مكافحة الإرهاب الالكتروني

countering cyber terrorism

مبروك فاطيمة♦
كلية الحقوق والعلوم السياسية
جامعة عمار ثليجي –الأغواط- الجزائر
mebroukf1985@yahoo.com

ذيب محمد
كلية الحقوق والعلوم السياسية
جامعة عمار ثليجي –الأغواط- الجزائر
Mohamedib80@gmail.com

تاريخ الإرسال: 2022/01/31 تاريخ القبول: 2022/05/29 تاريخ النشر: 2022/06/03

الملخص:

تهدف هذه الدراسة إلى تبيان مختلف الجهود لمكافحة الإرهاب الإلكتروني، حيث تتمايز هذه الجهود بين الطابع الدولي والوطني، والتي ومن خلالها كان الاهتمام بمكافحة هذا النوع من الإجرام الخطير والمستحدث على المستويين الدولي والداخلي، ولهذه الدراسة أهمية تتمثل في أن الإرهاب الإلكتروني هو خطر يهدد على حد سواء سلامة الكيان الطبيعي أو الكيان المعنوي، فالمجرم الإرهابي اليوم استفاد بشكل سلبي من تطور تقنية المعلومات والشبكات العنكبوتية التي هي مورد هام وأساسي في ارتكاب الجريمة الإرهابية الرقمية، مما حتم على الدول مجتمعة ومنفردة مكافحة هذا النوع الخطير من الإجرام بمختلف ألأساليب والطرائق، وقد خلصنا إلى أن هذه الجهود تلعب دورا هاما في مجابهة الإرهاب الإلكتروني إلا أنه وبالرغم من ذلك لا تزال هذه الظاهرة الإجرامية قائمة وتعاني منها الدول والأفراد على حد سواء، مما يستوجب إيجاد وسائل تكون أكثر وقائية ومجابهة لها.

الكلمات المفتاحية: الإرهاب الإلكتروني، الحرب الإلكترونية، مكافحة الإرهاب الإلكتروني.

Abstract:

This study aims to show the various efforts to combat electronic terrorism, as these efforts are distinguished between the international and national character, and through which the interest in combating this type of

♦ المؤلف المرسل

dangerous and emerging crime at the international and domestic levels, and this study is important in that electronic terrorism is a threat that threatens both Whether the integrity of the natural entity or the moral entity, the terrorist criminal today has negatively benefited from the development of information technology and the Internet, which is an important and essential resource in the commission of digital terrorist crime, which has made it imperative for countries collectively and individually to combat this dangerous type of crime in various ways and methods, and we have concluded that These efforts play an important role in countering cyber terrorism, but despite this, this criminal phenomenon still exists and both countries and individuals suffer from it, which requires finding means that are more preventive and confronting it.

keywords : Electronic terrorism, Electronic warfare, Countering electronic terrorism.

مقدمة:

يعتبر الإرهاب الإلكتروني آخر ما توصل إليه العقل الإجرامي، فبتنامي الثورة التكنولوجية والمعلوماتية تنامت العقول الإجرامية الإرهابية، وبالتوافر السهل لشبكة الإنترنت وملحقاتها المادية أصبح العالم دولا وأفرادا يتعرض اليوم لهجمات إرهابية عبر الفضاء الرقمي، وتختلف حدة هذه الهجمات حسب نوعها وهدفها وغايتها، فقد تصيب المصالح الأساسية للدول وأمنها أو سيادتها القومية، وقد تستهدف سلامة المواطنين وطمأنينتهم، فالإرهاب الإلكتروني هو أحد الجوانب الأكثر سلبية في استغلال التطور الحاصل في تقنية المعلومات.

وإن أهمية هذه الدراسة تتجلى أولا في خطورة جريمة الإرهاب الإلكتروني، والتي تتعدد ضحاياها بين الأفراد والدول والكيانات الأخرى، وثانيا لما أصبحت تثيره هذه الجريمة من مخاوف وقلق لدى المجتمع الدولي والمحلي بسبب تهديدها وتطورها المستمرين، وثالثا في الخصائص التي تميز الإرهاب الإلكتروني من تعقيد وصعوبة اكتشافه وملاحقة مرتكبيه وغيرها.

وغايتنا من هذه الدراسة ليس فقط إبراز مختلف الجهود الدولية والوطنية لمكافحة الإرهاب الإلكتروني، بل إثراء هذه الجهود، و إيجاد حلول أخرى من أجل التعاون الدولي لمجابهة هذه الجريمة.

وانطلاقا مما سلف نطرح الإشكالية التالية : ما هي الجهود الدولية والوطنية المبذولة في مكافحة الإرهاب الإلكتروني ؟

وللإجابة على الإشكالية السابقة اعتمدنا على المنهج الوصفي، وذلك بوصف ظاهرة الإرهاب الإلكتروني كما هي في الواقع من خلال تبيان المفاهيم المتعلقة بهذه الظاهرة وتحديد خصائصها، كما تم الاعتماد على المنهج التحليلي حتى نجيب على التساؤلات المطروحة ونستخرج حلولا لمعالجة ظاهرة الإرهاب الإلكتروني.

ورأينا أن نقسم هذه الدراسة إلى مبحثين رئيسيين حيث يتناول المبحث الأول

مفهوم الإرهاب الإلكتروني، والسمات التي يتميز بها بالإضافة إلى الأساليب المعتمدة في ارتكاب هذه الجريمة، أما المبحث الثاني خصصناه لمكافحة الإرهاب الإلكتروني، مبرزين في ذلك كل من جهود منظمة الأمم المتحدة، والجهود الإقليمية الأوربية والآسيوية والعربية، وجهود مجموعة من الدول في مكافحة الإرهاب الإلكتروني.

المبحث الأول : الإطار النظري للإرهاب الإلكتروني

للإحاطة نظريا بالإرهاب الإلكتروني وجب الحديث عن مفهومه (مطلب أول)، ثم عن اعتباره شكلا من أشكال الصراع الدولي الجديد (مطلب ثاني).

المطلب الأول : مفهوم الإرهاب الإلكتروني

في الفرع الأول من هذا المطلب سنعرف الإرهاب الإلكتروني، ثم في الفرع الثاني سنوضح أساليب الإرهاب الإلكتروني.

الفرع الأول : التعريف بالإرهاب الإلكتروني

كانت بدية استخدام هذه الكلمة cyber terrorism في فترة الثمانينات في دراسة " باري كولن " Barry Collin والتي خلصفيها إلى صعوبة وضع تعريف لظاهرة الإرهاب التكنولوجي بدقة، ناهيك عن الأسباب والحلول المطلوبة لمواجهته وكذلك تحديد دور الكمبيوتر والإنترنت في العمل الإرهابي[1]، ولكنه تبنى تعريفا للإرهاب الإلكتروني مقتضاه بأنه هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية،وأن الهدمة تكون ذات أثر مدمر وتخريبي مكافئ للأعمال المادية[2]

ويرى البعض أن الإرهاب الإلكتروني أنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية، أي أنه توظيف لأحدث التقنيات العلمية في الضغط والتوجيه والسيطرة على الآخرين أيا كانوا أفرادا أو مؤسسات أو دول أو أنظمة وكيانات سياسية أو اقتصادية أو حتى تكنولوجية وبهدف كسر إرادة هذا الآخر للتمكن منه[3].

[1] عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، الطبعة الأولى، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009، ص 140.

[2] الموسوعة السياسية، الارهاب الإلكتروني، انظر الموقع الإلكتروني https://www.translatetheweb.com/، تاريخ الإطلاع عليه 2021/02/06.

[3] غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، 2017، ص 76.

ويعرف عبد الله بن عبد العزيز بن فهد العجلان الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعة أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد[1].

وعرفته منظمة الأمم المتحدة عام 2012 بأنه استخدام الإنترنت لنشر أعمال إرهابية.

أما الاتفاقية الأولى لمكافحة الإجرام عبر الإنترنت في بودابست عام 2001 فقد عرفت الإرهاب الإلكتروني بأنه: " هجمات غير مشروعة أو تهديد بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجد من أجل الانتقام أو الابتزاز أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة[2].

وحسب ماسبق من تعريفات يتضح لنا أن الإرهاب الإلكتروني ومهما كان الدافع من ورائه يعتمد على عنصرين أساسيين فالأول يتمثل في التخويف والترويع والتهديد أما الثاني فهو شبكة الأنترنت والتي تكون عن طريقها الأعمال الإرهابية الإلكترونية.

الفرع الثاني : خصائص الإرهاب الإلكتروني

يمكن إجمال الخصائص التي يتميز بها الإرهاب الإلكتروني فيما يلي :

- لا يحتاج الإرهاب الإلكتروني في ارتكابه إلى القوة والعنف، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة

- يتسم الإرهاب الإلكتروني بأنه عابر للدول والقارات، وغير خاضع لدولة معينة[3].

- إن الإرهاب الإلكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة وإنما ما يحتاجه هو جهاز حاسب آلي وبعض البرامج وشبكة إنترنت، وعادة ما تتم العمليات الإرهابية بتعاون عدة أشخاص(منظمات إرهابية)[4].

- عادة ما يكون مرتكبو جريمة الإرهاب الإلكتروني من ذوي الاختصاص في مجال تقنية المعلومات، وعلى قدر كبير من المعرفة في التعامل مع الوسائل الإلكترونية[1].

---

[1] عبد الله بن عبد العزيز بن فهد العجلان، بحث قانوني ودراسة شاملة حول الإرهاب الإلكتروني في عصر المعلومات، منشور في الموقع الإلكتروني https://www.mohamah.net/law بتاريخ 2016/09/14، تاريخ الاطلاع عليه2021/02/06.

[2] الساجي علام، فوزية حاج شريف، واقع الإرهاب الإلكتروني آليات مكافحته، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول، ص 162، ص 163.

[3] مصطفى يوسف كافي، الإدارة الإلكترونية، إدارة بلا أوراق، إدارة بلا مكان، إدارة بلا زمان، إدارة بلا تنظيمات جامدة، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2011، ص 441.

[4] مهران زهير المصري، الإرهاب الإلكتروني، مقال منشور في الموقع الإلكتروني http://www.albahethon.com/ بتاريخ 2011/10/04، تاريخ الاطلاع عليه 2021/02/08.

- صعوبة اكتشاف جرائم الإرهاب بالوسائل الإلكترونية، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذه الجرائم[2]، فيتعسر إثبات مثل هذه الجرائم لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم.

- لا يشترط التنظيم في الإرهاب الإلكتروني فقد يرتكبه فرد بمفرده دون الانخراط في أي تنظيم إرهابي[3].

الفرع الثالث : أساليب الإرهاب الإلكتروني :

ترتكب جريمة الإرهاب الإلكتروني بواسطة مجموعة من الوسائل والأساليب وهي تستخدم في ذلك الإنترنيت، ويعد البريد الالكتروني من أعظم الوسائل لمستخدمي في الإرهاب الإلكتروني حيث يعد أسلوبا آمنا وسهلا للتواصل بين الإرهابيين وتبادل المعلومات بينهم والتخطيط للعمليات الإرهابية، كما يستخدم البريد الإلكتروني أيضا من طرف المتطرفين دينيا للترويج لأفكارهم وكسب تعاطف الآخرين[4] فتقوم الجماعات الإرهابية بإنشاء مواقع إرهابية إلكترونية لنشر أفكارهم والدعوة لمبادئهم، وتعليم صنع المتفجرات، وتدمير المواقع الإلكترونية، واختراق البريد الإلكتروني، وصنع الفيروسات.

كما يقوم الإرهابيون من صنف الهاكرز أو قراصنة الحاسوب باختراق المواقع الإلكترونية عن طريق استخدام الفيروسات للحصول على معلومات أماكن أو شركات معينة من أجل تنفيذ الأعمال الإرهابية[5]، ومن الوسائل المستخدمة لتدمير المواقع الإلكترونية ضخ مئات الآلاف من الرسائل الإلكترونية إلى الموقع المستهدف للتأثير على السعة التخزينية لديه، مما يشكل ضغطا يؤدي إلى انفجار الموقع الإلكتروني، فتشتت بذلك معلومات المستهدف وتنتقل إلى جهاز المعتدي، أو عن طري التجوال الحر للمعتدي في الموقع الذي تم تدميره[6].

وتستغل الجماعات الإرهابية شبكة الإنترنيت للحصول على التمويل لنشاطها الإرهابي وذلك من خلال الاستثمار الرقمي والتواصل مع مستخدمين من مختلف مناطق العالم[7].

---

[1] مصطفى سعد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، جانفي 2017، ص 37.

[2] المرجع نفسه، ص 38.

[3] سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، العدد 08، الجزء 01، جوان 2017، ص 345.

[4] الإرهاب الإلكتروني، طرقه ووسائل التصدي له، الموقع الإلكتروني https://crimedz.blogspot.com/2017/06/blog-post.html، اطلع عليه بتاريخ 20121/02/14.

[5] فوزية حاج شريف، واقع الإرهاب الإلكتروني وآليات مكافحته، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول، 2019، ص 166.

[6] مصطفى يوسف كافي، مرجع سابق، ص 446.

[7] نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحة مرتكبي جرائم الإرهاب، مركز الكتاب الأكاديمي، ص 53.

المطلب الثاني : الإرهاب الإلكتروني كشكل جديد من أشكال الصراع الدولي

انتقلت الحروب من الميادين البرية والجوية والبحرية إلى الميدان الإلكتروني وهو مايعرف بالحرب الإلكترونية، مستخدمة في ذلك وسائل وأساليب الإرهاب الإلكتروني، فماهي الحرب الإلكترونية في فرع أول، وتطبيقات الحرب الإلكترونية في فرع ثان.

الفرع الأول : الحرب الإلكترونية

يتميز هذا النمط من الصراع على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشئات العدو، ويتم استخدام[1] الروبوتات الآلية في الحروب والتي يتم إدارتها عن بعد فضلا عن الطائرات بدون طيار في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، ويتم استخدام الفضاء الإلكتروني في الإعداد لحرب المستقبل والقيام بتدريبات لتوجيه ضربة أولى لحواسيب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية، ولعل الهدف من وراء ذلك تحقيقا للهيمنة الإلكترونية الواسعة بشكل أسرع في حال نشوب صراع[2].

وينظر إلى الحرب الإلكترونية باعتبارها القدرة على الدفاع والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القدرة بالقيام بهذه الهجمات نفسها، حيث يرى كينث جريس أن الحر الإلكترونية تشمل خمسة عناصر رئيسية هي التجسس، الدعاية، الحرمان من خدمة الإنترنت، تعديل البيانات والتلاعب بها، والتلاعب أيضا بالبنية التحتية[3].

ويأخذ الصراع الإلكتروني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة المعلومات الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للتحكم في أسماء النطاقات وعناوين المواقع والمعلومات والعمل على اختراق الأمن القومي للدول، أو حتى انتهاك للحدود السيادية، بدون استخدام طائرات أو متفجرات، كهجمات قرصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له أثر في تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر[4].

---

[1] الدكتور. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الإلكتروني، 2018، ص 44.

[2] المرجع نفسه، ص 45.

[3] إيهاب خليفة، القوة الإلكترونية، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017، ص 81.

[4] إيهاب خليفة، حروب مواقع التواصل الاجتماعي، العربي للنشر والتوزيع، 2016، ص 28.

الفرع الثاني : تطبيقات الحرب الإلكترونية

يتم التقدم في مجال استخدام كافة أنواع الأسلحة الإلكترونية مثل أسلحة الميكروويف عالية القدرة، وتم توجيه هجمات إلكترونية باستخدام عدد من الفيروسات مثل هجمات فيروس سناكس في اكتوبر 2010 ضد المنشآت النووية الإيرانية ....

ويقدم النموذج الإيراني حالة فريدة لتحول الفضاء الإلكتروني لساحة قتال ذات طابع مرن وآخر ذو طابع صلب، وذلك في إطار المواجهة بين إيران وإسرائيل والولايات المتحدة الأمريكية والتي منها استخدامه في تحريك القوة الناعمة داخل إيران بدعم الاحتجاجات في عام 2009، وتقديم دعما للمعارضة عقب الانتخابات الرئاسية[1].

وقد أصبحت الحرب الإلكترونية تدعم الحرب الحديثة، فيمكن لطائرات القتال المجهزة بمعدات الحرب الإلكترونية أن تعمل مصاحبة للطائرات المقاتلة القاذفة أثناء قيامها بالاختراق العميق، لستر تقدمها[2]، كما يستخدم الفضاء الإلكتروني للتأثير على تحركات الأجهزة الأمنية ومجريات الأحداث بصفة عامة، فقد يتم توجيه أوامر ومعلومات خاطئة، وقد تم استخدام هذا الأسلوب في الحرب الأمريكية على العراق عبر اختراق أنظمة الاتصال ونشر معلومات مسبقة عن سقوط بغداد.

وعلى هذا النحو تم اختراق الاتصالات الليبية ونشر معلومات عن سقوط طرابلس مما أثر في القوات المحاربة إلى جانب القذافي، والذي تم تحديد مكانه عن طريق رصد المكالمات من الاستخبارات الأجنبية، وتزويد المعارضة بهذه المعلومة.

وفي نفس الأحداث قامت كل من الولايات المتحدة الأمريكية وتركيا والدول المتحالفة ضد نظام بشار الأسد في سوريا بتزويد المعارضة حول تمركز القوات النظامية السورية، وقامت باختراق أنظمة الاتصالات داخل الجيش السوري مما سمح للمعارضة باستخدامها ضد النظام السوري مثل القيام بتفجير اجتماع خلية الأزمة السورية الذي أدى إلى قتل كبار القادة في الجيش السوري[3].

المبحث الثاني : مكافحة الإرهاب الإلكتروني

في إطار هذا المبحث سنتطرق لمكافحة الإرهاب الإلكتروني عالميا في المطلب الأول، وفي المطلب الثاني إلى مكافحة الإرهاب الإلكتروني إقليميا ووطنيا.

---

[1] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في القانون الدولي الإنساني، مرجع سابق، ص 45.

[2] فيصل محمد عبد الغفار، الحرب الإلكترونية، الجنادرية للنشر والتوزيع، عمان، الأردن، 2015، ص 33.

[3] عادل عبد الصادق، الفضاء الإلكتروني والديمقراطية بين التحولات والتحديات، المركز العربي لأبحاث الفضاء الإلكتروني، 2012، ص 139.

المطلب الأول : مكافحة الإرهاب الإلكتروني عالميا

سعت منظمة الأمم المتحدة من خلال جهودها للتعاون الدولي من أجل مكافحة الإرهاب الإلكتروني وهذا ما سنتناوله في الفرع الأول، أما الفرع الثاني سيكون بخصوص واقع التعاون الدولي لمكافحة الإرهاب الإلكتروني.

الفرع الأول : جهود منظمة الأمم المتحدة في مكافحة الإرهاب الإلكتروني

حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المنعقد بهافانا بكوبا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالإرهاب الإلكتروني، بما في ذلك دخولها حسب الاقتضاء في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، وفتح آفاق جديدة للتعاون الدولي في هذا المضمار ولا سيما فيما يتعلق بوضع أو تطوير ما يلي :

-معايير دولية لأمن المعالجة الآلية للبيانات.

-تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.

-اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول[1].

عادت وأكدت الأمم المتحدة في فبراير 2015 خلال قمة مكافحة التطرف والعنف على مخاطر التهديدات الإلكترونية للمجموعات الإرهابية، والتي استطاعت في فترة وجيزة، تعزيز قبضتها على وسائل التواصل الاجتماعي، وتوظيفها في الترويج لأيديولوجيتها، واستقطاب أنصار جدد، كذلك تنبهت العديد من الدول إلى أن مواجهة الإرهاب الإلكتروني لا يمكن أن تتم إلا بتعزيز الإطار القانوني والتشريعي عبر إصدار قانون خاص لمكافحة الإرهاب على الإنترنت، وإرساء قواعد تعاون فاعل وحقيقي على المستويات الوطنية بين مختلف الإدارات وعلى المستوى الدولي بالعمل مع بلدان أخرى، وتبادل المعلومات بين أجهزة طوارئ الإنترنت، أو إنشاء خلايا مشتركة، تعمل على رصد التهديدات السيبرانية، وتبادل المعلومات بشأنها[2].

---

[1] نجيب بن عمر عوينات، الإرهاب الإلكتروني المفهوم والجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث للدراسات القانونية، العدد السادس، جوان 2017، ص 16.

[2] محمد البشاري، الإرهاب الإلكتروني ومسؤولية المجتمع الدولي، مقال منشور في جريدة العين الإخبارية يوم الأحد 2021/2/7، متوفر في الموقع الإلكتروني https://al-ain.com/article/electronic-terrorism-and-the-responsibilit بتاريخ 2017/10/20، تاريخ الاطلاع عليه 2021/02/06.

وتسعى الأمم المتحدة إلى التنسيق بين الدول الأعضاء لمواجهة خطر الإرهاب الإلكتروني من خلال القرارات 63/55 (2000) و 121/56 (2001) بخصوص مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية. ويعد الاتحاد الدولي للاتصالات (ITU) هو الهيئة الوحيدة المسئولة عن مكافحة الإرهاب الإلكتروني من بين هيئات الأمم المتحدة، كما أن الأمم المتحدة كانت قد أنشأت الشبكة الدولية الإعلامية للعدالة الجنائية (UNCIDIN)وهي متخصصة في المجال الإلكتروني. وبصفة عامة وبعد أحداث 11 سبتمبر بدأت الأمم المتحدة السعي لمكافحة الإرهاب بشتى أنواعه، لذلك أنشئت لجنة لمكافحة الإرهاب (CTC) لمراقبة تنفيذ القرار 1373 ولمساعدة الدول في تطوير القدرات المطلوبة لتنفيذه[1].

كما أشرفت منظمة الأمم المتحدة في 12 أفريل2000 على توقيع اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية حيث أكدت في مادتها الأولى على أنه:« ينبغي للدول أن تكفل عدم توفير قوانينها و ممارساتها ملاذا آمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية 2»

وعقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل ما بين19-12أفريل2010حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، حيث احتل هذا النوع من الجرائم موقعا بارزا على جدول عمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[3].

الفرع الثاني : واقع التعاون الدولي في مواجهة الإرهاب الإلكتروني

بالرغم على ما ينطوي عليه الإرهاب الإلكتروني من تهديد لأمن الدول وسيادتها وحماية مصالحها ومصالح مواطنيها وتطورها التكنولوجي لا يوجد اتفاق دولي واضح في التعامل مع هذه الظاهرة، مما ينعدم معه أي تعاون دولي في مجال مكافحة إرهاب الفضاء الإلكتروني[4]، فمن الضروري لمواجهته تفعيل التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المُجرمين، وإصدار عدد من القوانين التشريعية الجديدة لتجريم أي استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادُل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المُستمر من خلال عناصرِ الإجرامية المُحترفة والمُنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية.

---

[1] رانيا سليمان، فاتن فايز، نهى الدسوقي، سياسات مكافحة الإرهاب الإلكتروني، مصر والسعودية نموذجا، الموقع الإلكتروني www.acrseg.org/41483، مقال منشور بالمقع الإلكتروني بتارخ 2020/02/02، اطلع عليه يوم 2021/02/09.

[2] نجيب بن عمر عوينات، مرجع سابق، ص 17.

[3] المرجع نفسه، ص 18.

[4] غادة نصار، مرجع سابق، ص 77.

وذلك لأن الفضاء الإلكتروني بات يشكل بيئة إستراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع، ولظهور فاعلين جدد على الساحة الدولية[1].

المطلب الثاني : الجهود الإقليمية والوطنية في مكافحة الإرهاب الإلكتروني

سنستعرض في هذا المطلب الجهود الإقليمية لمكافحة الإرهاب الإلكتروني، ثم في الفرع الثاني الجهود الوطنية لمكافحة الإرهاب الإلكتروني.

الفرع الأول : الجهود الإقليمية في مكافحة الإرهاب الإلكتروني

بداية بالاتحاد الأوروبي فقد توجت جهوده في إصدار اتفاقية شاملة تتعلق بجرائم الحاسب الآلي[2] عرضت للتوقيع في بودابست في 2001، ودخلت حيز النفاذ في 2004، وهي متاحة لجميع الدول للانضمام إليها[3].

وصاغت الدول الأعضاء في مجلس أوروبا البروتوكول الإضافي لاتفاقية الجرائم الإلكترونية ، بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الكمبيوتر، ودخل البروتوكول حيز التنفيذ عام 2006 وهو مفتوح لجميع الدول التي وقعت على اتفاقية الجرائم الإلكترونية، ويتعين على الدول الموقعة أن تجرم مجموعة من الأفعال مثل نشر المواد العنصرية والمعادية للأجانب عبر أنظمة الكمبيوتر[4].

أما دول شرق آسيا تهتم رابطة أمم شرق آسيا (ASEAN) بالتعاون بين الدول لمكافحة الإرهاب الإلكتروني، وذلك من خلال منتدى الآسيان الإقليمي (ARF) والذي يتكون من 28 دولة يعملون من خلال هذا المنتدى على تبادل المعلومات ودراسة العديد من القضايا الخاصة بالإرهاب الإلكتروني[5].

وعلى المستوى العربي فقد عقدت اتفاقية لمكافحة جرائم تقنية المعلومات سنة 2010 بالقاهرة، والتي جرمت في المادة الخامسة عشرة منها الإرهاب الإلكتروني، وقد حصرت هذه المادة الإرهاب الإلكتروني في أربع فئات وهي نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، أو تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصال بين الجماعات الإرهابية، أو نشر كيفية صناعة المتفجرات والتي تستخدم في العمليات الإرهابية، أو

---

[1] عبد الرحمان عثمان، الإرهاب الإلكتروني، أنماطه وسبل مكافحته، مقال منشور بالموقع الإلكتروني:
https://www.maspero.eg/wps/portal/home/egynews/files/sport/details/bf
، بتاريخ 2016/11/26، اطلع عليه يوم 2021/02/09..

[2] فوزية حاج شريف، مرجع سابق، ص 169.

[3] نجيب بن عمر عوينات، مرجع سابق، ص 18.

[4] Council of Europe: Fight against Cybercrime انظر الموقع الالكتروني https://www.europewatchdog.info/en/international-treaties/treaties_and. اطلع عليه يوم 2021/02/15.

[5] رانيا سليمان، فاتن فايز، نهى الدسوقي، سياسات مكافحة الإرهاب الإلكتروني، مصر والسعودية نموذجا،مرجع سابق، مقال منشور بالموقع الإلكتروني بتارخ 2020/02/02، اطلع عليه يوم 2021/02/09.

نشر النعرات والفتن والاعتداء على الأديان والمعتقدات، كما تناولت الاتفاقية طرق التعاون الإجرائي كتسليم المعلومات والتعاون القضائي والقانوني بين الدول الأطراف كتسليم المجرمين والمساعدة المتبادلة [1].

الفرع الثاني : الجهود الوطنية في مكافحة الإرهاب الإلكتروني

أصبحت مكافحة الإرهاب الإلكتروني محليا ضرورة ملحة، وأدركت دول العالم عربية وغربية ضرورة استتباب

أمنها المعلوماتي، والدفاع عنه من الهجومات الإرهابية الإلكترونية، فمن الدول العربية الأردن التي سنت قانون منع الإرهاب الأردني رقم 55 لسنة 2006 والذي اعتبرت المادة الثالثة منه الأعمال التالية في حكم

الأعمال الإرهابية المحظورة استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع الإلكتروني لتسهيل القيام بإعمال إرهابية أو دعم لجماعة او تنظيم أو جمعية تقوم بإعمال إرهابية أو الترويج لأفكارها او تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم [2].

وفي المملكة العربية السعودية أصدرت بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال مخالفتها، منها قرار مجلس الوزراء رقم 163 في 1417/10/24 هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنيت والاشتراك فيها، ومن ذلك الامتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها[3].

أما في الجزائر فقد اعتمدت الحكومة عام 2006 قانونا يسمح بمراقبة الأجهزة الصوتية واعتراض المراسلات[4]، وسمح القانون باستخدام تقنية التسرب في التحقيق في الجرائم المتعلقة بالإرهاب، بالإضافة إلى مجموعة من القوانين مثل قانون العقوبات، وقانون الملكية الفكرية[5].

أما بالنسبة للدول الغربية ومكافحتها للإرهاب الإلكتروني فسنكتفي بفرنسا حيث تم إنشاء الوكالة الوطنية لأمن

---

[1] انظر في ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، المواد 5 و31 و32.

[2] مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، جانفي 2017، ص 30.

[3] بن يحي الطاهر ناعوس، مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية، منشور في الموقع الإلكتروني https://www.alukah.net/library/0/80823/2015/01/06 ، اطلع عليه بتاريخ 2021/02/15، ، ص 19، ص 20.

[4] فوزية حاج شريف، مرجع سابق، ص 169.

[5] [37]المرجع نفسه، ص 167.

أنظمة المعلومات(ANSSI) في 2009 وهي السلطة الوطنية المعنية بالأمن السيبراني بصفتها "رجل إطفاء" حقيقي للفضاء الإلكتروني الفرنسي، فهي مسؤولة عن الوقاية (بما في ذلك المعايير) ورد الفعل على حوادث الكمبيوتر التي تستهدف المؤسسات الحساسة، كما ينظم تدريبات على إدارة الأزمات على المستوى الوطني، وتوظف ANSSI الآن 600 شخص وتستمر في النمو[1].

خاتمة :

مما سبق نستطيع القول أن الإرهاب الإلكتروني هو تلك الأعمال الواقعة عبر الأجهزة الإلكترونية الموصولة بشبكة الإنترنت بحيث تنطوي هذه الأعمال على التخويف والتهديد، أو نشر أفكار ومعتقدات متطرفة وعنصرية، أو اختراق لنظم وبيانات لشخص بذاته أو شركة أو دولة معينة.

وخلصنا من خلال هذه الدراسة إلى النتائج التالية :

- أصبح الإرهاب الإلكتروني واقعا معاشا وذا أبعاد خطيرة لا يمكن التنبؤ بها خاصة مع ارتفاع عدد المستخدمين للإنترنت والنمو السريع لتقنيات الحاسوب، مما جعل سبل مكافحته صعبة.

- الإرهاب الإلكتروني من الجرائم غير المنتهية والمستمرة، ذلك لأن المجرم الإرهابي الإلكتروني لا يمكن ردعه ومحاسبته عن جرائمه، فإن تمت مواجهة أعماله الإرهابية الإلكترونية، يمكنه أن يعد ويخطط لأعمال غيرها، وإن تم اكتشاف هويته والقبض عليه فهناك من يخلفه إن كان منتميا لجماعة إرهابية.

- إن مختلف الجهود لمكافحة الإرهاب الإلكتروني لم تكن في مستوى خطورته، فمنظمة الأمم المتحدة لم تكن مساعيها في هذا المجال واضحة وثابتة مما يبرر عدم عقد اتفاقية دولية خاصة بمكافحة الإرهاب الإلكتروني وإن كانت اتفاقية بودابست لمكافحة جرائم الحاسب الآلي تناولت في محتواها مكافحة الأعمال الإرهابية عن طريق الإنترنت، فهذا لا يكفي خاصة مع التطور والتهديد المستمرين لمرتكبي جرائم الإرهاب الإلكتروني.

-ما قيل عن الجهود الدولية لا يقال عن جهود مختلف الحكومات فهناك من الدول من سنت قوانين وتشريعات خاصة لمكافحة الإرهاب الإلكتروني، وفي المقابل هناك دولا لم تستحدث تشريعاتها في هذا المجال خاصة دول العالم الثالث إلا في بعض جوانب هذه الجريمة كاختراق الأنظمة مثلا.

- ما تقوم به الدول المسيطرة على الساحة الدولية من أعمال عدائية إلكترونية اتجاه غيرها من الدول لا يختلف عما تقوم به الجماعات الإرهابية من خلال استعمالها للمعلوماتية، وبذلك فيمكن أن يكون مرتكب الإرهاب الإلكتروني إما فردا أو جماعة أو دولا.

- ضعف الجهود الدولية والإقليمية خاصة العربية منها في مكافحة الإرهاب الإلكتروني، لعل ذلك راجع إلى الأزمات المتتالية التي مر ويمر بها الوطن العربي.

[1]/ انظر الموقع الالكتروني https://www.diplomatie.gouv.fr اطلع عليه بتاريخ 2021/02/15.

نوصي من خلال هذه الدراسة بمايلي :

- يجب أن تكون هناك مكافحة وقائية من جريمة الإرهاب الإلكتروني وذلك من خلال توعية الأفراد والمواطنين عن طريق تثقيفهم حول هذه الجريمة، خاصة في المجتمعات الفقيرة والتي تعاني من الجهل والأحوال الاجتماعية المزرية، مما يجعلهم التحاقهم سهلا بالجماعات الإرهابية، ويجب أن تكون هذه التوعية على المستوى الوطني ومثلها على المستوى الدولي.

- وما يعتبر من المكافحة الوقائية من الإرهاب الإلكتروني أيضا البرنامج الدراسي في جميع مراحله الذي يمكن أن يكون من الوسائل الفعالة في التربية الإلكترونية للتلاميذ والطلاب خاصة وأن هذه الفئة من المجتمع تعتبر الأكثر استعمالا للإنترنت كمواقع التواصل الاجتماعي مثلا والتي عن طريقها تقوم الجماعات الإرهابية بالتواصل مع الأفراد والتعريف بتنظيمها الإرهابي.

- يجب تفعيل دور الجمعيات الوطنية والمنظمات الدولية من أجل مكافحة فعالة للإرهاب الإلكتروني، خاصة دور منظمة الأمم المتحدة.

- بالإضافة إلى المكافحة الوقائية من الإرهاب الإلكتروني يجب أن تلتزم الدول بالمكافحة التشريعية الداخلية كسن قوانين معاصرة يكون بمقدورها التصدي لهذا النوع من الجرائم الخطيرة.

- يجب على الدول مجتمعة أن تكاثف جهودها للتعاون من أجل مكافحة تشريعية ومؤسساتية دولية للإرهاب الإلكتروني، وذلك من خلال عقد اتفاقيات دولية، وإنشاء قضاء دولي مختص في مجال جرائم الإلكترونيات، ووضع إستراتيجية دولية شاملة وفعالة لمكافحة الإرهاب الإلكتروني.

- يجب أن يمتد التجريم ليس فقط للأعمال الإرهابية الإلكترونية، بل عليه أن يشمل أيضا مجموعة من السلوكيات المادية التي تتضمنها الحرب الإلكترونية والتي تقوم بها بعض الدول، كاختراق دولة ما لأنظمة جيش دولة أخرى، أو إصابة أنظمتها الأمنية المعلوماتية بفيروس حتى تبقيها تحت السيطرة.

- على حكومات الدول عصرنة تشريعاتها وحتى تكوين القضاة في مجال المعلوماتية، لأنه وفي عصر الرقمنة يجب استحداث مؤسسات قضائية مختصة في المجال الفضاء الرقمي الإلكتروني، مستعينة في ذلك بمختصين في هذا المجال.

- فيجب تأمين البيانات والمعلومات المهمة بصفة مستمرة سواء تتعلق هذه المعلومات بالفرد أو الدول أو الشركات.

قائمة المصادر والمراجع:

أولا: الموسوعات:

1. الموسوعة السياسية، الارهاب الإلكتروني، انظر الموقع الإلكتروني https://www.translatetheweb.com/، تاريخ الإطلاع عليه 2021/02/06.

ثانيا: الكتب:

1. إيهاب خليفة، القوة الإلكترونية، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017.

2. إيهاب خليفة، حروب مواقع التواصل الاجتماعي، العربي للنشر والتوزيع، 2016.

3. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الإلكتروني، 2018.

4. عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، الطبعة الأولى، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009.

5. عادل عبد الصادق، الفضاء الإلكتروني والديمقراطية بين التحولات والتحديات، المركز العربي لأبحاث الفضاء الإلكتروني، 2012.

6. غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، 2017.

7. فيصل محمد عبد الغفار، الحرب الإلكترونية، الجنادرية للنشر والتوزيع، عمان، الأردن، 2015.

8. مصطفى يوسف كافي، الإدارة الإلكترونية، إدارة بلا أوراق، إدارة بلا مكان، إدارة بلا زمان، إدارة بلا تنظيمات جامدة، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2011.

9. نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحة مرتكبي جرائم الإرهاب، مركز الكتاب الأكاديمي.

ثالثا: الرسائل الجامعية:

مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، جانفي 2017.

1. مصطفى سعد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، جانفي 2017.

رابعا: المقالات والبحوث:

1. عبد الله بن عبد العزيز بن فهد العجلان، بحث قانوني ودراسة شاملة حول الإرهاب الإلكتروني في عصر المعلومات، مقال منشور في الموقع الإلكتروني https://www.mohamah.net/law بتاريخ 2016/09/14، تاريخ الاطلاع عليه2021/02/06.

2. الساجي علام، فوزية حاج شريف، واقع الإرهاب الإلكتروني آليات مكافحته، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول.

3. ممران زهير المصري، الإرهاب الإلكتروني، مقال منشور في الموقع الإلكتروني http://www.albahethon.com/ بتاريخ 2011/10/04، تاريخ الاطلاع عليه 2021/02/08.

4. سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، العدد 08، الجزء 01، جوان 2017.

5. فوزية حاج شريف، واقع الإرهاب الإلكتروني وآليات مكافحته، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول، 2019

6. نجيب بن عمر عوينات، الإرهاب الإلكتروني المفهوم والجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث للدراسات القانونية، العدد السادس، جوان 2017.

7. رانيا سليمان، فاتن فايز، نهى الدسوقي، سياسات مكافحة الإرهاب الإلكتروني، مصر- والسعودية نموذجا، مقال منشور بالموقع الإلكتروني www.acrseg.org/41483، بتارخ 2020/02/02، اطلع عليه يوم 2021/02/09.

8. عبد الرحمان عثمان، الإرهاب الإلكتروني، أنماطه وسبل مكافحته، مقال منشور بالموقع الإلكتروني:

https://www.maspero.eg/wps/portal/home/egynews/files/sport/details/bf

بتاريخ 2016/11/26، اطلع عليه يوم 2021/02/09..

9. بن يحي الطاهر ناعوس، مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية، مقال منشور في الموقع الإلكتروني https://www.alukah.net/library/0/80823/2015/01/06 ، اطلع عليه بتاريخ 2021/02/15، ص 19، ص 20.

الجرائد:

1. محمد البشاري، الإرهاب الإلكتروني ومسؤولية المجتمع الدولي، مقال منشور في جريدة العين الإخبارية يوم الأحد 2021/2/7، متوفر في الموقع الإلكتروني https://al-ain.com/article/electronic-terrorism-and-the-responsibilit بتاريخ 2017/10/20، تاريخ الاطلاع عليه 2021/02/06.

خامسا: وثائق دولية:

1. Council of Europe: Fight against Cybercrime الموقع الالكتروني https://www.europewatchdog.info/en/international-treaties/treaties_and اطلع عليه بتاريخ 2021/02/15

سادسا: مواقع الإنترنت:

1. الإرهاب الإلكتروني، طرقه ووسائل التصدي له، الموقع الإلكتروني https://crimedz.blogspot.com/2017/06/blog-post.html، اطلع عليه بتاريخ 20121/02/14.

2. الموقع الالكتروني https://www.diplomatie.gouv.fr اطلع عليه بتاريخ 2021/02/15.