إستراتيجيات مواجهة التهديدات غير النمطية
"الإرهاب السيبراني انموذجا"

د. احمد حسين الربيعي
خبير وباحث في مكافحة الارهاب

إستراتيجيات مواجهة التهديدات غير النمطية
"الإرهاب السيبراني انموذجاً"

د. أحمد حسين الربيعي
خبير وباحث في جهاز مكافحة الارهاب

تاريخ الاستلام: 2024/3/7 ، تاريخ الارجاع: 2024/4/19 ، تاريخ الموافقة: 2024/5/6

أصبحت قدرة وقوة القوى الكبرى والاقليمية لا تقاس بإمكاناتها الاقتصادية والعسكرية فحسب، وإنما بقوتها التكنولوجيا وحصانة منظومتها السيبرانية، وبذلك فأن وجود بنية فضاء سيبراني وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار؛ إلا أن التوسع في استخدام التقنية يفتح آفاقاً جديدة للمخاطر والتهديدات الارهابية السيبرانية؛ مما يستوجب تعزيز ومكافحة الارهاب السيبراني عبر توفير الحماية للشبكات وللأنظمة التقنية والمعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، فضلاً عن حماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال في إطار الفضاء الرقمي.

وعلى مر التاريخ، كانت هناك العديد من أشكال وصور ظاهرة الإرهاب التي تهدد الأمن الدولي، وقد زاد خطرها بشكل مطرد مع الثورة التكنو معلوماتية والتطور التقني في مجال صناعة الحواسيب والاجهزة الالكترونية وتطوير شبكات الاتصال، فأصبحت طرق وأساليب الإرهاب أكثر تطوراً فمن الممكن تدمير البنى التحتية للدول دون إطلاق رصاصة عبر استخدام الجماعات الإرهابية للفضاء السيبراني لشن هجمات إرهابية باستخدام بعض البرامج المعقدة، ومن ثم أصبحت أعمال الإرهابيين أكثر خطورة وتدميرًا. وفضلاً عن ذلك أصبح الفضاء السيبراني يمثل عنصرَ جذب مهمًّا للتنظيمات المسلحة والإرهابية على اختلاف أنواعها وتباين أفكارها؛ نظرًا لما يتيحه لها من وسائل عالمية هي في الوقت نفسه سلاح خطير ويعدُّ تنظيم "داعش" الارهابي أكثرَ التنظيمات تهديداً وتوظيفاً لشبكات الإنترنت؛ باستخدامها في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات السيبرانية.

الكلمات المفتاحية: الإرهاب، الأمن الدولي، الأمن السيبراني، شبكات الاتصال، الفضاء السيبراني.

The ability and power of major and regional powers are not only measured by their economic and military capabilities, but also by their technological strength and the immunity of their cyber system. Thus, the existence of an integrated and secure national cyberspace structure is one of the most important possible factors for growth and prosperity. However, the expansion of the use of technology opens new horizons for cyber terrorist risks and threats. This requires strengthening and combating cyber terrorism by providing protection for networks, technical systems, information, operational technology systems, and their hardware and software components, as well as protecting the services they provide and the data they contain from any penetration, disruption, modification, entry, use, or exploitation within the framework of the digital space.

The forms and images of the phenomenon of international terrorism, and its danger has increased steadily with the information revolution and technological development in the field of manufacturing computers and electronic devices, the development of communication networks, so communication methods have become, roads have become, and it is possible to destroy the structures of countries without firing a bullet through terrorist organizations' use of cyberspace terrorists.

Some complex programs, and then the actions of terrorists became. In addition, cyberspace has become an important attraction for armed and terrorist organizations of all kinds

and differing ideas. Given the global means it provides, it is at the same time a dangerous weapon, and ISIS is the most threatening organization that uses the Internet; They are used to advertise, recruit, finance, gather information, and coordinate cyber-attacks.

Keywords: Terrorism, International security, Cyber security, Communication networks, Cyberspace.

المقدمة

إن ظهور شبكات الإنترنت في ستينيات القرن الماضي؛ نتيجة تطور الثورات التكنو–معلوماتية وتطور وسائل الاتصال الإلكترونية، أدى الى اتساع أُطر هذه الشبكات لتشكل بذلك بعداً جديداً من أبعاد الاستراتيجية وهو البعد الافتراضي والذي أخذ يطلق عليه بـ الإرهاب السيبراني، ما جعل العالم المعاصر يعيش سباق سيبراني لتطوير قدراته ووسائله الدفاعية والهجومية، وجميع الدول والحكومات أصبحت مهددة بالتعرض للهجوم السيبراني الارهابي، لاسيما مع اتساع نطاق التقنية وانتشار أجهزة إنترنت الأشياء وشبكات الجيل الخامس المتطورة، التي تسمح بمرور ونقل ومعالجة كميات ضخمة من البيانات، كما يتوقع الخبراء أيضاً زيادة حالات الخروقات السيبرانية الارهابية في دول العالم كافة لاسيما التنافس والصراع بين القوى الكبرى والقوى الاقليمية في جنوب شرق آسيا والشرق الأوسط، فضلاً عن ارتباط هذه الصراعات السيبرانية بالصراعات السياسية وتزايد الفواعل الارهابية من غير الدول مجموعات وعصابات الهاكر وما تمتلكه من قدرات الكترونية في الفضاء السيبراني.

وبناءً على ما تقدم، أصبحت قدرة وقوة القوى الكبرى والاقليمية لا تقاس بإمكاناتها الاقتصادية والعسكرية فحسب، وإنما بقوتها التكنولوجيا وحصانة منظومتها السيبرانية، وبذلك فأن وجود بنية فضاء سيبراني وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار؛ إلا أن التوسع في استخدام التقنية يفتح آفاقاً جديدة للمخاطر والتهديدات الارهابية السيبرانية؛ مما يستوجب تعزيز ومكافحة الارهاب السيبراني عبر توفير الحماية للشبكات وللأنظمة التقنية والمعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، فضلاً عن حماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال في إطار الفضاء الرقمي.

يعتمد العالم على التكنولوجيا أكثر من أي وقت مضى، نتيجة لذلك ازداد إنشاء البيانات الرقمية، اليوم تخزن الشركات والحكومات قدراً كبيراً من تلك البيانات على أجهزة الكمبيوتر وتنقلها

عبر الشبكات إلى أجهزة الكمبيوتر الأخرى، تحتوي الأجهزة والأنظمة الأساسية الخاصة بها على نقاط ضعف تؤدي عند استغلالها إلى تقويض صحة وأهداف المؤسسة.

أهمية البحث:

تأتي أهمية البحث من خلال تسليط الضوء على ظاهرة الإرهاب السيبراني وعدم توافر مراجع عن مكافحة الارهاب السيبرانية واستراتيجياته، بذلك يسعى البحث الى دراسة وتحليل وتحديد التهديدات السيبرانية التي تواجه أغلب دول العالم وخاصة العراق، وبما يساهم برفد المكتبات والباحثين في التراكم المعرفي للموضوع، فضلاً عن التركيز على الأبعاد العسكرية للقوة السيبرانية ومدى تأثيرها على الأمن الوطني في إطار تعزيز المكنّة الادائية السيبرانية لجهاز مكافحة الإرهاب العراقي.

هدف البحث:

يهدف البحث للوقوف على ماهية الإرهاب السيبراني، وكيفية بناء استراتيجية وطنية لمكافحته، والاطلاع على التجارب والنماذج والجهود المبذولة على المستوى العالمي والإقليمي لمكافحته لتعزيز قدرات المؤسسات الأمنية والاستخبارية في مواجهة الإرهاب السيبراني.

إشكالية البحث:

تتمثل اشكالية البحث في تساؤل رئيس مفاده، ماهي الكيفية التي تمكننا من مواجهة الإهاب السيبراني في ظل التطورات التكنولوجية المستمرة ومدى تأثير القوة السيبرانية على الأمن الوطني للدول؟

فرضية البحث:

تنطلق من وجود علاقة طردية عند تعزيز امتلاك الدول القدرات والقوة السيبرانية سيفضي الى تحصين أمنها الوطني والقومي السيبراني.

مناهج البحث:

تم توظيف المنهج الوصفي التحليلي، فضلاً عن المدخل الوظيفي، ومدخل دراسة الحالة للإجابة على اشكالية البحث واثبات فرضيته.

المحور الأول: الاطار النظري للأمن السيبراني

يعدّ الفضاء السيبراني[1] بأنه الوسط التقني الذي تعمل فيه شبكات هائلة من الادوات والوسائل الالكترونية بمكوناتها المختلفة، كأجهزة الكومبيوتر وأنظمة الشبكات والبرمجيات وحوسبة المعلومات ونقلها وتخزينها، فهو المجال الرقمي الممتد دولياً عبر خطوط الاتصالات الضوئية والمعدنية والألياف البصرية وموجات الأقمار الصناعية وقنواتها المتعددة في بث خدمة الإنترنت والموجات الاخرى.

تشير كلمة Cyber أو Cybernetics إلى "نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دارسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم دارسة الاتصال والتحكم الآلي في النظم العصبية للكائنات الحية ومحاكاة الآلات لها". بالتالي فالمجال السيبراني يتضمن "كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات. [2]

أولا: الأمن السيبراني

الأمن السيبراني يقصد به توفير الحماية للأنظمة المتصلة بالإنترنت مثل الأجهزة والبرامج والبيانات من التهديدات السيبرانية الارهابية، يتم استخدام هذه الممارسة من قبل الأفراد المهاجمين أو الجماعات الارهابية أو المؤسسات أو الدول من ذوي النوايا الخبيثة للوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسبة لتدمير البيانات وحذفها أو ابتزازها من الدول الأخرى، لذلك يهدف الأمن السيبراني، توفير وضع أمني عالٍ لأجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة والبيانات المخزنة على هذه الأجهزة.

كما ان الأمن السيبراني يعدّ مجال متغير ومتطور بإستمرار، نتيجة الاكتشافات المستمرة في التقنيات التي تفتح آفاقاً جديدة للهجمات الإلكترونية، وهذا ما يصعب عملية بناء استراتيجيات متكاملة لمكافحة الارهاب السيبراني.[3]

ويمكن تعريف الأمن السيبراني بأنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع"، ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي ونحو ذلك.

فضلاً عما تقدم، يرى عدد من الباحثين المتخصصين في مجال الأمن السيبراني، "أن أمن الاتصالات اللاسلكية ارتبط بموضوع الإنترنت وهي منظومة متداخلة ومعقدة من الشبكات،

وكان سابقاً التعامل مع الاتصالات الخاصة بالصوت فقط، وبعدها جاءت شبكات الإنترنت والكمبيوتر وأصبح لدينا كذلك شبكات المعلومات، ثم التحول من الاتصالات إلى أمن الاتصالات، ومن ثمة جاءت مرحلة الإنترنت، وتلاشت الحدود بين الاتصالات وبين تقنية المعلومات وبين الخدمات المقدمة عن طريق الإنترنت ثم أصبح أقرب تعريف ما يسمى بالسايبر وهو أي شيء مرتبط بالإنترنت وشبكات الاتصالات وتقنية المعلومات ومن ثم ظهر مفهوم الأمن السيبراني بشكل عام، وهو مرتبط بأمن الاتصالات اللاسلكية ومرتبط كذلك بأمن تقنية المعلومات ومرتبط بشبكة الإنترنت".[4]

إن أهمية الأمن السيبراني تنبع من كمية البيانات غير مسبوقة والمخزنة على أجهزة الكمبيوتر والسحابة الافتراضية والشبكات المرتبطة بها، والتي تتعلق بخصوصية عمل وأداء المؤسسات الحكومية والامنية والاقتصادية والشركات المالية والطبية، وقد يؤدي اختراقها الى كشف اسرار تلك المؤسسات وتعرضها الى خسائر فادحة، ومع نمو حجم وتعقيد الهجمات الإلكترونية، يتعين على الشركات والمؤسسات وخاصة تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي أو الصحة أو السجلات المالية، اتخاذ خطوات لحماية معلومات الأعمال والموظفين الحساسة الخاصة بهم، كما إن الهجمات الإلكترونية والتجسس الرقمي تشكل أكبر تهديد للأمن القومي وتتفوق حتى على الإرهاب التقليدي. [5]

ثانيا: عناصر ومرتكزات الأمن السيبراني

للحصول على أمن إلكتروني فعال، تحتاج المؤسسة إلى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها، وتشمل عناصر الأمن السيبراني ما يأتي:[6]

1. **أمن الشبكة:** عملية حماية الشبكة من المستخدمين غير المرغوب فيهم والهجمات والاختراق.
2. **أمان التطبيقات الالكترونية:** تتطلب التطبيقات تحديثات واختبارات مستمرة للتأكد من أن هذه البرامج آمنة من الهجمات.
3. **أمان نقطة النهاية:** يعد الوصول عن بُعد جزءاً ضرورياً من العمل، ولكنه قد يكون أيضاً نقطة ضعف للبيانات، أمان نقطة النهاية هو عملية حماية الوصول عن بُعد إلى شبكة الشركة.
4. **أمن البيانات:** توجد بيانات داخل الشبكات والتطبيقات، تعد حماية معلومات الشركة والعملاء طبقة منفصلة من الأمان.
5. **إدارة الهوية:** هذه هي عملية فهم الوصول الذي يتمتع به كل فرد في المؤسسة.

6. **قاعدة البيانات وأمن البنية التحتية:** كل شيء في الشبكة يتضمن قواعد بيانات ومعدات مادية، حماية هذه الأجهزة لا تقل أهمية.
7. **أمان السحابة:** توجد العديد من الملفات في البيئات الرقمية أو (السحابة)، تمثل حماية البيانات في بيئة عبر الإنترنت بنسبة 100% قدراً كبيراً من التحديات.
8. **أمان الأجهزة المحمولة:** تشتمل حماية الهواتف المحمولة والأجهزة اللوحية من الاختراقات السيبرانية.
9. **التعافي من الحروب والنزاعات والتخطيط لاستمرارية الأعمال:** في حالة حدوث خرق، يجب حماية بيانات الحروب والنزاعات وعمليات مكافحة الارهاب أو غيرها من بيانات الأحداث ويجب أن يستمر العمل، ولهذا ستحتاج إلى خطة.
10. **تعليم المستخدم النهائي:** قد يكون المستخدمون موظفين يصلون إلى الشبكة أو عملاء يسجلون الدخول إلى تطبيق الشركة، ويعد تعليم العادات الجيدة (تغيير كلمة المرور، والمصادقة الثنائية، وما إلى ذلك) جزءاً مهماً من الأمن السيبراني.

ثالثا: حروب الإنترنت

أن حروب الإنترنت والشبكات أصبحت ذات خطورة عالية، إذ أخذ العالم يعتمد أكثر فأكثر على الفضاء الإلكتروني (Cyberspace)، لا سيما في البنى التحتية المعلوماتية العسكرية والامنية والمصرفية والحكومية، فضلاً عن المؤسسات والشركات العامة والخاصة، ولا شك أنّ ازدياد الهجمات الإلكترونية والتي نشهد جزءاً بسيطاً منها اليوم يرتبط أيضاً بازدياد هذا الاعتماد على شبكات الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل، علماً أنّ أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المتخصصين.[7]

كما إنه لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية الآن، إذ تعرف وزارة الدفاع الأمريكية الحرب الإلكترونية بأنها "استخدام أجهزة الكمبيوتر والإنترنت لإجراء الحرب في الفضاء الإلكتروني" وقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرّف كل من (ريتشارد كلارك وروبرت كناكي) الحرب الإلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة

أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".[8] ومن المتوقع أن تصبح الحرب الإلكترونية انموذجاً تسعى إليه العديد من الجهات نظراً للخصائص العديدة التي تنطوي عليها، ومن أهمها:[9]

1. إن حروب الإنترنت هي حروب لا تناظرية (Asymmetric): إذ أن التكلفة المتدنية نسبياً للأدوات اللازمة لشن هكذا حروب، يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جداً مثل حاملات الطائرات والمقاتلات المتطورة لتفرض تهديداً خطيراً وحقيقياً على دولة عظمى مثل الولايات المتّحدة الأمريكية.
2. يمتّع المهاجم بأفضلية: في حروب الإنترنت يتمتع المهاجم بأفضلية كبيرة عن المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، إذ ان هذه الحروب لا تحتاج امكانات وقدرات كبيرة بقدر ما تحتاج الى عقلية ومهارة في مجال البرمجة والذكاء الصناعي.
3. فشل نماذج استراتيجيات (الردع) المعروفة، إذ يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنت، فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب، فقدرة الدول على رصد تحركات العدو والرد عليها في الحروب التقليدية، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد موقع الهجمات الإلكترونية، وفي بعض الحالات قد تتطلّب أشهراً لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها، وحتى إذا تم تتبع مصدرها وتبين أنها تعود إلى فاعلين من غير الدول، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها بشكل مباشر.
4. المخاطر تتعدى استهداف المواقع العسكرية والامنية: لا ينحصر إطار حروب الإنترنت على استهداف المواقع العسكرية والامنية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية الاقتصادية والسياسية والاستخباراتية الحسّاسة في الدول المستهدفة، وهو أمر أصبح واقعياً في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.

المحور الثاني: تهديدات الإرهاب السيبراني

إن مفهوم الإرهاب السيبراني Cyber terrorism ظهر في ثمانينيات القرن العشرين، فقد عرفه باري كولين (Barry Collin) آنذاك بتعريفٍ عام؛ بأنه "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة

يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب". كما عرفه دورثي دينينغ (Dorothy Denningg) بأنه "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبيّاً لتوليد الخوف بحيث يكون مشابهاً للأفعال المادية للإرهاب".[10]

فضلاً عن ما تقدم، يمكن **تعرف الإرهاب السيبراني إجرائِيّاً بأنه نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام بإستخدام الفضاء السيبراني والانترنت المظلم أو العميق[11] بوصفه عاملاً مساعداً ووسيطاً في عملية تنفيذ الهجمات الإرهابية بشكل مباشرة بالقوة المسلحة على مقدرات البنية التحتية للمعلومات، أو عبر ما يُعَدَّ تأثيراً مَعنويّاً ونفسيّاً، عن طريق التحريض على بث الكراهية الدينية وحرب الأفكار**، أو أن يتم في صورة رقمية عبر استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء السيبراني، والتي قد يقتصر تأثيرها على بعدها الرقمي أو قد تتعدى لإصابة أهداف مادية تتعلق بالبنية التحتية الحيوية للدول المستهدفة. كما عرفة هيئة الامم المتحدة الارهاب السيبراني بأنه "إستخدام الانترنت لنشر الاعمال الإرهابية".[12]

وعليه يمكن القول، بأن الإرهاب السيبراني يستخدم الأساليب الحديثة التكنولوجية، والتي تتضمن الإمكانيات التقنية، وتعتمد بالأساس على شبكات المعلوماتية، وذلك بقصد ترويع الأفراد من خلال تهديدهم أو إلحاق الضرر الفعلي بهم، وتأتي الهجمات الإلكترونية بجميع الأشكال والأحجام، قد يكون بعضها عبارة عن هجمات برامج الفدية العلنية (اختطاف منتجات أو أدوات تجارية مهمة مقابل الحصول على أموال مقابل إطلاقها)، في حين أن بعضها عبارة عن عمليات سرية يتسلل من خلالها المجرمون إلى نظام للحصول على بيانات قيمة فقط ليتم اكتشافها بعد أشهر من وقوعها. [13]

والارهاب السيبراني عبارة عن الدمج بين العنف وتوظيف التكنولوجيا في ظل مواكبة عصر الثورة المعلوماتية، تتسع ساحة الفاعلين الدوليين، والتي منهم : الدول القومية، المنظمات الحكومية العالمية والقومية، الفواعل فوق القومين مثل الاتحاد الأوروبي، التحالفات الدولية سواء اتخذت طابعاً عسكرياً أو سياسياً، المنظمات الدولية غير الحكومية أو العابرة للقارات مثل الصليب الأحمر، والفواعل العنفية من غير الدول مثل الجماعات الارهابية المتعددة الجنسية (تنظيم داعش الارهابي)، إذ تقوم بعمليات قرصنة لسرقة المعلومات، واختراق الحسابات البنكية،

وسرقة بطاقات الائتمان، وتعد القوة السيبرانية فعلاً إرهابياً مقصوداً ينفذ عبر الإنترنت بدوافع سياسية مثل التأثير على الرأي العام، أو قرارات الحكومة. [14]

أنواع الإرهاب السيبراني

هناك عديداً من انواع التهديدات الارهابية والهجمات التي تتم في إطار التنافس والصراعات بين الدول والفواعل من غير الدول لتحقيق اهداف ومصالح الجهات التابعة لها، ومن أهمها ما يأتي:

1. **الهاكرز واختراق الحيز الافتراضي** : جاءت القرصنة الإلكترونية كأحد نماذج الثورة المعلوماتية، ونواتها الهاكرز بوصفه شخصية محورية ظهرت في البعد الافتراضي–الرقمي، وهم اشخاص حقيقيون يعملون عبر الاختراق البرمجي لأجهزة الحاسوب ، في عام 2000 قام فريق من القراصنة بحذف محتويات موقع حزب الله بعد أسر جنود إسرائيليين، وتم الرد على هذا الهجوم بهجمات مماثلة على مواقع إسرائيلية ، أهمها مكتب رئيس الوزراء ، موقع الكنيست، وموقع بورصة إسرائيل، غرفة التجارة، وبلغ عدد المواقع التي تم مهاجمتها نحو 280 موقعا مقابل 34 موقعا عربياً، كما تعرض حوالى 80 موقعا إسرائيلياً في عام 2001 لهجمات ناجحة أدت إلى خروجها من الخدمة ، وأيضاً عام 2002 ، تعرض موقع الموساد الإسرائيلي لاختراق وسرقة معلومات عملائه الجدد، في 2013 نفذ مجموعة من الهاكرز هجمات إلكترونية، على مواقع إسرائيلية تمكنوا من خلالها من الحصول على معلومات سرية. ومن أهم اساليبها ما يأتي:[15]

– **البرمجيات الخبيثة:** تستخدم (البرامج الخبيثة) لوصف البرامج الضارة بما في ذلك برامج التجسس وبرامج الفدية والفيروسات، عادة ما تخترق الشبكات من خلال ثغرة أمنية، مثل النقر على روابط البريد الإلكتروني المشبوهة أو تثبيت تطبيق محفوف بالمخاطر، وبمجرد الدخول إلى الشبكة، يمكن للبرامج الخبيثة الحصول على معلومات حساسة، وإنتاج المزيد من البرامج الضارة في جميع أنحاء النظام، ويمكنها أيضاً حظر الوصول إلى مكونات شبكة الأعمال الحيوية (برامج الفدية).

– **التصيد والاحتيال:** هو ممارسة إرسال اتصالات ضارة (عادةً رسائل بريد إلكتروني) مصممة لتظهر من مصادر حسنة السمعة ومعروفة، تستخدم رسائل البريد الإلكتروني هذه الأسماء والشعارات والصياغة وما إلى ذلك، كشركة لتقليل الشكوك وجعل الضحايا ينقرون على الروابط الضارة، وبمجرد النقر فوق ارتباط التصيد، يمكن لمجرمي الإنترنت الوصول

إلى البيانات الحساسة مثل بطاقة الائتمان أو الضمان الاجتماعي أو معلومات تسجيل الدخول.

- **هندسة اجتماعية-نفسية:** الهندسة الاجتماعية هي عملية التلاعب النفسي بالناس لإفشاء معلومات شخصية، والتصيد هو شكل من أشكال الهندسة الاجتماعية، إذ يستغل المجرمون فضول الناس الطبيعي أو ثقتهم، ويعد التلاعب بالصوت أحد الأمثلة على الهندسة الاجتماعية الأكثر تقدماً، في هذه الحالة يأخذ مجرمو الإنترنت صوت الفرد (من مصادر مثل البريد الصوتي أو منشور على وسائل التواصل الاجتماعي) ويتلاعبون به للاتصال بالأصدقاء أو الأقارب وطلب بطاقة ائتمان أو معلومات شخصية أخرى. (16)
- **هجوم MitM:** تحدث هجمات Man-in-the-Middle عندما يقطع المجرمون حركة المرور بين المعاملات بين طرفين، على سبيل المثال: يمكن للمجرمين إدخال أنفسهم بين شبكة Wi-Fi عامة وجهاز الفرد، بدون اتصال Wi-Fi محمي، يمكن لمجرمي الإنترنت أحياناً عرض جميع معلومات الضحية دون أن يتم القبض عليهم.
- **هجوم Zero-day:** أصبحت هجمات Zero-day أكثر شيوعاً، تحدث هذه الهجمات بين إعلان ثغرة أمنية في الشبكة وحل التصحيح، باسم الشفافية والأمان، ستعلن معظم الشركات أنها وجدت مشكلة في أمان شبكتها، لكن بعض المجرمين سيغتنمون هذه الفرصة لشن هجمات قبل أن تتمكن الشركة من التوصل إلى تصحيح أمني.
- **لغة الاستعلام الهيكلية (SQL):** يعمل هذا التهديد عن طريق إدخال تعليمات برمجية ضارة في نموذج على موقع الويب أو التطبيق الخاص بالشركة، ما يسمح للمهاجم بالكشف عن المعلومات الحساسة.

2. **الجريمة السيبرانية الداخلية:** تعدّ نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة على الحاسوب، ومن أنواع الجريمة:(17)

- **التصنت على الهواتف:** هناك حادثة شهيرة في 2011 ، تم إلقاء القبض على خلية تضم 22 باحثاً إسرائيلياً باتهامهم بالتنصت على الهواتف النقالة عبر فيروس من نوع حصان طروادة .
- **سرقة الوثائق السياسية والعسكرية السرية:** قضية شهيرة شهدتها إسرائيل في عام 2008، مجندة تدعى عانات كام، جمعت الآف من الوثائق العسكرية والصور السرية

من الحاسوب الآلي العسكري التي كانت تستخدمه إلى جريدة (هارتس)، وحسب الاتهامات كانت بناءً على دوافع إيديولوجية.

- **تسريب بيانات الخصوصية للمواطنين:** في عام 2012 ، سرقة نسخة كاملة من السجل المدني لسكان إسرائيل وتسريبها على الانترنت، وهي من أخطر عمليات السرقة السيبرانية في إسرائيل .

ويتسم الإرهاب السيبراني بالعديد من الخصائص التي تميّزه عن الإرهاب في صورته التقليدية، والتي تسعى في نهاية الأمر لتحقيق أهداف غير مشروعة، ومن ذلك فالإرهاب السيبراني هو عابر للقارات والحدود، ولذا لا يخضع لأي نطاق جغرافي معين، ويندرج تحت مظلة الجريمة السيبرانية، مقابل صعوبة تقفي أثر الجاني في مرتكب واقعة الإرهاب السيبراني، إذ يوجد العديد من الصعوبات التي تقف حائلاً دون الوصول لدليل مادي يربط الجاني بالواقعة. [18] كما إن تنظيم داعش مثلاً دعم قدراته الإلكترونية بدمج أذرعه (السيبرانية) مثل: "الخلافة الشبح" Ghost Caliphate، و"جيش أبناء الخلافة" Sons Caliphate Army، و"جيش الخلافة السيبراني" The Caliphate Cyber Army، و"كلاشينكوف الأمن الإلكتروني" Kalashnikov E-Security فيما سُمي (مجموعة قراصنة الخلافة السيبرانية المتحدة) The United Cyber Caliphate Hacker Group. [19]

وتنطوي الهجمات السيبرانية على أبعاد متعددة بحسب الجهة التي تقوم بالهجوم وهدف ذلك الهجوم، وكما يأتي:

1- الهجمات السيبرانية الإرهابية: والتي يقوم بها افراد أو جماعات أو تنظيمات إرهابية تستهدف التخريب والاضرار بمصالح دولة أو فئة اجتماعية أو مواطنين محددين بالاستهداف.

2- الهجمات السيبرانية التي تقوم بها الشركات أو المنظمات أو البنوك والبورصات المتنافسة فيما بينها للتجسس وسرقة الاختراعات والاموال.

3- الهجمات التي تنشأ بين القوى العظمى والكبرى والاقليمية في إطار التنافس والصراعات السياسية والاقتصادية والعسكرية.

4- الهجمات التي تشنها قوى كبرى أو اقليمية ضد دول صغيرة أو شركات أو جماعات مسلحة أو أفراد.

المحور الثالث: إستراتيجيات مواجهة الإرهاب السيبراني (نماذج مختارة)

إن التطور التكنولوجي التقنيات الرقمية على المستوى العالمي، تركت عديداً من التأثيرات الايجابية التي دفعت الدول الى تبني أنظمة الحوسبة الالكترونية وانترنت الاشياء لتقديم خدمات أفضل على جميع المستويات والمؤسسات الرسمية وغير الرسمية، في مقابل ذلك كان لهذا التحول آثاره السلبية، فتم استخدام التكنولوجيا لتهديد أمن الدول من خلال اختراق المواقع الإلكترونية لرؤساء الدول والحكومات والوزارات والتجسس عليها وتدميرها، والاطلاع على مختلف المعلومات الأساسية للدول سيما الأمنية منها، فضلاً عن المؤسسات الاقتصادية مثل البنوك والبورصات العالمية وغيرها، مما يؤثر سلباً على الأمن الاقتصادي للدول، ولم تقتصر الهجمات على الجوانب السياسية والأمنية والاقتصادية فقط، بل مست أيضاً الجوانب الاجتماعية والثقافية بتدمير مواقع المستشفيات ومصانع توليد الطاقة، والماء، والغاز، والعمل أيضاً على نشر ثقافة التطرف الديني في أوساط الشباب وطمس الهوية وتجنيدهم إلى المنظمات الإرهابية، كل ذلك حتم على الدول التي تتبنى النمط التكنولوجي والحوكمة الالكترونية في مؤسساتها الاتجاه نحو بناء استراتيجية للأمن السيبراني ومكافحة جميع صور الارهاب السيبراني وتحقيق الأمن والاستقرار.

أولا: تجربة الولايات المتحدة في مواجهة الإرهاب السيبراني

تعمل الاستراتيجية السيبرانية الامريكية بهجمات سيبرانية على خصوم ومنافسي الولايات المتحدة، وفي المؤتمر الصحفي للكشف عن الاستراتيجية قال مستشار الأمن القومي السابق جون بولتون، أن "أيدينا ليست مكتوفة كما كانت في عهد إدارة أوباما". وأضاف أن الاستراتيجية تتضمن توجيهاً رئاسياً جديداً حل محل التوجيه الصادر في عهد الإدارة السابقة يسمح بأن تقوم المؤسسة العسكرية الأمريكية والوكالات الأخرى بعمليات سيبرانية، تهدف لحماية أنظمة وشبكات الولايات المتحدة الحرجة التي يؤثر استهدافها في القوة والمكانة الأمريكية الدولية. (20)

كما تتفق تصريحات بولتون مع توجه الإدارة الأمريكية لتبني سياسة ردع سيبرانية أكثر هجومية مقارنة بمواقف الإدارات الأمريكية السابقة، وسعيها لإنشاء هياكل الردع التي ستثبت للخصوم والمنافسين، وأن تكلفة استهدافهم وتحديهم لمصادر القوة والنفوذ الأمريكي يكون مكلفاً أكثر مما يتحملونه. وتأتي الاستراتيجية السيبرانية الجديدة للولايات المتحدة في إطار مساعي الرئيس الأمريكي لإنشاء فرع سادس للجيش الأمريكي يركز على الفضاء، ويُحقق هيمنة أمريكية عليه.

وتقوم استراتيجية الإدارة الجديدة لتعزيز الأمن السيبراني الأمريكية على أربع ركائز رئيسة، وهي: [21]

أولاً: تعزيز الأمن القومي الأمريكي، من خلال تبادل المعلومات عبر الوكالات الفيدرالية؛ لحماية شبكات الكمبيوتر الاتحادية، وتأمين البنية التحتية الحيوية للبلاد، وذلك من خلال إعطاء وزارة الأمن الوطني مزيداً من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، ومكافحة الجرائم السيبرانية من خلال التعاون مع الدول الأخرى لتعقب منفذيها.

ثانياً: تعزيز الاقتصاد الأمريكي الرقمي، بتشجيع الابتكار في قطاع التكنولوجيا، وذلك من خلال العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن السيبراني في المنتجات الجديدة، بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن السيبراني من خلال توظيف المتخصصين من ذوي الكفاءات في مجال الأمن السيبراني في المؤسسات والوكالات الأمريكية.

ثالثاً: مكافحة التهديدات السيبرانية، من خلال استخدام كافة أدوات القوة الأمريكية لردع أي هجمات سيبرانية إرهابية، وتعزيز المعايير الدولية في الفضاء السيبراني.

رابعاً: الدعوة إلى حرية الإنترنت في جميع أنحاء العالم، وتزويد حلفاء الولايات المتحدة بقدرات سيبرانية؛ للتعامل مع التهديدات السيبرانية التي تستهدف المصالح المشتركة.

وعلى الجانب الآخر تعرضت الاستراتيجية لبعض الانتقادات؛ لأن البيت الأبيض لم يقدم إلا القليل من التفاصيل حول كيفية تطبيقها بالفعل على أرض الواقع.

خلاصة القول، إن استراتيجية الرئيس الأمريكي للأمن السيبراني، بعد عقد ونصف من آخر استراتيجية لحماية الفضاء السيبراني، تهدف إلى وضع معايير عالمية لكيفية استخدام الدول والفاعلين ما دون الدولة للفضاء السيبراني، واستمرار الهيمنة الأمريكية سيبرانياً، وحماية مصالح الولايات المتحدة السياسية والاقتصادية داخلياً وخارجياً، وكذلك معاقبة "الجهات الفاعلة الخبيثة" مثل روسيا والصين والجماعات الارهابية التي تخطط لشن هجمات سيبرانية تقوّض مصادر القوة والنفوذ الأمريكي عالمياً. [22]

وقدم باري كولين في ورقته المشار إليها آنفاً قائمةً بالعناصر التي يجب توافرها عند إنشاء برنامج مكافحة الإرهاب السيبراني، وهي:

1. بناء فريق مكافحة الإرهاب الإلكتروني في الوقت المناسب، وبمرونة فائقة.
2. تغيير الطريقة التي نتعامل بها مع مكافحة الإرهاب الإلكتروني.
3. التعاون ومشاركة المعلومات الاستخباراتية بطرق جديدة.

4. الاستعانة بالأفراد الذين يمتلكون المعرفة والخبرة بالحرب السيبرانية.
5. معرفة القواعد الجديدة والتقنيات الجديدة واللاعبين الجدد، فبخلاف الإرهابيين التقليديين، إذا خسر الإرهابي الإلكتروني اليوم، فهو لا يموت بل يتعلم ويزداد خبرة مما لم ينجح فيه، وسيستخدم ما تعلمه في محاولة جديدة ناجحة مستقبلاً.

وتضيف كلٌّ من سوهانيا بونوسامي وغيثا روباسندرام في بحثهما (دراسة دَولية في مخاطر الإرهاب السيبراني) (An International Study on the Risk of Cyber Terrorism) المنشور في يناير 2019 عناصرَ أخرى ضروريةً لمواجهة الإرهاب الإلكتروني هي:

1. إيجاد إطار دَولي منسق وقوي لمكافحة الإرهاب السيبراني تتوافق عليه الحكومات والهيئات التنظيمية؛ لتكون قادرةً على تبادل المعلومات الاستخباراتية وغيرها من أشكال التعاون.
2. توفير قدر أكبر من التعليم لمؤسسات القطاعين العامّ والخاصّ؛ لتقوم بتطوير التقنيات المستخدمة التي قد تكون عُرضةً للإرهاب السيبراني، والتأكد من أن عنصر الأمن في صدارة الاهتمام عند إنشاء الأنظمة الجديدة، للحد من نِقاط الضعف التي قد تواجهها.
3. تطوير تقنية آمنة تكون قادرةً على تحديد الأنشطة المشبوهة بوساطة تحليل البيانات العامة والخاصة، وجعل الحواسيب وأنظمتها أقلَّ عرضة للخطر.

ثانيا: إستراتيجيات مواجهة الإرهاب السيبراني في العراق

ثمة تحدِّيات لمساعي مواجهة ومكافحة الإرهاب السيبراني في العراق، يتعلق أهمها بالتطورات السريعة والمتلاحقة في مجال التقنية، وتطوُّر أدوات التخفِّي وحجب تقنيَّات التتبع، وتقدم برامج تغيير المواقع. لذا يمكن ترتيب سُبل مواجهة هذا النمط من الإرهاب وَفقَ المراحل الآتية: [23]

المرحلة الأولى: التدابير السياسية والتنظيمية والتشريعية: وتشتمل على ما يأتي:

- **السياسات السيبرانية:** تبني سياسة التحفظ على العولمة السيبرانية، واعتبارها تعدِّياً على سيادة الدولة القومية، واقامة الحواجزَ اللازمة، وانشاء شبكة قوميةَ خاصَّة ضمن إطار شبكة الإنترنت العالمية، وبحسَب الضوابط الامنية العراقية، فضلاً عن تبنِّي جماعاتٍ سيبرانيةً وسيطة تعمل لصالحها مثل مؤسسات الرد السيبراني.

- **الجوانب التنظيمية والتشريعية:** إن التشريعاتِ القانونيةَ التي تراعي الجوانبَ الموضوعية والشكلية مهمَّة في مواجهة الإرهاب السيبراني على صعيد العراق؛ إذ يجب أن تنظمَ التشريعات العمل في المجال الرَّقْمي بإنشاء مؤسسات متخصِّصة بموجب قوانين الدولة، وتحديد طبيعة الجرائم والعقوبات الملائمة والرادعة لها، فضلاً عن والإجراءات الشكلية كالضبط والتحقيق والتوقيف وما شاكلها.
- **الإستراتيجيات السيبرانية:** الإستراتيجية السيبرانية للعراق تحدِّد توجُّهه في هذا المجال، وتشمل كلَّ السياسات والجوانب الأخرى ذات الصلة، مثل المؤسَّسات المخوَّلة بتنظيم النشاطات الرَّقْمية وضبطها، ومواكبة التشريعات للتطوُّر الحاصل في هذا المجال، والاهتمام بتوعية المستخدِمين بالمخاطر المحتمَلة.
- **الاتفاقيات الإقليمية والتعاون الدَّولي:** تشمل الاتفاقياتُ الثنائية بين الدول الجوانبَ القانونية اللازمة للتعاون في مجال التحقيق في حوادث الفضاء السيبراني الدولية والاقليمية، أمَّا التحالفاتُ السيبرانية بين الدول، أو مع القِطاع الخاصِّ؛ فهي مهمَّة في عمليات التتبُّع والتحقيق في الحوادث، وتبادل المعلومات عن أبرز الطرق الإجرامية المتَّبعة، وأهمِّ الأختام الرَّقْمية والبصَمات الإلكترونية المتعلقة بالتنظيمات الإرهابية، وأحدث البرمجيَّات والأسلحة السيبرانية المستخدَمة، ما يساعد على تحديد هُويَّة الجهة التي تنفِّذ الهجَمات الإرهابية.

المرحلة الثانية: التدابير الأمنية والاستخبارية السيبرانية، ويظهر أثرُ الجهات الأمنية السيبرانية في مجال التوعية والقيام بإجراءات الاستخبارات السيبرانية المضادَّة؛ لكشف ثُغرات الأنظمة المحلِّية ومعالجتها، ووضع التدابير لمواجهة الهجَمات، والقيام بالتحقيقات الفنية اللازمة، والتنسيق مع مؤسَّسات إنفاذ القانون والجهات الأخرى ذات العَلاقة. فضلًا عن متابعة النشاطات السيبرانية الحديثة، والأسلحة السيبرانية المستحدَثة، ومراقبة الفضاء الرَّقْمي، ومدى التزام المستخدمين بالمعايير المرعية محليّاً ودَوليًّا، والتعاون مع الجهات المناظرة لها إقليميّاً ودَوليّاً، وابرز المؤسسات الامنية والاستخبارية العراقية الجاهزة لهذا الغرض هما جهاز مكافحة الارهاب وجهاز المخابرات العراقي.

المرحلة الثالثة: التدابير الفنية وتتضمَّن هذه المرحلةُ تطوير البرمجيَّات والتطبيقات والأدوات والبنية التحتيَّة الإلكترونية اللازمة للمواجهة، وتشمل ما يأتي: [24]

1. إنشاء جُدران الحماية (Firewalls): لتكونَ خطَّ الدفاع الأول للأنظمة والمعلومات، وهي برمجيَّات لحماية الأنظمة والبيانات وكشف الهجَمات.

2. إجراءات أمن حسابات المستخدِمين وطرق التحقُّق من الهُوية: تتضمَّن حمايةَ الحسابات الرسمية والمصنَّفة، ويُعَدُّ الفرد هو العنصرَ الأهمَّ في هذا الجانب؛ إذ على مديري الأنظمة وضعُ الوسائل الآلية واليدوية اللازمة للتحقُّق من هُويَّة المستخدم.
3. تعمية البيانات: وهي من وسائل حماية البيانات عند إرسالها في الإنترنت أو عند تخزينها، بوصف ذلك عنصرَ إعاقة في حال حصلت جهةٌ غير مخوَّلة على البيانات، ما قد يمنع أو يؤخِّر استفادةَ هذه الجهة من البيانات.
4. تقنية المفتاح العام: وهي تعتمد تعمية (تشفير) البيانات وتقسيمها إلى أجزاء، وتوزيعها إلى عدَّة خوادم في مناطقَ مختلفة من العالم، من قِبَل المرسِل، ولا يتمكَّن المستقبِلُ من جمعها إلا باستعمال مفتاح التشفير مثل تقنية (Freenet).
5. تقنيَّة القفز المشفَّر: وهي تقنيَّة تعتمد انتقالَ البيانات المشفَّرة من المرسِل عبر عدَّة عُقَد متتالية في الشبكة، بأن تضيفَ كل عُقدة تشفيراً حتى تصلَ إلى المستقبِل، وهذه هي التقنيةُ المستخدَمة في شبكة (Tor) السرِّية المظلمة.
6. الشبكة الافتراضية الخاصَّة: وهي شبكة افتراضية فرعية عن شبكة الإنترنت، مصنَّفة كما هو حالُ شبكة (Linknet) الأمريكية، شبكةً سرِّية خاصَّة، تربط الأجهزة الأمنية والاستخباراتية والحكومية ذات العَلاقة بمواجهة الإرهاب السيبراني، وتستخدم المنظماتُ والدول بعضَ الشبكات الخاصَّة والمُعدة للاستخدام الخاص بين موظفيها ومديريها، وتكون معزولةً جزئيّاً عن الإنترنت، وتخضع لرقابة المختصِّين الدائمة لحمايتها.
7. تقنيَّة الفجوة الهوائية (Air-Gapping): وهي تقنيَّة تستخدمها أنظمةُ التحكم والإشراف والحوسبة للبُنى التحتية الحسَّاسة وإدارة البيانات فيها، بأن تجعلَ الأنظمة معزولة كليّاً عن شبكة الإنترنت، بإعداد فجَوات فنية، تُزال فقط وَفقَ إجراءات سرِّية محدَّدة وبأوقات سرِّية أيضاً.
8. مسجِّل لوحة المفاتيح (Key-logger): تقنيَّة تستخدمها الاستخباراتُ السيبرانية، وتُستخدَم للتجسُّس على أجهزة الجهات الإجرامية والمتطرفة، باستخدام البرمجيات اللازمة لاختراق أنظمة هذه المنظمات وإرسال برمجية التجسُّس للجهة المستهدَفة في الفضاء الرَّقْمي.
9. تقنيَّة خلية العسَل (Honey-cell) أو الطُّعم: وهي تقنيَّة تستخدمها الاستخباراتُ السيبرانية بوضع معلومات غير حقيقية على أحد الخوادم لتكونَ طُعماً للإرهابيين، وَفقَ خطة مُحكَمة، بهدف معرفة نشاطات الإرهابيين وإمكاناتهم، وتحديد مواقعهم.

10. تقنيَّة استمرار الأعمال: أي أن يستمر استعمالُ البيانات باستخدام النُّسَخ الاحتياطية (Backup)؛ إذ عادةً ما يُحتفَظ بنُسَخ احتياطية آليّاً وَفقاً لبرمجة محدَّدة تديرها إدارةُ النظام أو الجهة الأمنية المسؤولة.

الخاتمة

حاول بحثنا تسليط الضوء على الإرهاب السيبراني واستراتيجيات مواجهة تهديداته، وإن الطبيعة الديناميكية للتهديدات الإرهابي السيبرانية الذي تواجهه الدول والمؤسسات تتطلب التركيز المستمر على تطوير أنظمة جمع المعلومات وتحليلها فضلاً عن التحديث المستمر للبرامج لمواكبة قدرات التنظيمات الإرهابية السيبرانية والتغلب عليها ومنعها من استغلال الشبكات الافتراضية لصالحها، وتحقيق هدف مكافحة الإرهاب عبر جمع وتحليل المعلومات الاستخباراتية، لتمكين تعطيل الهجمات الإرهابية قبل تنفيذها، والتخطيط لها، وإعاقة أنشطتها الإرهابية. ومما تقدم تم التوصل الى عدد من الاستنتاجات أهمها ما يأتي:

1. أعداد فريق عمل متكامل من الخبراء والمبرمجين والفنيين والمتخصصين في مجال الذكاء الاصطناعي ضمن عمل مؤسساتي لبناء استراتيجية متكاملة لمواجهة التهديدات السيبرانية لتعقب الهجمات ومواجهتها بشكل مباشر وسريع.
2. إنشاء آليات مرنة للاستجابة التكيفية للإرهاب السيبراني وفق الأنموذج المنهجي الذي يبدأ بتصنيف الاستجابات، انطلاقاً من التصنيف المعتاد للهجمات والتهديدات الإلكترونية.
3. التعاون بين الدول في سبيل تبادل الخبرات والمعلومات لمكافحة الارهاب السيبراني.
4. إن ظاهرة الإرهاب السيبراني تعدّ إحدى أبرز الظواهر التي نتجت عن اتساع استخدام الفاعلين من غير الدول (الجماعات الارهابية)، سواء أكانوا من الأفراد أم الجماعات للفضاء السيبراني، والذي يشكل عالما افتراضيا نشأ عن التربيط بين الحواسب، وأجهزة الاتصال والخوادم وغيرها من مكونات البنية التحتية للإنترنت.
5. تتميز الحروب الإلكترونية بأنها أقل تكلفة عن الحروب التقليدية وصعوبة تحديد مصدرها، وبات الفضاء السيبراني مرتبطاً ارتباطاً وثيقاً بالأمن القومي للدول وأن الهجمات السيبرانية ستزداد مستقبلاً بالتزامن مع التطور التكنولوجي.
6. إن الدول تتسابق لتغيير القواعد على بيئة الحروب وذلك عبر الحروب السيبرانية والهجمات الإلكترونية، وتعمل العديد منها لاسيما القوى الكبرى في دخول سباق تسلح

سيبراني، على تطوير ترسانتها الإلكترونية عبر استحداث برامج للقرصنة وتدريب الجنود السيبرانيين وتوجيههم لأغراض وأهداف محددة.

7. إن الإرهاب السيبراني قد شكل قاعدة للتغيير والتعبير عن الرؤى المتطرفة التي تتبنى العنف أسلوباً ووسيلة واستخدمه لأغراض تجنيد المقاتلين في العراق.

المصادر والمراجع:

(1) الفضاء السيبراني (Cyberspace): عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكوّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. بلعسل بنت نبي ياسمين وعمروش الحسين، التهديدات الالكترونية والامن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، العدد الثاني، الجزائر، 2021، ص 165.

(2) غريب حكيم، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية. المجلد 50 -العدد 50، الجزائر، 2021، ص 3.

(3) See: Chen, Thomas M.;Jarvis, Lee , Cyber terrorism: Understanding, Assessment, and Respons, New York: Springer, June 2014, P 21.

(4) خالد محمد الربيش، أمن المعلومات مجال حيوي يمسّ فئات المجتمع كافة.. والأمن السيبراني جزء من السيادة الوطنية، صحيفة الرياض، الأربعاء 5 ربيع الآ خر 1440هـ -12 ديسمبر 2018، ص 3.

(5) See: Chen, Thomas M.;Jarvis, Lee , Op Cit, P 23.

(6) سارة سمير، الأمن السيبراني، بحث منشور في 14 ديسمبر 2020، على الرابط : https://www.alroeya.com/9-

(7) عمر حامد شكر، المجال الخامس . الفضاء الإلكتروني، المعهد المصري للدراسات، مجلة دراسات استراتيجية، 28 يونيو، 2019، ص 1.

(8) نقلاً عن: عمر حامد شكر، مصدر سبق ذكره، ص1.

(9) المصدر نفسه، ص 2.

(10) رانيا سليمان وآخرون، سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً، المركز العربي للبحوث والدراسات، مجلة دراسات، 2020، ص 3.

(11) الإنترنت العميق (Deep Web): هو مجموعة من المواقع المخفية عن محركات البحث لا يمكن الوصول إليها بالطرق التقليدية أو باستخدام المتصفحات المعروفة، ولا تجري أرشفة هذه المواقع في محركات البحث، وهي تشكل ما نسبته 84 في المائة من بيانات الإنترنت بأكملها، وتتميز مواقع "الإنترنت العميق" بوجود صفحات خاصة ووجود صفحات ذات وصول محدود، مع وجود صفحات غير نصية (الصفحات غير القابلة للفهرسة تحتوي على ملفات غير نصية، مثل عروض الفيديو والصور، وغيرها من الامتدادات غير القابلة للأرشفة)، إلى جانب استضافة الصفحات عبر بروتوكول "ftp" (مواقع تستخدم بروتوكولات ونطاقات خاصة موجودة بشكل كبير ويصعب تعقبها أو التجسس عليها نظراً لأن البروتوكول القياسي للصفحات هو "http")، ويعرف الإنترنت المظلم (Dark web): هو مجموعة من المواقع التي تقع في "الإنترنت العميق"، ولكنها تحتوي على أنشطة غير قانونية؛ قد تشمل تجارة المخدرات أو السلاح أو التجارة بالبشر، الشرط الرئيسي لاستخدام "الإنترنت المظلم" هو تشفير هوية المستخدم، وهي تشمل ما نسبته 3 في المائة من الإنترنت. خلدون غسان سعيد، جولة متخفية في أعماق "الإنترنت المظلم" استئجار قتلة وخدمات غير سوية لقاء عملات رقمية مشفرة، صحيفة الشرق الاوسط، الثلاثاء - 22 شهر ربيع الثاني 1442 هـ - 08 ديسمبر 2020 م، العدد 15351، ص 2.

(12) العشعاش اسحاق، الارهاب الالكتروني وتحديات الدول: دراسة مقارنة مع الاتفاقيات الدولية، كلية الحقوق، جامعة الجزائر، مجلة دراسات، العدد 12، 2018،الجزائر، ص 178 .

(13) رانيا سليمان وآخرون، مصدر سبق ذكره ، ص 3.
(14) السيد على أبو فرحة ونسرين الشحات، الأبعاد العسكرية للقوة السيبرانية على الأمن القومى للدول دراسة حالة إسرائيل منذ عام 2010، المركز الديمقراطي العربي، برلين، 2016، ص 11.
(15) مجموعة باحثين، الأمن السيبراني . الحكومة الإلكترونية، الخدمات الحكومية الرقمية، المركز الأوروبي لدراسات مكافحة الإرهاب و الاستخبارات-ألمانيا و هولندا، وحدة الدراسات و التقارير، على الرابط: https://www.europarabct.com
(16) بلعسل بنت نبي ياسمين وعمروش الحسين، مصدر سبق ذكره، ص 167-168.
(17) السيد على أبو فرحة ونسرين الشحات، مصدر سبق ذكره، ص 13.
(18) مجموعة باحثين، مصدر سبق ذكره، ص 4.
(19) عبدالستار عبدالرحمن، الإرهاب السيبراني - خطر يهدِّد العالم، موقع التحالف الإسلامي العسكري لمحاربة الإرهاب، بحث منشور على الرابط:: https://www.imctc.org/ar/eLibrary/Articles/Pages/aspx
(20) محمود الحمدان، مصدر سبق ذكره، ص 8.
(21) عمرو عبد العاطي، استراتيجية أمريكية هجومية ضد التهديدات السيبرانية، وحدة الدراسات الأمريكية، المركز المصري للفكر والدراسات الاستراتيجية، بحث منشور على الرابط: https://www.ecsstudies.com/2077
(22) عمرو عبد العاطي، مصدر سبق ذكره، ص 5.
(23) محمود الحمدان، الإرهاب الإلكتروني وسُبل المواجهة، موقع التحالف الإسلامي العسكري لمحاربة الإرهاب، بحث منشور على الرابط: https://imctc.org/ar/eLibrary/Articles
(24) محمود الحمدان، مصدر سبق ذكره، ص 5.