الجريمة الارهابية الالكترونية

د/ نصير لعرباوي
د/ فاتح النور رحموني

ملخص:

شكلت الثورة التكنولوجية نقلة نوعية في أسلوب حياة الأفراد والمجتمعات نحو الأفضل، من خلال الاستفادة من وسائل الاتصالات المتطورة التي أنتجتها. غير أن التوظيف السلبي لهذه الوسائل أصبح يشكل خطرا على حياة الأفراد واستقرار المجتمعات والدول، فقد أصبحت الجماعات الاجرامية والارهابية تستخدم وسائل الاتصال خاصة شبكة الأنترنت بشكل احترافي لتنفيذ والتخطيط لأعمالها الاجرامية، حيث شهدت السنوات الأخيرة استعمال مكثف للعديد من التطبيقات لنشر أفكارها والدعاية لمبادئها، وكذا تجنيد العناصر الجديدة أو تدريبها على صنع المتفجرات واستخدام الأسلحة، فضلا عن الاتصال والتخطيط للهجمات الارهابية، وهذا ما طرح تحديات كبيرة بالنسبة للحكومات والدول في مواجهة هذه الجرائم الارهابية الالكترونية الجديدة.

الكلمات المفتاحية: الجريمة، الارهاب، الجريمة الالكترونية، الارهاب الالكتروني، الجريمة الارهابية الالكترونية، الأنظمة الالكترونية.

Abstract :

Technology revolution has constituted aremarkable transition in life style of individuals and societies to the best through taking advantage of the developed mass media that it has brought. However, the negative use of this mass media has become a danger onlives of individuals as well as the stability of societies and nations. Criminal and terrorist groups are using mass media, especially Internet, in aprofessional way to accomplish and plan their criminal operations. The last years have witnessed an intense use of various applications, by these groups, to spread their ideas and make propaganda for their principals as well as enrolling new elements with them, or training them on how to make explosives and use weapons, in addition to communication and planning of terrorist attacks which have posed an enormous challenges fo r governments and nations to face these electronic new terrorist crimes.

keywords: Crime, Terror, Online Crime, Terror Electronic, Crime Terror Electronic, Electronic systems.

عنوان المقال: الجريمة الارهابية الالكترونية

مقدمة :

عرفت بعض المفاهيم والظواهر تحولات جوهرية بعد نهاية الحرب الباردة، ويرجع ذلك بالأساس الى جملة التغيرات التي شهدتها البيئة الدولية، ويمكن اعتبار الثورة التكنولوجية والمعلوماتية في مجال وسائل الاعلام والاتصال، أو ما يصطلح عليه الثورة الصناعية الثالثة، أهم هذه التغيرات والتي انعكست بدورها على العديد من المجالات الأخرى، حيث تحولت المجتمعات التقليدية الى مجتمعات رقمية تربط أفرادها علاقات افتراضية. ومن ابرز هذه المجالات الجريمة بمختلف أشكالها، حيث أصبحت الجماعات الاجرامية تستخدم مختلف وسائل الاتصال والمعلومات في هذا الاطار لتحقيق أهدافها، فاستطاعت من خلال ذلك تطوير اساليبها الاجرامية لخدمة أغراضها وتهديد أمن المجتمعات والدول، فاصبح هذا الاجرام يعرف بالجريمة الالكترونية. وقد تكون الجريمة الارهابية الالكترونية أخطر اشكال الجريمة، حيث أصبحت التنظيمات الارهابية تستخدم الأنترنت في تجنيد وتدريب العناصر الارهابية، وكذا في تنفيذها وعرضها للرأي العام. وعلى هذا الاساس تمحورت اشكالية الدراسة في **السؤال التالي: كيف وظف الارهاب الانظمة الالكترونية في تنفيذ جرائمه؟**

وتندرج تحت هذا السؤال **الاسئلة الفرعية التالية:**

- ما المقصود بالجريمة الارهابية الالكترونية ؟
- كيف توظف الأنظمة الالكترونية لتجنيد وتدريب الارهابيين؟
- كيف تعاملت التشريعات الدولية والمحلية مع الجريمة الارهابية الالكترونية؟
- ما هي أهم سبل وآليات التصدي للجريمة الارهابية الالكترونية؟

المنهج المستخدم في الدراسة:

تم توظيف **المنهج الوصفي التحليلي**، وهو منهج مناسب لتحليل الموضوع ، حيث يساعد على تقديم وصف علمي موضوعي لظاهرة الجريمة الارهابية الالكترونية، وكشف أسبابها والعوامل المختلفة المتعلقة بها، وابراز حجم خطورتها وكذا تأثيراتها وانعكاساتها على أمن الدول والمجتمعات.

خطة الدراسة: للإجابة على الاشكالية المذكورة تم اعتماد الخطة التالية:

المحور الاول: اطار مفهوماتي للدراسة.

المحور الثاني: دور الأنظمة الالكترونية في تجنيد وتدريب الارهابيين.

المحور الثالث: الجريمة الارهابية الالكترونية في التشريعات الدولية والمحلية.

المحور الرابع: سبل وآليات التصدي للجريمة الارهابية الالكترونية.

01/ اطار مفهوماتي للدراسة

أ - مفهوم الجريمة الالكترونية:

الجريمة الإلكترونية أو السيبرانية (Cybercrime) هي مصطلح حديث يتألف من مصطلحين، الأول اجرام أو جريمة (Crime) والمصطلح الثاني سيبراني أو الكتروني (Cyber)، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسوب أو

عصر المعلومات. وهي كما يصفها الدكتور طارق عبد الوهاب سليم "**الجرائم الهادئة**" التي لا تتطلب القوة أو العنف أو السلاح.[1] فالجريمة الالكترونية هي فعل غير مشروع يرتكب بواسطة نظام حاسوبي مرتبط بشبكة الأنترنيت.[2]

ورغم تعدد الميزات الايجابية لتطور وسائل الاتصال الحديثة، غير أن هذا التطور صاحبه من جهة ثانية توظيف مكثف لهذه الوسائل في مجال الجريمة بمختلف أنواعها، فأصبحت بذلك الجريمة الالكترونية ظاهرة اجرامية جديدة وسمة بارزة في بداية القرن الواحد والعشرين، وتتميز بالعديد من الخصائص التي تجعلها مختلفة عن الجرائم التقليدية، حيث أن المجرمون في هذا المجال أو كما يسمون "**الهاكرز**" يتميزون بالذكاء في استخدام وسائل تقنية متطورة، وتنفيذ جرائمهم بكل دقة وسرية بعيدا عن الخطر والمتابعات الأمنية والقضائية، سواء في عمليات ارسال الفيروسات المخربة للأنظمة والمواقع، أو سرقة الأموال والسطو على المصارف وتحويل الأموال، أو سرقة البيانات المهمة أو اتلافها. كما تتميز الجريمة الإلكترونية بالسرعة في التخطيط والتنفيذ، وبجهد وتكاليف أقل بكثير من الجهد والأموال الكبيرة التي كانت تنفق في تنفيذ الجرائم التقليدية، اضافة الى أنها تتخطى قدرات الدولة وحدودها السيادية فيمكن تنفيذها من الخارج وفي أي منطقة من العالم، فالجريمة الإلكترونية أقرب الى مفهوم الجريمة الدولية أكثر منها الى مفهوم الجريمة المحلية.

ب – مفهوم الارهاب:

في اللغة العربية مصطلح ارهاب مشتق من الفعل "رهب" بمعنى خاف وفزع ورعب وهي مصدر للفعل "أرهب"، وأرهبه بمعنى خوفه، وفي المعاجم العربية القديمة عرف الفعل "رهب" يرهب رهبة ورهبانا، أي خاف ورهبه أي أخافه وأفزعه، والرهبة هي الخوف والفزع والرعب، يقال هو راهب من الله تعالى: أي يخاف من عقابه، وأرهبه أي توعده، والرهبوت تعني "الخوف العظيم"، قال تعالى في سورة الأعراف الآية مئة وستة عشر "واسترهبوهم وجاءوا بسحر عظيم"، أي: استدعوا رهبتهم وأرهبوهم – ورهبه أي أخافه وأفزعه.[3] ويعتبر جناية اجتماعية وسياسية، يكون تنفيذها أو التعبير عنها بمختلف الوسائل طريقا لنشر الفزع العام وعدم الاستقرار في المجتمع والنظام السياسي، فالإرهاب خطر حقيقي يهدد أمن الفرد والمجتمع والدولة. وعرفها سكيميد (schmid's) بأنه "طريقة لإثارة البلبلة والاضطراب عن طريق العنف، المستخدم بواسطة فرد أو جماعة أو دولة أو ممثلين سريين، ويكون هذا العنف لأسباب سياسية أو خاصة ، فالضحايا هم الأهداف المباشرة للعنف، ولكنهم ليسوا الأهداف الرئيسية ، ويكون هؤلاء الضحايا مختارين بشكل عشوائي من السكان، وهذا يحمل رسالة معينة، فالعنف والتهديد والتخـــويف ما هما إلاّ وسيلة لاتصال المنظمات الإرهابية بالإعلام، والضحايا هنا هم الجمهور الذين تحولوا الى أهداف، ولكنهم في الحقيقة وسيلة وليس غاية.[4] وأخذ الارهاب في نهاية القرن العشرين البعدين السياسي والدولي ، فاصبح وسيلة أساسية لتحقيق الأهداف السياسية(الارهاب السياسي)، كما أصبح

[1] - طارق عبد الوهاب سليم، **الجرائم المرتكبة بواسطة الأنترنت وسبل مكافحتها**، تونس (د.د.ن)، ط 1، 1997، ص 150.

[2] –سمير ابراهيم جميل العزاوي، "**المسؤولية الجنائية الناتجة عن استخدام الأنترنت**" ، رسالة ماجستير، كلية القانون جامعة بغداد، 2005، ص 09.

[3] – علي بن عبد العزيز بن علي العميريني ، **مفهوم الارهاب في الفقه الاسلامي والقانون الوضعي** (جزء01) ، الرياض : مكتبة عبد العزيز العامة ، ط1 ، 2007 ، ص ص67،68.

[4] - Joseph S. Tuman, **CommunicatingTerror (the RhetoricalDimonsions of Terrorism)** , San Francisco: SAG Publications , p 13.

أيضا يحمل الطابع الدولي (الارهاب الدولي) حيث تجاوز نشاط الجماعات الارهابية الحدود السيادية للدولة، وهذا ما جعل منه جريمة دولية وليست داخلية فحسب.

شهدت السنوات الأخيرة نوعا جديدا من الجرائم الارهابية، وبالأحرى تحولا نوعيا في أساليب وأدوات تنفيذ الجرائم الارهابية، على غرار اختطاف الطائرات المدنية وتفجيرها، واستخدام المتفجرات والأحزمة الناسفة، وتخريب شبكات الاتصال ومواقع الأنترنت الخاصة بالمصالح الأمنية، أو استخدامها لتجنيد عناصر جديدة ونشر الفكر الجهادي والتكفيري، وحتى تنفيذ هجمات ارهابية فائقة الدقة. حيث أصبح امتلاك الدولة لوسائل التكنولوجيا والمعلومات من أهم عناصر القوة في السياسة الدولية، ويكتسي أهمية أكثر من القوة العسكرية والاقتصادية، وذلك في ظل التطور الكبير في وسائل الاجرام واستخدامها بكفاءة عالية من طرف الارهابيين، وهذا ما يؤكده المفكر الأمريكي جوزيف ناي (Joseph Nye).[5]

ت – مفهوم الارهاب الالكتروني:

المقصود بالإرهاب الالكتروني هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.[6] فالإرهاب الالكتروني في دوافعه لا يختلف عن الارهاب، حيث تبقى الدوافع السياسية المحرك الأساسي لهذا النشاط الاجرامي، غير أن وسائله تختلف عن الارهاب التقليدي من خلال استخدام وسائل متطورة كنظم المعلومات والوسائل التكنولوجية والرقمية المتطورة، خاصة في ظل الاستخدام الواسع لهذه الوسائل في مختلف مجالات الحياة، وقد تكون خطورتها أكبر بالنسبة للشركات الاقتصادية الكبرى والبنوك ونظم المعلومات التابعة للأجهزة الأمنية للدول، وبالتالي فان ضرر الارهاب الالكتروني يتجاوز بكثير الضرر الذي يخلفه الارهاب التقليدي.

تتضاعف خطورة الارهاب الالكتروني اذا نظرنا الى سهولة استخدام هذا السلاح، حيث يقوم الارهابي بعمله التخريبي من منزله أو غرفته في الفندق أو من مقهى عمومي، وهذا ما جعل هذا النوع من الارهاب هاجسا حقيقيا، فكل منطقة من العالم أصبحت عرضة لهجمات الارهابيين عبر الانترنت.[7] ورغم سعي العديد من الدول لمواجهة وتفادي ضرر هذه الهجمات الارهابية، الا أنها لا تزال بعيدة عن المستوى المطلوب وتعتبر اعتداءات 11 سبتمبر 2001 دليلا على عجز الأنظمة الأمنية للدول الكبرى على كشف مختلف المخططات الارهابية سواء كانت عن طريق الأنترنت أو من خلال طرق ووسائل مشابهة.

ث – مفهوم الجريمة الارهابية الالكترونية:

هي نوع من الارهاب الحديث الذي وظف واستثمر تقنيات المعلومات والاتصال بشكل يلائم متطلباته وأهدافه، وذلك بغرض اثارة الخوف وزعزعة استقرار المجتمعات، فهو يعتد في تنفيذ والتخطيط للعمليات الاجرامية الارهابية على وسائل الاتصال الالكترونية، فخلال العقدين الأخيرين اصبحت التنظيمات الارهابية تعتمد في نشاطها على هذه الوسائل الالكترونية بشكل مكثف، وهو ما انتج شكل جديد من الارهاب وهو ما أطلق عله الجيل الثاني من الارهاب أو الإرهاب الالكتروني وهو "العدوان أو التخويف أو التهديد ماديا أو معنويا، باستخدام الوسائل الالكترونية الصادرة عن الدول والجماعات أو الأفراد عبر الفضاء

---

[5] – ريهام مقبل ، " **مركب القوة – عناصر وأشكال القوة في العلاقات الدولية** " ، ملحق مجلة السياسة الدولية ، العدد 188 ، المجلد 47 ، أفريل 2012 ، ص 07

[6] - بن يحيى الطاهر ناعوس، **"مكافحة الارهاب الالكتروني ضرورة بشرية وفريضة شرعية"**، متوفر على الرابط http://www.alukah.net/library/0/80823/ تاريخ الدخول الى الموقع 2017/12/13

[7] - نفس المرجع.

الالكتروني، أو أن يكون هدفا لذلك بما يؤثر على الاستخدام السلمي له".[8] ويعرفه جميل عبد الباقي أيضا بأنه: "ذلك النوع من الارهاب الحديث الذي يعتمد بصورة كلية على استخدام كل الوسائل والامكانيات العلمية والتقنية لشبكات الانترنت وشبكات الاتصالات المعلوماتية، في سبيل ادخال الخوف والرعب والحاق الضرر بالأفراد أو الجماعات المدنية أو المؤسسات الحكومية".[9] ومنه فقد أصبح هذا النوع من الارهاب شكل جديد من أشكال الجريمة الالكترونية في بداية القرن الواحد والعشرين، وقد تناولت العديد من الدراسات هذا الموضوع، ومن بينها في الجزائر دراسة (مقال) للأستاذة فضيلة عاقلي تحمل عنوان "الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، ودراسة لياسمينة بونعارة تحمل عنوان "الجريمة الالكترونية".

ان تطور وسائل الاتصال وشبكات المعلومات ومختلف الامكانيات العلمية والتقنية، جعل استغلالها في تنفيذ العمليات الارهابية أكثر سهولة خاصة وأنها تتميز بالدقة والسرعة والخطورة، حيث يمكن تنفيذها على الأهداف الحكومية بدقة كبيرة تقل فيها نسبة الخطأ، وذلك بفضل التوجيه والتحكم في وسائل نقل المتفجرات والاتصال بين العناصر الارهابية أثناء عملية التنفيذ بوسائل اتصال جد متطورة، كما أن استهداف تدمير وتخريب البنية التحتية لشبكة المعلومات الحكومية أو العامة للمؤسسات الاقتصادية والشركات، قد يتم بسرعة فائقة ويكلف خسائر كبيرة جدا تتجاوز الخسائر التي تكون نتيجة العمليات الارهابية بالشكل التقليدي، والأخطر من كل ذلك أن الجماعات الارهابية قد تنفذ هذه العمليات وهي في أماكن بعيدة وآمنة عن الشرطة. فقد أصبحت فواعل الى جانب الدول فبإمكانها تهديد أمن الدول وتغيير مجرى الأحداث الدولية، فهذه الأخيرة لم تعد اللاعب الوحيد في العلاقات الدولية، ومنه لم تعد تتمتع بالسيادة المطلقة مثلما كانت سابقا.[10]

لقد أصبحت التنظيمات الارهابية في السنوات الأخيرة تمتلك قدرات كبيرة في توظيف الوسائل التكنولوجية، حتى أصبح استخدام مصطلح "**الارهاب التكنولوجي** " موضوعيا الى أبعد الحدود، كما توضح الدراسة التي نشرها –**مركز الأبحاث لدراسات الصراع والارهاب**– في لندن بعنوان: "**التكنولوجيا والارهاب: التهديد الجديد للألفية الجديدة**" والتي كتبها كل من –**ستيفن أرباورز** –و**كمبرلي أركيز**، حيث أكدت هذه الدراسة أن التنظيمات الارهابية أصبح بإمكانها حاليا الحصول على كل ما تريد من معلومات عبر الاستخدام المقنن للكمبيوتر، ومن خلال استغلال ثغرات شبكات المعلومات أو باللجوء الى عمليات القرصنة المعلوماتية والدخول الى بنوك المعلومات العسكرية والأمنية للدول، واستغلالها في التخطيط للعمليات الارهابية، كما يمكنها ايضا الدخول الى شبكات البورصة والأسواق المالية وتدميرها بقصد المساس بالقوة الاقتصادية للدول المستهدفة.

02/ دور الأنظمة الالكترونية في تجنيد وتدريب الارهابيين:

أ – العوامل المساعدة على توظيف الارهاب للأنظمة الالكترونية :

ساهمت بعض **العوامل** في نجاح التنظيمات الارهابية في استغلال الأنظمة الالكترونية والمعلوماتية لتنفيذ أهدافها الاجرامية ومن أهمها:

---

[8] – عادل عبد الصادق، **الارهاب الالكتروني نمط جديد وتحديات مختلفة** ، المركز العربي لأبحاث الفضاء الالكتروني، 2013 .

[9] – حسن تركي عمير ، "**الارهاب الالكتروني ومخاطره في العصر الراهن**"، مجلة العلوم القانونية والسياسية، جامعة ديالي، عدد خاص ص327.

[10] - Thomas Quiggin, **Seeing the Invisible National Security Intelligence in an Uncertain Age**, London World ScientificPublishing, 2007. p13.

- الانفتاح الذي تتميز به أنظمة المعلومات عموما والانترنيت على وجه الخصوص، حيث أنها متاحة لكل من يرغب في دخول عالمها واستعمالها، فالبنية الخاصة بالشبكة المعلوماتية تفتقد للقيود والحواجز والرقابة الأمنية، وهي الثغرة التي تتسلل من خلالها التنظيمات الارهابية لتحقيق أهدافها التخريبية.
- صعوبة تحديد هوية وملاحقة مرتكبي الجـريمة الارهابية الالكترونية، وهذا ما يسهل ويؤمن العمل الاجرامي.
- سهولة التواصل بين العناصر الارهابية والتخطيط لتنفيذ الجريمة دون الحاجة للاجتماع في مكان واحد مما يعرضها للخطر، ودون تكاليف مادية كبيرة فهي لا تتطلب موارد مالية ضخمة مثل العمليات الارهابية التقليدية.
- سهولة استخدام شبكة المعلومات والدخول اليها في أي منطقة من العالم، فهي تتجاوز الحدود الجغرافية للدول ويمكن تنفيذها من دولة بعيدة وبهوية وهمية أو انتحال شخصية غير موجودة أصلا.
- ضعف التشريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول، خاصة في البلدان النامية مثل ما هو الحال بالنسبة للجزائر، فتطور الجريمة الإلكترونية بشكل سريع لم يسايره تطور التشريع وآليات اثبات وقوع هذه الجريمة.

الأمر الذي يفسر تنامي وتزايد التنظيمات الارهابية في هذا المجال، حيث أصبح نشاط الجماعات الارهابية على شبكة الأنترنت مكثف ومؤثر بشكل كبير في توجيه نشاطاتها الاجرامية، سواء في التواصل بين فروعها وخلاياها، أو في تنفيذ جرائم التخريب ضد المواقع الحكومية أو التجسس عليها، أو حتى في تجنيد العناصر الجديدة في صفوفها ونقل رسائلها التهديدية، وفي هذا الاطار نشرت قناة DW الألمانية بتاريخ : 2006/10/15 تقريرا يؤكد وجود حوالي 4500 موقع إلكتروني على الشبكة العنكبوتية له نشاطـــات ذات طابع ارهابي، كما تشير احصائيات أخرى بوجود نفس الرقم (4500) موقع الكتروني يعمل على تضليل العقول ونشر الفكر التكفيري والجهادي.[11]

وتوفر شبكة الأنترنيت كل المعلومات الثمينة التي يحتاجها الإرهابيين لتنفيذ أعمالهم الاجرامية، مثل مواعيد الرحلات الجوية، وتحديد أماكن مراكز توليد وتوزيع الطاقة الكهربائية، والمواقع الرئيسية للتحكم في أنظمة الاتصالات والمعلومات، ومواقع المنشآت النووية وغيرها من المواقع والمراكز الحساسة.

ب – وسائل تنفيذ الجريمة الارهابية الالكترونية:

تعتمد الجريمة الارهابية الالكترونية على ثلاث **وسائل أساسية:**[12]

-**خدمة البريد الإلكتروني:** البريد الالكتروني (E-mail) هو خدمة تسمح بإرسال الرسائل وتبادل المعلومات عبر شبكة الأنترنت في أي منطقة من العالم، وتستخدم بشكل كبير في قطاع الأعمال كونها أكثر سرعة وسهولة في ايصال الرسائل، غير أنها أصبحت أيضا من أهم الوسائل التي تستخدمها التنظيمات الارهابية في التواصل بين الارهابيين وتبادل المعلومات والتخطيط للعمليات الارهابية الالكترونية من بلدان مختلفة، كما تستخدم لنشر أفكـــار التنظـيم والترويج لها، وتم

[11] – إبراهيم فؤاد عباس ، **الارهاب (المعالجة –المواجهة –الظاهرة)**، القاهرة : دار الكتب العلمية للنشر والتوزيع، ط1 ، 2008 ، ص ص 170، 171 .

[12] – سعد عطوة الزنط ، "**الارهاب الإلكتروني واعادة صياغة استراتيجيات الأمن القومي**" ، أعمل مؤتمر دولي بعنوان: الجرائم المستحدثة –كيفية اثباتها ومواجهتها" المركز القومي للبحوث الاجتماعية والجنائية، المنعقد بالقاهرة في 15 و16 ديسمبر 2010.

استخدامها أيضا في اختراق البريد الكتروني للموظفين الحكوميين أو رجال الأمن والاطلاع على معلوماتهم وبياناتهم والتجسس على مراسلاتهم والاستفادة منها في عملياتهم الارهابية.

-**استحداث مواقع على الأنترنت**: تقوم التنظيمات الارهابية بإنشاء مواقع وصفحات على شبكة الانترنت، تكون بمثابة نافذة على العالم لنشر أفكارهم والدعوة لمبادئهم من اجل كسب أكبر قدر ممكن من المجندين والمتعاطفين، ومن جهة أخرى وسيلة تساعد عناصرهم في القيام بتنفيذ عمليات ارهابية من خلال تعليمهم طريقة صنع المتفجرات والتحكم في تفجيرها عن بعد وكيفية اختراق وتدمير المواقع الالكترونية ونشر الفيروسات، وطرق اختراق البريد الالكتروني وغيرها، وبالتالي فهي طريقة لتبادل الأفكار والآراء والمعلومات بين الارهابيين دون الحاجة الى الاجتماع في قاعة واحدة وتعريض أنفسهم لخطر أجهزة الأمن، وهي أيضا طريقة مباشرة وسريعة للاتصال بالعالم الخارجي وتنفيذ نشاطهم أو توسيعها.

-**اخراق وتخريب المواقع الالكترونية**: ويقصد بها الدخول غير المشروع الى نقطة ارتباط أساسية أو فرعية متصلة بشبكة الانترنت، وذلك بهدف تخريبها من خلال الثغرات المتعددة في التطبيقات، وتستخدمها التنظيمات الارهابية غالبا لتخريب الأنظمة الأمنية أو أنظمة الاتصالات، وذلك من أجل افشال عمليات المراقبة والتتبع التي تفرضها الأجهزة الحكومية لكشف مخططاتهم، وتتبع اتصالاتهم ومشاريعهم أو أماكن تحركهم وغيرها...

ت – توظيف الأنظمة الالكترونية لتجنيد وتدريب الارهابيين:

أصبح الارهاب يوظف الأنترنت لتجنيد وتدريب العناصر الارهابية، وذلك من خلال بث الأفكار والخطابات المظللة بطرق وأساليب ذكية ومغرية، وتغليط الشباب المتحمس ببعض الفتاوى المحرضة واثارة مشاعر الغيرة والتعصب للقيم والمبادئ الدينية، واعتماد بعض الأساليب الخاطئة في نشر سير السلف الصالح، خاصة ما تعلق منها بالجهاد وتأويلها بطرق مختلفة، وأيضا في المقابل استخدام أساليب تحريضية ضد الحكومات وسياساتها، والدعوة الى الخروج عليها ومحاربتها بالأسلحة والمتفجرات، وذلك حسبهم لعدم جدوى الوسائل السلمية للتغيير. وتمنح شبكة الانترنت تأمين عمليات الاتصال والتخفي، وذلك عن طريق مختلف المواقع والبريد الالكتروني وغرف الحوار الالكتروني ومنتديات الدردشة وغيرها من التطبيقات، التي تسمح لهم بوضع رسائل مشفرة تحميهم من الرقابة والتتبع الأمني.

فقد أصبح استخدام التنظيمات الارهابية للأنترنت بشكل مكثف في اطار نشر ثقافة الارهاب والترويج لها، وتوظيف كل الأفكار والمبادئ والفلسفات التي تصب في تحقيق هذا الهدف، فتعمل على تكوين قاعدة فكرية تضم كل من لهم استعداد للانخراط في الأعمال الارهابية، وتعمل على تجنيدهم وتحضيرهم نفسيا لتنفيذ عمليات ارهابية في المستقبل. وتمر عملية التجنيد بأربع **مراحل** أساسية هي:

- **مرحلة العزل** : وتقوم على استراتيجية عزل العنصر المستهدف للتجنيد عن محيطه من الأصدقاء والأقارب، فتعطى له نصائح وتعليمات عبر الانترنت لمقاطعة الجميع والاتصال الدائم بالتنظيم.
- **مرحلة الملازمة** : وتعتمد على ملازمة المجند للتنظيم وتعزيز الانتماء له واعلانه عضوا مهما ومؤثرا في التنظيم، وحثه على تبني بعض الشعارات الخاصة بالتنظيم وترديدها باستمرار، واقناعه بمشروع التنظيم الذي حسبهم يهدف لإنهاء الاستبداد السياسي والتدخل الأجنبي واقامة الحكم الاسلامي، مع العمل على اقناعه بأن يكره ويكفر كل من هو خارج التنظيم.

- **مرحلة المشاركة** : حيث يقدم التنظيم مطالب صغيرة للمجند لاختبار انتمائه، كبعض المهمات الثانوية.
- **مرحلة الانخراط العملي** : يطلب من المجند اعلان انتمائه الى التنظيم عن طريق وسائل التواصل الاجتماعي أو على وسائل الاعلام، وهي المرحلة التي تجعله غير قادر على التراجع عن الالتزام تجاه التنظيم.

وقد نجح في هذا الاطار كل من تنظيم القاعدة وتنظيم الدولة الاسلامية في العراق والشام "**داعش**" في تجنيد عدد كبير من العناصر من خلال الدعوة على الأنترنت، فالتنظيم الأول يضم قسما خاصا بالمعلومات يمثل شركة اعلام نشطة جدا تسمى "**شركة السحاب**"، أما التنظيم الثاني فيعمل من خلال خلايا للإعلام توظف قناتي "**الفرقان**" و "**الفجر**" والعديد من الشركات الاعلامية المستقلة الأخرى، التي تبث الرسائل التي يتبنى فيها التنظيم مسؤوليته عن العمليات الارهابية.[13]

كما يستخدم تنظيم القاعدة العديد من الأساليب كاستخدام مقاهي الأنترنت لإرسال المواد الإعلامية والدعائية دون تمكن مصالح الأمن من القبض على عناصره، فيقوم العناصر المكلفين بذلك بالتنقل الى مقاهي أنترنت تكون بعيدة جدا عن مقار سكناهم، ويقومون بإرسال هذه الرسائل في شبكة الأنترنت عبر هذه المقاهي، مع الحرص على أن لا تتجاوز مدة مكوثهم بالمكان أكثر من 05 دقائق، ثم مغادرة المكان فورا، حتى لا يقعوا في قبضة أجهزة الأمن.[14]

من جهة اخرى أتاحت شبكة الانترنت للتنظيمات الارهابية أسلوبا جديدا من التدريب النمطي لأفرادها، فعوض اقامة معسكرات تدريب قابلة للاكتشاف من طرف الأجهزة الأمنية، أصبحت تقوم باستغلال شبكة الانترنت في تقديم تدريب نوعي لعناصرها، حيث أن الاطلاع على بعض المواقع يتيح لنا اكتشاف الكم الهائل من المعلومات المتعلقة بكيفية عمل المتفجرات واستخدام مختلف أنواع الأسلحة، وطريقة صناعة المتفجرات، والتدريب على العديد من طرق القتل المختلفة.[15] فقد أصبحت التنظيمات الارهابية في السنوات الأخيرة تقدم دروسا على الانترنت تعتبر بمثابة ميدان للتدريب، وذلك من خلال نشر كتيبات عن أنواع الأسلحة وطرق استخدامها، وتقديم دورات في طرق صنع المتفجرات وارشادات حول كيفية صناعتها محليا في المنازل، وموضوعات أخرى ذات صلة على غرار مجلة "**معسكر البتار**" التابعة لتنظيم القاعدة ذات الطبيعة العسكرية، والمنشورة على الأنترنت من طرف "**جماعة المقاتلين في الجزيرة العربية**".[16] وهناك أيضا العديد من المواقع الأخرى التي تعتبر نوافذ اعلامية لهذه التنظيمات الارهابية، مثلما هو الحال لموقع "**النداء**" الذي استخدمه تنظيم القاعدة بعد أحداث 11 سبتمبر 2001 لإصدار بياناته الاعلامية، أو "**صوت الجهاد**" الذي يستخدمه تنظيم القاعدة في جزيرة العرب.

03/ الجريمة الارهابية الالكترونية في التشريعات الدولية والمحلية:

دعت منظمة الأمم المتحدة الدول الأعضاء في مؤتمرها الثامن المتعلق بمنع الجريمة، الى ضرورة اتخاذ اجراءات فعالة لمحاربة الجريمة الارهابية الالكترونية، وذلك من خلال العمل على تحديث القوانين والتشريعات من جهة، وتفعيل التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من جهة ثانية، وذلك في ظل مراعاة حريات وحقوق الانسان الأساسية واشراك المجتمع المدني

---

[13] – هشام الهاشمي، **عالم داعش – من النشأة الى اعلان الخلافة**، لندن : دار الحكمة للنشر والتوزيع، ط1، 2015 ، ص ص 88 ، 89.

[14] – نفس المرجع، ص81.

[15] – عدنان هاشم سلطان، **صناعة الارهاب**، مصر: المكتب المصري الحديث ، ط1 ، 2008 ، ص131.

[16] – هشام الهاشمي، مرجع سابق، ص 88.

في محاربة هذه الجرائم، وتدعم هذا المؤتمر باتفاقية أخرى عقدتها هيئة الأمم المتحدة سنة 2000، والتي حملت عنوان "مكافحة اساءة استعمال التكنولوجيا لأغراض إجرامية".[17] والذي أكدت خلاله على الحاجة لتعزيز التعاون والتنسيق بين الدول في مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية أو ارهابية. أما على مستوى الدول فتعتبر السويد أولى الدول التي وضعت قوانين لمحاربة الجريمة الالكترونية وذلك سنة 1973.[18] وتبعتها الولايات المتحدة الأمريكية وبقية الدول الأوروبية تدريجيا، حيث طورت الدول الأوروبية تشريعاتها تماشيا مع تطور الجريمة الالكترونية، ثم مع ظهور الجريمة الارهابية الالكترونية.

تأخر اهتمام الجزائر بالتشريع لمواجهة الجريمة الارهابية الالكترونية نسبيا مقارنة بالدول الأوروبية، وقد يعود ذلك الى محدودية استخدام الأنظمة الالكترونية، سواء على مستوى المؤسسات الخاصة والعمومية أو على مستوى الأفراد، حيث جرم القانون الجزائري الجريمة الالكترونية (دون وصفها أو ربطها بالإرهاب) في المادة 394 من قانون العقوبات (بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156)، فنصت هذه المادة على تعرض "كل من يدخل أو يبقي عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك"، للحبس من ثلاثة أشهر الى سنة وبغرامة مالية من 50.000 دج الى 100.000 دج، وتضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.[19]التدقيق في الفقرات السبعة لهذه المادة من قانون العقوبات الجزائري يظهر لنا بأن المشرع الجزائري قام بتجريم جرائم المعلومات دون مختلف الجرائم الالكترونية الأخرى بما فيها الجرائم الارهابية الالكترونية، وقد يعود ذلك الى الاستخدام المحدود جدا للعناصر الارهابية في الجزائر للأنظمة الالكترونية، فالجماعات الارهابية في الجزائر لا زالت تعتمد على وسائل تقليدية أقرب الى الوسائل المستخدمة في العشرية السوداء، وهذا خلافا لبقية التنظيمات الارهابية الأخرى في العالم.

04/ سبل وآليات التصدي للجريمة الارهابية الالكترونية:

- تعتبر السبل القانونية المتمثلة في التشريعات الدولية والعمل على تطويرها بما يتناسب مع تطور الجريمة الارهابية الالكترونية من بين اهم سبل وآليات التصدي لهذه الجريمة، وقد تم تناولها في العنصر السابق فلا داعي لإعادة ذكرها هنا.
- اعادة النظر في طرق ومناهج عمل الشبكة المعلوماتية، وخلق أنظمة مراقبة ومتابعة متطورة للقضاء على ظاهرة الجريمة الارهابية الالكترونية او الحد من خطورتها.
- تطوير التشريعات القانونية باستمرار، وذلك لمواكبة التطور المستمر للجرائم الارهابية الالكترونية وتماشيا مع تطور استخدام مختلف تقنيات التكنولوجيا الحديثة.
- استخدام نفس الأساليب التي تعتمدها التنظيمات الارهابية في هذا المجال، مثل التجسس والقرصنة واختراق المواقع واستخدام العملاء وغيرها...
- التواصل عبر شبكة الانترنت مع هؤلاء المجرمين والحوار معهم بغرض اقناعهم لتغيير مبادئهم وأفكارهم، فالحوار كما يعتبره (Jacques Bourrinet) وسيلة ونداء للعمل العقلاني السلمي الهادف الى تغيير الوضع نحو الأحسن.[20]

---

[17] - اتفاقية هيئة الأمم المتحدة، رقم 55/63 - 2000 ، حول **مكافحة اساءة استعمال المعلومات لأغراض إجرامية**، ديسمبر 2000.

[18] - عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، القاهرة: دار النهضة العربية، ط1، 2002، ص 308.

[19] - قانون العقوبات الجزائري، معدل - صادر سنة 2012.

[20]- Jacques Bourrinet ,**Le Dialogue Euro-Arabe**, Paris :Economica, 1979 , p p 16-17.

- تطوير أنظمة التكوين والتدريب والتوعية بالنسبة لفئة الشباب، من أجل تفادي استغلالهم من طرف المجرمين على شبكة الأنترنت.
- استخدام وسائل الاعلام لنشر ثقافة التبليغ لدى المواطنين على كل حالات الاستخدام غير القانوني أو الأخلاقي لشبكة الانترنت خاصة في الأماكن العمومية مثل مقاهي الأنترنت.

الخاتمة :

في النهاية يمكن القول أن التطور الذي شهدته الجريمة الارهابية الإلكترونية، جعل منها شكلا جديدا من الجرائم التي تختلف اختلافا جذريا عن بقية أشكال الجريمة الأخرى التي عرفها التاريخ، فهي تهديدات أمنية خطيرة جدا غير ظاهرة وغير ملموسة بإمكانها احداث انهيار في الاقتصاد العالمي، وهذا ما أصبح يطرح تحديات كبيرة بالنسبة للمجتمعات والدول على حد سواء، ويتطلب ضرورة تطوير سبل وآليات التصدي لها، فدور الدولة وحده أصبح غير كافي في ظل اتساع دائرة هذا النوع من الجريمة، وهو ما يتطلب تعاون وتحالف على المستوى الدولي بين الدول والمنظمات الدولية هذا من جهة، ومن جهة ثانية تعاون على المستوى المحلي بين الأجهزة الأمنية للدولة ومنظمات المجتمع المدني والمواطنين، كما أنه من الضروري العمل على تطوير التشريعات القانونية الدولية لمعاقبة مثل هذه الجرائم، وتطوير الوسائل والآليات الرقابية على استخدام الأنظمة الالكترونية بصفة عامة.

قائمة المراجع:

1 - طارق عبد الوهاب سليم، **الجرائم المرتكبة بواسطة الأنترنت وسبل مكافحتها**، تونس (د.د.ن)، ط 1، 1997، ص 150.

2 - سمير ابراهيم جميل العزاوي، "**المسؤولية الجنائية الناتجة عن استخدام الأنترنت**" ، رسالة ماجستير، كلية القانون جامعة بغداد، 2005، ص 09.

3 - علي بن عبد العزيز بن علي العميريني ، **مفهوم الارهاب في الفقه الاسلامي والقانون الوضعي** (جزء01) ، الرياض : مكتبة عبد العزيز العامة ، ط1 ، 2007 ، ص ص 101،102.

4- Joseph S. Tuman, **Communicating Terror (the Rhetorical Dimonsions of Terrorism)** San Francisco: SAG Publications , p 13.

5 – ريهام مقبل ، " **مركب القوة – عناصر وأشكال القوة في العلاقات الدولية** " ، ملحق مجلة السياسة الدولية ، العدد 188 ، المجلد 47 ، أفريل 2012 ، ص 07 .

6 – بن يحي الطاهر ناعوس، "**مكافحة الارهاب الالكتروني ضرورة بشرية وفريضة شرعية**"، متوفر على الرابط http://www.alukah.net/library/0/80823/ تاريخ الدخول الى الموقع 2017/12/13

7 – نفس المرجع.

8 – عادل عبد الصادق، **الارهاب الالكتروني نمط جديد وتحديات مختلفة** ، المركز العربي لأبحاث الفضاء الالكتروني، 2013 .

9 – حسن تركي عمير ، "**الارهاب الالكتروني ومخاطره في العصر الراهن**"، مجلة العلوم القانونية والسياسية، جامعة ديالي، عدد خاص ص327.

10- Thomas Quiggin ,**Seeing the Invisible National Security Intelligence in an Uncertain Age**, London World Scientific Publishing, 2007. p13.

11 إبراهيم فؤاد عباس ، **الارهاب (المعالجة –المواجهة –الظاهرة)**، القاهرة : دار الكتب العلمية للنشر والتوزيع، ط1 ، 2008 ، ص ص 170، 171.

12 سعد عطوة الزنط ، "**الارهاب الإلكتروني واعادة صياغة استراتيجيات الأمن القومي**" ، أعمل مؤتمر دولي بعنوان: الجرائم المستحدثة –كيفية اثباتها ومواجهتها" المركز القومي للبحوث الاجتماعية والجنائية ، المنعقد بالقاهرة في 15 و16 ديسمبر 2010.

13 هشام الهاشمي ، **عالم داعش – من النشأة الى اعلان الخلافة** ، لندن : دار الحكمة للنشر والتوزيع، ط1، 2015، ص ص 88 ، 89.

14 هشام الهاشمي ، مرجع سابق ، ص81.

15 عدنان هاشم سلطان ، **صناعة الارهاب** ، مصر : المكتب المصري الحديث ، ط1 ، 2008 ، ص131.

16 هشام الهاشمي ، مرجع سابق ، ص 88.

17 -اتفاقية هيئة الأمم المتحدة، رقم 55/63 – 2000، **حول مكافحة اساءة استعمال المعلومات لأغراض إجرامية**، ديسمبر 2000.

18 -عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، القاهرة:دار النهضة العربية، ط1، 2002، ص 308.

19 -قانون العقوبات الجزائري، معدل – صادر سنة 2012.

20-Jacques Bourrinet ,**Le Dialogue Euro-Arabe**, Paris :Economica, 1979 , p p 16-17