قضايا سياسية

اسم المقال: الإرهاب السيبراني: أزمة عالمية جديدة
اسم الكاتب: م.م. محمد زهير عبد الكريم
رابط ثابت: https://political-encyclopedia.org/index.php/library/1561
تاريخ الاسترداد: 2026/11/01 22:09 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهرين ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

الإرهاب السيبراني: أزمة عالمية جديدة

The Cyber space terrorism : a new global crisis

م.م. محمد زهير عبد الكريم*

المُلخص:

يعيش العالم مُنذُ ثمانينيات القرن العشرين، ثورة تكنُولوجية في الإعلام والمعلومات والاتصالات، وأهم نتائجها انتشار الإنترنت بصورة واسعة.

إذ تحول "الفضاء السيبراني"، الذي يشمل البيانات والمعلومات والشبكات الى ساحة للتفاعلات العالمية. تتغير اساليب الإرهاب وأدواته المستخدمة بمرور الوقت، ولا يبقى على نسق واحد. نتيجة للتطورات التكنولوجية في مجال الاتصالات والمعلومات؛ برز "الإرهاب السيبراني" بعدهُ تحدياً وازمة عالمية جديدة. وأضحى الإنترنت ساحة جديدة للهجمات السيبرانية، التي تستهدف تدمير أو تعطيل المواقع الالكترونية لترويع الحكومات أو الشعوب لأسباب سياسية أو دينية أو أيديولوجية أو اجتماعية. فضلاً عن استغلاله من الجماعات الإرهابية، لخدمة اغراضها المُختلفة. وزاد الاهتمام الدولي بمُكافحة "الإرهاب السيبراني" من خلال تبني سياسات وقوانين وإجراءات على المستوى الوطني وعلى مستوى التعاون الدولي نتيجة لمخاطر "الهجمات السيبرانية" وتهديدها الكبير.

Abstract:

The world lives since 1980s of the past century, the technological revolution in the media, information and communication, and the most important of its results is the widely spread of the Internet. where the "cyber space " which includes data, information and networks, transferred to a environment of global interactions.

The methods and tools of terrorism change over time, as they do not remain in the same format .As a result of developments in technology in the area of information and communication; emerged as " cyber space terrorism " as a challenge and a new global crisis. the Internet became a new

* كلية العلوم السياسية- جامعة الموصل.

environment of "cyber-attacks" which is targeted to destroy or disable websites to intimidate governments or peoples for political, religious, ideological or social reasons. As well as it's the exploitation by the terrorist groups, to serve their purpose different. the international attention to combating the "cyber terrorism" increased through the adoption of policies, laws and procedures at the national level and at international level of cooperation as a result of the risks of "cyber-attacks" and its great threat.

الكلمات المفتاحية: الانترنت، السيبرانية، الارهاب السيبراني، التطرف السيبراني.

المقدمة:

يعيش العالم مُنذُ مطلع ثمانينيات القرن العشرين ثورة تكنولوجية غير مسبوقة، في الإعلام والمعلومات والاتصال. وأهم ما ترتب عليها انتشار شبكة الإنترنت بصورة واسعة.ومع تطورات الثورة التكنولوجية تحول "الفضاء السيبراني" العالمي الى ساحة للتفاعلات العالمية، برز العديد من الانماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية او العسكرية.

إنّ تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية مثل:"الشركات التكنولوجية العابرة للحدود، وشبكات الجريمة، والجرائم والقرصنة الإلكترونية، والجماعات الإرهابية وغيرها"، فرض تحديات عدة في الحفاظ على الأمن السيبراني العالمي.

تتغير تكتيكات الإرهاب وأدواته المستخدمة بمرور الوقت، ولايبقى على نسق واحد. ونتيجة للتطورات التكنولوجية في مجال الإتصال والمعلومات، يلوح شبح الإرهاب السيبراني في الأفق بوصفه أزمة عالمية جديدة، الامر الذي جعل هذا الفضاء، مجالاً للأعمال والهجمات والجرائم الالكترونية الارهابية من جانب افراد اوجماعات اومؤسسات. وتتردد سيناريوهات اجرامية عدة يقوم بها الإرهابيون باستهداف البنى التحتية للدول، وأنظمة معلوماتها، وقواعدها العسكرية، والبنى الاقتصادية والتجارية من خلال هجماتٍ سيبرانية، تفوق اثارها تلك التي قد تنتج عن الإرهاب التقليدي. فضلاً عن إستغلال "الفضاء السيبراني" من قبل الجماعات الإرهابية، في خدمة اغراضهاالمُختلفة.

اهمية البحث: تكمن أهمية البحث في تركيزه على "الارهاب السيبراني"، وهو نوع جديد من الارهاب، ظهر مع قيام الثورة المعلوماتية وتطورها، ودخولنا في عصر العولمة، وهو إرهاب جديد يستهدف أنظمة

المعلومات، يختلف عن الارهاب التقليدي، من حيث التهديد والخطورة والقدرة التدميرية والآثار الأمنية والإقتصادية والإجتماعية والسياسية، الامر الذي جعله يشكل أزمة عالمية جديدة.

هدف البحث: يهدف البحث للتعريف والتوضيح بـ"الإرهاب السيبراني"، الذي ولد المخاطر الأمنية الالكترونية بفعل "الهجمات السيبرانية" الإرهابية، التي تستهدف أنظمة البيانات والمعلومات فضلاً عن "التطرف السيبراني". ممادى أدى لظهور تحدي كبير بمثابة أزمة عالمية جديدة للدول، تستدعي الحل على المستوى الوطني، وضرورة التنسيق والتعاون الدولي.

إشكالية البحث: تتركز إشكالية البحث حول السؤال البحثي الرئيسِ: ماهو الخطر الذي يُشكلُه "الارهاب السيبراني" المُعتمد على الهجمات والجرائم الالكترونية، والتوظيف الارهابي للفضاء الالكتروني، ليُصبح أزمة وتهديد عالمي جديد؟

ومن السؤال البحثي الرئيسِ تتبع الأسئلة البحثية الفرعية الآتية:

_ ماهو "الفضاء السيبراني"؟

_ ماهو "الإرهاب السيبراني"؟

_ ماهي طبيعة الهجمات السيبرانية الإرهابية وماهي خطورتها؟

_ كيف توظف الجماعات الإرهابية "الفضاء السيبراني" لخدمة اغراضها؟

_ ماهي الجهود الوطنية والدولية لبعض الدول لمكافحة الإرهاب والتطرف السيبراني؟

فرضية البحث: تقوم فرضية البحث على أساس أن "الارهاب السيبراني" الذي ظهر نتيجة للتوسع في استخدام تكنولوجيا المعلومات، اخذ يشكل ازمة عالمية جديدة بتهديده لانظمة المعلومات والبيانات المُرتبطة بالافراد والدول، وهو مادى لبعض الدول للتحرك لمُكافحته على المستوى الوطني والدولي.

مناهج البحث: من اجل اثبات صحة فرضية البحث، والإجابة على الإشكالية البحثية، اعتمد البحث على المنهج الوصفي.

هيكلية البحث: تم تقسيم البحث إلى محورين، فضلاً عن المقدمة والخاتمة التي ذُكر فيها اهم النتائج، المحور الأول تناول: الإطار النظري وجاءَ في جُزئين الأول: مفهوم "الفضاء السيبراني"، والثاني: مفهوم الارهاب السيبراني. وأماَ المحور الثاني فكشف: مجالات "الارهاب السيبراني" وجهود مُكافحتُه، وجاء في ثلاثة أجزاء بينَ:الاول:الهجمات السيبرانية الارهابية، أما الثاني فدرس: توظيف الجماعات الإرهابية للفضاء السيبراني، والثالث بين:جهود مُكافحة "الإرهاب السيبراني".

أولا: الإطار النظري.

هذا المحور يركز على المعلومات الاساسية التعريفية، التي تعد اساس والمدخل لفهم الموضوع، إذ يتم توضيح مفهوم الفضاء السيبراني ومفهوم "الإرهاب السيبراني"، لذلك تم تقسيمه إلى جُزئين وعلى النحو الآتي:

1- **مفهوم الفضاء السيبراني:** تغير التاريخ وتغيرت طبيعة الحياة البشرية عبر القرون الماضية، بفعل الثورتين الزراعية والصناعية. أما الآن فإن البشرية تعيش ثورة "تكنولوجيا المعلومات" التي يُطلق عليها: الثورة الثالثة،وأساسها المعرفة والحاسوب والأنترنت. هذا التقدم الكبير ثمرة الدمج بين تكنولوجيا الإتصال والإعلام الآلي، الذي أنتج الثورة الألكترونية [1]. إذ شهد القرن الحادي والعشرين بشكل خاص تطور تكنولوجي كبير في ميادين الحياة كافة، مثل: تكنولوجيا الإتصال الذكية وتكنولوجيا الإعلام وتطور الخدمات الإلكترونية، مما أدى إلى ظهور اسلوب قوامه المعرفة والرقمنة والتطبيقات الذكية. وفي عالم الإنترنت تم الإعتماد على الوسائط الإفتراضية التي حلت محل الوسائط التقليدية[2]. بحُكم أن العالم يعيش حالة مابعد الصناعة أوما بعد الحداثة، فأصبح يُطلق عليه بالمجتمع العالمي الرقمي، الذي أدى لظهور الإنسان الرقمي والإنسان الأنترنيتي، واصبح الفضاء السيبراني العالمي يضم فعالية إتصالية على شكل تيار جارف، لايستطيع أحد أن يُعزل عنه، بحكم أن الإنسان في حياته يواجه كم هائل من المعلومات والأفكار، إذ أن الزيادة الإتصالية باتت أهم ظواهر العصر الحديث[3].

تم ذكر "الفضاء السيبراني" لأول مرة في احدى روايات الكاتب الأمريكي المشهور "وليام جيبسون"، في ثمانينيات القرن العشرين. هذا الفضاء الإفتراضي يستند على الحاسوب والإنترنت والخزين الهائل من البيانات والمعلومات. وعن طريق الهواتف واجهزة الحواسيب يتم التواصل عبر هذا الفضاء، دون إعتبار للحدود الجغرافية. وقد عرفت "الوكالة الفرنسية لأمن وأنظمة الإعلام" "ANSS" "الفضاء السيبراني": "فضاء التواصل المُشكل من خلال الربط البيني العالمي لمُعدات المُعالجة الألية للمُعطيات الرقمية".

---

(1) حكيم غريب، الجريمة الألكترونية والجهود الدولية لمكافحتها، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر- الجزائر، العدد3،حزيران-2015،ص72.

(2) احمد العقبي، خدمات الإعلام والإتصال الذكية، بحث منشور في كتاب خاص بوقائع مؤتمر بعنوان: المدن الذكية في ظل التغيرات الراهنة(واقع وآفاق)، برلين-المانيا،ج2، ط1، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والإقتصادية، 2019،ص97.

(3)جمال سند السويدي، وسائل التواصل الإجتماعي ودورها في التحولات المستقبلية من القبلية إلى الفيسبوك، جدة- المملكة العربية السعودية ط4، مركز الخليج للأبحاث،2014،ص60.

والبعض عرفه على أنه: "فضاء شامل مُتكون من شبكة مُحبكة تضم المنشآت التكنولوجية للإعلام، بما فيها من أنترنت، وشبكات الإتصال السلكي واللاسلكي، ومُتعامل الخدمات على الخط"[1]. وترمز كلمة cyper أوcypernetics إلى: نظرية الإتصالات والتحكُم المُنظم في التغذية المُرتدة، التي تعتمد عليها دراسات الإتصالات والتحكم في الحياة وفي الأليات التي يصنعها الإنسان، أي علم دراسة الإتصال والتحكم الألي، في النظم العصبية للكائنات الحية ومُحاكات الألات لها [2]. في حين اشار البعض "الفضاء السيبراني" بأنه:"الشبكات والإتصالات والبيانات ومصادر المعلومات"[3].ويمكن تعريف "الفضاء السيبراني" على انه:"هو ذلك المدى المفتوح المُشترك لجميع الأفراد في المُجتمعات، الذين لهم القدرة في الدخول لشبكة الأنترنت، والذي يُتيح لهم الحصول على المعلومات وإجراء مُناقشات مع الأخرين، وحرية التعبير عن الرأي، دون التقيد باللقاء المُباشر أو بالزمان والمكان"[4].

يتشكل "الفضاء السيبراني" من ثلاث طبقات هي:[5]

أ-الطبقة المادية: تتألف من المُعدات المادية مثل: اجهزة الحاسوب وأنظمة الإعلام الآلي، والمُنشآت المهمة للربط البيني، ومُختلف اسلاك الإتصال والكوابل والإتصال بواسطة الأمواج.

ب- الطبقة المنطقية: تتألف من مجموعة البرمجيات أو البرامج، التي تقوم بترجمة المعلومات، بشكل مُعطيات رقمية.

ج- الطبقة الدلالية أو الإعلامية: التي تتعلق بالبعد الإجتماعي، لمجموعة المُستخدمين، مع التأكيد انه لايوجد مبدأ وحدة الهوية للشخص في الفضاء السيبراني، إذ هناك عدة هويات رقمية للشخص.

د-ويضم الفضاء السيبراني عدة فواعل تُصنف إلى نوعين:[6]

1. الفواعل الدولاتية: الدولة هُنا هي من يمارس السلطة في الفضاء السيبرانيعلى الإشخاص بواسطة الوسائل التي تملكها مثل: الأجهزة الحكومية وقوات الأمن والإدارات.

(1) نقلاً عن: يوسف بوغرارة، الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الأفريقية وحوض النيل، المجلد1-العدد3، المركز الديمقراطي العربي، برلين- المانيا، ايلول-2018،ص103.

(2) غريب حكيم، الإرهاب السيبراني والأمن الدولي،: التهديدات العالمية الجديدة وأساليب مواجهتها، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، بن عنكون- الجزائر، المجلد5- العدد2، كانون الأول-2018،ص106.

(3) نقلاً عن: المصدر نفسه ص106.

(4) نقلاً عن: رضوان قطبي، شبكات التواصل الإجتماعي والفضاء العمومي في المغرب، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، برلين-المانيا، العدد4، آب-2018،ص1.

(5) بلفرد لطفي لمين، الفضاء السيبراني: هندسة وفواعل، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر- الجزائر، العدد5،حزيران-2016،ص-ص152-154.

(6) يوسف بو عزارة، مصدر سبق ذكره،ص104.

2. الفواعل غير الدولاتية: وتضم فواعل أُخرى تتعامل معهم الدولة في الفضاء السيبراني مثل: الأفراد والمُنظمات غير الحكومية والمجموعات الإفتراضية.

2- **مفهوم "الإرهاب السيبراني"**: إن "الإرهاب السيبراني" قد ارتبط بمصطلح "الفضاء السيبراني"، وذلك نتيجة للتوسع في الإعتماد على الإتصالات والمعلومات، في تسيير الشؤون الحياتية للأفراد والمؤسسات والدول، كما ويرتبط بنوع البيئة التي يمارس فيها[1]. وظهر مصطلح الإرهاب السيبراني في الثمانينيات من القرن العشرين، ويرجع للباحث"كولن" Collin وهو اختصاصي في المعلوماتية والوقاية والأمن، إذ يرى إن "الأرهاب السيبراني" مُرتبط بتغييرات بنيوية اصابت المجال العالمي وتشمل عاملين: الأول: تفكك الإتحاد السوفياتي والكتلة الإشتراكية، وهو ماولد مخاطر جديدة ترتبط بالأمن السيبراني، مثل الحروب الألكترونية وعمليات التجسس السيبراني والجرائم السيبرانية, أما العامل الثاني: فيتعلق بالأنترنت الذي جلب الكثير من المخاوف من إخصائيي الأمن والقادة السياسيين. الأمر الذي ولد مخاطر في أن الإرهاب الحديث بإمكانه أن يولد مخاطر وضرر كبير، ليس بواسطة قنبلة وإنما بلوحة مفاتيح[2].

بعد احداث 11 ايلول 2001، أصبح هُناك إرتباط واضح بين الأنترنت والإرهاب، إذ اضحت المواجهة الكترونية ضد الإرهابيين، بعد أن كانت قد إقتصرت على مواجهه مادية فقط، وتحولت الحروب إلى رقمية، بعد أن اصبح الإنترنت أكثر الأسلحة تدميراً وتأثيراً، وتم إستخدامه تجاه أهداف إرهابية، ليظهر "الإرهاب السيبراني"، الذي يتكون من كلمتين هما "cyber terrorism"، وكلمة "cyber" تعني الأنترنت أو "الفضاء السيبراني"،أما كلمة "terrorism " تعني الإرهاب. والإختلاف الوحيد بين "الارهاب السيبراني" وبين الإرهاب العام، في نوعية الأداة المُستعملة لتحقيق الهدف الإرهابي[3].

تنوعت تعاريف "الارهاب السيبراني" إذ ليس هناك تعريف مُتفق عليه دولياً، بسبب تعدد اساليب وأشكال وانواع هذا الإرهاب، ومن ثم تنوعت وجهات النظر[4]. واقدم تعريف له ظهر عام 1997 من قبل "مكتب التحقيقات الفدرالي الامريكي""Federal Bureau of Investigation " عندما تم تعريفه على أنه:"الهجوم المُتعمد ذو الدوافع السياسية ضد المعلومات وانظمة وبرامج الكومبيوتر والبيانات، الذي ينتج

(1)منى الأشقر جبور،السيبرانية هاجس العصر،القاهرة-مصر، ط1،المركز العربي للبحوث القانونية والقضائية،2018،ص85.

(2) محمد سويلم، في الإرهاب والإرهاب الألكتروني التباسات المفهوم وتقاطع المقاربات، مجلة قضايا التطرف والجماعات المسلحة، المركز الديمقراطي العربي، برلين-المانيا، السنة1- العدد1،أيار-2019،ص21.

(3) الهاشمي ناصر،الإرهاب الجذور المظاهر وسبل المكافحة، عمان- الأردن، ط1، دار ومكتبة الحامد للنشر والتوزيع، 2016،ص-ص185-186.

(4) المُختار لمجيدري، الإرهاب الألكتروني إشكاليات الإثبات الجنائي والقضاء عليه، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، برلين- المانيا، المجلد3-العدد14،آذار-2019،ص257.

عن العُنف المُسلط على اهداف غير قتالية[1]. كما عرف الباحث "دورثي دينينغ" "الارهاب السيبراني" بأنه:"هجمات غير مشروعة وتهديدات بالهجوم على اجهزة الكومبيوتر والشبكات والمعلومات المُخزنة فيها لتخويف او اجبار الحكومة أو شعبها لتحقيق أهداف سياسية أو إجتماعية" [2]. وتم وصف "الارهاب السيبراني" بأنه:"التهديدات على أنظمة المعلومات بدوافع سياسية أو دينية"[3]. كما أن "المركز الوطني لحماية البنية التحتية في الولايات المتحدة الأمريكية" عرف "الأرهاب السيبراني" بأنه:" أي هجوم سيبراني يستغل شبكات المعلومات أو شبكات الإتصال لإحداث تدمير كافٍ،لإثارة الرعب وإرهاب المجتمع لإهداف ايديولوجية"[4].

"الارهاب السيبراني" هو جُزء من جُهد مُنظم لإرهابيين سيبرانيين، أو وكالات مُخابرات اجنبية، أو أي جماعات تسعى لإستغلال ثغرات أمنية مُحتملة في الأنظمة المعلوماتية الحيوية. والارهابي السيبراني هو الشخص الذي يدفع حكومة أو مُنظمة أو جهه لتلبية اهدافه السياسية أو الإجتماعية، من خلال إطلاق هجوم الكتروني على انظمة الحواسيب، ونُظم تشغيلها، ممايؤدي إلى إنهيار النظام[5].

وبهذا فإن "الإرهاب السيبراني" يشمل مهاجمة وتغيير البيانات والتلاعب والتعطيل التي تُعرقل سير المعلومات في الشبكات لإلحاق الضرر لإسباب دينية أو أيديولوجية أو إجتماعية أو سياسية، أيضاً التهديد بهذه العمليات للإبتزاز والضغط يُعد من الأعمال الإرهابية، يُسبب إحداثها الرعب والترويع للناس[6].

ومن خلال هذا المحور يمكن القول بإن "الفضاء السيبراني" الذي ظهر نتيجة الثورة التكنولوجية هو فضاء واسع الكتروني، يضم الشبكات الالكترونية والإتصالات والبيانات ومصادر المعلومات كافة. هذه المكونات دخلت مُختلف ميادين حياة الأفراد من أجل التسهيل والسرعة وتقليل التكلفة والخدمة الأفضل. إلاّ أن هذا الفضاء اصبح مجال لمُمارسة انواع من الأعمال الإرهابية التي تستهدف انظمة المعلومات والبيانات الالكترونية للأفراد والدول، وإلحاق الضرر بها، لأسباب سياسية أودينية أو أجتماعية أو

(1) نقلاً عن: محمد سويلم، مصدر سبق ذكره،ص-ص 21.

(2) نقلاً عن: المصدر نفسه ،ص-ص 21-22.

(3) نقلاً عن : منى الاشقر جبور، مصدر سبق ذكره،ص85.

(4) نقلاً عن: المصدر نفسه،ص85.

(5) فاطمة عبد الفتاح، تطور توظيف جماعات العُنف للارهاب السيبراني، مجلة السياسة الدولية، مركز الاهرام القاهرة-مصر، العدد208، 2017،ص27.

(6) منى الأشقر جبور، مصدر سبق ذكره،ص85.

ايديولوجية، وهو ماأدى لبروز نوع جديد من الإرهاب سمي بـ "الإرهاب السيبراني"، الذي ينتج عنه خوف وترويع للأفراد والدول. والذي يتضمن مجالات عدة سيتم تناولها في المحور الثاني.

ثانيا: مجالات الإرهاب السيبراني وجهود مُكافحتُه.

تتعدد مجالات وتفرعات "الارهاب السيبراني"، لذلك يحاول هذا المحور التطُرق لها وتوضيحها، من اجل الإلمام بها، فضلاً عن توضيح الجهود الوطنية والدولية لمُكافحة هذا النوع من الإرهاب، ولذلك تم تقسيم هذا المحور إلى ثلاثة أجزاء وكالأتي:

1- **الهجمات السيبرانية الإرهابية:** نتيجة للتطورات التكنولوجية في مجال الإتصال وتقنية المعلومات، أصبح بإمكان أجهزة الحاسوب أن تحدث أضراراً كبيرة في البنى التحتية للدول، بشكل لاتستطيع الجيوش العسكرية إحداثه. إذ أضحت الشبكة العنكبوتية بمثابة ساحة جديدة للهجمات السيبرانية، هذه الهجمات التي من الصعب معرفة هوية من قام بها[1]. إذ اضحى "الفضاء السيبراني" مجالاً لظهور أنواع جديدة من الإرهاب غير التقليدي،هدفه القيام بعمليات هجومية لتدمير البنى التحتية للمعلومات، وهو مانتج عنه مخاطر سياسية وأمنية وقانونية. فأستفاد الأرهابيون بشكل كبير من التحديثات التكنولوجية والثورة المعلوماتية، واصبح بإستطاعتهم الحصول على النتاجات التكنولوجية والإستفادة من البحث والتطوير، وذلك بالحصول على أجهزة للتواصل كونية المدى وفائقة السرعة ومُتعددة ومُعقدة وسرية، دون تكاليف كبيرة، بواسطة فضاء الأنترنت[2]. هذه الهجمات والعمليات التخريبية التدميرية، تُشكل تهديداً لمصلحة المُستخدمين لهذا الفضاء في مُختلف مجالات الحياة: الإجتماعية والإقتصادية والسياسية والثقافية[3].

يقصد بالهجمات السيبرانية الإرهابية: "فعل يقوض من قدرات وظائف شبكة الحاسوب، من خلال إستغلال نقطة ضعف مُعينة تُمكن المُهاجم من التلاعب بالنظام"[4]. وتستهدف هذه الهجمات أنظمة الحاسوب وخوادم الشبكات والبنى التحتية التابعة لها، عن طريق الإختراق الألكتروني للحواسيب أو نشر فيروسات الحواسيب أو البرامج المضرة أو عمليات الإغراق. هذه الأعمال التخريبية تحمل خصال العمل

(1) رغدة البهى، الوكالة السيبرانية عوامل النشأة وأنماط الفواعل، ملحق بعنوان" إتجاهات نظرية" مجلة السياسة الدولية، مركز الأهرام ، القاهرة- مصر ،العدد218، تشرين الأول-2019،ص15.

(2) غريب حكيم، مصدر سبق ذكره، ص،ص 105،107،109.

(3) بلفرد لطفي لمين، مصدر سبق ذكره،ص156.

(4) نقلاً عن: يوسف بوغرارة، مصدر سبق ذكره، ص 107.

الإرهابي بما فيه إثارة الرعب لتحقيق أهداف إجتماعية أو سياسية[1].كما أن الاختراق السيبراني في البيئة الاستراتيجية، هو قُدرة الوصول إلى هدف تكنولوجي بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص بالهدف[2].

تتميز "الهجمات السيبرانية" الإرهابية بأنها تحدث دماراً دون دماء ودون أشلاء، إذ يقوم الإرهابيون السيبرانيون بعمليات تسلل وتجسس ثم النسف، دون غُبار أو أنقاض أو دُخان، وهو مايحدث نتائج خطيرة سواء بواسطة تدمير المواقع أو عمليات القصف والنسف بهجوم فايروسات، أو باقي أسلحة الفضاء الألكتروني المتنوعة، للتمكن من تلك المواقع، هذه الاسلحة من السهل الحصول عليها[3].كما أن "الإرهابي السيبراني" يقوم بفعله وهو داخل مكتبه أو بيته بعيداً عن رقابة أجهزة السلطات[4].

إن "الارهاب السيبراني" يستهدف تهديد المُجتمعات الحديثة في بناها التحتية،عبر إستخدام التكنولوجيا الحديثة في تلك الهجمات ضد مُؤسسات الدول والشركات الإقتصادية، وأضحى وسيلة بيد الإرهاب عن طريق شبكة الإنترنت، "فالإرهاب السيبراني" هو نوع جديد من الإرهاب لايستخدم السلاح التقليدي، بل يعتمد على توظيف الإرهابيين للمنظومات المعلوماتية والتقنية، في إستهداف الأنظمة المدنية والعسكرية،وهو مايُشكل خطراً على الأمن الوطني والدولي[5].إذا تُلحق "الهجمات السيبرانية" الإرهابية اضرار بأنظمة المياه والطاقة التي تؤثر بشكل كبير على سلامة الناس، والتي تسبب الهلع والرعب، ايضاً قد تستهدف أنظمة الطاقة النووية والشبكات الألكترونية، التي تدير النقل البحري والبري والجوي، والسيطرة على بيانات وأنظمة الحكومة الألكترونية، بما يؤدي إلى تدمير وتعطيل الخدمات، أيضاً السيطرة على وسائط الإتصال والأنترنت، بهدف تغيير وجهات الرأي العام، بما يؤدي لزعزعة إستقرار نُظم الحُكم[6].

ايضاً قد تهدف "الهجمات السيبرانية الإرهابية" عملية إغراق الشبكات وهو مايؤدي إلى تعطيلها وتوقفها، من أجل اهداف سياسية. مثال على ذلك عندما تسبب أحد الأشخاص في عام 2000 بإيقاف

(1) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تقرير: إستخدام الأنترنت في أغراض إرهابية،، فينا- النمسا، مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، حزيران-2012،ص-ص11-12.

(2) موسى زناد، حرب النجوم والحرب العالمية الثالثة، بيروت-لبنان، ط2، دار الرائد العربي للطباعة، 2010،ص213.

(3) نورة شلوش، القرصنة الألكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، مركز بابل للدراسات الانسانية- جامعة بابل، المجلد8-العدد2،أيلول-2018،ص195.

(4) المُختار لمجيدري، مصدر سبق ذكره، ص258.

(5) حكيم غريب، مصدر سبق ذكره، ص-ص74-75.

(6) منى الأشقر جبور، مصدر سبق ذكره،ص86.

شبكة "CNN" عن البث، ومواقع آي باي وامازون على شبكة الانترنت[1]. ايضاً عندما تعرضت استونيا في 27نيسان2007 لسلسلة هجمات إرهابية الكترونية، ضد مواقع مُرتبطة بالحكومة وأُخرى عامة، مانتج عنه اضرار وخلل كبير في تسيير الحياة اليومية، بسبب توقف الخدمات الأساسية لدى السكان، كون أستونيا من الدول التي تعتمد على الإنترنت بشكل كبير[2].

إن تدمير شبكات المعلومات عبر "الهجمات السيبرانية" الإرهابية، ينتج عنها خسائر تُعادل أضعاف خسائر قصف أو تدمير مبنى أو تفجير جسر أو خطف طائرة. والمثال على ذلك في عام 2008 أنقطع سلك في البحر المتوسط، يربط الشرق الأوسط بأوربا، وهو مانتج خسائر فادحة بملايين الدولارات، واسباب القطع المُفاجئ بقيت مجهولة[3]. وايضاً الهجوم الذي تعرضت له شبكة التحكم والسيطرة الكهرُبائية في الولايات المتحدة عام 2009 مما ادى لتوقفها نتيجة لإختراق نظام السيطرة[4]. وفيروس شمعون والمُشتبه مصدره إيران، الذي إستهدف تعطيل شركات الطاقة لبعض دول الخليج، وأحدث ضرراً بشركة ارامكو السعودية[5].

2- **توظيف الجماعات الإرهابية للفضاء السيبراني:** في العصر الحديث، أصبح هُناك إرتباط كبير بين مواقع شبكة الإنترنت وبين إنتشار المخاطر الأمنية، التي ترقى لتهديد الإستقرار والأمن، مثل التطرف والإرهاب[6]. إذ يوفر الأنترنت منبراً مُهماً يظهر الإرهاب بواسطته في ترويع المُجتمع[7]. ويتم استخدام الأنترنت من قبل المجاميع الإرهابية وانصارها لتحقيق عدة اهداف منها: الإتصال والتدريب والجانب العملياتي والدعاية والتجنيد[8]. ولتوضيح ذلك سيتم شرح كل جزء وفق الآتي:

أ- **الإتصال:** تستخدم المجاميع الإرهابية فضاء الإنترنت، لتحقيق الإتصال بالمُناصرين والأعوان والإتصال بالعالم الخارجي، ومن خلال الانترنت، يقوم الإرهاب بتوجيه الرسائل للمناصرين وللعالم

(1) شادية احمد أحزاب سياسية لقراصنة الأنترنت، مجلة آفاق المُستقبل، مركز الإمارات للدراسات والبحوث الإستراتيجية، ابوظبي- الإمارات العربية المتحدة، السنة1- العدد3، كانون الثاني- شباط-2010،ص103

(2) بلفرد لطفي، مصدر سبق ذكره، ص149.

(3) المختار لمجيدري، مصدر سبق ذكره، ص261.

(4) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المُحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، السنة8-العدد4، 2016،ص623.

(5) رغدة البهى، مصدر سبق ذكره، ص 16.

(6) جمال سند السويدي، مصدر سبق ذكره،ص88.

(7) منى الأشقر جبور، مصدر سبق ذكره، ص87.

(8) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مصدر سبق ذكره، ص1.

كافة[1]. وتقدم برامج التواصل الإجتماعي قدرة في تحقيق إتصال فاعل بين المجاميع الإرهابية للتفاعل مع بعضها بشكل آمن، وهي عابرة للحدود، وفي الوقت نفسه لها خاصية الإتصال الشخصي والتأثير والتأثُر في فضاء إفتراضي، لاتستطيع الدول السيطرة عليه بشكل كامل[2].

ب- التدريب والتخطيط والتنفيذ للعمليات الإرهابية: في عصر الإرهاب المُبتكر إزدادت فاعلية عمليات التنظيمات الإرهابية، عن طريق الإستفادة من الوسائل التقنية الحديثة ومُميزاتها[3].إذا تستخدم المجاميع الإرهابية الأنترنت للتدريب العسكري لأعضائها، عن طريق نشر كُتب تخص الأسلحة والجوانب التكتيكية في القتال، وكيفية صناعة المُتفجرات. كما تستخدم، برامج حديثة لمُساعدتها في عملياتها مثل برنامج: غوغل إرث الموجود في مُوقع مُهاجرون، الذي يشرح بشكل صوري إفتراضي المباني في جميع أنحاء العالم، والقيام بتنفيذ إفتراضي للعمليات، لأجل التدريب على العملية الحقيقية[4].ومن ضمن الوسائل التقنية التي تستخدمها التظيمات الإرهابية لاسيما تنظيم داعش الارهابي برنامج "Qgruond control" في عمليات التخطيط للمهمات والسيطرة بطيران الطائرات المُسيرة التي يستخدمها التنظيم الارهابي في الهجمات، وهذا البرنامج يعتمد على خرائط"Google "على الأنترنت[5].

ج- الاعلام والدعاية ونشر الأفكار: خلال السنوات الأخيرة إتجهت المجاميع الإرهابية للإستفادة من الوسائط التقنية الحديثة لاسيما الإنترنت، في عرض ونشر أفكارها، لبُعد هذه الشبكة عن الأجهزة الرقابية، والمرونة التي تتصف بها، وذلك لتحقيق أهدافها المُتعددة[6]. وعن طريق الإنترنت يقوم الإرهاب بتوجيه رسائله إلى العالم والحكومات والسلطات، من اجل نشر الخوف والهلع، والقيام بعمليات نفسية ضد أعداءه[7].

---

(1) منى الأشقر جبور، مصدر سبق ذكره، ص88.

(2) جمال سند السويدي، مصدر سبق ذكره،ص90.

(3) سركان بالكان، تقرير: إستراتيجية داعش في إستخدام الطائرات المُسيرة، ترجمة: مركز الخطابي للدراسات، د.ن، مركز الخطابي للدراسات، 2019،ص-ص6-7.

(4) هشام الهاشمي، عالم داعش: تنظيم الدولة الإسلامية في العراق والشام، بغداد- العراق، ط1، دار بابل للطباعة والنشر،2015،ص،ص 88،63.

(5) سركان بالكان، مصدر سبق ذكره،ص18.

(6) نايف احمد ضاحي الشمري وعمر عباس العُبيدي، دور مجلس حقوق الإنسان في مُكافحة التطرف الديني، مجلة قضايا التطرف والجماعات المُسلحة،المركز الديمقراطي العربي، برلين-المانيا،السنة1- العدد2، تشرين الثاني- 2019،ص77.

(7) منى الأشقر جبور، مصدر سبق ذكره،ص88.

وهناك العديد من الخلايا الإعلامية في المواقع الإرهابية، تتولى عملية تجهيز المواد الإعلامية ثُم تحول إلى المواقع الألكترونية العالمية[1].واحتل الإعلام والدعاية مكانة كبيرة لدى الإرهاب لاسيما عند تنظيم "القاعدة" الارهابي والذي انبثق منه تنظيم داعش الارهابي، واصبح الجانب الإعلامي لديهم يواكب التطورات التكنولوجية، بعد إدراك أهمية التواصل وادواته الجديدة المؤثرة. إذ تم إضافة المجال التكنولوجي للجهاد والذي لايقل أهمية عن المجال الأرضي الواقعي. على سبيل المثال يقوم تنظيم "داعش" الارهابي ببث الكثير من المواد بأنواعها المكتوبة والمرئية والمسموعة، والتي تحتوي على دعايات وأخبار التنظيم الارهابي عبر الأنترنت، بعد أن استفاد من التطور التكنولوجي، لاسيما برامج التواصل ليستغلها بشكل يخدم مصلحته الدعائية ونشر افكاره[2]، كونها تتمتع بميزات عدة منها أنه يُمكن استخدامها دون رقابة، ومُنتشرة بشكل واسع وكلفتها المادية قليلة[3]. وتُمثل المُنتديات الألكترونية وبرامج التواصل الإجتماعي بأنواعها مثل: يوتوب و فيس بوك و تويتر وأنستِكرام والوتس آب أدوات مهمة بيد المجاميع الإرهابية للدعاية والترويج للمعتقدات والأفكار[4].

د- التجنيد: تستخدم المجاميع الإرهابية فضاء الإنترنت، في عمليات التجنيد والتأثير على الأشخاص[5].وأشار "بيتر آر نيومان" "Peter R.Neuman" وهو استاذ في كلية "كينغز" بلندن "king,s college London":" أن عمليات التجنيد عبر الأنترنت، أسهمت بتوسيع القاعدة السكانية للمجتمع الجهادي"[6]. وتتم عمليات تجنيد الأشخاص في المُنظمات الإرهابية عبر غرف الدردشة في مواقع الأنترنت، أو بواسطة الهواتف الذكية أو برامج التواصل الإجتماعي، مُستغلة الظروف الإجتماعية اوالإقتصادية اوالنفسية التي يعيشها هؤلاء الشباب[7]. ويؤكد بعض الباحثين في المجال الأمني أن أغلب

(1) هشام الهاشمي، مصدر سبق ذكره،ص81.

(2)نجلاء مكاوي وآخرون، تنظيم الدولة دراسة تحليلية في بنية الخطاب، بيروت–لبنان، ط1،مركز صناعة الفكر للدراسات والأبحاث،2016،ص،ص57- 58 ،61 ،106.

(3) نصيف جاسم، التوظيف الدعائي للوسائل الإعلامية والرقمية عند تنظيم الدولة الإسلامية"داعش"، مجلة إتجاهات سياسية، المركز الديمقراطي العربي، برلين–المانيا،العدد2، كانون الثاني–2018،ص238.

(4) جمال عبده عبد العزيز، تجنيد التنظيمات الدولية الإرهابية للمُقاتلين عبر شبكات التواصل الإجتماعي، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، برلين- المانيا، المُجلد3- العدد16، تموز-2019، ص194.

(5) محمد سويلمي، مصدر سبق ذكره،ص23.

(6) نقلاًعن: غراييم وود، ماتريده داعش فعلاً، ترجمة:محمد عبده ابو العلا، ترجمات: مؤمنون بلا حدود، الرباط–المملكة المغربية، قسم الفلسفة والعلوم الإنسانية – مؤسسة مؤمنون بلاحدود،نيسان-2017،ص12.

(7) منى الأشقر جبور، مصدر سبق ذكره،ص89.

الذين أنظموا للجماعات الإرهابية، جندوا بواسطة الإتصال أو برامج التواصل الإجتماعي عبر اصدقائهم أو اقاربهم أو زُملائُهم في الجامعة.وهذه الروابط ساهمت بنقل الأفكار بواسطة الوسائل التكنولوجية[1].ويستخدم تنظيم "داعش" الارهابي برامج التواصل الإجتماعي للترويج وتوسيع الشهرة، والدعوة للعمل مع التنظيم، وعمليات التجنيد للمُقاتلين الأجانب[2].فمثلاً إستطاعت المجاميع الإرهابية في سوريا مُنذُ بداية عام 2015 تجنيد أكثر من 20 الف مُقاتل، أغلبُهم كانوا قد أنظموا لتنظيم "داعش" الارهابي. ويعود نجاح عمليات التجنيد، لخبرة ومهارة أعضاء التنظيم، ولاسيما في استخدام برامج التواصل الإجتماعي للدعاية، ليُصبح عنصر جذب عالمي. وتشير البيانات إلى إن80% من الذين أنظموا لتنظيم داعش الارهابي جندوا بواسطة هذه البرامج[3].

3- **جهود مُكافحة الإرهاب السيبراني:** إنتشر إهتمام الدول بالأمن السيبراني، وتوضح ذلك من خلال تبني سياسات أمنية عدة، من أجل تأمين أنظمة المعلومات، من المخاطر التي تُهدد الأمن الإقتصادي والأمن المحلي والدولي. وقامت الدول بإصدار قواعد تشريعية حديثة، للتعامُل مع هذه التهديدات وفق منظور وطني جديد ومن ثُم الإتجاه للتعاون الدولي[4]. ويُمكن تقسيم جهود مُكافحة "الارهاب السيبراني" إلى صعيدين وطني ودولي وعلى النحو الآتي:

أ- **على الصعيد الوطني:** اضحى أمن "الفضاء السيبراني"، قضية كبيرة تدخل في إستراتيجيات الأمن القومي لدول عدة، من أجل منع تعرض بُنيتها التحتية المعلوماتية للضرر، من جراء الهجمات ضد مواقعها الإلكترونية[5].بعد أن ادركت الحكومات أهمية تكوين نهج شامل في هذا المجال، للتصدي للهجمات للهجمات السيبرانية على المؤسسات الرسمية والصناعات والافراد، فضلاً عن وضع إجراءات وسياسات لحماية "الأمن السيبراني"[6]. ولما كان الفضاء السيبراني مُهم للأمن الوطني للدول، ولهذا أتخذت الخطوات

(1) جمال سند السويدي، مصدر سبق ذكره،ص90.

(2) صادق علي حسن، الهياكل المالية للتنظيمات الإرهابية: العراق انموذجاً، بيروت-لبنان، ط1، شركة المطبوعات للتوزيع والنشر،2018،ص80.

(3) نورة بلعيدي، توظيف تنظيم ا"لدولة الإسلامية" للأنظمة الإتصالية الرقمية في إستراتيجياته الإرهابية، المجلة الجزائرية الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر-الجزائر، العدد8، كانون الثاني-2017،ص193.

(4) غريب حكيم، مصدر سبق ذكره،ص116.

(5) نورة شلوش، مصدر سبق ذكره،ص197

(6) أكاديمية الدفاع الكندية، تقرير: الأمن السيبراني منهج مرجعي عام، تورنتو-كندا،أكاديمية الدفاع الكندية، تشرين الأول-2016،ص48.

اللازمة لضبط السيطرة على هذا الفضاء، فضلاً عن الإستعانة بأدوات الردع الإفتراضية(*) للتصدي لكل مايُهدد ذلك[1]. ولما كان "الفضاء السيبراني" يضُم نشاطات من افراد ومؤسسات حكومية، الأمر الذي يُحتم إصدار تشريعات قانونية، تحكُم التعامُلات في هذا الفضاء، وتحميه من "الجرائم السيبرانية"، وضرورة أن تكون هذه التشريعات مواكبة للمُستجدات الحديثة في هذا المجال[2]، لهذا اتجهت العديد من الدول لإصدار تشريعات تُنظم امن المعلومات، وتُجرم الأفعال الإجرامية الإرهابية الالكترونية، ومن هذه الدول: الولايات المتحدة ودول غرب أوربا وبعض الدول الآسيوية مثل الصين. ايضاً اتجهت بعض الدول العربية لإصدار تشريعات لمُكافحة الارهاب السيبراني ومنها: دول الخليج العربي والجزائر والمغرب ومصر[3].

ب- على الصعيد الدولي: لما كانت "الجريمة السيبرانية" عابرة للحدود، لذلك فإن مُكافحتها تتطلب وجود هيئات دولية تقوم بإتخاذ التدابير اللازمة، لمنع إنتشارها وفرض العقوبة على مُرتكبيها. الأمر الذي يلزم وجود تعاون بين المؤسسات القضائية والأمنية الدولية، لاسيما في موضوع تبادل المعلومات والمُلاحقة والتحري، وتقديم المُساعدات التقنية والقانونية، ومثلما اصبح من اللازم أن تملك الدول تشريعات للتصدي للجرائم السيبرانية، أصبح من الضروري ايضاً أن تكون هذه التشريعات متوائمة ومتناسقة كونها تحمي المصلحة العالمية الجماعية[4].إذ إنه في "الجريمة السيبرانية" يمكن أن يجري الدخول إلى نظام الحاسوب من دولة معينة، ومن ثم يتم العبث وتغيير البيانات أو إتلافها في دولة ثانية، وقد تُسجل هذه النتائج في دولة ثالثة. وبهذا يستطيع الإرهابي جعل هويته سرية، ونقل هذه البيانات بين عدة دول، و من ثم تقع الجريمة أو الهجمة في عدة دول، وتخضع لعدة قوانين وقواعد، وهومايُشكل تحدياً للجهات القضائية لهذه

(*) يُعرّف الردع الافتراضي بأنه: منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني لتأمين أجهزة الحاسب الآلي، وأنظمة المعلومات، والبنى التحتية، والحيلولة دون حدوث أو تكرار الهجمات السيبرانية من خلال تحديد الخصم على نحوٍ دقيق، وتوعده بالانتقام ردًّا على هجومه. و تقوم اداوت الردع الافتراضي على: ردع الهجمات السيبرانية فيما يُعرف بـ: الردع بالمنع، والردع بالتهديد بشن هجمات سيبرانية فيما يُعرف بـ"الردع بالانتقام. للمزيد أنظر: رغدة البهي، الردع السيبراني المفهوم والاشكاليات، متاح على الموقع:www.ecsstudies.com . كذلك انظر: عبدالغفار الديواني، القرن السيبراني:الردع الالكتروني بين المنع والانتقام، متاح على الموقع:www.futureuae.com

(1) جمال سند السويدي، مصدر سبق ذكره،ص92.

(2) يوسف بورغرارة، مصدر سبق ذكره،ص109-110.

(3) عبد الخالق صالح عبد الله معزب، الإطار القانوني للمُعاملات الألكترونية في التجارية الدولية: دراسة قانونية وفقاً للإتفاقيات الدولية المُتعلقة بالقانون التجاري الدولي، برلين-المانيا، ط1،المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والإقتصادية ،2019،ص102.

(4) صورية بورباية،التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية،المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والأمنية، برلين- المانيا، العدد1، حزيران-2019،ص89.

الدول[1].وبعد أن تفشت عمليات إستخدام الإنترنت لمقاصد إرهابية، وهو مايتطلب على الدول أخذ زمام المُبادرة لمُكافحةالظاهرة بالتعاون، وكونها عابرة للحدود، تتطلب تكاتف الجهود لمُكافحتها وفق نظام عابر للحدود[2].

إن موضوع التعاون الدولي لمُكافحة الجرائم السيبرانية يأخُذ شكلين: الأول: يتعلق بالتعاون في عملية تنفيذ القانون في المُلاحقات والمُتابعات وإصدار العقوبات بحق المُجرمين. فضلاً عن عمليات تبادل المعلومات البيانات بين الدول. والثاني: يتعلق بالتعاون الدولي في الجوانب ذات الطابع التكنولوجي الفني، بما في ذلك المُساعدات التكنولوجية وعمليات تبادل الخبرات والتدريب والمهارات[3].

وقد حظي موضوع "الجريمة الألكترونية" و"الارهاب السيبراني" بإهتمام المُجتمع الدولي، لما له من نتائج كبيرة تضر بأمن وإقتصاد الدول. وتم تنظيم العديد من المؤتمرات الدولية، وإقرار العديد من الإتفاقيات الدولية التي تتعلق بمُكافحة الجرائم السيبرانية، مثل المؤتمر الخامس عشر لقانون العقوبات بشأن جرائم الكومبيوتر الذي عُقد في مدينة ريودي جانيرو البرازيلية وتم تبنيه من قبل مُنظمة الأُمم المتحدة. وايضاً القرار الذي صدر عن مؤتمر الأمم المتحدة بشأن الجرائم ذات الصلة بالحاسوب الذي عقد في مدينة هافانا عام 1995، وإتفاقية بودابست المُتعلقة "بالجرائم الألكترونية"[4]. وقد اصدر مجلس اوربا إتفاقية تتعلق بمُكافحة "الجرائم السيبرانية" عام2001، تضمنت التنسيق بين قوانين الدول الوطنية التي تتصدى للجرائم السيبرانية، للكشف عن هذه الجرائم ومُتابعتها، وعمليات التحقيق فيها والمُلاحقة القضائية لها[5].

أكد الأمين العام السابق للأُمم المتحدة بان كيمون:"إن الأنترنت هو المثال الأهم لكيفية عمل الإرهابيين بطريقة عابرة للحدود الوطنية،ولذلك فإن الدول تحتاج أن تعمل وتفكر بطريقة مُتناسقة"[6]. وفي تقرير الأمم المتحدة عام 2012 بعنوان:"إستخدام الأنترنت لأغراض إرهابية" والصادر عن مكتبها المعني بالمُخدرات والجريمة أكد: على اهمية التعاون الدولي والإقليمي والوطني وبكافة المُستويات الرسمية وغير الرسمية لمُكافحة "الارهاب السيبراني"[7].

---

(1) المختار لمجيدري،مصدر سبق ذكره،ص–ص266–267.

(2) مكتب الأمم المتحدة المعني بالمُخدرات والجريمة، مصدر سبق ذكره،ص15.

(3) صورية بوربابة، مصدر سبق ذكره،ص–ص95–97.

(4) عبد الخالق صالح عبدالله معزب،مصدر سبق ذكره،101.

(5) مكتب الأمم المتحدة المعني بالمُخدرات والجريمة، مصدر سبق ذكره،ص20.

(6) نقلاً عن: منى الأشقر جبور، مصدر سبق ذكره،ص94.

(7) نقلاًعن: المصدر نفسه،ص94.

كما دعا مجلس الأمن لضرورة زيادة التعاون الدولي، لمُكافحة إستخدام الأنترنت لأغراض إرهابية[1].

أتجهت العديد من الدول لتبني إستراتيجية دولية تؤمن "الفضاء السيبراني" بالتعاون، ومنها:"مُبادرة الشراكة الدولية المُتعددة الأطراف لمُكافحة الإرهاب السيبراني" International Multilateral Partnership Initiative to combat cyber terrorism وتهدف لحشد الطاقات الدولية في هذا المجال، كما اكدت المُبادرة اهمية التعاون في مجال المهارات والتدريب والخبرات. وتم إنشاء مواقع على الأنترنت تُكافح "الارهاب السيبراني"، والتي مثلت نقطة إلتقاء للسياسيين وخبراء المعلومات من مُختلف الدول، للتفاهم حول موضوع "الارهاب السيبراني" وكيفية مُكافحته.مثل مجموعة SITE Intelligence Group للإستخبارات وهي جهاز لرصد الإرهاب الألكتروني بإنواعه[2].

هناك جانب مُهم من الإجراءات والتدابير، التي تهدف للتصدي ومُكافحة "التطرف السيبراني"[3]، إذ في عام 2017 استضافت المانيا قمة العشرين في مدينة هامبورغ، للتعاون في مُكافحة تمويل الإرهاب والدعاية له، واكدت الدول حرصها على التصدي للإرهاب ودعاياته بأنواعها. واشارت المُسشارة الألمانية "أنجلينا ميركيل":" إن الدول المُجتمعة أتفقت على زيادة التعاون لجهود مُكافحة الإرهاب، وزيادة الإجراءات للتصدي لدعايات الإرهاب عبر الأنترنت ومُكافحة التطرُف [4]. فيما قامت العديد من دول العالم ومنها دول الخليج العربي، بتكوين فرق أمنية لمُلاحقة وغلق المواقع المُتطرفة ومنها مواقع تنظيم "داعش" الارهابي على برامج التواصل الإجتماعي[5]. وصرحت شرِكات برامج التواصل الإجتماعي الرئيسة: فيس بوك وتويتر ويوتوب: "أنها تعمل على ضرورة توحيد الجهود بالتنسيق مع الدول، لحذف كل المواد المُتطرفة من مواقعها"[6]. كما اشار "مُلتقى مُغردون" الذي عُقد في الرياض في 21 آيار 2017 إلى أهمية أهمية تكوين حُلفاء رقميين سيبرانيين لمُكافحة التطرُف[7].

(1) نايف احمد ضاحي الشمري و عمر عباس خضير العُبيدي،مصدر سبق ذكره،ص77.

(2) غريب حكيم،مصدر سبق ذكره،ص116-117.

(3) نايف احمد ضاحي الشمري و عمر عباس خضير العُبيدي،مصدر سبق ذكره،ص77.

(4) نقلاً عن: صادق علي حسن، مصدر سبق ذكره، ص145.

(5) عبدالله بن ناصر الحمود، رؤية نقدية لمُخاطبة الآخر:إستراتيجية النقاط السبع لإتصال خليجي فعال عربياً وعالمياً، مجلة آراء حول الخليج، مركز الخليج للأبحاث،جدة-المملكة العربية السعودية، العدد17، آذار-2017،ص22.

(6) نقلا عن: حنان خرباش، دور شبكات التواصل الإجتماعي في تشكيل الوعي بالظاهرة الإرهابية، مجلة إتجاهات سياسية، المركز الديمقراطي العربي، برلين- المانيا، العدد3، كانون الثاني-2018، ص143.

(7) المصدر نفسه، ص144.

من خلال هذا المحور يتبين بأن "الهجمات السيبرانية" الإرهابية، ظهرت نتيجة للتطور التكنولوجي في مجال الكومبيوتر واستخدام الانترنت، وهي نوع جديد من أنواع التهديد للدول والمجتمعات والافراد، تستهدف تدمير البنى التحتية للبيانات والمعلومات."فالارهاب السيبراني" ذات كلفة تدميرية للدول والافراد تفوق كلفة الإرهاب التقليدي. كما انه مُتخفي ومن الصعوبة التعرف على من يقوم به. ويضاف إلى ذلك استغلال المجاميع الإرهابية هذا التطور التكنولوجي الكبير لتجعل هذا الفضاء في خدمة اهدافها الارهابية. وهذا ماجعل "الارهاب السيبراني" يُشكل ازمة عالمية جديدة، تُهدد الدول والمُجتمعات، مما دفع الدول لإصدار تشريعات وإتخاذ اجراءات تُكافح هذا الارهاب الجديد، على الصعيد الوطني، وايضاً التعاون الدولي في انفاذ القوانين والمُلاحقة القضائية والعقوبات وتبادل المعلومات وتبادل الخبرات والمساعدات التكنولوجية من خلال إتفاقيات وشراكات دولية. فضلاً عن التعاون في عمليات مُكافحة "التطرُف السيبراني".

الخاتمة:

ومن خلال الدراسة تبين بأن "الفضاء السيبراني"، هو ذلك المدى المفتوح لجميع الأفراد في المجتمعات، الذين لهم قدرة الدخول لشبكة الأنترنت، الذي يُتيح الحصول على المعلومات والتواصل وإجراء اتصالات. وإن "الارهاب السيبراني" ارتبط بمصطلح "الفضاء السيبراني"، نتيجة للتوسع في الإعتماد على الإتصالات والمعلومات في تسيير الشؤون الحياتية.

نتيجة للتطورات التكنولوجية في مجال الإتصال والمعلومات وزيادة الاعتماد عليها، اضحى الانترنت بمثابة ساحة جديدة للهجمات السيبرانية، هذه الهجمات من الصعب معرفة هوية من يقوم بها. وأصبح بإمكان أجهزة الحاسوب أن تحدث أضراراً كبيرة في البنى التحتية للدول، بشكل لاتستطيع الجيوش العسكرية إحداثه. واضحى "الفضاء السيبراني" مجالاً لظهور أنواع جديدة من الإرهاب، وهو إرهاب غير تقليدي،هدفه القيام بعمليات هجومية لتدمير البنى التحتية للمعلومات والبيانات لُيحدث نتائج خطيرة سواء بواسطة تدمير المواقع أو عمليات القصف والنسف بهجوم فايروسات، ممايُنتج مخاطر سياسية واقتصادية وأمنية، لتُشكل أزمة وتهديد عالمي جديد. وأن اهداف الارهاب السيبراني تتخطى الجانب العسكري لتصل إلى البنى التحتية المدنية والعسكرية الحساسة للدول المُستهدفة. ويمتاز "الارهاب السيبراني" بإنخفاض تكلُفته المادية مُقارنة مع التكلُفة العالية للأسلحة التقليدية، فضلاً عن المخاطر التشغيلية، كما يمتاز ايضاً بالسُرعة والمُرونة والمُراوغة. حيث اصبح في العصر الحديث إرتباط كبير بين مواقع شبكة الإنترنت وبين إنتشار المخاطر الأمنية، مثل التطرف والإرهاب. إذ يوفر الأنترنت منبراً مُهماً يظهر الإرهاب بواسطته

في ترويع المُجتمع. ويتم استخدام الأنترنت من قبل المجاميع الإرهابية وانصارها، لتحقيق أغراض عِدة منها:الإتصال والتدريب والجانب العملياتي والدعاية والتجنيد.

نتيجة لمخاطر "الهجمات السيبرانية" الارهابية، وتهديدها الكبير وتشكيلها أزمة للأمن العالمي، حيث إنتشر اهتمام الدول بـ"الأمن السيبراني"، وتوضح ذلك من خلال تبني سياسات أمنية عديدة، من أجل تأمين أنظمة المعلومات من المخاطر التي تُهدد الأمن الإقتصادي والأمن الوطني والدولي. وقامت الدول بإصدار قواعد تشريعية حديثة لمُكافحة هذه التهديدات، وفق منظور وطني جديد للأمن. ومن ثُم إتجاه الدول للتعاون الدولي، الذي يقوم على اساس عقد إتفاقيات للتعاون في "الأمن السيبراني"، والتنسيق في مجالات التشريعات والمُلاحقات والمُحاكمات، وتبادل المعلومات والخبرات والمهارات التكنولوجية والفنية فضلاً عن الإتفاق للتصدي "للتطرُف السيبراني".