسبب إزعاجا وإرباكا فقط.

2- **أنظمة الهاكرز:** حيث يستخدم الهاكرز احد برامج التجسس التي ترتبط مع ملف Batch الذي يعمل كسيرفر يستطيع إن يضع له الهاكرز (اسم مستخدم) و (رمز سري) تخوله إن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى أجهزة الحواسيب ويستطيع أن يجعل جهاز الحاسب مفتوحا؛ فيستطيع أي هاكرز أن يدخل إليها، ومن أشهر برامج الهاكرز نذكر: Serveur SVB7, Netbus Haxporf, Web cracker 4 .

3- **البريد الالكتروني:** البريد الإلكتروني email أكثر سهولة و سرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني؛ حيث يتم من خلال استخدامه التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، كما يقومون باستغلاله في نشر أفكارهم والترويج لها والسعي لتكثير الإتباع والمتعاطفين معهم عبر الرسائل الإلكترونية، ومما يقوم به الإرهابيون أيضا اختراق البريد الالكتروني وهتك أسرارهم والاطلاع على معلوماتهم، وبياناتهم والتجسس عليهم؛ لمعرفة مراسلاتهم وخاطباتهم والاستفادة منها في عملياتهم التخريبية. (الغثير وبن هيشة 1429هـ، ص. ص. 26-27)

4- **إنشاء المواقع على الشبكة العنكبوتية الانترنت:** يتم إنشاء وتصميم مواقع على هذه الشبكة المعلوماتية العالمية لنشر الأفكار والدعوات الإرهابية؛ بل ولتعليم الطرق و الوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أُنشئت مواقع لتعليم صناعة المتفجرات وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الالكتروني وكيفية الدخول على المواقع المحجوبة وطريقة نشر الفيروسات وغيرها. (العسيري 2010، ص. 5)

5- **تدمير المواقع:** من بين وسائل الإرهاب الإلكتروني الأخرى هي تدمير المواقع، والذي يقصد به الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بالانترنت من خلال نظام آلي (server-pc) أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال.

وليس هناك وسيلة تقنية يمكن تطبيقها وتحول تماما دون تدمير المواقع أو اختراق المواقع بشكل دائم، فالمتغيرات التقنية وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (open source) سواء أكان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة أو البرمجة، وجعلت الحيلولة دون الاختراقات صعبة جدا، إضافة إلى إن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق و تدمير المواقع، ومن المعلوم إن لدى المؤسسات من الإمكانيات و القدرات ما ليس لدى الأفراد.

يستطيع قراصنة الحاسب الآلي (Hackers) التحصل على المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، و ذلك راجع إلى إن التطور المذهل في عالم الحاسب الآلي بصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولاسيما وأن مرتكبيها ليسوا مستخدمين عاديين؛ بل قد يكونون خبراء في مجال الحاسب الآلي.

وتتم عملية الاختراق الإلكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الالكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي. (السند 1430هـ، ص. 37).

3. طرق مواجهة الإرهاب الالكتروني

إذا كانت الانترنت مجالاً للحرية، فهذه الحرية لا يمكن أن تكون مطلقة؛ فقد استخدمت لتقويض أمن الدولة ومواطنيها؛ حيث تسببت الهجمات في الفضاء الالكتروني في معاناة الأفراد والشركات جراء الضرر الذي ألحق بهما، والذي نتج عنه إعاقة الأداء الوظيفي للمؤسسات وللمشغلين الأساسين لحياة الأمة، لذلك فهي تشكل اعتداءات غير مقبولة على أمن هذه الجهات الفاعلة.

ولمواجهة تطور الإرهاب الالكتروني، يجب على الدول والحكومات العمل على وضع إستراتيجية شاملة تستهدف التصدي لهذه الجريمة الالكترونية، والتي يمكن تفصيلها فيمايلي:

- التعرف بشكل معمق على التهديدات السيبرانية: يجب وضع سياسة شاملة لتوقع التهديد، وذلك بإعداد التقارير وتحليل إشارات الهجوم من المصادر الداخلية الأربعة وهي: الذكاء، أنظمة الكشف التابعة لمركز الدفاع الالكتروني، الخدمات المكلفة بمكافحة الجرائم الالكترونية، خدمات المراقبة التي لها معرفة بالتهديد مع جميع شركائها.
- السيطرة على أمن نظام المعلومات الخاصة: من خلال تصميم وتشغيل أنظمة المعلومات الآمنة والتي تستطيع التكيف مع التهديد مع استخدام الموارد على مستوى الأمن والحماية، وتحديد ميزانيات نظام المعلومات والدفاع عنه.
- المساهمة في حماية الأنظمة الحكومية الحساسة: من خلال تنفيذ توجيهات السلامة الوطنية المتعلقة بالأنشطة المدنية للدولة، بوضع هيكل حماية المصالح الإستراتيجية للدولة، بما ذلك نظم المعلومات الهامة.
- تطوير الممارسات الجيدة في خدمات الرقابة التشغيلية ضد جرائم الانترنت عن طريق توحيد العلاقات مع مقدمي الخدمات الرقمية وتعزيز الشبكات الإقليمية السيبرانية من خلال التدريب والموارد المادية، وتسريع إجراءات التعاون الدولي، أي لابد من استباقية في تطوير عمل مبتكر متكيف مع تحديات مكافحة الإرهاب الالكتروني .
- دعم نظام المساعدة الوطني لضحايا البرمجيات الخبيثة عبر الإنترنت عن طريق نظام وطني لمساعدة ضحايا البرمجيات الخبيثة السيبرانية يهدف إلى تحسين الوقاية ومساعدة الضحايا، والسلطات المحلية والشركات والأفراد، كما يعتبر هذا النظام آلية للإبلاغ عن الحوادث. (https://bit.ly/3sjKHV5)
- دعم صناعة الأمن السيبراني وتعزيز العلوم والتقنيات في مجال الأمن الإلكتروني: يجب على مؤسسات البحث الجامعي أن تستمر في جذب عقول المهن الأكثر ذكاءً في مجال الأمن السيبراني؛ ولتحقيق ذلك، يجب تعزيز تطوير مراكز التميز القادرة على جذب العلماء الأكثر ديناميكية والأكثر موهبة، وتعميق الشراكة النشطة بين الجامعات والحكومة. لتلبية احتياجات القطاعات على الصعيد الوطني .

- وجود الدفاع الإلكتروني النشط والفاعل، و هو مبدأ تطوير الإجراءات الأمنية لتقوية شبكة أو نظام لجعلهما أكثر صمودا في مواجهة الهجمات. في السياق التجاري، عادة ما يشير الدفاع الإلكتروني الفاعل إلى قيام محللي أمن المعلوماتية بتطوير فهمهم للتهديدات التي تتعرض لها شبكاتهم، ومن ثم وضع وتطوير إجراءات استباقية لمكافحة تلك التهديدات أو الدفاع ضدها، كما يرصد أنشطة الجماعات الإرهابية على الشبكات الاجتماعية وتحليل محتواها وأهدافها والاستراتيجيات المعتمدة، ويرصد نشاط المتعاطفين مع الجماعات الإرهابية وتحليل خطاب العنف والكراهية والتحريض على الإرهاب. (https://bit.ly/3s9Tvgr)

- تعزيز القدرات السيادية (التشفير): إن القدرة على التشفير ضرورية لحماية أهم ما نمتلك من معلومات حساسة، مع الاستعانة بمهارات وتقنيات القطاع الخاص التي تضمنها القيادة المركزية الحكومية للاتصالات.

- ضمان المستوى الأول من التدريب لجميع وحدات مكافحة التهديدات السيبرانية من خلال تكييف أساليب عملها وسلوكها وتطوير التحقيقات في الأشكال الجديدة للانحراف التي تمثلها التهديدات السيبرانية.

- إن حملة التوعية الإلكترونية، المعروفة سابقا باسم Streetwise Cyber، تقدم المشورة التي يحتاجوها المواطنون لحماية أنفسهم من مجرمي الإنترنت وتستعمل الرسائل الموجهة التي تُنشر عبر وسائل التواصل الاجتماعي والإعلانات، وبالتعاون مع الشركات على الترويج للنصيحتين التاليتين: استخدام ثلاث كلمات منتقاة عشوائيا للخروج بكلمة مرور قوية؛ والحرص دائما على تنزيل آخر تحديثات البرامج؛ كما يتفق الخبراء على أن إتباع هذه السلوكيات سيوفر للشركات الصغيرة والأفراد الحماية ضد الجرائم الإلكترونية.

- تطوير الثقافة الأمنية للمواطنين من خلال التحديد المبكر للأسباب والعوامل التي تؤدي إلى انتشار التطرف العنيف المؤدي إلى الإرهاب وعدم تشجيع البيئة على استقطاب الشباب للمشاركة في الأنشطة الإرهابية؛ حيث يتم التضييق على قاعدة تجنيد الإرهابيين من خلال تدابير مخطط لها، ومنسقة عبر أنظمة اتصالات عالية التقنية، والشبكات الرقمية المرنة، للحد من انتشار الراديكالية والتطرف العنيف ()https://bit.ly/3s9Tvgr

- تحسين مستوى الوعي بأمن نظم المعلومات عن طريق نشر ثقافة البيانات داخل مؤسسات الدولة وتوفر الحد الأدنى من المعرفة لتحديد حساسية أو عدم حساسية البيانات، إضافة إلى حملات التوعية بالأمن السيبراني التي توفر أساسا التواصل، وبالتالي زيادة القوة والرؤية خاصة مع جماهير الحساسة (الشباب وكبار السن) من خلال المشاركة في تنظيم حملات اتصال وتوعية مما يسمح بنشر الممارسات الجيدة في هذا المجال. (https://bit.ly/3sjKHV5) .

- خلق منظومة تشريعية تتضمن قوانين توضح ماهية الإرهاب الالكتروني، الأفعال و النشاطات التي تنسب له، كذلك طرق التعامل مع تلك الأنشطة و العقوبات الجزائية التي تنجم عنها؛ أي أننا هنا بصدد احتواء هذا النوع من الأفعال وجعله جريمة كغيره من الجرائم يعاقب عليها القانون نضرا لخطورته وأثاره المدمرة على الدولة المجتمع و الفرد.

- التركيز على التعاون الدولي في مجال مكافحة الإرهاب من خلال تبادل المعلومات والخبرات والاستفادة من المنظمات الدولية المختصة ذات الخبرة للإفادة والاستفادة نظرا للبعد الدولي للأعمال الإرهابية؛ فهناك دول

عانت الكثير من ويلات الإرهاب ودول أخرى تعتبر في بداية مشوارها مع هذه الآفة التي تزداد انتشارا يوما بعد يوم مستعملة كل الوسائل والتقنيات الرقمية، كما يرتكز التعاون الدولي على مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة على أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي بمساعدة المنظمات الدولي والهيئات المتخصصة في محاربة ومكافحة الإرهاب الإلكتروني .(https://bit.ly/39fVJSQ)

4. التجربة القطرية في التصـــدي للإرهاب الالكتروني

في ظل تطور تحديات الأمن السيبراني على مستوى العالم، تأتي حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات على رأس أولويات الدولة القطرية؛ فالفوائد العظيمة التي يقدمها الفضاء الإلكتروني محفوفة بعدد من التحديات التي قد تهدد البنية التحتية التي تعزز من القدرة على الاستخدام الآمن للإنترنت، وسعيًا منها لمواجهة هذه التحديات، بذلت دولة قطر العديد من الجهود الرامية للتصدي إلى ظاهرة الإرهاب الالكتروني وتعزيز الأمن السيبراني.

أ. أهمية الأمن السيبراني لدولة قطر

كغيرها من دول العالم تواجه دولة قطر تحدياً في مجال الأمن السيبراني على مستوى الوزارات والمؤسسات والأجهزة المختلفة في الدولة وجمعيات المجتمع المدني وكذلك الأفراد، لاسيَّما القطاعات الحيوية المتعددة، ومنها قطاع الإعلام والاتصالات وقطاع المال والأعمال وقطاع التجارة وقطاع الطاقة وغيرها. ويعتبر الفضاء الإلكتروني من أكثر الفضاءات أهمية وإستراتيجية والأكثر عرضة للاختراق وللتلاعب في أي لحظة، والإضرار ببيانات الدولة والوزارات والشخصيات العامة والحكومات ويعتبر من التحديات التي تؤرق مختلف دول العالم، ومن هنا، يتوجب تكثيف الجهود والتعاون في هذا المجال للحيلولة دون تمكين المغرضين من تحقيق أهدافهم للحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية في المؤسسات وتدعيمها بكل وسائل الأمن والحماية. فجريمة قرصنة وكالة الأنباء القطرية (قنا) ما هي إلا مثال صارخ على خطورة التلاعب بالأمن السيبراني والعبث بسيادة وكرامة الدول. (https://bit.ly/2LAFU0X)

لقد مكنت الاستثمارات الكبيرة لدولة قطر في مجال تكنولوجيا المعلومات والاتصالات من أن تعتلي مكانة رائدة في المنطقة؛ حيث حلت دولة قطر في المرتبة الأولى عربيا والـ «26» عالميا في مؤشر القوة التكنولوجية الصادر عن مجلة (غلوبال فاينانس) العالمية والذي يقيس أكثر الدول تقدما في قطاع الاتصالات والتكنولوجيا بين 67 دولة حول العالم، حيث سجلت «3.21» نقطة، متفوقة على 41 دولة حول العالم من ضمنها دول كبرى مثل: ايطاليا، والصين والهند أمر الذي يؤكد نجاح دولة قطر في تطورها التكنولوجي وتعزيز قطاع الاتصالات وتكنولوجيا المعلومات وقدرتها على زيادة مستوى الثقافة والمهارات الرقمية بين جميع شرائح المجتمع القطري؛ بهدف تمكينهم من الإسهام في الحياة الاقتصادية والثقافية لدولة قطر من خلال الاستخدام الفعال والآمن لتكنولوجيا المعلومات والاتصالات، بما يدعم توفير قوى عاملة مؤهلة في سوق العمل القطري.

ويعتمد مؤشر القوة التكنولوجية على أربعة (4) معايير في ترتيب الدول، وهي أولاً: أعداد مستخدمي الهواتف الذكية والإنترنت، وثانياً: شبكات تكنولوجيا الجيل الرابع للاتصالات بالمقارنة مع اجمالي عدد السكان، وثالثاً :درجة التنافسية الرقمية التي تقيس مدى الاستعداد لتطوير تكنولوجيات جديدة، ورابعا: القدرة على استغلال الابتكارات الجديدة والبناء عليها. (https://bit.ly/3bo9Sju)

كما احتلت دولة قطر ترتيباً متميزاً بين دول العالم في استخدام الإنترنت والتكنولوجيا الحديثة في ظل الخطوات التي تقطعها الدولة للتحول نحو اقتصاد المعرفة وفقا، وفقا للتقرير حالة شبكات الإنترنت ذات النطاق العريض «البرودباند» 2018 الراصد لحالة دول العالم واستخدامها للأدوات التكنولوجية والاتصال بالإنترنت، وقد كان ترتيب قطر في مؤشرات التقرير في ما يخص عملية اشتراكات النطاق العريض للهاتف الثابت، والعملية التقديرية لكل 100 نسمة في 2017، سابقا للكثير من الدول؛ حيث حققت 9.7 درجة بينما حققت السعودية الأكثر في عدد السكان نسبة أقل 7.6 درجة، ولم تحقق دول كبيرة كماليزيا سوى 8.5 درجة فيما سجلت المغرب 3.9 درجة وجنوب إفريقيا 3 درجات فقط، وهو الأمر الذي يجعل قطر في طليعة الدول العربية وفي منطقة الشرق الأوسط وشمال إفريقيا في مستوى اشتراكات النطاق العريض للهواتف الثابتة.

أما في الشق المتعلق باشتراكات النطاق العريض «البرودباند» للهواتف الجوالة لكل 100 نسمة في 2017، فكان ترتيب قطر بارزاً؛ إذ حققت نمواً سنوياً بنحو 117.4 درجة، متفوقة على السعودية التي حققت نموا بواقع 90 درجة ودول متقدمة مثل بريطانيا التي سجلت نموا بواقع 88.1 درجة وقريبة من الولايات المتحدة الأميركية التي سجلت 132.9 درجة.

كما أن مؤشرات قطر التكنولوجية متميزة في ما يخص النسبة المئوية للأفراد الذين يستخدمون الإنترنت في 2017 والتي سجلت 94 % وهو مستوى ضمن الأعلى عالميا؛ حيث تفوقت قطر على الولايات المتحدة الأميركية التي لم تحقق سوى نسبة 76.2%. (https://bit.ly/3bo9Sju)

وقد كانت دولة قطر قد قفزت 12 مركزاً في مؤشر التجارة الإلكترونية في العام 2019 الصادر مؤخراً عن منظمة الأمم المتحدة للتجارة والتنمية «أونكتاد»؛ حيث ارتفع ترتيبها من المرتبة الـ59 عالميا في تصنيف العام 2018 إلى المرتبة 47 عالميا في تصنيف العام 2019، لتنضم إلى الخمسين الكبار عالمياً في التصنيف الذي يضم 152 دولة حول العالم، وهو ما يعني تفوق قطر على 105 دول ضمن التصنيف، ويرصد مؤشر التجارة الإلكترونية لعام 2019، مدى تقدم الدول وفقاً لأربعة (04) مؤشرات فرعية تشمل: مدى انتشار استخدام الإنترنت، ومدى توفر حسابات إلكترونية للمواطنين فوق عمر 15 عاماً، وانتشار الحسابات المصرفية، والموثوقية البريدية.

كما تقدمت في حزمة معايير متعلقة بالتجارة الالكترونية وهو ما يتماشي مع الاستبيان الذي أجرته وزارة المواصلات والاتصالات، بدعم من مستشاري شركة أبحاث السوق العالمية إبسوس، والذي كشف أن 60 % من جمهور المستهلكين في قطر لديهم الرغبة في التسوق عبر الإنترنت. (https://bit.ly/3bo9Sju)

لقد استثمرت دولة قطر المليارات البنية التحتية والتي تعتمد بشكل كبير على تكنولوجيا المعلومات والاتصالات المتطورة والمبتكرة التي توفر توفر فرصا كبيرَة، ليس فقط لتحقيق نمو اقتصادي وتوسع مستدامين؛ بل لضمان أمن سيراني خلال الدورة الحياتية لتنفيذ كل المشاريع .

ب. تهديدات وتحديات الأمن السيبراني في قطر

يحقق استخدام تكنولوجيا المعلومات والاتصالات منافع هائلة للحكومة والشركات والمؤسسات والأفراد. ومع ذلك، كثيرا ما تنطوي هذه التقنيات على نقاط ضعف، ونظرا لما نتميز به دولة قطر من كونها أحد المنتجين للوقود النظيف، ومقرا لشركات عالمية، ومن أوائل الدول التي تبنت التقنيات الرقمية، ودورها الرائد

في الشؤون الإقليمية؛ تعد قطر مطمعا للجهات المغرضة التي تسعى لعرقلة مسيرتها وهدم ما أحرزته من تقدم.

- **التهديـــــدات**

وقد تطورت التهديدات الإلكترونية من كونها ناتجة عن مجموعات فردية مـن محترفي القرصـنة الإلكترونية إلى جماعات فائقة التنظيم وعصابات إجرامية متقدمة، وأصبحت الهجمات أكر تحديدا للأهداف وأكر تطـورا، وقد ظهرت برمجيات ضارة جديدة وقوية، قادرة على سرقة البيانات السرية، وتعطيل البنية التحتية للشبكات، وتمـثل الهجمات على البنية التحتية الحيوية وما تتضمنه من أنظمة التحكم الصناعية تهديداً متزايداً، لقدرتها على تعطيل الآلات الرئيسية والتسبب بعطل كارثي في المعدات، بل وخسائر في الأرواح.

ودولة قطر، مثل العديد من الدول الأخرى، يجب أن نكون مستعدة لمجابهة الأنواع التالية من التهديدات؛ (https://bit.ly/39kRHIF)

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

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

- **مجموعات الجرائم الإلكترونية:** تسعى المجموعات المتخصصة في ارتكاب الجرائر الإلكترونية إلى التسلل إلى معلومات الحسابات الشخصية لتتمكن من إجراء معاملات احتيالية أو سرقة الأموال الخاصة بصاحب الحساب، كما تهدف هذه المجموعات عادة إلى سرقة المعلومات، حيث تقوم بتسريبها إلى جهات وأفراد غير مصرح لهم بالاطلاع على مثل هذه المعلومات في مقابل مبلغ مالي. ويعمل مجرمو الفضاء الإلكتروني على إيجاد طرق متعددة لتحقيق أهدافهم، بما في ذلك إرسال كميات هائلة من رسائل البريد الإلكتروني منتحلين صفة أحد المصارف أو غيرها من الجهات، وذلك بهدف الحصول على المعلومات المالية للعملاء وبيانات التعرف على هويتهم، وقد يستخدمون هجمات موزعة على نطاق واسع لحجب الخدمة، وذلك لاختراق الشركات التي تعتمد على الإنترنت، ونحن نتوقع أن تقوم مجموعات الجرائر الإلكترونية بهجمات احتيالية نتبع أسلوب الدفع مقدما، وذلك لاستهداف الأفراد غير الحذرين بهدف تحقيق ربح مالي قبل استضافة كأس العالم 2022 في قطر.

- **أشخاص مطلعون ذوو نوايا خبيثة:** وهر الأفراد الموثوق بهم والمصرح لهم بالوصول إلى المعلومات

الداخلية، والذين دفعهم الكسب المادي أو الرغبة في الانتقام أو المصالح الأيديولوجية إلى تهديد سرية أو سلامة أو توافر معلومات المؤسسة ونظم المعلومات الخاصة بها، ونظرا لأنهم مصرح بهم لهم بالوصول إلى الأنظمة والمعلومات، فهم لا يحتاجون لاختراق دفاعات الشبكة، ويمكنهم استخدام عدة طرق للإضرار بأنظمة الحكومة والشركات أو إتلافها.

- **التحديـــات**

إن اعتماد تقنيات جديدة مثل الحوسبة وتطبيقات الهاتف النقال الجديدة وتنفيذ تكنولوجيا الشبكة الذكية، والزيادة الكبيرة في عدد المستخدمين، توفر فرصا مميزة للتطوير والابتكار، إلا أن هذه الفرص من شأنها إيجاد بيئة سريعة التطور تفرض مجموعة خاصة من التحديات التي تؤثر على قدرة فطر في الابتكار والمنافسة على مستوى الاقتصاد العالمي، والتي تتمثل في التالي: (https://bit.ly/39kRHIF)

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

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

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

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

ج. المبادرات الإستراتيجية لتحقيق الأمن السيبراني في قطر

يمكن إبراز المبادرات والجهود القطرية في مجال محاربة الإرهاب الالكتروني وتحقيق الأمن السيبراني من خلال مايلي: (https://bit.ly/3s9hEUi)

- أنشأت قطر اللجنة الوطنية للأمن السيبراني، والهدف من ذلك هو ضمان وجود إطار تشريعي فعال للتصدي للجرائم الإلكترونية وأمن أصولها الحيوية. مع تطبيق قوانين الجرائم الإلكترونية، تعمل الحكومة على إصدار قانون خصوصية البيانات وقانون حماية البنية التحتية للمعلومات الحيوية.

- تم إصدار السياسة الوطنية لضمان المعلومات التي تعزز الإطار التشريعي وتبني أساسًا قويًا للأمن السيبراني، إلى جانب شد معايير أمن المعلومات من ICS لتأمين أصول المعلومات وأنظمة التحكم.

- إنشاء برنامج CIIP للعمل بشكل وثيق مع القطاعات الحيوية لتحسين أمنهم وتزويدهم بالمبادئ التوجيهية بشأن مواجهة تحديات الأمن السيبراني.

- التركيز على برامج التدريب والتوعية (سواء داخل الشركة أو تلك التي تم تطويرها بالشراكة مع شركاء عالميين) لبناء القدرات البشرية.

- تفعيل وظيفة استخبارات التهديدات هي المسؤولة عن مراقبة الفضاء الإلكتروني القطري. يعمل فريق التعامل مع الحوادث مع القطاعات الهامة والجمهور للرد على الانتهاكات الإلكترونية.

- قانون خصوصية البيانات ويتضمن أفضل الممارسات والتشريعات والفروق الدقيقة العالمية في منطقة الاتحاد الأوروبي، ومن المحتمل أن يكون القانون الأول في المنطقة. وتركز إرشادات خصوصية البيانات حول كيفية تعامل المؤسسات مع البيانات الشخصية. سيكون للمستخدمين الحق في الإذن صراحة باستخدام معلوماتهم الشخصية، وفهم مصدر البيانات الثانوي.

- حماية البنية التحتية الحرجة بإنشاء مركز QCERT للتعامل مع أنشطة بناء القدرات وتبادل المعلومات، وقد كانت البداية ببرنامج البنية التحتية الحيوية (CIIP) في عام 2009، وقد حددت 10 قطاعات مهمة بما في ذلك الحكومة، الطاقة، التمويل، الاتصالات، النقل والصحة كجزء من نموذج الشراكة بين القطاعين العام والخاص، حيث تم العمل على تحسين نضج امن المعلومات، بإصدار عددا من السياسات للتعامل مع تهديدات محددة.

- إنشاء لجان خبراء مخاطر المعلومات للقطاعات الحيوية للطاقة والتمويل والحكومة (المزيد قيد الإعداد). من خلال IRECs، بإنشاء منصة للحوار داخل القطاع، وتحديد نقاط الألم والعمل لمعالجتها.

- تطوير إطار عمل وطني لإدارة مخاطر معهد التأمين القانوني لتوجيه تحديد أصول ومؤسسات معهد التأمين القانوني؛

- تقييم التهديدات ونقاط الضعف والعواقب، بالإضافة إلى تطوير ملفات تعريف المخاطر؛

- إجراء تقييمات منتظمة للمخاطر لمنظمات المجتمع المدني والمنظمات الأخرى CII؛

- إجراء تقييمات التبعية والاعتماد المتبادل لتحديد المخاطر النظامية التي تشمل القطاعات الحاسمة.

- رعاية القوى العاملة لأمن المعلومات من طرف فريق الأمن السيبراني من خلال توفير مجموعة المهارات المطلوبة، و توفير كفاءات أمن المعلومات وآليات بناء القدرات. يتم تحقيق ذلك بكفاءة من خلال

القدرات الداخلية المختصة والتعاون الاستراتيجي مع المنظمات ذات السمعة الطيبة والمؤسسات المعتمدة دوليًا. (State of Qatar, Q-SERT , 2014, p25)

- تدريب المتخصصين في مجال الأمن السيبراني؛ حيث تم تدريب أكثر من 300شخص على تنفيذ سياسة NIA إلى جانب العمل مع الجامعات لزيادة الوعي بأمن المعلومات لإعداد المهنيين الشباب للعمل في مجال أمن المعلومات، والعمل مع الكليات للتأكد من أنها تقدم تخرج في مجال أمن المعلومات.

كما أشارت الإستراتيجية الوطنية للأمن السيبراني في قطر 2014 إلى ما يجب أن تقوم به دولة قطر من إجراءات للتقدم نحو تحقيق أهداف محاربة الإرهاب الالكتروني وتحقيق الأمن السيبراني والمتمثلة فيمايلي: (State Of Qatar 2014, p.p. 10-11)

الهدف الأول: حماية البنية التحتية للمعلومات الحيوية الوطنية

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

الهدف الثاني: الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها

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

الهدف الثالث وضع الإطار الثانوي والتنظيمي تعزيز سلامة وحيوية الفضاء الالكتروني

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

الهدف الرابع تعزيز ثقافة الأمن السيبراني

- تعزيز وعي المجتمع بالأمن السيبرانى باستخدام وسائل وقنوات متعددة؛

- تطوير مناهج تثقيفية حول الأمن السيبراني وإتاحتها في المدارس والكليات والجامعات؛
- تشجيع الأفراد على استخدام أدوات وحلول السلامة على الإنترنت للوقاية من الهجمات الإلكترونية.

خاتمة

على الرغم من الأهمية القصوى لاستخدام تكنولوجيا الاتصالات في عالمنا المعاصر في شتى المجالات الأمنية والاقتصادية والتجارية وغيرها، إلا أن إساءة استخدام هذه التكنولوجيا أصبحت تهدد أمن الدول والعلاقات الودية فيما بينها، علاوة على الاعتداء على المجال الخاص للأفراد والأضرار الاقتصادية.

و إدراكا منها للدور الرئيسي الذي تؤديه تكنولوجيات المعلومات والاتصالات في كل مجالات الحياة المختلفة، وفي ظل تطور تهديدات الإرهاب الالكتروني تحديات الأمن السيبراني على مستوى العالم، أطلقت قطر العديد من مبادرات الأمن السيبراني التي تهدف إلى حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات لدولة قطر من هجمات الإرهاب الالكتروني، وكان أبرزها مناقشة القضايا المتعلقة بالأمن السيبراني ومواجهة الجريمة الالكترونية من خلال وضع إستراتيجية وطنية لمحاربة الإرهاب الالكتروني.

وقد وفرت هذه الإستراتيجية تدابير متطورة لتعزيز حماية الشبكات والأفراد في قطر ضد التهديدات السيبرانية وضمان توفر فضاء سيبراني منفتح وآمن، وتتناول هذه الإستراتيجية، التي تم صياغتها من قبل وزارة الاتصالات وتكنولوجيا المعلومات واللجنة الوطنية لأمن المعلومات، خمسة (05) محاور رئيسية هي: حماية البنية التحتية للمعلومات الحيوية للدولة، والتصدي للهجمات السيبرانية والتعافي من آثارها، ووضع إطار قانوني وتنظيمي مناسب لتعزيز فضاء سيبراني آمن وحيوي مع منظومة متكاملة من قوانين السلامة السيبرانية ومكافحة الجرائم السيبرانية، ونشر ثقافة الأمن السيبراني عن طريق رفع الوعي وتشجيع تبادل المعلومات بين الجهات الحكومية ومؤسسات الأعمال والمؤسسات الأخرى، وتعزيز القدرات الوطنية في مجال الأمن السيبراني من خلال المزيد من البرامج التعليمية والتدريبية.

ولم تغفل دولة قطر أيضا الاهتمام بالجانب القانوني، وتنظيم التعامل مع التحديات المُعقَّدة الناجمة عن تزايد الجرائم الإلكترونية للحيلولة دون وقوعها، لذلك كثفت دولة قطر جهودها في مجال الأمن السيبراني، حيث قامت بمراجعة وتحديث التشريعات الوطنية ذات الصلة، بموضوع الأمن السيبراني.

لقد مثلت هذه الإستراتيجية طريقا محدداً يرمي إلى تحقيق الرؤية المستقبلية لدولة قطر بشأن الأمن السيبراني وإيجاد بيئة الكترونية أكثر أمانا، من خلال الاستفادة من الفرص والكفاءات التي تقدمها تكنولوجيا المعلومات والاتصالات المتطورة.

قائمة المراجع

أولا: الكتب

1. البداينة، ذ. م. (2008). الإرهاب المعلوماتي: التعريف، المفهوم، المجالات والنتائج، القاهرة: حلقة علمية بعنوان الانترنت والإرهاب، كلية التدريب جامعة نايف لعلوم الأمنية، مع جامعة عين شمس.
2. السند، ع. ن.ع. أ. (1430ه). وسائل الإرهاب الإلكتروني: حكمها في الإسلام وطرق مكافحتها، الرياض: مجلة الأمن الحياة، جامعة نايف للعلوم الأمنية. العدد 325. جمادى الآخرة 1430ه،

3. العسيري، م. ع. أ. آ. ف. (2010). الإرهاب الالكتروني وبعضا من وسائله، والطرق الحديثة لمكافحته، الرياض: ندوة علمية استعمال الانترنت في تمويل الإرهاب وتجنيد الإرهابيين. مركز الدراسات والبحوث جامعة نايف للعلوم الأمنية.

4. الشهري، ح. ب. أ. (2015). الإرهاب الالكتروني - حرب الشبكات -، الرياض: المجلة العربية الدولية للمعلومات المجلد الرابع. العدد الثامن.

5. الغثير، خ. ب. س. بن هيشة، س. ب. أ.(2009). الاصطياد الالكتروني: الأساليب و الإجراءات المضادة الرياض: مكتبة الملك فهد الوطنية.

ثانيا: المكتبة الالكترونية

6. محمد، ق. إستراتيجية وطنية للأمن السيبراني بتاريخ 05/29/ 2020. الرابط الالكتروني:

(https://bit.ly/3qdeOvx)

7. محمد، س. مؤشرات قطر التكنولوجية متميزة. بتاريخ 2021/01/05، الرابط الالكتروني:

(https://bit.ly/3bo9Sju)

8. دولة قطر، الاسترتيجية الوطنية للأمن السيبراني، بتاريخ: 2021/01/02، الرابط الالكتروني:

ثالثاً: المراجع بالأجنبية

9. State of Qatar (2014), Cybersecurity Strategy National.

10. State of Qatar, (2014 Cybersecurity Division, Q-SERT, Annual Report.

11. Abdul-Sattar abdul Rahman, le Cyber-Terrorisme: Une menace pour le monde, accessed on: (13/12/2020) at: (https://bit.ly/39fVJSQ).

12. le Royume -Unis, HM Government , STRATEGIE NATIONAL DE CYBERSECURITE, acessed on (25/12/2020) at (https://bit.ly/3s9Tvgr).

*13 l*a République Française *(2015),* STRATÉGIE DE LUTTE CONTRE ES CYBERMENACES, accessed on (10/01/2021) at: *(*www.interieur.gouv.fr*)*

14. Khalid Al Hashmi, Qatar's National Cybersecurity Strategy, accessed on (30/12/2020) at: : (https://bit.ly/3s9hEUi)