World Research of Political Science Journal
An International Journal

http://dx.doi.org/10.18576 /WRPSJ/030204

Cyberterrorism: Methods, Objectives and Coping Mechanisms

A. M. Aldada[*] *and O. Ali*

Department of International Relations Applied Science University, Bahrain.

Received: 20 Oct. 2022; Revised: 2 Nov. 2022; Accepted: 15 Nov. 2022.
Published online: 1 Dec. 2022.

Abstract : Cyberterrorism is distinguished from other types of terrorism by the modern way of using information resources and electronic means brought by the technology civilization in the information age. Therefore, electronic systems and information infrastructure are the target of terrorists. The criminal danger of terrorist groups and organizations has increased, so they have employed their energy to benefit from this technology and exploit it to complete their criminal operations and illegal purposes. The danger of electronic terrorism is increasing in developed countries, whose infrastructure is managed by computers and information networks, which makes it an easy target. In which explosives are used, where a terrorist attack can be launched to close vital sites and paralyze command, control and communications systems, or cut communication networks between units and central commands, or disable air defense systems, or derail missiles, or control air and sea navigation lines, or penetrate the banking system and harm the work of banks and financial markets.

Keywords*:* Electronic Terrorism, Terrorist Crimes, Computer Crimes, Information Network.

[*] Corresponding author E-mail: ali.aldada@asu.edu.bh

الإرهاب الإلكتروني: الأساليب والأهداف وآليات المواجهة

د.علي موسى الددا – أستاذ العلاقات الدولية المساعد – رئيس قسم العلوم السياسية – جامعة العلوم التطبيقية – البحرين

د. أسامة علي زين العابدين – أستاذ العلوم السياسية المشارك – جامعة العلوم التطبيقية – البحرين

الملخص: يتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب، بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية، التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية، هي هدف الإرهابين. لقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للإستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة. إن خطورة الإرهاب الإلكتروني، تزداد في الدول المتقدمة، والتي تدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات، تستطيع الجماعات الإرهابية، من خلال الضغط على لوحة المفاتيح، تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها التي يتم فيها استخدام المتفجرات، حيث يمكن شن هجوم إرهابي لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبحرية، أو إختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال.

كلمات مفتاحية: الإرهاب الإلكتروني، جرائم الإرهاب، جرائم الحواسيب، الشبكة المعلوماتية.

مقدمة:

أفرز عصر تكنولوجيا المعلومات وثورة الاتصالات، العديد من التطبيقات الحديثة، والتي ظهرت في الآونة الأخيرة، وأفرزت معها أوجهاً جديدة من النشاط الاقتصادي والاجتماعي والإداري والتشريعي، وتمثلت تلك الأوجه في التجارة الإلكترونية، والحكومة الإلكترونية، والتعليم عن بعد، والعمل عن بعد...الخ، كما ظهر النظام العالمي لتداول البيانات والمعلومات، وأصبحت المعرفة العلمية متاحة لكل البشر من خلال شبكة الإنترنت، وأصبح الحق فى تداول المعلومات والمعرفة، من حقوق الإنسان.

ولقد أدت سرعة تداول المعلومات، إلى تيسير الحصول على الخدمات والأعمال، وساعدت التكنولوجيا على استرجاع المعلومات واستخدامها في التعليم والإدارة والخدمات البنكية والخدمات الطبية والعلمية. وتتصف التكنولوجيا بكافة صورها، بسرعة سريانها الفائقة في المجتمعات، ودون إرادة من تلك المجتمعات، سواء كانت راغبة فيها أم كارهة لها. ومع الاستناد إلى التكنولوجيا في مناحي الحياة المتعددة، ظهر موضوع الخروج على الشرعية والنظام العام والآداب العامة، وذلك عن طريق استخدام أدوات التكنولوجيا، كوسائل يتم بها ارتكاب الجرائم، من سرقه للأموال أوتشهير وقذف، أوإضرار بالمصالح وانتهاك للخصوصية، أوتحريض على ارتكاب الجرائم ونشر الأفكار المتطرفة.

من هنا، سعت الدول الى تأمين أنفسها من خلال ما يطلق عليه "الأمن السيبراني" باستخدام التكنولوجيات ومن خلال العمليات التقنية والضوابط، الهادفة إلى حامية الأنظمة والشبكات والبرامج من الهجمات الرقمية، والتي تتضمن عادة، محاولة الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها. وبحيث يمكن أن تؤدي هذه الهجمات– في حالة نجاحها– إلى ابتزاز المال من الضحية، أو التعدي على حقوق الملكية الفكرية، أو تعطيل تقديم الخدمات.

ولعل من أخطر تلك الصور، جريمة الإرهاب الإلكتروني، والتي يتم فيها استخدام شبكة الإنترنت بهدف إيقاع اعتداء، يخلف ضرراً ما

في موقع ما. ومن هنا تظهر لنا مشكلة الدراسة التي نحن بصددها، والتي ترتكز على محاولة الإجابة على سؤالين اثنين: الأول، ماهي العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية؟ والثاني، ماهي الصعوبات التي تواجه ضبط جرائم الإرهاب الالكتروني؟

وتنطلق الدراسة من فرضية مؤداها أن الإرهاب الإلكتروني، يعتمد على التكنولوجيا المتطورة، والتي زادت من رقعة مسرح العمليات، وساهمت باتساعه بطريقة فائقة. وفي سبيل اختبار الفرضية وحل الإشكالية آثر الباحثان، استخدام المنهج الوصفي التحليلي، من خلال وصف موضوع الإرهاب الإلكتروني، وصفاً دقيقاً تعبيرياً، يساهم في اكتمال بناء محاور الدراسة، والتي تم تقسيمها الى: المقصود بالإرهاب الإلكتروني (أولاً)، ثم الانتقال الى تحليل العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية (ثانياً)، والتطرق الى أساليب وأهداف الإرهاب الإلكتروني (ثالثاً)، وانتهاءً باستعراض الصعوبات التي تواجه ضبط جرائم الإرهاب الإلكتروني وآليات مواجهتها (رابعاً).

أولاً: المقصود بالإرهاب الإلكتروني

ساعدت التكنولوجيا بمعناها الحديث، على تحقيق العديد من الإنجازات في العديد من المجالات. وهذا يستدعي افتراض أن القائمون على الإرهاب، سيسعون الى تحقيق أهدافهم من خلال أدوات تكنولوجية ملائمة، بل وافتراض أنهم يمتلكون أحياناً، معرفة تكنولوجية تضاهي معرفة وقدرات الدولة التي تواجههم1. يشير ذلك الى أنه تمت إساءة استخدام هذه التكنولوجيا، لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها، وبما يشمله ذلك، من خطر هجمات الإرهاب الإلكتروني، التي تشنها الجهات الفاعلة الإرهابية على البنى التحتية الحيوية.

كانت بداية استخدام مصطلح الإرهاب الالكتروني Cyberterrorism، في فترة الثمانينات، على يد " باري كولين Barry Collin "، والتي خلص فيها الى صعوبة وضع تعريف شامل للإرهاب التكنولوجي. ولكنه تبنى تعريفاً لهذا المصطلح، باعتباره "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"2.

وعرفه "جيمس لويس" من جهته، على أنه "استخدام أدوات شبكات الحاسوب، في تدمير أو تعطيل البني التحتية الوطنية المهمة، مثل: الطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين3". كما أشار الى أن الإرهاب الإلكتروني يتميز بصعوبة اكتشافه، أو إثباته، مع تعدد في مجالاته، وتنوع في أنشطته وممارساته[4].

1- أحمد إبراهيم محمود، الأبعاد التكنولوجية للإرهاب، مجلة السياسة الدولية، العدد 113، يوليو 1993م، ص 83

2- عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية، 2009م، ص109

3 -A .lewi ، Center for Strategic and International Studies، Cyber War and Other Cyber Threats،James, Assessing the Risks of Cyber Terrorism .December, 2002

4- قد يكون الإرهاب موجها إلى الأفراد من خلال التلصص على حساباتهم الشخصية، وسرقة المعلومات الخاصة بهم، الأمر الذي يجعلهم يقعون تحت طائلة الابتزاز من قبل الإرهابيين. وقد يكون الإرهاب الإلكتروني موجها الى المؤسسات: شركات، أو وزارات، أو دول، من خلال سرقة بيانات الشركات، أو أرصدتها، أو العبث بالبيانات الموجودة لديها، أو التلصص على بيانات الدول، والتعرف على المعلومات السرية الخاصة بها، الأمر الذي يوقعها تحت طائلة التهديد من أعدائها. وقد يكون الإرهاب الإلكتروني، من خلال ما يبث من أفكار مغلوطة وهدامة تعمل على إثارة الفتن والقلاقل في المجتمعات، ونشر الإشاعات الكاذبة.- **د.عبد الحليم منصور، الإرهاب الإلكتروني إشكالات وحلول، موقع الأهرام المسائي، 30 سبتمبر 2021م.**

https://gate.ahram.org.eg/News/2971756.aspx

أما" دورثي دينينغ Dorothy denning " فترى أن الإرهاب الإلكتروني هو "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبياً ،لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب".

ووفقا لوزارة الدفاع الأمريكية، فإنها تعرّف الإرهاب الالكتروني على أنه "عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات، ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات، بما يسبب الارتباك وعدم اليقين، وذلك بهدف التأثير على الحكومة أو السكان، لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة".

وتبعاً لإحدى وثائق حلف الناتو، فقد تم تعريف الإرهاب الإلكتروني، على أنه "هجوم بواسطة الإنترنت عن طريق استخدام أو استغلال شبكات الكمبيوتر أو الاتصالات، بما يسبب دماراً من شأنه توليد خوف وترويع المجتمع، وفقاً لهدف أيديولوجي"5.

وبقدر ما يكون الإرهاب أداة لصراع سياسي، تفرضه إمكانيات وظروف القوى التي تلجأ إليه، بقدر ما يعني أنه عند توافر ظروف مناسبة، وتوافر الإمكانيات، فإن تلك القوى ستكون على استعداد لتطوير أدواتها وأساليبها، وهذا الإرهاب منظم ومخطط له، أي أنه يعتبر جزءاً من استراتيجية ذات أهداف محددة ومعدة مسبقاً6.

وتستخدم الجماعات الإرهابية الفضاء الإلكتروني، من أجل غايات غير مشروعة، ويشتمل هذا النوع من الإرهاب، على العديد من التقنيات التي من خلالها، يتم السعي الى تحقيق هذه الغايات، مثل7: التخطيط، والتحريض، والتجنيد، وزيادة التطرف، والتمويل، والتنفيذ من خلال الهجمات الإلكترونية أو السيبرانية، والتي تستهدف بالأساس: (النظم العسكرية، والبنية التحتية الاقتصادية، ومحطات توليد الطاقة والماء، ونظم الاتصالات، ونظم المواصلات)8.

وطبقاً لما سلف يمكن أن نعرف الإرهاب الإلكتروني9 بأنه " كل فعل تستخدم فيه شبكة الحاسب الآلي، ويحقق الجاني من خلالة النتيجة المجرمة والمنصوص عليها في المواد التي تعرف الإرهاب" . فمن يدعو من خلال شبكة الإنترنت إلى تكوين جماعة محظورة، أو من يرهب المواطنين من خلال بث الرهبة والخوف في نفوسهم، أو من خلال الرسائل التي ترسل لمواقعهم أو عناوينهم الإلكترونية، يعد مرتكباً لجريمة الإرهاب الإلكتروني. وقد يتخذ الإرهاب الإلكتروني بمفهومة السابق، إحدى الصور الآتية10:

إرتكاب جرائم ماسة بسلامة وأمن الدولة، سواء من جهة الخارج أو الداخل، وذلك بغرض إرهابي وللتخويف وبث الرهبة .

5- أحمد ناصر أبو السعود، الموسوعة السياسية.

/https://political-encyclopedia.org/dictionary

6- د. أسامة الغزالي حرب، الإرهاب والسياسة الدولية، مجلة السياسة الدولية، العدد 111، 1992م، ص 6

7- د. علي الدا ود. محمود خليفة، تأثير التحولات الجديدة في مفهوم الإرهاب على العلاقات الدولية، مجلة World Research of Political Science Journal، الولايات المتحدة الأمريكية، المجلد 5، العدد 1، 2022م، ص 79

8- وجيه المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، ص148-149.

9- انظر ايضاً في تعريف الإرهاب الإلكتروني- د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات

https://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-31&Itemid=294&option=com_content

10- ريهام العباسي، أثر الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدولية، المركز الديمقراطي العربي.

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

اختراق المواقع الإلكترونية، وهنا يتم اختراق المواقع الإلكترونية، لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل في الموقع تعلن اختراقه.

إرهاب مستخدمي الحاسب الآلي، ببث الرهبة والرعب فيهم، بمعنى إرتكاب الجرائم المعلوماتية في صور تؤدي إلى إثارة الرعب والخوف بين مستخدمي شبكة الإنترنت، سواء بغلق نظم التشغيل أو إجراء هجوم إلكتروني أو بإزالة المعلومات.

الحرب الإعلامية: حيث يعد الفضاء الإلكتروني، ذو تأثير هائل على الرأي العام العالمي، ذلك أنه يخاطب ملايين المستخدمين للشبكة العنكبوتية، من شتى أنحاء العالم، بوسائل مختلفة، "الصوت– الصورة– النص"، وبالتالي فإن أي جماعة أو منظمة، يمكن لها القيام بإنشاء مواقع إلكترونية خاصة بها، تروج أفكارها من خلالها، بل وتساعدها على نشر هذه الأفكار في مختلف أنحاء العالم11.

جرائم تطوير ونشر الفيروسات، حيث أن فيروسات الحاسب الآلي، تتميز بقدرتها على الانتشار بسرعة كبيرة، عن طريق شبكة الإنترنت، وذلك راجع الى عدد الملفات الهائل الذي يتم تبادله بين مستخدمى الشبكة العنكبوتية. كما أن الفيروسات، عبارة عن برامج تستنسخ نفسها فى الجهاز، وعندما تنشط، تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها، مما ينتج عن ذلك، أضراراً مختلفة، تتمثل في فقدان الملفات المخزنة، وقد تصل تلك الأضرار الى تحطم نظام التشغيل في الجهاز.

تدمير أنظمة المعلومات، والتي تتضمن محاولة اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد، بهدف تشويش نقطة الاتصال، وتخليق أنواع جديدة من الفيروسات، التي تسبب دماراً وعطباً لأجهزة الكمبيوتر وللمعلومات التي تحتويها12.

ثانياً: العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية13

تعد شبكة الإنترنت، بمثابة عالم شديد النمو، سريع التطور، ونتيجة لذلك تغيرت النظرة الى الإرهاب الإلكتروني، والتي كانت محصورة في الأعمال التخريبية التي عرضنا لها سابقاً، لتصبح مشتملة على أنشطة أكثر خطورة، تمثلت في الاستخدام اليومي للإنترنت من قبل المنظمات الإرهابية، بهدف تنظيم وتنسيق عملياتها المتفرقة والمنتشرة حول العالم. فالوجود الإرهابي النشط على الشبكة العنكبوتية، يعد متفرقاً ومتنوعاً ومراوغاً بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم، فسرعان ما يغير نمطه الإلكتروني، ثم يختفي ليظهر مرة أخرى بعد فترة قصيرة، بشكل جديد وعنوان إلكتروني جديد.

والمواقع الإلكترونية لتلك المنظمات، لا تخاطب أعوانها ومموليها فحسب، بل توجه رسائلها أيضاً، للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول العدوة، فهي تعرض أفلاماً مرعبة للرهائن والأسرى أثناء إعدامهم، في نفس الوقت الذي تدعي فيه هذه المنظمات أنها تتبنى قضايا نبيلة، بل وتشتكي من سوء المعاملة من قبل الآخرين.

وفيما يلي نعرض الى أهم العناصرلاستخدام الإنترنت في اغراض إرهابية14:

التنقيب عن المعلومات: ينطلق هذا الغرض، من أن شبكة الانترنت تعد في حد ذاتها، مكتبة إلكترونية هائلة الحجم، تمتليء بالمعلومات

11– د. جمال علي الدهشان، الإرهاب في العصر الرقمي: صوره مخاطره آليات مواجهته، مجلة International Journal of Research in Educational Sciences، المجلد 1، العدد 3، 2018م، ص 103

12– د. هشام بشير، مرجع سابق.

13– شبكات رقمية، مصايد لاستقطاب الشباب وتنفيذ جرائم عابرة للحدود، جريدة الشعب، الجزائر، 3 –5– 2016م.

http://www.ech-chaab.com/

14– يتم استخدام الفضاء الالكترونى فى الارهاب، بصورة غير مباشرة، عن طريق تسهيل عملية تنفيذ العمل الارهابي، من خلال توفير المعلومات والحصول على التمويل، وكذلك يتم استخدامه لنشر الخوف والفزع والرعب وبث الكراهية، أو عن طريق استخدام أدوات ذات طابع إلكتروني فى الصراع، ويكون الفضاء الإلكتروني هو مسرح ذلك الصراع. هذه الأدوات يصعب الفصل بينها، بمعنى أنه قد يتم استخدام كل هذه الأدوات فى عملية واحدة، ويصعب الفصل بين الأدوات المستخدمة فيها. انظر في استخدامات الإرهاب الإلكتروني بالتفصيل– ريهام العباسي، مرجع سابق.

الهامة عن الأهداف المطلوبة، والتي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت الحيوية، والمطارات الدولية.

سهولة الاتصالات: في هذا الغرض، تساعد شبكة الإنترنت المنظمات الإرهابية المتفرقة، في الاتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظراً لقلة تكاليف الاتصال باستخدام الإنترنت، مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها. وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية، وكل ذلك بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية. وبهذا يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدد15.

التعبئة والتجنيد لإرهابيين جدد: إن استقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهي تستغل اجتذاب هؤلاء السذَّج، بعبارات براقة وحماسية، من خلال غرف الدردشة الإلكترونية16.

إعطاء التعليمات والتلقين الإلكتروني: حيث يعد الإنترنت مليئاً بكم هائل من المواقع، التي تحتوي على كتيبات وإرشادات، تشرح طرق صنع القنابل، والأسلحة الكيماوية والجرثومية الفتاكة17.

التخطيط والتنسيق: وهنا يعتبر الإنترنت وشبكات التواصل الاجتماعي، وسائل اتصال بالغة الأهمية، بالنسبة للمنظمات والخلايا الإرهابية، حيث تتيح التنسيق لشن هجمات إرهابية. كما يستخدم أعضاء الخلايا الإرهابية شبكات التواصل الاجتماعي، لتدبير الهجمات الإرهابية، وتوزيع الأدوار وتنسيق الأعمال والمهام لكل عضو في الخلية18.

الحصول على التمويل: وذلك عن طريق استعانة الإرهابيون، ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية، التي يقوم المستخدمون بإدخالها على الشبكة، من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، وذلك في سبيل التعرف على الأشخاص المناسبين لاستجدائهم بدفع تبرعات مالية لأشخاص اعتباريين، يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الإلكتروني بطريقة ماكرة، لا يشك فيها المتبرع، بأنه يساعد إحدى المنظمات الإرهابية. وبهذا يستخدم الانترنت للحصول على التبرعات، باستخدام التحويلات المالية عبر الإنترنت، وقد يتم استخدام منظمات عالمية ذات طابع إنساني أو خيري، كمظلة لتوفير التمويل أو للعمل تحت غطائها19.

ضمان عنصر السرية: يعتمد نجاح الجرائم الإرهابية، بصفة أساسية، على عنصر السرية الذي يكفل عدم اختراقه، ووسائل الاتصال الحديثة تؤدي دوراً هاماً في ضمان عنصر السرية.

خلق الإرهاب المعلوماتي: ساهمت ثورة المعلومات والاتصالات، في انتشار أنماط جديدة من الإرهاب، حيث وضعت عملية حوسبة البنى التحتية في كثير من دول العالم بين أيدي التنظيمات الإرهابية، القدرة على تحقيق أضرار اقتصادية بالغة، بدون أن تكون مضطرة للمواجهة مع الأجهزة الأمنية، وما تتخذه من إجراءات لحماية الأهداف الحيوية من الاعتداءات الإرهابية20.

15- شرقي صبرينة وغريب حكيم، الإرهاب الإلكتروني والتحول في مفهوم القوة، مجلة الباحث للدراسات الأكاديمية، المجلد 7، العدد 2، 2020م، ص 563

16- شريفة كلاع، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، المجلد 2، العدد 6، 2018م، ص 85 – وانظر أيضاً إيمان عبد الرحيم السيد الشرقاوي، جدلية العلاقة بين الإعلام الجديد والممارسات الإرهابية: دراسة تطبيقية على شبكات التواصل الاجتماعي، ورقة بحثية مقدمة في المؤتمر الدولي بعنوان دور الإعلام العربي في التصدي لظاهرة الإرهاب، أيام من 16الى 18-12- 2014م ،جامعة نايف العربية للعلوم الأمنية، الرياض، 2014م، ص 16

17- عزمي بشارة، في ما يسمى التطرف، مجلة سياسات عربية، المركز العربي للبحوث ودراسة السياسات، العدد 14 ، 2015م ، ص. 18

18- شريفة كلاع، مرجع سابق، ص 86

19- ريهام العباسي، مرجع سابق.

20- شريفة كلاع، مرجع سابق، ص 85

ثالثاً: أساليب الإرهاب الإلكتروني

يُعدُّ استخدام الفضاء الإلكتروني كوسيلة للإرهاب الإلكتروني، من قبل الجماعات الإرهابية، أخطر أنواع الإرهاب، حيث يمتد ضرره بشكل أوسع من الإرهاب التقليدي، كما يوفِّر كافة القدرات اللازمة للجماعات الإرهابية، الأمر الذي يهيء لها تحقيق أهدافها بسهولة21.

وتستخدم الجماعات الإرهابية الفضاء الإلكتروني، من أجل تحقيق العديد من الغايات غير المشروعة، بحيث يشتمل الإرهاب الإلكتروني على العديد من التقنيات، التي من خلالها تتحقق هذه الغايات، كما ورد معنا سابقاً، مثل: التخطيط، والتحريض، والتجنيد، وزيادة التطرف، والتمويل، والتنفيذ من خلال الهجمات الإلكترونية، والتي تستهدف بالأساس: (النظم العسكرية، والبنية التحتية الاقتصادية، ومحطات توليد الطاقة والماء، ونظم الاتصالات، ونظم المواصلات)22، ويمكن بلورة أساليب استخدام الجماعات الإرهابية للفضاء الإلكتروني، على النحو الآتي:

تستخدمه الجماعات الإرهابية، لتنظيم عملياتها والتخطيط لها، ويحدث ذلك من خلال استخدام التكنولوجيا الحديثة، والتي تتمثل في أحيان كثيرة باستخدام البريد الإلكتروني، والمواقع الإلكترونية، ووسائل التواصل الاجتماعي، وذلك من أجل تفادي مخاطر استخدام الأساليب الأخرى، من لقاءات مباشرة، كما أن تلك الوسائل يصعب تتبعها.23

نشر البيانات الخاصة بالجماعات الإرهابية، فضلًا عن الترويج لأيدلوجياتها، وعلاوة على ذلك نشر الأخبار الكاذبة والشائعات، من أجل التحريض على الأعمال الإرهابية والعنف والفتنة.

التجسس على المواقع وتدميرها، ويحدث ذلك من قبل مبرمجين متخصصين في اختراق المواقع الإلكترونية والشبكات، من أجل تدمير البنية التحتية المعلوماتية، للجهات الحكومية والخاصة، على حد سواء24.

الحرب الدعائية، وتستهدف غايتين، تتمثل الأولى في جذب العديد من الأفراد لها وتجنيدهم وخاصة القُصَّرَ، والثانية في الحصول على الدعم والموارد المالية25.

رابعاً: الصعوبات التي تواجه ضبط جرائم الإرهاب الإلكتروني وآليات مواجهتها

يواجه البحث عن مرتكبي جرائم الإرهاب الإلكتروني، وإقامة أدلة الإثبات عليهم وتقديمهم للعدالة للقصاص منهم، العديد من الصعوبات، خاصة في مجال الإثبات الجنائي والشرعية الإجرائية، الواجب الاستناد إلى قواعدها، حتى يتصف الدليل الجنائي بالمشروعية. ويجب أن

21- Dogrul ، Aslan and Murat،Adil،Celik and Eyyup، "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism،" 3rd International Conference on Cyber Conflict، Tallinn، P.32 , 2011 Estonia,

22 – الدسوقي وجيه المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014م، ص ص148-149.

23- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث المجلد2، العدد 7، 2018م، ص ص 56-67

24- شرقي صبرينة وغريب حكيم، مرجع سابق، ص 564

25- Weimann،Gabriel، Terror on the Internet: The New Arena، the New Challenges Washington، D.C.: United States Institute of Peace Press، 2006, pp. 37-38

تكون وسيلة الحصول على الدليل مشروعة حتى يوصف الدليل بأنه دليل شرعي، وقد يكون الدليل شرعي، إلا أن وسيلة الحصول عليه، هي التي توصف بعدم المشروعية، مما يجعل البطلان ينصرف إلى قيمة الدليل في الإثبات. ولعل من أهم الصعوبات التي تواجه ضبط جرائم الإرهاب الإلكتروني ما يلي26 :

صعوبة الوصول إلى مرتكبي الجريمة، حيث يعتمد الإرهاب الإلكتروني على التكنولوجيا المتطورة، والتي زادت من مساحة رقعة مسرح العمليات، بل واتساعه بطريقة فائقة27.

سهولة إخفاء الجريمة، وصعوبة الإثبات، حيث لا توجد أدلة مادية واضحة، كما هو الحال في الهجمات التقليدية، ويرجع ذلك الى العديد من الأسباب، مثل أن من يقوم بارتكاب الجريمة الإرهابية، يكون ذو درجة كفاءة عالية، أو بسبب ارتفاع درجة الخداع والتضليل المستخدمة28.

تعارض التفتيش عن الأدلة في الجرائم الإرهابية المعلوماتية مع الحق في الخصوصية، نظراً لكون التفتيش عن الأدلة في هذا النوع من الجرائم، لا يكون في محل محدد كالجرائم التقليدية، التي يتم فيها تحديد المكان الذي سيجرى فيه التفتيش والدليل الجاري البحث عنه، على وجه الدقة. هنا ينصب التفتيش – غالباً – على نظم الحاسب الآلي، وعلى قواعد البيانات، ونظم المعلومات وشبكاتها، مما يؤدى حتماً إلى تجاوز المشتبة فيه محل التفتيش، إلى أنظمه أخرى مرتبطة به، سواء في الشبكات الدولية أو الشبكات المحلية. بالإضافة إلى أن التفتيش عن الأدلة الرقمية، يحتاج إلى توافر خبرة فنية عالية لدى القائمين بالتفتيش .

إحجام بعض الأشخاص والهيئات والمؤسسات، عن الإبلاغ عن الجرائم الإرهابية المعلوماتية، خشية التشهير أو الإساءة للسمعة المالية للجهة، وخوفاً من فقدان الثقة في التعامل .

التعارض القائم بين تجاوز الحدود، لضبط الجرائم الإرهابية المعلوماتية، والمبادئ القانونية المعمول بها في الدول، والتي تحكم تطبيق القانون من حيث المكان، مما يجعل الحاجة ملحه لنصوص تشريعية تنظم هذا الأمر، وتحتاج إلى نوع من التعاون الدولي لمكافحة تلك الجريمة، مع الحفاظ على ثوابت السيادة الوطنية للدول، لكون تلك الجريمة من الجرائم العابرة للحدود .

إن الفراغ التنظيمي والقانوني، لدى بعض المجتمعات العالمية حول جرائم الإرهاب الإلكتروني، يعتبر من الأسباب الرئيسة في انتشار هذه الجرائم، وكذلك لو وجدت قوانين تجريمية متكاملة، فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة، ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق29.

كما أن عدم وجود جهة مركزية موحدة، تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها، يعدُّ سبباً مهماً في تفشي ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة، وكل ما تملكه الجهات التي تحاول فرض الرقابة، هو المنع من الوصول إلى بعض المواقع المحجوبة، أو إغلاقها وتدميرها بعد نشر المجرم لما يريده فيها30.

26– علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط1، بيروت، منشورات زين القانونية، 2011م، ص74

27– يعد استخدام الوسائل الإلكترونية المستحدثة اداة تساعد المجرمين على ارتكاب العديد من الجرائم بدون إمكان القبض عليهم، ومثال ذلك استخدام البريد الإلكتروني كوسيلة اتصال بين المجرمين، يتعذر معه مراقبتهم. كذلك فإن التحويلات المالية الإلكترونية، قد تتم بين الجناة، والذين قد يكونوا أفراداً أو جماعات، بغرض تمويل العمليات الإجرامية أو المخططات الإرهابية بدون أن يتم اكتشافها.– بعجي عبد النور ومالك نسيمة، الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة، مجلة الدراسات والبحوث القانونية، المجلد 7، العدد 2، 2022م، ص 72

28– د. جمال علي الدهشان، مرجع سابق، ص97

– 29 غادة نصار، الارهاب والجريمة الالكترونية، العربي للنشر والتوزيع، القاهرة، 2017م، ص82

30– انظر شعنبي صابرة، الإرهاب الإلكتروني: الأشكال والدوافع، مجلة العلوم الاجتماعية والإنسانية، المجلد 8، العدد 1، 2015م، ص 443

خاتمة

في ظل الترابط الوثيق بين أجزاء العالم، عبر تقنيات المعلومات والاتصالات والتطبيقات، التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات، بات من الضروري لكل بلد، حماية أفراده ومؤسساته ومقدراته وحضارته، من آثار هذا الانفتاح. ولقد سعت الدراسة الى بيان أساليب الإرهاب وأغراضه من خلال حل الإشكالية التي انطلقت منها، والإجابة على أسئلتها، وذلك بتحليلها للعناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية. وكذلك من خلال تحديد الصعوبات التي تواجه ضبط جرائم الإرهاب الالكتروني. كما ثبت لنا من خلال اختبار الفرضية، صحتها، وهي التي استندت الى أن الإرهاب الإلكتروني، يعتمد على التكنولوجيا المتطورة، والتي زادت من رقعة مسرح العمليات، وساهمت باتساعه بطريقة فائقة.

قائمة المراجع:

أولاً: المراجع العربية:

1- أحمد إبراهيم محمود، الأبعاد التكنولوجية للإرهاب، مجلة السياسة الدولية، العدد 113، يوليو 1993م
2- عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية، 2009م
3- د. أسامة الغزالي حرب، الإرهاب والسياسة الدولية، مجلة السياسة الدولية، العدد 111، 1992م
4- - د. علي الدا ود. محمود خليفة، تأثير التحولات الجديدة في مفهوم الإرهاب على العلاقات الدولية، مجلة World Research of Political Science Journal، الولايات المتحدة الأمريكية، المجلد 5، العدد 1، 2022م
5- وجيه المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية
6- شرقي صبرينة وغريب حكيم، الإرهاب الإلكتروني والتحول في مفهوم القوة، مجلة الباحث للدراسات الأكاديمية، المجلد 7، العدد 2، 2020م
7- الدسوقي وجيه المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014م
8- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث المجلد2، العدد 7، 2018م
9- علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط1، بيروت، منشورات زين القانونية، 2011م
10- بعجي عبد النور ومالك نسيمة، الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة، مجلة الدراسات والبحوث القانونية، المجلد 7، العدد 2، 2022م
11- غادة نصار، الارهاب والجريمة الالكترونية، العربي للنشر والتوزيع، القاهرة، 2017م
12- د. جمال علي الدهشان، الإرهاب في العصر الرقمي: صوره مخاطره آليات مواجهته، مجلة International Journal of Research in Educational Sciences، المجلد 1، العدد 3، 2018م
13- شريفة كلاع، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، المجلد 2، العدد 6، 2018م
14- إيمان عبد الرحيم السيد الشرقاوي، جدلية العلاقة بين الإعلام الجديد والممارسات الإرهابية: دراسة تطبيقية على شبكات التواصل الاجتماعي، ورقة بحثية مقدمة في المؤتمر الدولي بعنوان دور الإعلام العربي في التصدي لظاهرة الإرهاب، أيام من 16الى 18-12- 2014م ،جامعة نايف العربية للعلوم الأمنية، الرياض، 2014م.
15- عزمي بشارة، في ما يسمى التطرف، مجلة سياسات عربية، المركز العربي للأبحاث ودراسة السياسات، العدد 14 ، 2015م
16- شعنبي صابرة، الإرهاب الإلكتروني: الأشكال والدوافع، مجلة العلوم الاجتماعية والإنسانية، المجلد 8، العدد 1، 2015م

ثانيًا: المراجع الأجنبية

1- A .lewi James, Assessing the Risks of Cyber Terrorism، Cyber War and Other Cyber Threats، Center for Strategic and International Studies، December، 2002
2- Dogrul ،Murat and Aslan ،Adil، and Celik، Eyyup، "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism"، 3rd International Conference on Cyber Conflict، Tallinn، Estonia, 2011.

3- Weimann ،Gabriel، Terror on the Internet: The New Arena، the New Challenges Washington، D.C.: United States Institute of Peace Press ,2006.

ثالثاً: المواقع الإلكترونية:

1- د.عبد الحليم منصور، الإرهاب الإلكتروني إشكالات وحلول، موقع الأهرام المسائي، 30 سبتمبر 2021م.

https://gate.ahram.org.eg/News/2971756.aspx

2- د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات
https://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-31&Itemid=294&option=com_content

3- ريهام العباسي، أثر الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدولية، المركز الديمقراطي العربي

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

4- شبكات رقمية، مصايد لاستقطاب الشباب وتنفيذ جرائم عابرة للحدود، جريدة الشعب، الجزائر، 3 -5- 2016م
http://www.ech-chaab.com/