الإرهاب السيبراني والأمن القومي:
قراءة في تحولات الإستراتيجية الدفاعية.

Cyber Terrorism And National Security:
Reading In Defense Strategy Shifts.

طالة لامية [1]

[1]كلية علوم الإعلام والاتصال، جامعة الجزائر 3، (الجزائر)، talla.lamia@univ-alger3.dz

تاريخ الإرسال: 2020/08/14 تاريخ القبول:2021/10/31 تاريخ النشر: ديسمبر /2021

الملخص:

من المؤكد أنه من بين أهم القضايا التي باتت تشغل العالم في عصرنا الحالي تأتي قضية العالم الافتراضي والفضاء السيبراني، ذاك الذي أضحى واقعا موازيا للعالم الحقيقي، وقد لا نبالغ إن قلنا أنه في بعض الأوقات يكون خطره أكثر دموية، لا سيما وأن صداماته تجري بعيدا عن الأعين، في محاولة للتأثير على مجريات العالم السياسية والاقتصادية من جهة، والمعطيات الأمنية والعسكرية من جهة ثانية، ومرد هذا وذاك أن جزءا كبيرا من الصراعات بين القوى العظمى في العالم، قد انتقلت من ميادين القتال الكلاسيكية إلى شبكات الإنترنت والعالم الرقمي، حيث من المتوقع أن تكون الحرب الإلكترونية السمة الغالبة، إن لم تكن الرئيسة للحروب المستقبلية.

تسعى الهجمات الإلكترونية، وعلى رأسها الإرهاب الالكتروني، أو الإرهاب السيبراني Cyberterrorism، إلى الإخلال بأمن المجتمعات وبث الرعب والخوف لدى المواطنين، فيمكن أن تكون شبكات البنية التحتية الحيوية التي تحتفظ بها الحكومات في جميع أنحاء العالم عرضة للهجمات الإلكترونية الرئيسية في أي لحظة.

الكلمات المفتاحية: الأمن السيبراني، الإستراتيجية الدفاعية، الأمن القومي، الإرهاب السيبراني.

Abstract:

Certainly, among the most important issues that occupy the world in our current era comes the issue of the virtual world and cyberspace, which has become a parallel reality to the real world, and we may not exaggerate if we say that at times its danger is more bloody, especially since its clashes are taking place far from The eyes, in an attempt to influence the political and economic course of the world on the one hand, and the security and military data on the other hand, and the reason for this and that is that a large part of the conflicts between the great powers in the world have moved from the classic battlefields to the Internet networks and the digital world, where it is expected that Electronic warfare will be the dominant feature, if not the main feature of future wars.

المؤلف المرسل: لامية طالة ، الإيميل المهني: talla.lamia@univ-alger3.dz

Cyber attacks, on top of which are cyber terrorism, or cyberterrorism, seek to disrupt the security of societies and spread fear and fear among citizens. The vital infrastructure networks maintained by governments around the world can be vulnerable to major cyber attacks at any moment.
Key words: Cyber Security, Defense Strategy, National Security, Cyber Terrorism.

مقدمة:

تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت إمكانية تعرض المصالح الإستراتيجية للدولة للتهديدات السيبرانية، وهددت بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف.

هذا، إضافة إلى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الأكثر ديمقراطية كبريطانيا والولايات المتحدة الأمريكية.

وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للتهديد، من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنيت في العالم، والثورة الكبرى في انترنيت الأشياء، حيث أصبحت قواعد البيانات القومية في حالة انكشاف خارجي، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي.

وعليه فلم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى مثل الإبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها، وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمي للفضاء السيبراني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات.

إضافة إلى أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود، وبروز أخطار القرصنة والجريمة السيبرانية **والجماعات الإرهابية.**

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ومن ثم فإن أي هجوم على إحدى تلك المصالح يكون سببا لحدوث عدم توازن استراتيجي، ومهددا خطيرا للأمن القومي، وهذا ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن إستراتيجيتها للأمن القومي.

وهو محور مقالنا والتي نطرح من خلاله الإشكالية التالية: **ما هو الدور الذي يلعبه الأمن السيبراني في الإستراتيجية الدفاعية للأمن القومي ضد ما يصطلح عليه بالإرهاب السيبراني؟.**

1. مفهوم الأمن السيبراني:

إن اعتماد عالم اليوم على المعلومة حقيقة ثابتة، وهي تفرض اعتمادا أكثر على الأنظمة الالكترونية التي تعالجها، والحديث عن الأمن يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف والثغرات، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر، ونتيجة زيادة التهديدات والمخاطر في الفضاء السيبراني التي تواجه الدول ظهر مفهوم الأمن السيبراني.

يعرف الأمن السيبراني بأنه:"**أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو على الأقل الحد من آثارها** "[1].

يعرف ريتشارد كمرر Richard A.Kemmerer الأمن السيبراني بأنه:" **عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة**".

بينما عرفه إدوارد أمورسو Edward Amorso على أنه: " **وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها،.. "**[2].

كما يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، علها يتيح إعادة التوسع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.

فهو النشاط أو العملية، والقدرة، أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المسرح به أو التعليل، أو الاستغلال.

ومن الناحية العملية الإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية:

- يتعاون الأمن السيبراني إلى حل كبير من وسائل دفاعية تستخدم لكشف وإحباط المتسللين.
- الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل.

➢ الأمن السيبراني ينطوي على الحل من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات، وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات، ومنع وصولها، وفرض التوثيق، وتمكين الاتصالات المشفرة.

➢ الأمن السيبراني هو مجموعة من الأدوات والسياسات والمفاهيم والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن استخلاصها لحماية البيئة الإلكترونية وتنظيم أصول الاستخدام[3].

من خلال ما ورد من تعريفات يمكن القول بالأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يته استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار عمل نظم المعلومات وتعزيز حماية سرية البيانات الشخصية وخصوصيتها واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

إذا فالأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد، لاسيما أن الحرب السيبرانية* أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول .."، ويشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسوب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسوب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث.

2. أبعاد الأمن السيبراني:

يطال الأمن السيبراني جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لابد من توضيح أبعاد الأمن السيبراني، التي نوردها كالآتي:

➢ **البعد العسكري:** كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والانجازات العلمية، التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده بين الاتحاد السوفيتي، والولايات المتحدة الأميركية في مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية[4].

وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بها يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية، ومن ثمة تحقيق الأهداف عن بعد، ومن دون شك فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد عن أي اختراق خارجي، سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات، وما يلحقه من مخاطر.

حيث أنها يمكن أن تشكل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة: طائرات بدون طيار، صواريخ موجهة، أقمار صناعية وغيرها.

➢ **البعد الاقتصادي:** لقد أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، وهو ما دفع بالدول في الآونة الأخيرة إلى زيادة استثماراتها في المعرفة، وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم بالاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين[5].

كما أن استخدام الكمبيوتر وشبكة الانترنت في تسيير وتطوير الصناعات وتحريك الاقتصاد، ومعالجة كل المعاملات الاقتصادية والمالية وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

➢ **البعد الاجتماعي:** من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسئول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن، والمسؤولية الفردية والتدابير الرادعة وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة، إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات[6].

فحسب آخر إحصائيات يفوق مستخدمي الانترنيت 4 مليارات شخص في العالم، منهم أكثر من 2,6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي[7].

➢ **البعد القانوني:** يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني، نتائج قانونية، وموجبات تسترعي اهتماما خاصا، لحل النزاعات اللي يمكن أن تنشا عنها، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، فظهرت حقوق أخرى، حق النفاذ إلى الشبكة

العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية، كما ظهرت موجبات جديدة ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى، كل هذه التغيرات والتحولات تستوجب وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات[8].

ذلك أن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم الحالات والبلدان أطرا قانونية صارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

- **البعد السياسي:** هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعل السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، علما أنه لا ينكر أحد الدور المعالم الشبكات التواصل الاجتماعي على المستوى السياسي: حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية، ... كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها.

وفي سياق آخر يجب أن لا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت[9].

هذا إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

3. أهمية الأمن السيبراني في إستراتيجية الأمن القومي:

تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت إمكانية تعرض المصالح الإستراتيجية للدولة للتهديدات السيبرانية، وهددت بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف[10].

هذا، إضافة إلى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الأكثر ديمقراطية كبريطانيا والولايات المتحدة الأمريكية.

وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن

الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للتهديد، من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنيت في العالم، والثورة الكبرى في انترنيت الأشياء، حيث أصبحت قواعد البيانات القومية في حالة انكشاف خارجي، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي[11].

وعليه فلم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى مثل الإبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها، وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمي للفضاء السيبراني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات.

إضافة إلى أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود، وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية[12].

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ومن ثم فإن أي هجوم على إحدى تلك المصالح يكون سببا لحدوث عدم توازن استراتيجي، ومهددا خطيرا للأمن القومي، وهذا ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن إستراتيجيتها للأمن القومي.

4. الانترنت العميق والانترنت المظلم Dark & Deep Web:

تستخدم الجماعات الإرهابية في العالم تقنيات رقمية غاية في التعقيد والتطور بدء بالانترنت المظلم (Dark Net) الذي يعتبر وسيلة للمجهولية (Anonymat) وإخفاء الأثر مما يجعل الدول والسلطات تجد صعوبة هائلة في مصدر التهديدات، ثم إن الإرهاب لم يقتصر وجوده في المواقع المخفية بل انتقل إلى الفضاء المفتوح أو الشبكة العالمية للانترنت، وفي كل الأحوال فتلك الأساليب لا تختلف في مضمونها مع تلك المستخدمة في الجرائم السيبرانية المنظمة أو العادية ضد الأشخاص أو الشركات.

الانترنت المظلم هو جزء من الانترنت الخفي (Hidden Net) الذي لا يمكن الوصول إليه باستخدام المتصفحات العادية (Navigateur) أو محركات البحث (Moteur de Recherche) مثل "Google" و "Yahoo" أو غيرها ، فلهذا النوع من الاستخدام متصفحات خاصة مثل "TOR و "Freepto" أو "FreeNet وغيرها، أما الميزة الأساسية لهذه المتصفحات فهي إخفاء الأثر الذي يمكن

أن يتركه المتجول على الانترنت، ومنع تعقب الأجهزة الأمنية ومراقبته مما يتيح له حماية هويته ومعلومات عن مصدر اتصاله، إنشاء مواقع على الانترنت دون الكشف عن المنشئ، تجاوز برامج الحجب التي تستخدمها الدول لحجب بعض المواقع وتكوين شبكة اتصال آمنة وغير مرئية تذلل عقبات إرسال المعلومات السرية، ويتم تأمين ذلك عبر تقنية ترتكز أساسا على نظام تشفير للبيانات وعلى شبكة مؤلفة من آلاف والموزعات حول العالم، التي تستقبل طلبات الدخول إلى المواقع، إذ تقوم بترميزها قبل إعادة إرسالها، وهذا ما يؤمن إخفاء الهوية وسرية التصفح والحركة[13].

كما تجدر الإشارة إلى أن معظم هذه البرمجيات بدأت مشاريع بحث تابعة للقوات البحرية الأمريكية على عكس الانترنت التي يعتقد الكثير خطأ أن نشأتها كانت موجهة في المقام الأول للاحتياجات العسكرية غير أن الصواب هو أنها كانت موجهة لأغراض علمية وبحثية من خلال مشروع Arpanet Network Advanced Research Projects Agency (شبكة وكالة مشاريع البحوث المتقدمة) بدعم وتمويل مالي من وزارة الدفاع الأمريكية، ومع ذلك فقد تم تطويرها داخل جامعات ومؤسسات بحثية لتكون أداة للعلماء لمشاركة المواد العلمية لغير الأغراض العسكرية، وهذا قصد تأمين خصوصية الاتصالات والمعلومات التابعة للأجهزة المتصلة بها، ثم بدأ تعميم هذه الميزة إلى موظفي المنظمات الدولية والهيئات الحكومية والأجهزة الأمنية[14].

إلا أنها لم تتأخر بالوصول إلى مجرمي الفضاء السيبراني وبالتالي إلى الجماعات الإرهابية بصفة عامة، فقد استخدمت في الاتجار بالمخدرات والأسلحة وتأمين المرتزقة وجرائم القتل والاتجار بالبيانات العسكرية وغيرها، غير أن الإرهاب السيبراني أصبح علنيا من خلال الانترنت المفتوح بحيث أصبح يؤمن عملياته العدائية من خلال الانترنت المظلم بينما يقوم بنشر أفكاره على الانترنت المفتوح من خلال صفحات التواصل الاجتماعي والمواقع العلنية، ثم إن الصعوبة ذاتها تتلقاها الأجهزة الأمنية في تتبع وحجج تلك المواقع، حيث تقوم تلك الجماعات باستخدام أسلوب الكر والفر لتختفي وتعود للظهور بعناوين جديدة.

5. الإرهاب السيبراني: مساءلة المفهوم:

مع نمو شبكة الإنترنت بشكل واسع في جميع أنحاء العالم ، ظهرت العديد من التغيرات والتطورات، فقد كان لظهور الإنترنت جانبين أحداهما إيجابي وذلك من خلال سرعة اتصال العالم ببعضه البعض واستخدام الحكومات له ، والآخر سلبي حيث استخدمته الجماعات الإرهابية لكي تنشر أخبارها وأعمالها الإرهابية ومحاولتها لجذب الأفراد إليها، وأصبح ظهور الإنترنت مرتبط بالعديد من التهديدات التي شهدها العالم من خلال العديد من الجماعات الإرهابية، منها على سبيل المثال تنظيم "داعش "، والعديد من التنظيمات الإرهابية ، وذلك أدى إلى ظهور ما مصطلح " الإرهاب الإلكتروني"، وقد كانت بداية استخدام هذه الكلمة " cyber terrorism" أو "electronic terrorism" في فترة الثمانيات في دراسة "باري كولن" Barry Collin والتي أشار فيها إلى صعوبة تعريف ظاهرة الإرهاب الإلكتروني بدقة، ناهيك عن الأساليب والحلول المطلوبة لمواجهته وكذلك تحديد دور أجهزة الحاسب الآلي والإنترنت في العمل الإرهابي.

عرف جيمس لويس James Lewiss الإرهاب السيبراني على أنه: " **استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين**"[15].

ويعرفه مكتب التحقيقات الفيدرالي بأنه "**الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر، والبيانات المخزنة من قبل مختلف الفاعلين**"، وهو التهديد أو الهجوم غير القانوني بشن هجماتٍ على أجهزة الكمبيوتر، وأنظمة المعلومات، والبرامج، والبيانات؛ بهدف ترهيب وإكراه الحكومات تحقيقًا لمختلف الأهداف[16].

ومن ثم يشير الإرهاب السيبراني إلى ارتكاب أعمالٍ إرهابية باستخدام أنظمة تكنولوجيا المعلومات، ولذا يمكن اعتباره أداةً تكنولوجية جديدة للإرهاب التقليدي، وبهذا المعنى، يتمكن الإرهاب السيبراني من تجاوز الحدود الوطنية، وهو قادر على التأثير في الدول والمجتمعات بصرف النظر عن الموقع الجغرافي للإرهابيين، ويتمثل الهدف الرئيس له في جذب الانتباه، وإثارة الفزع والخوف بين السكان المدنيين، وإكراه الحكومات على سياساتٍ غير مرغوبة[17].

ويمكن القول إن الإرهاب السيبراني هو **النقطة التي يتقاطع فيها الإرهاب مع الفضاء السيبراني**، وبهذا المعنى فإنه يختلف عن الجرائم الإلكترونية، مثل: سرقة البيانات، والاحتيال المصرفي، وما إلى ذلك ومن شأن ذلك النوع من الإرهاب أن يستهدف الأشخاص أو الممتلكات، أو البنى التحتية، مخلفًا أضرارًا متباينة قد تصل إلى حد الوفاة أو الإصابة الجسدية أو الانفجارات أو الخسائر الاقتصادية الشديدة، حيث يمثل الفضاء السيبراني عنصر جذب مهما للتنظيمات الإرهابية على تعدد أنواعها واختلاف أيديولوجياتها، نظرا لما يتيحه من وسيلة إعلام دولية وسلاح في ذات الوقت، إذ يمكن استخدامه من قبل الأطراف المتعددة.

أهداف الإرهاب السيبراني:

إن الإرهاب السيبراني يهدف إلى تحقيق مجموعة من الأهداف غير المشروعة، والتي نذكر منها ما يلي:

- تحقيق تواصل تنظيمي آمن لبعض عناصر التنظيمات الإرهابية وإثبات تواجدهم علي الساحة من خلال بث العديد من مواقع ومنتديات الحوار الإرهابية واتخاذها كأبواب دعائية لهم.
- التهديد والترويع من خلال بث بعض المواد الإعلامية، وذلك من خلال الدعاية والإعلان وجذب انتباه الرأي العام، وذلك لإبراز قوة هذه التنظيمات وترويع أي من المتعاونين مع الأجهزة الأمنية.
- جمع الأموال والاستيلاء عليها بطرق غير مشروعة، وذلك في إطار تمويل عملياتهم الإرهابية.
- الإخلال بالأمن المعلوماتي وزعزعة الطمأنينة وتدمير البني المعلوماتية التحتية والإضرار بوسائل الاتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة.
- الترويج لحرب نفسية، حيث قد يستخدم الإنترنت باعتباره وسيلة للخداع التكتيكي من قبل المنظمات الإرهابية، وذلك مثل تصوير الرهائن وقتلهم، والتي تصل إلي كل بقاع العالم[18].

6. استخدام الجماعات الإرهابية للفضاء السيبراني: تعمل الجماعات الإرهابية على استخدام التكنولوجيا المتطورة لنشر مبادئها وتصوراتها، والقيام بعدة أعمال تخريبية، وذلك من خلال ما يلي:

✦ **الاتصال:** تستخدم الجماعات الإرهابية الانترنت للاتصال بين أعضائها وتمويل عملياتهم، والحصول على المعلومات الحساسة.

✦ **نشر الأفكار المتطرفة:** تعمل الجماعات الإرهابية على نشر التطرف من خلال مواقع التواصل الاجتماعي وغرف الدردشة خاصة فئة الشباب لاستغلالهم في العمليات الإرهابية.

✦ **التخطيط والتنسيق:** تستخدم الجماعات الإرهابية الانترنت للتخطيط والتنسيق فيما بينها وتدبير الهجمات الإرهابية.

✦ **التلقين الالكتروني:** تسعى الجماعات الإرهابية من خلال الوسائل الالكترونية إلى تقديم إرشادات وطرق صنع القنابل اليدوية والأسلحة الكيماوية الفتاكة وأساليب التفخيخ والتفجير.

✦ **التمويل الالكتروني:** تحظى الجماعات الإرهابية بتمويل إلكتروني، وتنظم حملات لجمع التبرعات المالية، خاصة مع انتشار العملات الالكترونية مثل البيتكوين[19].

يعد تجنيد الشباب من أهم خصائص هذا النوع من الإرهاب ، حيث تجند الجماعات الإرهابية من خلال الإنترنت عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية ، وهم في ذلك يعتمدون علي فئة الشباب خصوصا ضعاف العقل والفكر ، فتعلن هذه الجماعات عبر مواقعها على الإنترنت عن حاجتها إلى عناصر انتحارية ، كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني ، حيث دائما ما تصف الأهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوة الشباب إلى الجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة".

ويعد تنظيم "داعش" الإرهابي أكثر التنظيمات التي مثلت تهديدا حقيقيا لسلامة شبكة الإنترنت العالمية باستخدامها في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات الإرهابية، ووسيلة لحشد المتعاطفين معه، وهم المنتشرون في كثير من دول العالم. ويستخدم تنظيم "داعش" الإرهابي مواقع التواصل الاجتماعي بغرض للتجنيد ونشر فكره في أوساط الشباب، وكان بإمكان حمَلاته عبر الإنترنت في بعض الأحيان أن تكون كافية لإثارة أعمال العنف والخوف والرعب لدى الدول والمجتمعات.

في هذا الإطار، يحدد "أبو بكر ناجي" في كتابه "إدارة التوحش" أساليب توظيف الإعلام الجهادي ضمن إستراتيجية التنظيمات الإرهابية، وهي بالنسبة لتنظيم "داعش" تستهدف وتركز على فئتين:

★ **فئة الشعوب:** بحيث يتم العمل على دمج أكبر عدد منهم للانضمام إلى صفوف الجهاد ودعمها، من جهة أخرى، التعاطي السلبي مع من لا يلتحق بالتنظيم.

★ **جنود العدو:** خاصة أصحاب الرواتب الدنيا، للدفع بهم نحو الانضمام إلى صفوف المجاهدين أو على الأقل الفرار من خدمة العدو[20].

في عام 2015 أصدر الكاتب والصحفي عبد الباري عطوان كتابا تحت عنوان "**الدولة الإسلامية... الخلافة الرقمية** "**The Digital Caliphate** فصل من خلاله الإستراتيجية الالكترونية لداعش" الدولة الإسلامية بالعراق والشام"، وتناول بالتدقيق تلك الإستراتيجية بالتحليل في عدة فصول من كتابه، مفصلا أن التنظيم الإرهابي استغل البيئة الفوضوية التي أعقبت الثورات العربية بعد عام 2011، ويرى عطوان أن تنظيم الدولة الإسلامية تتوافر لديه عناصر الدولة الثلاث من شعب وإقليم وحكومة؛ وأن المشروع التي تنفذه ما هو إلا الإستراتيجية التي بناها وسطرها أحد منظري التنظيم أبي بكر ناجي" في كتابه "**إدارة التوحش**" الذي يناقش فيه كيفيات استخدام العنف والتوحش من خلال مراحل تفضي في الأخير إلى بناء الدولة الإسلامية الكبرى.

وقد تناول الكاتب في كتابه الأساليب التي ابتكرها التنظيم في مجال الحرب السيبرانية أو الالكترونية والتي لولاها لكان من الصعب جدا قيام تنظيم مثل هذا الحجم في مدة زمنية قصيرة، ويرجع هذا بالأساس إلى تجنيده "لجيل رقمي" بامتياز وبالاعتماد على أحدث التكنولوجيات في التواصل أو نشر الأفلام أو غيرها من وسائل التنظيم في تسيير وقيادة الحرب الرقمية**21.**

7. الجهود الدولية في مجال مكافحة الإرهاب السيبراني:

اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني والثنائي والإقليمي والدولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة في إطار صياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدولي، وقد فرض تلك الحاجة إلى تحديد ما يمكن أن يمثل بنية تحتية حرجة، في ظل تبني إجراءات قانونية وأمنية صارمة بإمكانها الوقاية والتصدي للتهديدات ذات الخصائص غير التقليدية كحال الإرهاب الإلكتروني.

وقد عكست الجهود الدولية في مجال الأمن السيبراني اهتماما واضحا ومتزايدا من جانب القطاعين الخاص والعام أو بالتعاون فيما بينهما، كما سعى العديد من البلدان المتقدمة إلى تبني إستراتيجية دولية في مجال تأمين الفضاء السيبيري، من خلال جملة من القوانين وأهمها مبادرة الشراكة الدولية المتعددة الأطراف لمكافحة الإرهاب السيبراني IMPACT، التي تهدف إلى حشد الجهود الدولية من جانب القطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهة التهديدات المتزايدة التي يمثلها الإرهاب السيبراني.

كما سعت المبادرة إلى جمع الرؤى والأفكار حول التدريب وتبادل الخبرات، وتم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الرقمي وحماية الأمن السيبراني، وكانت تلك المواقع نقطة التقاء بالنسبة لخبراء أمن المعلومات والسياسيين من أجل التباحث حول ماهية خطر الإرهاب السيبراني وكيفية مواجهته، مثل مجموعة "SITE" للاستخبارات، التي تعد جهاز استخبارات متخصصا في رصد الإرهاب عبر الإنترنت ودراسة المصادر الأولية للإرهابيين والمرجعيات الفكرية لهم، وترجمة أحاديثهم، ومراقبة دعاية الإرهابيين[22].

خاتمة:

من خلال ما سبق يتضح أننا لابد أن نعترف أمام إرهاب إلكتروني بمعني أننا أمام مجتمع افتراضي تحكمه ديمقراطية وحرية وفوضى بلا حدود ولا قيود، حيث يساعد التنظيمات الإرهابية على بناء علاقات بين أعضائه في الفضاء الخارجي بعيدة عن المراقبة الأمنية, ويستفيد من ذلك أعداد هائلة من المشاركين من مختلف الجنسيات واللغات مما يمكن لهذه التنظيمات أن تجند بعضهم وأن تكسب تعاطف البعض الآخر.

فقد شكل قاعدة للتغيير والتعبير عن الرؤى المتطرفة التي تتبنى العنف أسلوبا ووسيلة، مستفيدًا في ذلك مما آل إليه الإنترنت من تقسيم الجمهور إلى فئات ومجموعات صغيرة، وأخذ هذا التنوع في تنمية ظاهرة التشتت الثقافي، بوصفه إعلاما فئويا يستخدم لإذكاء نيران الصراعات العنصرية وتنمية اتجاهات الكراهية لدى الكثير من الفئات المناهضة للفئات الأخرى، وفي مقابل تلك النظرة التفتيتية للمجتمعات، جاء ذلك الإعلام للترويج لرؤى عالمية، ففي حين تستغله الولايات المتحدة للترويج للرأسمالية والهيمنة، تستغله تنظيمات إرهابية للترويج للخلافة الإسلامية أو للجهاد العالمي.

إن التعامل من منطلق السيادة لم يعد واردا، فالسيادة في عصرنا الحالي نسبية، والفضاء السيبراني خير دليل على ذلك بالنظر إلى التهديدات التي تحيط به وتؤثر على الأمن القومي للدول مجتمعة وحتى أمن الفرد والمجتمع بشكل خاص، بالتالي نقول بأن التصدي لظاهرة بحجم الإرهاب الإلكتروني يتطلب تعاونا دوليا مشتركا، بدءا بالأطر القانونية والأمنية، لكن الظاهرة تظل أوسع وأعقد مما يتصوره البعض، لأنها مرتبطة بمجال مطاطي وغير مرئي، وطبيعة هذا المجال هي التي شجعت تكاثر الجرائم الإلكترونية ومن ضمنها الإرهاب السيبراني.

الهوامش:

1- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 25.

2- ج. رضوان: الأمن السيبراني، أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، الجزائر، جانفي 2016، ص 40.

3- بارة سمير، الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، ص 257-258.

* ولعل أفضل تعريف مبسط للحرب السيبرانية هو ذلك الذي يعتبرها مجموعة الأعمال العدائية الموجهة ضد معطيات الدولة الإلكترونية المخزنة أو المعالجة أو المتبادلة من حاسوب إلى آخر، بهدف كشفها أو نسخها أو تعديلها أو إتلافها أو عرقلة تدفقها كالهجوم على أنظمة المراقبة الجوية، وأنابيب نقل الغاز والنفط، والمفاعلات النووية.

4- منى الأشقر جبور، الأمن السيبري: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، 2012، ص 15.

5- محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟، مجلة اتجاهات الأحداث، العدد 6، مركز المستقبل للأبحاث والتطوير، أبو ظبي، 2015، ص 06.

6- الاتحاد الأوروبي للاتصالات، دليل الأمن السيبراني للبلدان النامية، جنيف، 2009، ص 16-17.

7- محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟، مرجع سابق، ص 6-7.

8- منى الأشقر جبور، الأمن السيبري: التحديات ومستلزمات المواجهة، مرجع سابق، ص 17.

9- محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟، مرجع سابق، ص 7.

10- عادل عبد الصادق، القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد 188، مؤسسة الأهرام، مصر، 2012، ص 32.

11- إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت؟، دار العربي، 2017، ص 54.

12- خالد وليد محمود، الهجمات عبر الانترنت: ساحة الصراع الالكتروني الجديد، سلسلة دراسات، المركز العربي للأبحاث ودراسة السياسات، أبو ظبي، 2013، ص 47.

13- إسحاق العشعاش، الإرهاب السيبراني وتحدّيات الدُول: دراسة مُقارِنة مع الاتفاقيات الدولية، مجلة بحوث، المجلد 12، العدد 1، جامعة بن يوسف بن خدة الجزائر، 2018، ص 180.

14- دوتون، استخدام بيئة الألاعيب في دراسة سياسات الاتصالات وتطوير الإنترنت، جريدة معلومات اليوم (Information Today) 1992، نيوجيرسي، 499-517.

15- Alix Desforges, Cyberterrorisme: Quel Périmètre ?, Fiche de l'IRSEM n° 11, 2011, P 03.

16- علي محمود عبد الوهاب، الإرهاب الالكتروني، مجلة مركز بحوث الشرطة، العدد 39، مارس 2011، ص 321.

17- سماح عبد الصبور، الإرهاب الرقمي: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي، اتجاهات الأحداث، مركز المستقبل للأبحاث والدراسات، المجلد الأول، العدد 2، سبتمبر 2014، ص 87.

18- أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، 2014، ص 11-12.

19- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 2008، ص 12-13.

20- حكيم غريب، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المجلد 05، العدد 02، 2018، ص 107-108.

21- إسحاق العشعاش، الإرهاب السيبراني وتحدّيات الدُول: دراسة مُقارِنة مع الاتفاقيات الدولية، مرجع سابق، ص 201-202.

22- حكيم غريب، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، مرجع سابق، ص 116-117.