مجلة الباحث للدراسات الأكاديمية
ISSN: 2352-975X ELBAHITH for Academic Studies EISSN: 2588-2368
المجلد: 08 / العدد: 01 / السنة: 2021 / ص ص: 27- 45

الجهود الدولية في مكافحة الإرهاب الإلكتروني

International efforts to combat cyber terrorism

تاريخ الإرسال: 2020/09/28 تاريخ القبول: 2021/01/05

ناصر العلي*
معهد الحقوق - جامعة روسيا للنقل
موسكو- روسيا
1042051@edu.rut-miit.ru

ملخص:

ساهم تطور تكنولوجيا الاتصالات والمعلومات الذي يشهده العالم اليوم في ظهور شكل جديد للإرهاب والمعروف بإسم "الارهاب الإلكتروني" والذي أصبح يشكل خطرا كبيرا ليس فقط على الأمن والسلم الدوليين بل وعلى الأمن القومي للدول، حيثُ أصبحت البنية التحتية لأغلب الدول تدار عن طريق أجهزة الكمبيوتر والإنترنت، مما يعرضها لهجمات متعددة من قبل الإرهابيين . تلك الهجمات التي تستطيع إلحاق الضرر بخدمات عامة مثل شبكات الكهرباء والمياه، وأيضاً بالنظام المالي للدول، وإعاقة حركة الملاحة الجوية أو البحرية، وعلى المنشآت العسكرية، وأن تتسبب في قتل الأبرياء وفي خسائر مادية ومعنوية هائلة.

تكمن مشكلة البحث في مدى فعالية التعاون الدولي في مكافحة الإرهاب الإلكتروني ومدى فعالية الاتفاقيات الدولية والآليات الدولية في محاربته.

والهدف من هذه البحث إلقاء الضوء على أهمّ المعاهدات الدولية والآليات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني وإيجاد أرضية مشتركة لصياغة منظومة قوانين وتشريعات دولية وآليات ووسائل فعالة تتصدى لجذور وامتدادات الظاهرة الإرهابية في الفضاء الإلكتروني.

تم اتباع المنهج الوصفي والمنهج الاستقرائي والمنهج التحليلي، وذلك من خلال استعراض وتحليل واستقراء الاراء الفقهية والاتفاقيات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني.

الكلمات المفتاحية: الإرهاب الإلكتروني؛ جرائم إلكترونية؛ الأمم المتحدة؛ روسيا الاتحادية.

Abstract:

The development of communication and information technology in the modern world has contributed to the emergence of a new form of terrorism - "cyber terrorism". Numerous attacks by cyber terrorists have become a

*- المُؤَلف المُراسل.

serious threat to both international peace and security and the national security of countries. Cyber attacks can damage public services such as electricity and water networks, the financial system of states, military installations, obstruct air or sea traffic, lead to the death of innocent people, and cause enormous material and moral damage.

The paper examines the effectiveness of international cooperation in the fight against cyber terrorism and the effectiveness of international conventions and mechanisms to combat it.

The purpose of the study is to highlight the most important international treaties and mechanisms to combat cyber terrorism and find a common basis for the development of a system of international law and legislation, as well as effective mechanisms and means to address the root causes of terrorism in cyberspace.

The descriptive approach, the inductive method and the analytical approach used in the work are accompanied by a review, analysis and extrapolation of doctrinal opinions and international conventions related to the fight against cyber terrorism.

Keywords: *Cyber terrorism; cybercrime; United Nations; Russian Federation.*

مقدمة:

تعد جريمة الإرهاب الإلكتروني من الجرائم المعلوماتية المعاصرة والعابرة للحدود والتي ظهرت مؤخرا مع انتشار تكنولوجيا المعلومات وأصبحت أداة هذه الجريمة تتمثل في وجود شبكة الانترنت. تثير هذه الجريمة العديد من الإشكاليات من مختلف النواحي كصعوبة اكتشافها أو إثباتها لا سيما وأنها تتسم بطابع الحيلة والدهاء من قبل مرتكبيها من خلال استخدام تقنيات معلوماتية عالية الكفاءة مما يؤدي إلى اختراق الشبكات وأجهزة الكمبيوتر المرتبطة بالأنترنت حيث أصبح يشكل خطرا كبيرا ليس فقط على الأمن والسلم الدوليين بل وعلى الأمن القومي للدول، حيثُ أصبحت البنية التحتية لأغلب الدول تدار عن طريق أجهزة الكمبيوتر والإنترنت، مما يعرضها لهجمات متعددة من قبل الإرهابيين .

ارتبط الاهتمام بالإرهاب الإلكتروني بظهور الاعتداءات والجرائم الإلكترونية، وما يمكن أن تتسبب به من كوارث، في حال استهدافها المصالح الحيوية للدول. فالإعتداءات على الأنظمة التي تدير الطاقة والمياه، والصحة، والدفاع، والنقل، وغيرها، ذات تأثير مباشر وأكيد، على السلامة العامة، حيث يمكنها أن تثير

الذعر، وتخلق جواً من الهلع، وتعرض حياة الناس للمخاطر، في جميع البلدان، دون استثناء.

بالنظر لخطورة الإرهاب الإلكتروني وصعوبة الكشف عنه وغياب الدليل المادي الذي يدين مرتكبيه فإنه أصبح اليوم يطغي على ساحة الإجرام نتيجة لغياب استراتيجية دولية فعالة لمحاربته والتقليل منه خاصة في ظل غياب الاتفاقيات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني وغياب الآليات الدولية وحتى غياب أو صعوبة التعاون الدولي في هذا المجال.

وفي ضوء ما تقدم تكمن مشكلة البحث في ما يلي: **ما مدى فعالية التعاون الدولي في مكافحة الإرهاب الإلكتروني وما مدى فعالية الاتفاقيات الدولية والآليات الدولية في محاربته؟**

تبرز أهمية دراسة الإرهاب الإلكتروني في أنه أصبح يشكل خطورة كبيرة على الأمن والسلم الدوليين. كما تستمد هذه الدراسة اهميتها في توعية الأفراد من كافة المجتمعات في الوسائل والطرق التي تلجأ اليها التنظيمات الإرهابية لغايات استقطاب وتجنيد هؤلاء الأفراد. كما تتجلى أهميتها في القاء الضوء على التعاون الدولي في مكافحة هذه الظاهرة الخطيرة.

يهدف البحث إلى إلقاء الضوء على أهمّ الإتفاقيات الدولية والآليات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني وكذا إيجاد أرضية مشتركة لصياغة منظومة قوانين وتشريعات دولية، وآليات ووسائل فعالة تتصدى لجذور وامتدادات الظاهرة الإرهابية في الفضاء الإلكتروني .

تم اتباع المنهج الوصفي والمنهج الاستقرائي والمنهج التحليلي، وذلك من خلال استعراض وتحليل واستقراء الآراء الفقهية والاتفاقيات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني.

سيتم معالجة هذا الموضوع على اساس تقسيمه إلى محورين، يتناول المحور الأول الإرهاب الإلكتروني في المواثيق الدولية ومفهوم الإرهاب الإلكتروني وخصائصه، أما المحور الثاني فيتصدى للكشف عن التعاون الدولي في مكافحة الإرهاب الإلكتروني عبر التركيز على منظمة الأمم المتحدة وجهود ودور المنظمات الإقليمية

(الأوربية والعربية) في مكافحة الإرهاب الإلكتروني . ثم خاتمة تضمنت أهم النتائج والتوصيات التي تم التوصل اليها في ضوء معطيات البحث.

المحور الأول: الإرهاب الإلكتروني في المواثيق الدولية:

أولا- مفهوم الإرهاب الإلكتروني:

يتكون مصطلح (Cyber Terrorism) من اندماج كلمتين: "Cyber" ("الفضاء الإلكتروني") و"Terrorism" "الإرهاب". وأول محاولة لظهور هذا المصطلح كانت عام 1997 من قبل موظف مكتب التحقيقات الفدرالي الأمريكي T. Pollitt

الإرهاب الإلكتروني هو استخدام أجهزة الكمبيوتر كسلاح أو هدف للهجوم من قبل مجموعات دولية أو مجموعات عرقية أو عملاء سريين ذات دوافع سياسية، يهددون أو يتسببون في العنف ويغرسون الخوف من أجل التأثير أو إجبار الحكومة على تغيير سياساتها[1].

وعرفته "دينينج دوروثي" على أنه "التقاء الارهاب وعالم الكمبيوتر وأنه الاستخدام غير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر والشبكات والمعلومات المختزنة فيها من أجل ترويع واكراه الحكومات وشعوبها من أجل تحقيق أهداف سياسية واجتماعية، ولكى يعتبر ذلك ارهاب لابد أن يؤدى إلى ترويع واكراه الحكومات والأشخاص والممتلكات أو على الأقل التسبب فى الضرر والخوف، وكذلك احداث ضحايا وايذاء بدنى وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية واعاقة عمل الخدمات الأساسية"[2].

ويعرف الأستاذ "جابريل ويمان"، أحد الباحثين في مجال مكافحة الإرهاب الإلكتروني، أنه "استخدام أدوات الشبكات الحاسوبية لتدمير أو إغلاق البنية التحتية الوطنية (على سبيل المثال، الطاقة، النقل، العمليات الحكومية، إلخ.) [3].

عرف الصليب الأحمر الإرهاب الإلكتروني على أنه " عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف إلى تحقيق اغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير أو تغيير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الاهداف في العالم الحقيقي كالصناعات والبنى الاساسية"[4].

وعرفه الدكتور هشام بشير على انه " نشاط هجومى متعمد ذو دوافع سياسية بغرض التأثير علي القرارات الحكومية أو الرأي العام باستخدام الحاسبات ووسائل الاتصال للتأثير على إنتاج ومعالجة وتخزين المعلومات أو تعطيل خدمات لينتج عنه ترويع وتخويف وتدمير للبنية التحتية الحيوية"[5].

وقد عرّفت الأمم المتحدة في تشرين الأول/ أكتوبر 2012 الإرهاب الإلكتروني بأنه "استخدام الانترنت لنشر أعمال إرهابية".

لقد تعددت تعاريف الإرهاب الإلكتروني واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي إلى تعريف جامع مانع متفق عليه للإرهاب بشكل عام ولا تعريف للإرهاب الإلكتروني بشكل خاص.

يتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

فهذا النوع من الإرهاب أصبح يشكل خطرا يهدد العالم بأسره، إن خطورة الإرهاب الإلكتروني تزداد يوما بعد يوم لأن البنية التحتية في كثير من الدول أصبحت تدار بالحاسوب وشبكات الاتصال، مما يجعلها هدفا سهل المنال وتحقق آثار تدميرية كبيرة .

لقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي قد تلحق أضرارا جسيمة بالأفراد والمنظمات والدول[6].

إن من أبرز الإشكاليات التي تواجه طرق معالجة ظاهرة الإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص هو تأخر المجتمع الدولي حتى الآن في الوصول إلى تعريف واضح محدد لمعنى الإرهاب، مما فتح المجال لاجتهادات واسعة غير موفقة أُضطهدت بسببها الشعوب، وأُنتهكت الحقوق، وخرقت المعاهدات الدولية تحت ستار

دعوى مكافحة الإرهاب. فالقانون الدولي إلى غاية الان لم يعطِ تعريفاً واضحاً، ومنهجاً معيناً للتعامل مع هذا النوع الجديد من الإرهاب.

إن السبب الحقيقي الكامن وراء عدم وضع تعريف محدد ومتفق عليه، يرجع إلى الاختلاف والتباين الشديدين في وجهات النظر والإرادات السياسية تبعا لاختلاف الأيدولوجيات والمصالح.

ثانيا- المعاهدات والقرارات الدولية الخاصة بالإرهاب الإلكتروني:

التعاون الدولي للدول في مجال مكافحة الإرهاب الإلكتروني لم يتم تنظيمه بعد على المستوى العالمي. وينظر له وكأنه ظاهرة تهدد فقط الأمن المعلوماتي. وكثير من الهجمات على المواقع الإلكترونية لا يمكن أن تقع بشكل رسمي تحت التأثير المحظور للاتفاقيات العالمية الحالية المناهضة للإرهاب، وهي لا تنشئ التزامات دولية على الدول للتصدي لها بشكل مشترك.

اعتمدت الأمم المتحدة على مستوى الجمعية العامة ومجلس الأمن عدة قرارات دولية مخصصا للإرهاب بشكل عام، ولا يوجد أي قرار منفصل حول الإرهاب الإلكتروني. وفي عام 2006 اعتمدت الجمعية العامة للأمم المتحدة قرارا بعنوان "استراتيجية الأمم المتحدة لمكافحة الإرهاب " تشير الفقرة (1) من المادة 12 إلى "تنسيق الجهود على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت؛ (ب) استخدام الإنترنت كأداة لمكافحة انتشار الإرهاب، مع الاعتراف بأن الدول قد تحتاج إلى المساعدة في هذا الصدد[7].

في عام 2011، اقترحت روسيا مشروع اتفاقية بشأن أمن المعلومات الدولية، ولكن للأسف لم يتم اعتماده بعد. تضمن الفصل الثالث من هذا المشروع التدابير الأساسية لمواجة استخدام الفضاء المعلوماتي للأغراض إرهابية وحسب المادة 8 تدرك الدول الأطراف إمكانية استخدام الفضاء المعلوماتي لتنفيذ الأنشطة الإرهابية، أما المادة 9 تنص على التدابير الأساسية للتصدي لاستخدام الفضاء المعلوماتي للأغراض الإرهابية ومن هذه التدابير:

-اتخاذ تدابير لمواجهة استخدام الفضاء المعلوماتي للأغراض إرهابية والاعتراف بالحاجة إلى اتخاذ إجراء مشترك وحاسم ؛ العمل على وضع نهج مشترك لإنهاء تشغيل موارد الإنترنت ذات الطبيعة الإرهابية؛

-الحاجة لإقامة وتوسيع تبادل المعلومات بشأن التهديدات بارتكاب هجمات الكمبيوتر، وعن العلامات والحقائق والأساليب ووسائل استخدام الإنترنت لأغراض إرهابية، حول تطلعات المنظمات الإرهابية وأنشطتها في الفضاء المعلوماتي، وكذلك تبادل الخبرات وأفضل الممارسات في رصد موارد المعلومات على شبكة الإنترنت، والبحث عن ومراقبة محتوى المواقع الإرهابية؛

-اعتماد تدابير تشريعية وغيرها من التدابير لتمكين السلطات المختصة تنفيذ إجراءات تحقيقية وغيرها من الإجراءات الرامية إلى منع وقمع وإزالة الآثار المترتبة على القيام بأنشطة إرهابية في الفضاء المعلوماتي، وكذلك معاقبة الجناة والمنظمات؛

-اتخاذ التدابير التشريعية وغيرها من التدابير اللازمة التي تكفل بشكل قانوني الوصول إلى أراضي الدولة الطرف إلى أجزاء معينة من البنية التحتية للمعلومات والاتصالات شريطة وجود سبب شرعي للاعتقاد بأنها تُستخدم للقيام بأنشطة إرهابية في الفضاء المعلوماتي أو تيسير أنشطة المنظمات الإرهابية أو الجماعات الإرهابية أو الأفراد الإرهابيين[8].

عرف مشروع هذه الاتفاقية الارهاب المعلوماتي على انه استخدام موارد المعلومات و/ أو التأثير عليها في الفضاء المعلوماتي للأغراض الإرهابية وهذا التعريف مأخوذ من اتفاقية بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات على الصعيد الدولي لعام 2009.

ويتم التعاون بين الدول في مجال مكافحة الإرهاب الإلكتروني بشكل رئيسي على المستوى الإقليمي، وتحت رعاية مجلس أوروبا اعتمدت اتفاقية بودابست اتفاقية الجرائم الإلكترونية 2001، انضمت 54 دولة إلى الاتفاقية، بما في ذلك الولايات المتحدة وبريطانيا .

وقامت الاتفاقية بتدوين وتنظيم الجرائم في الفضاء الإلكتروني، بما في ذلك التزوير باستخدام تكنولوجيات الحاسوب؛ الاحتيال باستخدام تكنولوجيا

الكمبيوتر. الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية؛ الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.

نلاحظ من ذلك الاتفاقية لم تدون جريمة الإرهاب الإلكتروني.

في عام 2009 تحت رعاية منظمة شنغهاي للتعاون تم اعتماد اتفاقية بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات على الصعيد الدولي.

عرفت هذه الاتفاقية الارهاب المعلوماتي على انه استخدام موارد المعلومات و/ أو التأثير عليها في الفضاء المعلوماتي للأغراض الإرهابية. ويشير الملحق الثاني لهذه الاتفاقية على أن مصدر هذا التهديد هو المنظمات الإرهابية والأشخاص المتورطين في أنشطة إرهابية، ويقومون بأنشطة غير مشروعة عن طريق موارد المعلومات أو فيما يتعلق بها.

تنص المادة: 02 على التهديدات الرئيسية في مجال أمن المعلومات الدولي ومن إحدى هذه التهديدات الإرهاب المعلوماتي. حددت المادة 3 من هذه الاتفاقية المجالات الرئيسية للتعاون ومن احدى هذه المجالات التصدي للتهديدات باستخدام تكنولوجيا المعلومات والاتصالات لأغراض إرهابية[9].

المعاهدة الدولية الوحيدة ذات الطابع الإقليمي التي تتناول جزئياً قضايا مكافحة الإرهاب الإلكتروني هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في 21 ديسمبر 2010. تسرد المادة 15 الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات[10].

نستنتج من ذلك ان الجرائم المنصوص عليها في المادة 15 من إحدى وسائل ارتكابها هي وسيلة تقنية المعلومات . إن هذه الاتفاقية لا تحتوي على احكام تهدف إلى مواءمة

القانون الجنائي للدول الأطراف في هذه الاتفاقية والتي تنص على المسؤولية عن الأفعال غير المشروعة التي ترتكب لأغراض إرهابية ضد شبكات المعلومات والاتصالات أو شبكات الكمبيوتر أو الأنظمة لتي تتسبب في عواقب وخيمة كالحاق أضرار في الممتلكات، الأضرار في حياة وصحة الناس أو الكشف عن أسرار الدولة.

ومن إحدى نواقص هذه الاتفاقية أنها لم تنص على إنشاء آلية أو مركز عربي اقليمي لمكافحة الإرهاب الإلكتروني.

في عام 2013 تم اعتماد اتفاقية تعاون الدول الأعضاء في الكومنولث الدول المستقلة في مجال أمن المعلومات. والغرض من هذه الاتفاقية هو القيام بأعمال مشتركة ومنسقة تهدف إلى ضمان أمن المعلومات في الدول - الأطراف في هذا الاتفاق. ان هذه الاتفاقية لم تحتوي على نص صريح عن جريمة الإرهاب الإلكتورني سوى المادة الثانية التي عرفت الإرهاب المعلوماتي - استخدام موارد المعلومات و/أو التأثير عليها في الفضاء المعلوماتي للأغراض الإرهابية[11].

في عام 2012 تم إبرام وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون الخليجي، وقد نصت المادة 29 على ضرورة معاقبة من يقوم بإنشاء مواقع إلكترونية أو نشر معلومات عن طريق الشبكة الإلكترونية أو إحدى وسائل تقنية المعلومات، من أجل تسهيل الاتصالات بين أعضاء جماعة إرهابية، أو بقصد ترويج أفكارها أو تمويلها، أو نشر كيفية صناعة الأجهزة الحارقة أو المتفجرة، أو أية أدوات أخرى يمكن استخدامها في أعمال إرهابية[12].

في عام 1999 اعتمد مجلس الأمن الدولي قرار 1269 والذي دعى فيه جميع الدول إلى التنفيذ الكامل للاتفاقيات الدولية الخاصة بمكافحة الإرهاب والانضمام الدول إلى تلك الاتفاقيات التي ليست أطرافًا فيها. كما يقترح في أقرب وقت ممكن اعتماد المزيد من الاتفاقيات التي لم يتم تبنيها بعد، ولا سيما فيما يتعلق في قضايا الإرهاب الإلكتروني[13].

وفي 20 ابريل عام 2018 في اطار الجمعية العامة تم اعتماد قرار" أنشطة منظومة الأمم المتحدة في مجال تنفيذ استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب" .

EISSN: 2588-2368 _____ ISSN: 2352-975X

ويوجز هذا القرار الاتجاهات والتحديات الرئيسية في المشهد العالمي المتطور للإرهاب ويتضمن هذا القرار التهديدات والتحديات الناشئة: شن هجمات باستخدام الذكاء الاصطناعي والطائرات بدون طيار أوالهجمات الإلكترونية، ويشدد على أهمية التعاون الدولي في مكافحة الإرهاب بشكل فعال. ويقدم التقرير لمحة عامة عن الجهود الدولية للتصدي للخطر العابر للحدود الوطنية الذي ينطوي عليه الإرهاب وبعض أوجه القصور الرئيسية التي ما زال يتعين معالجتها في المستقبل القريب، ويختتم القرار بتقديم ملاحظات وتوصيات بشأن طرائق إقامة شراكات دولية جديدة في مجال مكافحة الإرهاب، ستكون ذات أهمية أساسية لمواكبة التهديد الذي تشكله الجماعات الإرهابية[14].

إن مواجهة الإرهاب الإلكتروني، لا يمكن أن تتم إلا بتعزيز الإطار القانوني والتشريعي على جميع المستويات الوطنية الإقليمية والعالمية، عبر إصدار قوانين وطنية خاصة في مكافحة الإرهاب على الإنترنت وتجريمه، وإرساء قواعد تعاون فعالة وحقيقية على المستويات الوطنية بين مختلف الإدارات، وعلى المستوى الإقليمي والدولي، من أجل مكافحة الإرهاب الإلكتروني، من الضروري تكثيف التعاون الدولي من خلال سن اتفاق دولي لضمان الاستخدام السلمي للفضاء السيبراني ومن اجل التعاون بين الدول في مكافحة الإرهاب الإلكتروني، ووضع إطار قانوني مناسب، وتجريم الإرهاب الإلكتروني، وإيجاد نهج متكامل لضمان الأمن في مكافحة الإرهاب إلكتروني.

المحور الثاني: التعاون الدولي في مكافحة الإرهاب الإلكتروني:

أولا- الجهود الدولية والإقليمية في مكافحة الإرهاب الإلكتروني:

1- دور الأمم المتحدة في مكافحة الإرهاب الإلكتروني: تشكل مكافحة الإرهاب جزءًا لا يتجزأ من ولاية الأمم المتحدة التي يجعل ميثاقها من صون السلم والأمن الدوليين مقصداً رئيساً، ويوجب إتخاذ تدابير جماعية لمنع التهديدات للسلام ولقمع العدوان وتعزيز حقوق الإنسان والتنمية الاقتصادية، ليظهر الإرهاب ضمن هذا المنحى بوصفه انتهاكاً وتهديدا لشروط ومقتضيات اشاعة الأمن والسلم الدوليين، فضلا عن

انتهاكه الواضح لحقوق الإنسان، والتسوية السلمية للمنازعات، التي حرص الميثاق الأممي على تكريسها وتأمينها.

أصدرت الأمم المتحدة مجموعة من القرارات عبر جمعيتها العامة التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات وخطورة استخدامها الغير سلمي، ففي 22 نوفمبر 2002 اتخذت قرار بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس السنة اتخذت قرار إرساء ثقافة عالمية لأمن الفضاء الالكتروني.

اعتمدت الدول الأعضاء في 8 أيلول/سبتمبر 2006 استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. وهذه الاستراتيجية بمثابة قرار وخطة عمل في نفس الوقت. وهذه هي المرة الأولى التي اتفقت فيها الدول الأعضاء جميعها على نهج استراتيجي موحد لمكافحة الإرهاب بجميع أشكاله وأنواعه. وتنص هذه الاستراتيجية على اتخاذ خطوات عملية فرديا وجماعيا لمنعه ومكافحته. وتلك الخطوات العملية تشمل طائفة واسعة من التدابير التي تتراوح من تعزيز قدرة الدول على مكافحة التهديدات الإرهابية إلى تحسين تنسيق أنشطة منظومة الأمم المتحدة في مجال مكافحة الإرهاب[15].

أنشئ في اطار الأمم المتحدة مكتب فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، اكتسبت مكتب فرقة العمل طابعا مؤسسيا في إدارة الشؤون السياسية التابعة للأمم المتحدة في ديسمبر 2009 عبر قرار الجمعية العامة A/RES/64/235 . وفي سبتمبر 2011 أنشئ مركز الأمم المتحدة الدولي لمكافحة الإرهاب من أجل تعزيز التعاون الدولي لمكافحة الإرهاب ودعم الدول الأعضاء في تنفيذ الاستراتيجية العالمية لمكافحة الإرهاب.

اعتمدت الجمعية العامة القرار 291/71 والمؤرخ في 15 يونيه عام 2017 بإنشاء مكتب الأمم المتحدة لمكافحة الإرهاب. وكما اقترح الأمين العام أنطونيو غوتيريس في تقريره (A/71/858) بإنشاء مكتب جديد لمكافحة الإرهاب برئاسة وكيل للأمين العام.

أما بالنسبة لدور مجلس الأمن في مكافحة الإرهاب فإنه يقع على عاتقه التزام حسب المهام المخوله له في الميثاق أن يتخذ كل ما في وسعه لمكافحة الإرهاب الدولي بجميع اشكاله وانواعه.

صدر عن مجلس الأمن عدة قرارت حول مكافحة الإرهاب وأشهر قرار اتخذه مجلس الأمن قرار رقم 1373 والذي نص على جملة من التدابير الملزمة للدول أهمها: التزام جميع الدول بتحريم تقديم المساعدة للأنشطة الإرهابية؛ رفض توفير الدعم المالي للإرهابيين والجماعات الإرهابية؛ عدم توفير ملاذ آمن للإرهابيين والجماعات والتنظيمات الإرهابية؛ ضرورة تبادل المعلومات بشأن الجماعات التي تخطط لشن هجمات إرهابية.

كما أنشئت لجنة تتألف من جميع أعضاء المجلس لتراقب تنفيذ هذا القرار، وطلب من جميع الدول تقديم تقارير لهذه اللجنة عن الخطوات التي اتخذتها لتنفيذ هذا القرار[16].

وبغية تنشيط اللجنة، اتخذ مجلس الأمن القرار1535 في مارس 2004، والذي نص على إنشاء المديرية التنفيذية للجنة مكافحة الإرهاب، بهدف توفير مشورة الخبراء إلى اللجنة في جميع المجالات التي يتناولها القرار 1373، أوكذلك من أجل تقديم المساعدة التنفيذية للبلدان، فضلا عن زيادة توثيق التعاون والتنسيق داخل منظومة مؤسسات الأمم المتحدة وفيما بين الهيئات الإقليمية والحكومية الدولية.

ودعى الأمين العام للأمم المتحدة في المؤتمر المجتمع الدولي والقطاع الخاص والأوساط الأكاديمية على تبادل المعارف والخبرات والموارد بغية «منع التكنولوجيات الجديدة من أن تصبح أسلحة إرهابية فتاكة». وشدد على أهمية دور الشباب في مكافحة الرسائل التي ينشرها الإرهابيون وضرورة إعادة تأهيل المتشددين. وقال: «يتعين أن نشارك النساء في مكافحة الإرهاب، فهن غالباً ما يكنّ سباقات في رصد مؤشرات مبكرة للتشدد بين الشباب أو المستضعفين». وأشار إلى مشاركة منظمات المجتمع المدني في المؤتمر، مؤكداً ضرورة التعلم منها. وأضاف أنه يدرس إنشاء وحدة جديدة في مكتب مكافحة الإرهاب لضمان إدماج رؤى المجتمع المدني بشكل كامل في سياسات وبرامج مكافحة الإرهاب. ورحب بإنشاء المنتدى الدولي للإنترنت

لمكافحة الإرهاب، وغيره من الشراكات المشابهة لمنع نشر محتوى التطرف العنيف على الإنترنت[17].

-2 دور مؤسسات الاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني: في عام 2004، طبقًا للائحة الاتحاد الأوروبي رقم 2004/460، تم إنشاء الشبكة الأوروبية للأمن وأمن المعلومات (ENISA) ومقرها في هيراكليون (كريت). يشمل هيكل ENISA: جهاز الإدارة، مجموعة من الممثلين الدائمين من الدول الأعضاء، ضابط اتصال أو ارتباط عن كل دولة من الدول الأعضاء، بالإضافة إلى مجموعات عمل مؤقتة حول قضايا خاصة محددة. ويشكل موظفو الاتصال في البلدان المشاركة معاً شبكة ضباط الاتصال الوطنيين. وضعت هذه المنظمة عددا من الوثائق الأساسية في مكافحة الإرهاب الإلكتروني، على سبيل المثال، تم وضع دليل تفصيلي خطوة بخطوة لإنشاء مجموعات خاصة بأمن الحواسيب والاستجابة للحوادث، مجموعة عالمية من التدريبات للخدمات للاستجابة للحوادث الحاسوبية، مشروع الاستراتيجية الوطنية للأمن السيبراني داخل الاتحاد الأوروبي.

في تنفيذ هذه الأنشطة، تشارك المنظمات التالية أيضًا في العمل: وكالة الدفاع الأوروبية، ومعهد الاتحاد الأوروبي للدراسات الأمنية ؛ ومركز القمر الصناعي الاتحاد الأوروبي؛ (Europol) يوروبول هي وكالة تطبيق القانون الأوربية، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوربي في مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب؛ (Eurojust) يوروجست تتعاون قضائياً في المسائل الجنائية. مقر اليوروجست في لاهاي بهولندا، الوكالة التنفيذية للتعليم والسمعيات البصرية والثقافة، إلخ.

المعرفة والخبرة المكتسبة من قبل الاتحاد الأوروبي تلعب دور كبير في مكافحة الإرهاب الإلكتروني وفي تحقيق الأمن الدولي العالمي[18].

3- دور جامعة الدول العربية في مكافحة الإرهاب الإلكتروني: بدأت جامعة الدول العربية بالاهتمام في مسألة مكافحة الإرهاب عندما اعتمد مجلس وزراء الداخلية العرب في عام 1997" الاستراتيجية العربية لمكافحة الإرهاب" . وتتجلى مجالات ومقومات هذه الاستراتيجية على سن سياسات وطنية تشمل الوقاية وتحديث التشريعات

EISSN: 2588-2368 _____ ISSN: 2352-975X

وتعزيز البحث العلمي لتوظيف التقنيات الحديثة في العمل الأمني، وتعزيز التعاون العربي-الدولي من خلال المشاركة في المؤتمرات الدولية، المساهمة في وضع مدونة دولية لقواعد سلوك الدول في مكافحة الإرهاب.

وتتضمن هذه الاستراتيجية ثمانية أهداف تمحورت حول حماية الدول والمواطنين والمؤسسات وايضاح الصورة الحقيقية للإسلام وتعزيز وتطوير علاقات التعاون الثنائي والمتعدد الأطارف.

اتفقت الدول العربية في الخطة السادسة لتنفيذ هذه الإستراتيجية والتي امتدت من (2013-2015) على[19]:

1 - متابعة تنفيذ بنود الإستراتيجية لتحقيق مواجه فعالة للإرهاب بكافة أشكاله وصوره؛

2 - تفعيل دور الرقابة على وسائل الإعلام المختلفة وعلى شبكة الأنترنت من قبل المكتب العربي للإعلام الأمني؛

3 - بذل جهود مكثفة لمنع استغلال مواقع التواصل الاجتماعي من قبل الإرهابيين؛

4 - تنص هذه الاستراتيجية على سن تشريع خاص بمكافحة جرائم تقنية المعومات بالنسبة للدول التي لا تمتلك مثل هذا التشريع؛

5 - تنص على المساهمة العربية الفاعلة في الجهود الدولية الرامية لمكافحة الإرهاب التي تقودها منظمة الأمم المتحدة من خلال تنفيذ ما ورد في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب.

وفي اطار الجامعة العربية تم ابرام العديد من الاتفاقيات المتعلقة بالإرهاب ومنها: الاتفاقية العربية لمكافحة الإرهاب عام 1998؛ الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب عام 2010؛ والاتفاقية العربية المتعلقة بالجرائم المعلوماتية عام 2010.

ثانيا- التدابير اللازمة لمكافحة الإرهاب الإلكتروني:

كأساس لمنع وقمع أو القضاء على عواقب الإرهابيين السيبرانيين في الوقت المناسب، يمكن أن نستند إلى اتجاهين رئيسيين:

1 -إجراءات تهدف إلى تدمير البنية الأساسية للشبكة والوصول غير المصرح به إلى المعلومات بدرجة عالية من السرية ؛

-2 الإجراءات التي تسعى إلى احتمال التشويه المتعمد للمعلومات في وسائل الإعلام المنشورة على الإنترنت.

لمواجهة هجمات الإرهابيين على الإنترنت، ينبغي توخي التدابير التالية:

ضرورة إدراج جرائم الإرهاب الدولي في قائمة الجرائم الدولية المنصوص عليها في الفقرة الأولى من المادة الخامسة من النظام الأساسي للمحكمة الجنائية الدولية مع إرجاء ممارسة الاختصاص القضائي في شأنها إلى حين التوصل إلى تعريف وشروط لممارسة هذا الاختصاص يكونا مقبولين من جانب المجتمع الدولي ممثلاً في موافقة ثلثي الدول الأطراف في النظام الأساسي.

من أجل مواجهة الإرهاب الإلكتروني بفاعلية ومثمرة، ينبغي الاعتماد على المعايير الأساسية التالية: اتباع قواعد ومبادئ القانون الدولي؛ الإدانة العالمية والاعتراف بعدم شرعية الإرهاب بجميع مظاهره وايضا الإرهاب الإلكتروني؛ التعاون الدولي وتبادل المعلومات بين الدول حول الظواهر الإرهابية؛ حتمية مسؤولية الإرهابيين السيبرانيين الذين ارتكبوا الجريمة الإرهابية ؛ فعالية إجراءات مكافحة الإرهاب السيبراني.

وأبرزت تهديدات الإرهاب الإلكتروني الحاجة إلى تضافر الجهود الدولية من أجل العمل على تعزيز الأمن والسلم الدوليين والحماية لدور الفضاء الإكتروني. ومن ضمن تلك الجهود: الدعوة إلى إبرام اتفاقية دولية للحد من التسلح داخل الفضاء الإلكتروني مثل تلك الاتفاقيات التي تم إنجازها في مجال الإنتشار النووي والكيماوي والبيولوجي.

من الضروري اعتماد اتفاقية دولية تحدد واجب الدول في تقديم المساعدة القانونية في التحقيق في هذه الجريمة بناء على طلب دولة أخرى على أساس المعاملة بالمثل وبطريقة متسارعة. تحديد المسؤولية الجنائية للإرهاب الإلكتروني كجريمة خطيرة في التشريعات الوطنية وفي الوثائق الدولية. إنشاء جهاز خاص في الدولة لمكافحة الإرهاب الإلكتروني.

سعت العديد من الدول إلى اتخاذ التدابير والإجراءات اللازمة لمواجهة الارهاب الالكتروني. إلا أن هذه الجهود محدودة ومازالت بحاجة إلى المزيد من الدراسات

والبحوث والتشريع والتنظيم لإحتواء هذه الظاهرة الخطيرة ومن بين هذه التدابير والإجراءات التي يجب أن تتخذها الدول لمكافحة الارهاب الالكتروني ما يلي: -

1. اعتماد إطار قانوني مناسب على المستويات الوطنية والإقليمية والعالمية لمكافحة هذه الجريمة. إن تشريعات معظم الدول لا تفرد الإرهاب الإلكتروني كجريمة مستقلة؛
2. رصد أنشطة الجماعات الإرهابية على الشبكات الاجتماعية وتحليل محتواها وأهدافها والاستراتيجيات المعتمدة فيها ؛
3. إيجاد منظومة قانونية دولية تحت مظلة الأمم المتحدة يعهد إليها توثيق وتوحيد جهود الدول والمنظمات الدولية لمكافحة ومواجهة الارهاب الالكتروني؛
4. تعزيز التعاون الدولي والإقليمي من خلال مراقبة كل دولة للأعمال الإجرامية الالكترونية الواقعة على أراضيها ضد دولة أو جهات أخرى خارج هذه الأراضي بمساعدة المنظمات الدولية والهيئات المتخصصة بمكافحة الارهاب الالكتروني؛
5. العمل على تعزيز التعاون بين الدول الأعضاء في ظل احترام تشريعاتها الداخلية والترتيبات والاتفاقيات الدولية من أجل مواجهة ومكافحة الأعمال الإرهابية ومعاقبة مرتكبيها أو تسليمهم إلى بلدانهم الأصلية أو إلى الدولة التي أرتكب فيها العمل الإرهابي طبقاً للاتفاقيات والترتيبات الثنائية وكذلك التعاون بين هذه الدول في مجال تبادل المعلومات ذات الصلة بشأن الإرهابيين وأنشطتهم.

خاتمة:

لقد أصبح الارهاب واقعنا الأليم الذى نعانى منه كأفراد وجماعات ودول، وعلى الرغم من خطورة هذه الظاهرة وانتشارها بشكل هائل الا أنه كان من الصعب الوصول إلى تعريف محدد ودقيق للإرهاب كونه يختلف من دولة لآخرى فما تعتبره بعض الدول ارهاب لا تعتبره الدول الأخرى هكذا ، ومن ثم لم يتمكن الباحثين من التوصل إلى تعريف محدد ودقيق للإرهاب الإلكتروني، ولكن الارهاب الإلكتروني هو نوع جديد من أنواع القوة فالقوة لم تعد تقتصر على القوة الصلبة سواء العسكرية أو الاقتصادية والتى كانت محتكرة من قبل الدول ليس كل الدول وانما الدول الكبرى فقط، فظهور القوة الافتراضية أدى إلى انهاء احتكار القوى التقليدية للقوة

فأصبح كل من لديه معرفة تكنولوجية ولديه قدرة على استخدامها يمتلك القوة والقدرة على التأثير ومن ثم ظهور فواعل آخرى غير الدول فى النظام العالمى.

كما أن الارهاب الإلكتروني يمثل عنصر جاذب للجماعات الارهابية حيث يتميز بانخفاض التكلفة، وضعف الرقابة وتنوع وسائله وانتشاره وتخطيه للحدود وقدرة الأفراد على التأثير فيه، ومن ثم يستخدم الارهابيون الفضاء الإلكتروني فى التأثير على الرأى العام وتجنيد أعضاء جدد من مختلف أنحاء العالم والتمويل، ونشر رسالتهم والوصول إلى أكبر عدد ممكن من الجمهور وشن حرب نفسية ضد الأعداء والدعاية للتنظيم. وتستخدم الجماعات الارهابية أيضا الإرهاب الإلكتروني لفرض سيطرتها ونشر أفكارها، وقدرتها على تطويع الاعلام والاستفادة من ثورة التكنولوجيا والاتصالات، وتوظيف الفضاء الإلكتروني على النحو الذى يحقق أهدافها.

وفي هذا الإطار يمكننا رصد مجموعة من التوصيات والإقتراحات لمواجهة الإرهاب الالكتروني وتحقيق أمن واستقرار الدول:

- العمل على مواجهة أسباب الإرهاب وتحقيق رفاهية الشعوب عامة والشباب خاصة.

- تطوير تقنيات مراقبة شبكة الانترنت وتعزيز إجراءات الأمن والحراسة للمواقع الرسمية.

- تجريم الإرهاب الالكتروني في التشريعات الوطنية والقوانين الدولية والإقليمية.

- تعزيز التعاون الثنائي والإقليمي والدولي في كافحة ظاهرة الإرهاب الالكتروني لتسليم المجرمين وتحقيق أمن واستقرار الدول.

- إقامة شراكات دولية جديدة لمكافحة الإرهاب لترجمة الرؤية المشتركة للدول الأعضاء المجسدة في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب إلى واقع وإحداث تأ ثير حقيقي على أرض الواقع.

- انشاء غرفة عمليات دولية متخصصة في مراقبة الهجمات السيبرانية، التي تتعرض لها أنظمة معلومات المؤسسات الحساسة، كتلك الخاصة بالدفاع، والجيش والمؤسسات الأمنية، من قبل كادرات قادرة على احباطها، والحد من آثارها.

- تعزيز الجهود الدولية في مكافحة الإرهاب الإلكتروني والاستفادة من الخبرة الدولية في مجال مكافحته وإنشاء مراكز دولية متخصصة لوضع سياسات

وإستراتيجيات لرصد ومجابهة مخاطر الإرهاب الإلكتروني. ابرام اتفاقية دولية تتضمن تحديد مفهوم الإرهاب الإلكتروني وخطوات عملية لمنعه ومكافحته وضرورة وضع إطار تشريعي شامل لتجريم الإرهاب الإلكتروني وتحديد أركانه وإعتباره جريمة دولية والأعمال الإرهابية على شبكة الإنترنت والتعاون الدولي في تبادل البيانات والمعلومات بشأن فرض التزام دولي على مرتكبي الإرهاب الإلكتروني.

- ضرورة إيجاد إطار تشريعي شامل لتجريم الإرهاب الإلكتروني، دون الإضرار بحقوق الإنسان. ضرورة سد الفراغ التشريعي، لتعقب المجرمين والإرهابيين الذين اتخذوا الفضاء الإلكتروني لممارسة أعمالهم في تدمير الحضارة الإنسانية وبث الكراهية والتحريض على التطرف العنيف، وأن المعركة مع الإرهاب انتقلت إلى الشبكة المعلوماتية، ولابد أن يقضى عليه بداخلها. وأن تجريم الإرهاب الإلكتروني في العالم يجب أن يكون جزءاً من سياق التشريعات المحلية المتعددة والمتنوعة.

على ضوء ما تقدم، تبدو الحاجة واضحة إلى اتفاقية دولية بشأن أمن المعلومات الدولية، تساهم في دفع الدول، نحو اعتبار الامن العلوماتي جزءا لا يتجزأ من مهمات الدفاع المشترك، بين الدول الاعضاء، والاقرار بمسؤولية كل دولة، عن ضمان أمن شبكة اتصالاتها وبنيتها التحتية، وب التزامها التعاون مع الدول الاخرى، لاعتماد المعايير والمقاييس الدولية الخاصة، بالحماية والامن .

الهوامش والمراجع:

(1)- Тропина, Т. Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы: моногр./ Т. Л. Тропина. - Владивосток, 2009 - 181-137 с

(2)- ريهام عبدالرحمن رشاد العباسى، أثر الارهاب الإلكتروني على تغير مفهوم القوة فى العلاقات الدولية، المركز الديمقراطي العربي.

https://democraticac.de/?p=34528

(3)- Вейманн Г. Как современный терроризм использует Интернет: специальный доклад № 116// Владивостовскйи центр исследования организованной преступности.2004.

(4)- تقرير اللجنة الدولية للصليب الاحمر، القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة، الحادي والثلاثين، 2011، ص 67.

(5)- د.هشام بشير، "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المُواجهة"، ندوة المركز الدولي للدراسات المُستقبلية والاستراتيجية في 11 أبريل 2012 على الرابط:

http://www.siyassa.org.eg/UI/Front/InnerPrint.aspx?NewsContentID=2450

(6)- عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، جدة، 2004، ص8.

(7)- قرار الجمعية العامة " RES/60/288 A" 8 أيلول 2006

http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288&referer=/english/&Lang=A

(8)- http://www.mid.ru/foreign_policy/official_documents /-/asset_publisher/CptICkB6BZ29/content/id/191666

(9)- https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISA greement Russian .pdf

(10)- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، العدد الخامس، يناير-يونيو 2015، ص 138.

(11)- http://www.e-cis.info/page.php?id=23899 Соглашение о сотрудничестве государств – участников Содружеств Независимых Государств в области обеспечения информационной безопасности.

(12)- http://www.gcc-sg.org/ar- sa/CooperationAndAchievements/ Achievements /LegalandJudicialCooperation/Pages/Legalandjudicialcooperation.aspx.

(13)- قرار مجلس الأمن رقم 1269/ 1999

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/303/90/PDF /N9930390.pdf?OpenElement

(14)- قرار الجمعية العامة " أنشطة منظومة الأمم المتحدة في مجال تنفيذ استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب"

http://www.un.org/ar/documents/viewdoc.asp?docnumber=A/72/840

(15)- استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/86/PDF/N0550486.pdf?OpenElement

(16)- انظر قرار مجلس الأمن رقم 1437 الصادر بتاريخ 28 سبتمبر 2001.

(17)- http://www.un.org/ar/counterterrorism/hlc/index.shtml

(18)- Дмитриева В.В. Межгосударственное сотрудничество в борьбе с международным кибертерроризмом на примере Европейского Союза, журнал, Вопросы экономики и права. 2107. №1.с 58.

(19)- ورقة جامعة الدول العربية في الملتقى العلمي أثر الإرهاب على الأمن والسلم العالمي، الرباط، 14-2014/10/16، ص3.

EISSN: 2588-2368 _____ ISSN: 2352-975X