

الترويج للإرهاب عبر الإنترنت

الأستاذ: طيبي محمد بلهاشمي الأمين

جامعة وهران 2

الملخص:

عبارة الترويج للإرهاب عبر الإنترنت ، أصبحت لصيقة بمفهوم تكنولوجيا المعلومات والإنترنت وكل ما يتعلق بالعالم الافتراضي، الأمر الذي دفع بالمجتمع الدولي إلى تبني أول اتفاقية دولية لمكافحة الإجرام عبر الإنترنت في المجر ببودابست سنة 2001، مباشرة بعد أحداث 11 سبتمبر من نفس السنة ، لمواجهة أخطر أنواع جرائم الإرهاب الإلكتروني ، وظهرت بوضوح العلاقة بين الإرهاب والإنترنت، لتتحول مواجهة مجرمي الإرهاب الإلكتروني وملاحقتهم ، تتم بدءا من متابعتهم وتبعتهم في العالم الافتراضي قبل الانتقال إلى العالم الحقيقي لمحاكمتهم.

الكلمات المفتاحية: إرهاب ; أنترنت ; إعلام ; اتفاقية

Abstract

The terrorism's propaganda through the internet has become one of the most serious crimes of informatics at the present time, especially with the use of the internet in all areas of daily life, for this reason this study search for causes and prevention. The word terrorism propaganda over the internet , has become inherent to the concept of information technology and the virtual world, which pushed the international community to adopt Budapest Convention 2001, to face the most dangerous types of crimes of terrorism, clearly demonstrated the relationship between terrorism and the internet , into the face of electronic terrorism and prosecute criminals, starting from the pursuit of tracing in the virtual world before moving the real world for trial.

مقدمة:

أضحى الترويج للإرهاب عبر الانترنت من أخطر الجرائم المعلوماتية في الوقت الحاضر، خاصة وباتساع استعمال الانترنت في كل مجالات الحياة اليومية، لهذا السبب تخص هذه الدراسة البحث عن أسبابه و الوقاية منه . فعبارة الترويج للإرهاب عبر الانترنت ، أصبحت لصيقة بمفهوم تكنولوجيا المعلومات والانترنت وكل ما يتعلق بالعالم الافتراضي، الأمر الذي دفع بالمجتمع الدولي إلى تبني أول اتفاقية دولية لمكافحة الإجرام عبر الانترنت في المجر ببودابست سنة 2001، مباشرة بعد أحداث 11 سبتمبر من نفس السنة ، لمواجهة أخطر أنواع جرائم الإرهاب الإلكتروني ، وظهرت بوضوح العلاقة بين الإرهاب والانترنت، لتتحول مواجهة مجرمي الإرهاب الإلكتروني وملاحقتهم ، تتم بدءا من متابعتهم وتتبعهم في العالم الافتراضي قبل الانتقال إلى العالم الحقيقي لمحاكمتهم.

إن الترويج للإرهاب عبر الشبكات المعلوماتية يحتاج إلى استخدام وسائل الاتصالات التقنية الحديثة والدقيقة وعلى الخصوص الانترنت، سواء باستعمال الحاسوب أو الهواتف الذكية، لغرض بث الرعب والخوف، أو التهديد ، وأحيانا حتي بإلحاق أضرارا مادية أو معنوية بهم.

فقد تلحق فيروسات تضعها تنظيمات إرهابية إلى إتلاف أجهزة كمبيوتر، حيث قدرت في هذا الشأن الأضرار التي تسببها فيروسات النت، بأكثر من 12 مليار دولار أمريكي سنويا حسب تقرير مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت . وبالتالي فلكي يعطى وصف الإرهابي عبر النت لشخص معين ، فيجب أن تلحق الاختراقات والهجمات التي يشنها، أضرارا بالأشخاص أو الممتلكات، وإلا اعتبر مخترقا فقط، لانعدام الغاية أو الغرض من وراء هذه الجرائم ألا وهو إلحاق الضرر لبث حالة من الرعب.

أصبح الإنترنت سلاح تستعمله الجماعات الإرهابية أو حتى بعض الدول والأطراف لتحقيق أغراض إرهابية أو غرس الفتن في دول أخرى، فصار هذا النوع من الجرائم الالكترونية يمس بكيان الدول وسيادتها من جهة، ويهدد السلام والأمن الدوليين على المستوى العالمي من جهة أخرى، لهذا السبب تغيرت مواجهة المجتمع الدولي للإرهاب ، وأصبحت تختلف في طريقتها واستراتيجياتها فيما يتعلق بمكافحة الارهاب الرقمي، وانتقلت من الحروب الواقعية إلى الحروب الإلكترونية.

تهتم الدول والمنظمات الدولية، الحكومية وغير الحكومية إلى وضع خطط استراتيجية وتكتيكية لمواجهة الإرهاب والقضاء عليه، كما يقوم مراكز البحث والمخابر العلمية بدراسة هذه الظاهرة من خلال البحوث والدراسات والبحث عن المقصود بالإرهاب الإلكتروني ، والبحث عن لحماية القانونية للفضاء الرقمي من جرائم الإرهاب والترويج له.

تسعى هذه الدراسة إلى محاولة استكشاف وتحديد معالم الظاهرة الإرهابية المستحدثة التي تعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصالات وشبكات المعلومات، وذلك من حيث البحث عن مفهوم هذه الجريمة الإرهابية المستحدثة، وبيان أسبابها ودوافعها، وطرق معالجتها على المستوى الدولي ثم على المستوى الوطني ؟

أولاً: تهديد الإرهاب الإلكتروني للأمن المعلوماتي

لقد أدى ظهور الحاسوب إلى تغيير نمط الحياة ، وصار استعمال على طرق الاتصال الإلكتروني ضرورة ملحة، في مختلف الميادين المالية والثقافية والاقتصادية والعسكرية، أو الأمنية، غير أن استعمال الفضاء الإلكتروني أضى في حد ذاته عرضة للتهديدات الأمنية و لهجمات الإرهابيين عبر التكنولوجيا الحديثة عن طريق الترويج للإرهاب ، وبث أفكارهم ، لتحقيق أغراض سياسية ومما يزيد الأمر صعوبة أنَّ التقدم التكنولوجي لا يتوقف لحظة ، لذا يصعب على الدول مواجهة هذه العمليات الإرهابية التي تجعل من الإنترنت أداة لتنفيذ مخططاتها. فالترويج للإرهاب عن طريق الإنترنت يركز على ممارسة الأعمال التخريبية لشبكات الحاسوب والإنترنت من جهة، ومن جهة أخرى أن الإنترنت أصبحت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف وللاتصال ببعضهم البعض. لهذا فإن وسائل الاتصال الحديثة قد تركت بصمتها على مختلف الأنظمة القانونية والركائز التي تقوم عليها، فأصبح مفهوم الأمن مرتبط بالأمن المعلوماتي. فما المقصود بالأمن المعلوماتي وما علاقته بالأرهاب كصورة من صور الجرائم الإلكترونية ؟

1- مفهوم الأمن المعلوماتي

يقصد بالأمن المعلوماتي حماية المعلومات الموضوعة تحت تصرف الشبكة العنكبوتية من المخاطر التي تجعلها محل الاعتداء عليها.. باتخاذ جملة من

التدابير ، تتعلق بأنظمة حماية نظم التشغيل وأنظمة حماية البرامج والتطبيقات. وأنظمة حماية قواعد البيانات، وكذا البرمجة الأمنية، إدارة أمن المعلومات وحماية الأنظمة ، حيث صارت النظم المعلوماتية في عالم اليوم أساس المجالات والمالية والبنكية والاقتصادية والاجتماعية والثقافية ، وأصبح من الضروري الحفاظ على أمن المعلومات في سريتها واستمراريتها وكذا صحتها . فعلى المستوى الدولي لضمان أمن المعلومات يبرز نظام الأيزو للاعتماد والتقييم والتقييس 27001. أيضا وضعت الولايات المتحدة مجموعة من الأنظمة، لضمان أمن المعلومات COBIT و ISACA وأيضا HIPAA¹. من وجهة قانونية، هدف تشريعات حماية المعلومات من الأنشطة غير المشروعة يكمن في تحقيق أمن المعلومات بحماية سرية وسلامة المعلومات ومكافحة الأفعال التي تمس البيانات واستخدام نظمها في ارتكاب الجريمة الالكترونية.

يميز أرغويلا Arquilla و رونفلد Ronfeldt بين ثلاثة مستويات لتعريف الفعل الإجرامي في المجال الافتراضي²

أ- الجريمة الإلكترونية، وهي الأفعال التي يعاقب عليها القانون، وتعتبر الشبكة العنكبوتية والفضاء المعلوماتي أدواتها وساحتها وهدفها. ويدخل تحت هذه الخانة طيف واسع من الجرائم الإلكترونية كالقرصنة، التجسس، النصب، سرقة المعلومات. فالقراصنة Hijackist وهم الذين يقتحمون مواقع الانترنت لتعطيلها ويدخل فعلهم في خانة الجرائم الإلكترونية

ب- الأعمال الإرهابية التي تمارس عبر شبكة الانترنت: ويقصد بها الأنشطة التي تقوم بها منظمات أو جماعات إرهابية تقليدية، من أجل تدعيم أعمالها على أرض الواقع. وتشمل من بين ما تشمل أنشطة: التجنيد، الدعاية، المواد التعليمية الخاصة بالأعمال الإرهابية، التمويل، تبادل الأوامر... الخ، فالناشطون Activist وهم الذين يستخدمون الانترنت للترويج لقضية سياسية معينة أو يدافعون عن أيديولوجية معينة.

¹ - د.حسن مظفر الرزق، الفضاء المعلوماتي، الطبعة الأولى، (بيروت: مركز دراسات الوحدة

العربية، 2007، ص12

² Arquilla, J. and Ronfeldt, D. (2001) 'Networks and Netwars' RAND, Santa Monica P10

ج- الإرهاب الإلكتروني: وهي الأعمال والأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات والشبكة العنكبوتية، بقصد إحداث دمار للبنى التحتية المرتبطة والمدايرة بواسطة مثل هذه التكنولوجيا، كشبكات توزيع المياه والكهرباء، أنظمة الخدمات المصرفية، السجلات الصحية، الأنظمة العسكرية، وغيرها من البنى التحتية التي من شأن تدميرها أن يحدث أضرارا مباشرة وغير مباشرة بالمواطنين والدول. فالإرهابيون terrorist-Cyber وهم أشخاص يحركهم دافع سياسي، يهاجمون المواقع الإلكترونية وأنظمة معلومات البنية التحتية المرتبطة بالانترنت بغية إحداث دمار كبير بشري أو مادي¹.

2- الجدول حول تعريف الإرهاب الإلكتروني

إن الفراغ التشريعي أو القانوني في غالبية الدول حول تعريف الإرهاب الإلكتروني يعتبر من أهم الأسباب في انتشار الجريمة، إلى جانب تعدد الأفعال و التطور السريع للمجال المعلوماتي وكذا ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق لسهولة، ضف إلى ذلك صعوبة اكتشاف وإثبات الجريمة الإرهابية الإلكترونية ، لأن التكنولوجيا لا تستطيع تحديد هوية مرتكب الجريمة الإلكترونية إلا عن طريق أجهزة معينة تمتلكها بعض المؤسسات الأمنية. الأمر الذي دفع بالفقه إلى تقديم بعض التعريفات في هذا المجال مما اثار جدلا حول التجريم.

أ-تعريف الإرهاب المعلوماتي يرى بعض الفقه الإرهاب الإلكتروني بأنه الاعتداء أو التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد ضد الأشخاص، مع استعمال المجال الافتراضي كمسرح للجريمة. وذهب جانب آخر إلى اعتبار الإرهاب الإلكتروني بأنه نشاط أو هجوم متعمد، لدوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام .. كما يسعى لإحداث تأثير معنوي ونفسي عبر التحريض على بث الكراهية الدينية وحروب الأفكار. ويأتي هذا العمل في صورة رقمية عبر استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني، وقد يقتصر تأثيرها على بعدها الرقمي، أو تتعداه لتصل إلى الإضرار بأهداف مادية تتعلق

¹ Arquilla, J. and Ronfeldt, op.cit- pp15-16

بالبنية التحتية الحيوية.¹ في حين عرفه الحسيني على أنه يستطيع من خلال هذه أدوات الاتصال والانترنت من تحقيق عدة أهداف، منها التغيرير بالشباب واستقدام المقاتلين وكذلك الحصول على التمويل وبث الرعب والذعر بين الناس الآمنين يرى كولمان Colman أن الترويج للإرهاب عبر الإنترنت هو ببساطة طلب للإرهاب على الإنترنت، ويعتبر باري كولن Barry Collin هو من اعتبر الإرهاب الإلكتروني هو إرهاب العالم السيبراني، وهي تسمية ذات دلالة تميزه عن الإرهاب العادي الذي يقوم على استخدام القضاء الفيزيائي المحسوس، ويعرف بأنه القدرة على اختراق شبكات الإنترنت لتحقيق أهداف عدوانية ذات طابع سياسي، وإن خلف وراءه آثارا سلبية تنال كثيرا من جوانب الحياة الأخرى. الأمر الذي جعل الإرهاب الإلكتروني يتميز عن غيره من الجرائم الإلكترونية بمجموعة من الخصائص.²

ب- خصائص الإرهاب الإلكتروني

يمتاز الإرهاب الإلكتروني بمجموعة من الخصائص، ويتميز بها عن الكثير من الجرائم الإلكترونية الأخرى، ويهدف في نفس الوقت إلى تحقيق أغراض غير مشروعة. فالإرهاب المعلوماتي لا يحتاج إلى العنف والقوة، بل يتطلب وجود حاسوب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، كما يتسم بكونه جريمة إرهابية عبر وطنية، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود الأمر الذي يريد من صعوبة اكتشاف هذه الجرائم، ضف لذلك قلة الخبرة لدى المؤسسات الأمنية والأجهزة القضائية في التعامل مع مثل هذا النوع من الجرائم، كما يتعذر أحيانا تقديم الأدلة نظرا لسرعة تغيير البيانات المعلوماتية، أو إخفاءها من طرف مرتكبي ومروجي الإرهاب عبر الأنترنت.

¹ - د. رائد العدوان-المعالجة الدولية لقضايا الإرهاب الإلكتروني - الرياض-2013 ص7
انظر كذلك: يونس عرب، الاطار القانوني للإرهاب الإلكتروني واستخدام الانترنت للأغراض الارهابية، بحث مقدم لمؤتمر جامعة نايف العربية للعلوم الامنية حول الإرهاب، 25-27 اكتوبر 2010 القاهرة ص 12

² - د. هديل مصطفى الخولي، الإرهاب عبر الشبكة الالكترونية القاهرة، 2015 ص 72 في كتابه ل كولمان: الإرهاب السيبراني

راجع أيضا: أحمد ناصر أبو السعود، "الإرهاب الإلكتروني"، الموسوعة السياسية للعلاقات الدولية، 2017 ص2

يقوم ويروج للإرهاب عبر الشبكة العنكبوتية عادة مجموعة من الأشخاص أي بأنه يتم عادة في إطار جماعي منظم كتنظيم إرهابي أو جماعات إرهابية، تروج لأفكارها وسياسيتها بواسطة في هذا العالم الافتراضي. ويكون هؤلاء القائلين بأفعال الترويج أو التحريض عادة من ذوي الخبرة العالية في فلك العالم السراني، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.¹

في حين يهدف الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف غير المشروعة ، كنشر الخوف والرعب بين الأفراد مما يؤدي إلى الإخلال بالنظام العام، في المجتمع و يضرب بالأمن المعلوماتي، و يعرض سلامة المجتمع وأمنه للخطر، حيث يسعى هذا النوع من الإرهاب إلى إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة. بما فيه تهديد للسلطات العامة في الدولة وابتزازها، عن طريق الدعاية والإعلان، وجذب الانتباه، وإثارة الرأي العام.

3- الأعمال التي تشكل جريمة الإرهاب الإلكتروني

إن خطورة الإرهاب الإلكتروني تزداد في عالم اليوم وتمس البنى التحتية للدول، فعوض أن تقوم الجماعات الإرهابية بوضع المواد المتفجرة في مسرح الجريمة، فهي تقوم من خلال استعمال الحاسوب تدمير البنية الرقمية، وتحقيق نتائج مدمرة قد تتجاوز خساراتها أحيانا تلك المستخدمة في جرائم الإرهاب التقليدي، كأن يقوم مروج للإرهاب عبر صفحات الويب بتخريب برامج معينة ذات صلة بمرافق ضرورية، أو شل عمل صفحات الأجهزة الحكومية، أو إتلاف المواقع الرقمية للمؤسسات المالية والاستحواذ على الأموال، ، المساس بنظام أجهزة التحكم في المعدات الحربية، أو قطع الكهرباء وتخريب شبكة صرف المياه بالتحكم في أنظمة الامداد عن بعد.

¹ - د. عيد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجريمة المنظمة ،

وعليه فالتقدم المعلوماتي يجب أن يواكب أي تقدم قانوني ويحقق أمنه، لأن النزاع الرقمي تغذيه دوافع سياسية تجعل من الترويج للإرهاب في الفضاء الإلكتروني يتميز بوصفين اثنين، الوصف الأول يأخذ صورة العنف والهمجية لإتلاف الشبكات والنظام المعلوماتي والبنى التحتية باستعمال الفيروسات والأحصنة والقرصنة والتجسس الإلكتروني، أما الوصف الآخر يعطيه الخاصية المرنة، فيسعى مروج الإرهاب عبر النت في التأثير التام في مشاعر وأفكار الضحايا، بشن حرب نفسية وإعلامية.¹

أ- تخريب شبكات العالم الافتراضي

يمكن اعتبار الأعمال التخريبية التي يشنها الإرهاب عبر النت بمثابة صورة لاستعمال القوة في العلاقات الدولية، تعوض ما ينتج من استخدام أسلحة تقليدية وغير تقليدية فيمكن لمستعمل الحاسوب أن يخترق نظام التحكم للأجهزة الأمنية أو العسكرية ويقوم بإطلاق الصواريخ أو تغيير اتجاهها عن بعد فيستهدف من يريد الهجوم عليه، كما قد يسيطر على نظام شبكات الري فيفتح سدود مملوءة وتلحق الكارثة، وما ينتج عن ذلك من أثار تدميرية، فافتحام شبكة العالم الافتراضي والسيطرة على مفاتيح التحكم من بعد يمكن أن تضرب أهداف عسكرية أو مالية أو صحية وغيرها، والتي من شأنها المساس بالنظام الأمني للدولة. فمن الممكن على سبيل المثال اختراق صفحة إلكترونية.

ويجب التذكير أن الشخص الذي يقوم بتخريب شبكات النت أو اختراق برامج مؤسسة حكومية لا يحتاج سوى لرباط الأنترنت وقليل من الاحترافية، بنقرات بسيطة على لوحة المفاتيح، ودون أن يترك أثرا، ودون أن يحتاج إلى قنابل أو متفجرات، ودون التحرك من مكانه. وحصلت فعلا حالات لهذه الأعمال في أرض الواقع كالاختراقات التي تعرضت لها مواقع وزارات ومؤسسات إيطاليا المالية من قبل جماعات الألوية الحمراء عام 1998. وكذا قيام إحدى الجماعات الإرهابية المعروفة في استونيا باسم الجسر الأحمر سنة 2007 بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية لتلفت الأنظار إلى أفكارها ومعتقداته. وفي عام 2011 أخترق متسللون

¹ د.حسن مظفر الرزو، المرجع السابق، ص15

انظر كذلك: عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية، مركز الدراسات السياسية والاستراتيجية، 2009 ص5

صينيون حاسبات شبكة كهرباء كاليفورنيا بالولايات المتحدة.. وما حصل أيضا في أمريكا لما قام أحد الإرهابيين من السيطرة التامة على برامج التحكم في مطار في نيويورك ، وأطفأ مصابيح إضاءة ممرات الهبوط، ما هدد بحصول كارثة¹

ب- الاستعمال الإرهابي لشبكة الإنترنت من قبل جماعات

على خلاف العام الحقيقي، فالعالم الافتراضي يتقدم بشكل سريع، الشيء الذي يتطور معه استخدام الانترنت ولم يبق الإرهاب الإلكتروني منحصرًا في الصور المذكورة آنفا بل وصارت تعم وتخص أعمالا أكثر فتاكة، تشم التحضير والتنظيم والتحريض التنسيق للهجمات الإرهابية في مناطق متفرقة في العالم، أكثر من ذلك ، هذه التنظيمات أو الجماعات تستعمل رموزا وشيفرات معقدة يصعب حلها من قبا الجهات الأمنية ، كما إذا ما ظبطت أو اكتشف أمرها تغير من عنوانها وصفحاتها لتختفي بالشكل السابق وتظهر من جديد في صورة صفحة جديدة مما يصعب معه على الجهات الأمنية من مراقبة ملايين الصفحات الالكترونية المنتشرة في ارض المعمورة والمكتوبة بكل لغات العالم .

ضف إلى ذلك أن هذه المنظمات الإرهابية لا تكتفي بالترويج للغرهاب والتحريض كتابة فقط بل تستعمل كل وائل الاتصال السمعية والمرئية عبر الشبكة العنكبوتية بهدف شن حملات نفسية ضد الدول العدو ، فهي تعرض أفلاما مرعبة للرهائن والأسري أثناء إعدامهم ، في نفس الوقت يدعي الإرهابيون أنهم أصحاب قضايا نبيلة، ويشتكون من سوء المعاملة من قبل الغير.

أكثر من ذلك، فإذا كان الإرهاب التقليدي يحتاج إلى ساحات وأماكن لتدريب الإرهابيين، ويحتاج بكل هذا وفرة من الوقت المناسب للتحضيرات لشن الهجمات الإرهابية فإن الإجرام عبر النت في صورة الإرهاب الإلكتروني يمتاز ببساطة تامة ، فيكفي إرسال فيروسا أو احصنة طروادة وتحققت النتيجة الإرهابية. بل وعوض التحدث مع جماعة من أشخاص تم انتقاءهم سلفا وعدده محدود ، فإن متصفح شبكة الانترنت يقدر عددهم بالملايين.

¹ د.علاء الحسيني، الإرهاب الإلكتروني وكيفية التصدي له ، النبأ، كريلاء ، 2016، ص46

وعلى الرغم من أن البريد الإلكتروني أصبح من أكثر الوسائل استخداماً في مختلف القطاعات، وخاصة قطاع الأعمال؛ لكونه أكثر سهولة وأماناً وسرعةً لإيصال الرسائل، إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، بل إن كثيراً من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتنقلها بين القائمين بالعمليات الإرهابية والمخططين لها، ويقوم الإرهابيون كذلك باستغلال البريد الإلكتروني والاستفادة منه في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية.

فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة، والتي تتعارض مع مصلحة المجتمع. ويستخدم الإرهابيون الشبكة العالمية للمعلومات بشكل يومي لنشر أفكارهم الهدامة وتحقيق أهدافهم ومن الممكن إبراز أهم استخداماتهم للشبكة فيما يلي:

- البحث عن البيانات: إن شبكة الانترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم، وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت النووية، والمطارات الدولية، ومتنوعة المصادر، وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية والمعلومات المختصة بسبل مكافحة الإرهاب، وبذلك يكون غالب مخزونهم المعلوماتي معتمداً في الأساس على مواقع إلكترونية متاحة للجميع، دون خرق لأي قوانين أو بروتوكولات الشبكة.¹

- الاتصالات: تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظراً لقلّة تكاليف الاتصال باستخدام الانترنت، مقارنة بالوسائل الأخرى، كما أنها تتمتع بوفرة المعلومات التي يمكن تبادلها،

¹ Cybercriminalité et enfance en algerie mostafa khiyati, edition FOREM 2007. p 58

وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية، وكل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية. البريد الإلكتروني أو المواقع والمنتديات وغرف الحوار الإلكتروني حيث يمكن وضع رسائل مشفرة تأخذ طابعاً لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته، كما أنها لا تترك أثراً واضحاً يمكن أن يدل عليه .

-التعبئة وتجنييد إرهابيين جدد: إن استقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الانترنت مع قضاياهم، ويجتذبون هؤلاء السذج بعبارات بارقة وحماسية من خلال غرف الدردشة الإلكترونية، ونحن نعلم أن تسلية الشباب والمراهقين هي الجلوس بالساعات الطويلة في مقاهي الانترنت للثرثرة مع جميع أنواع البشر في مختلف أنحاء العالم. تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويع لها، وبث الأفكار والفلسفات التي تنادي بها، كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها¹.

ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدى من لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية، مما يوفر لديها قاعدة ممن تجمعهم نفس الأفكار والتوجهات، فيسهل تجنيدهم لتنفيذ هجمات إرهابية في المستقبل فتكون جرائم الإنترنت جرائم إرهابية، إذا اقتصرت تحقيقاً لأهداف إرهابية، مثل بث أفكار متطرفة سواء كانت سياسية أو دينية أو عنصرية، بما يعرض سلامة المجتمع وأمنه للخطر أو يضر بالنظام العام².

-إعطاء التعليمات والتلقين الإلكتروني: يمتلئ الانترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل، والأسلحة الكيماوية الفتاكة، وعند استخدام محرك البحث "غوغل Google" عام 2005 للبحث عن

¹ - ن.الحياي، العالم أمام التحديات الأمنية، مجلة الجيش، العدد 519، أكتوبر 2006، ص10

² - ن.الحياي، المرجع السابق صص 11-14.

راجع أيضاً: نعيم مغيب، حماية برامج الانترنت، منشورات الحلبي الحقوقية، البعة الأولى 2006،

مواقع تضم في موضوعاتها كلمات مثل "إرهابي terrorist و"دليل handbook"، فكانت نتائج البحث ما يقرب من ثمانية آلاف موقع.

-التخطيط والتنسيق: تعتبر شبكة الانترنت وسيلة للاتصال بالغة الأهمية بالنسبة للمنظمات الإرهابية، حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات إرهابية محددة، ويضيف ويمن أن أعضاء منظمة القاعدة البارزين اعتمدوا بشكل مكثف على الانترنت في التخطيط لهجمات 11 سبتمبر، ويستخدم الإرهابيون الرسائل الالكترونية العادية email وغرف التثيرة chat rooms، لتدبير الهجمات الإرهابية وتنسيق الأعمال والمهام لكل عنصر إرهابي.

العمليات الإرهابية عمل على جانب من التعقيد والصعوبة، فهي تحتاج إلى تخطيط محكم، وتنسيق شامل، وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية؛ حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيداً عن أعين الناظرين، مما يسهل على الإرهابيين ترتيب تحركاتهم، وتوقيت هجماتهم.

الحصول على التمويل: يستعين الإرهابيون ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، في التعرف على الأشخاص ذوي القلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين، يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الإلكتروني بطريقة ماهرة لا يشك فيها المتبرع بأنه يساعد إحدى المنظمات الإرهابية.

ثانياً: الجهود الدولية والوطنية في القضاء على الإرهاب الإلكتروني

التعاون بين الدول يشكل جزءاً مهماً من تعقد المشكلة، ما يؤثر في معرفة الهجمات الإلكترونية ومواجهتها، إذ يتمثل هدف التعاون في حماية السيادة والأمن والمصالح الأساسية المشتركة. كما أن تعرض الدول لهجمات الشبكات وقواعد البيانات، يمثل تهديداً لمصالحها الوطنية ويؤثر في تطورها تكنولوجياً، وفي مساعيها لحماية أمنها وخصوصية مواطنيها.

وتشكل القواعد القانونية ضغطاً دبلوماسياً على الدول التي لا تدرك أو تعترف بأن الإرهاب الإلكتروني يعتبر جريمة دولية. وبقول آخر، يمهد الضغط الدبلوماسي الطريق أمام تعزيز الرؤى حول خطورة استخدام الهجمات الإلكترونية في الصراعات، ما يحتم نمطاً جديداً من التعاون بين الدول.

1- التعاون الدولي للقضاء على الإرهاب الإلكتروني

لإيجاد حل لهذه الجرائم الإلكترونية تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية بتاريخ 20 نوفمبر 2000، بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت الحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001.

عرفت الأمم المتحدة في أكتوبر 2012 الإرهاب الإلكتروني بأنه "استخدام الانترنت لنشر أعمال إرهابية". موقف القانون الدولي من استخدام الإرهاب الإلكتروني في الصراع الدولي، يثير تساؤلات هامة تتعلق بمدى اعتبار العدوان والهجمات الإلكترونية استخداما للقوة بالمعنى الذي ورد في المبادئ العامة التي أقرها القانون الدولي، أن آثار استخدام الأسلحة والهجمات الإلكترونية أكثر خطرا من الأسلحة الأخرى التقليدية خاصة تميزها بعشوائية الاستخدام وانتهاكها لمبدأ التمييز بين المقاتلين والمدنيين وما بين الأهداف العسكرية والمنشآت المدنية وانتهاك عملية استخدام تلك الأسلحة لمبادئ القانون الدولي الإنساني، لتنص على حق أطراف أى نزاع في اختيار أساليب ووسائل القتال ليس حقا "لا تقيده قيود"، وأن هناك حدود حتى في سبيل استخدام تلك الأسلحة بحجة الدفاع الشرعى عن النفس، مع اتساع الفضاء الإلكتروني ليشمل العديد من المصالح التي تهتم المجتمع الدولي، ومن ثم يصعب عمليا استهداف أى دولة لأن عملية الهجوم ستصيب دول أخرى، وستؤدى إلى عسكرة الفضاء الإلكتروني والذي هو مرفق دولي وتراث مشترك للإنسانية¹.

دور المجتمع الدولي في دعم الاستخدام السلمي للفضاء الإلكتروني، فغياب اتفاقية واضحة على المستوى الدولي للتعامل مع ظاهرة الفضاء الإلكتروني وتنظيم استخدامها، وتوضيح الحقوق والواجبات قد يجعل الدول لا تشعر بأي إلزام للتعاون مع غيرها، ومن ثم فإن عدم التعاون يشكل جزءا مهما من تعقيد المشكلة، كذلك يجب حث ودعم جهود كافة الفاعلين في مجتمع المعلومات العالمي من أجل

¹ عبد النور بن عنتر، تطور مفهوم الأمن في العلاقات الدولية، السياسة الدولية، العدد 160،

الحفاظ على الطابع السلمى للفضاء الإلكتروني، وهو ما يستلزم تعاون الدول والقطاع الخاص والمجتمع المدني والأفراد من أجل بيئة آمنة وموثوقة في الفضاء الإلكتروني، فيهتم المجتمع الدولي بإبرام اتفاقيات تقنن التشريعات اللازمة لمكافحة تلك الجرائم، وتنظم الجهود الدولية لمحاربتها، بما في ذلك بحث إنشاء "نظام للإنذار المبكر من الهجمات الإلكترونية"، وتطوير برامج أمنية، وزيادة وعي المسؤولين التنفيذيين والعملاء بالحاجة إلى إجراءات أمنية أفضل.

يجب تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الإلكترونية، وتوفير التقنيات اللازمة لمواجهتها، عبر تطوير أمن شبكات الحاسب باستخدام أنظمة التشفير المتقدمة و"الجدران النارية" في الشبكات، وأنظمة اكتشاف المخترقين عالية الدقة، والبرامج المضادة للفيروسات كما وأن إنشاء إدارات لمكافحة "الإرهاب الإلكتروني" في أنظمة الأمن، خصوصاً في الدول التي تشهد تقدماً مطرداً في اعتمادها على تكنولوجيا المعلومات، أمر حيوي، خاصة وأن التطور الحاصل في هذا المجال يتسارع، والثغرات التكنولوجية فيه تتسع، وهو الأمر الذي يستلزم مواجهة كفؤة متخصصة للحد من احتمالات نجاح التهديدات الإرهابية في هذا المجال¹

بروز ظاهرة تشكيل التحالفات الدولية العابرة للدول من جماعات الهاكر مثل "اينيموس" كجماعة ضغط دولية، أو ببروز دور الفرد في مواجهة الدول مثل قضية ويكيليكس، وإعادة تشكيل الدبلوماسية الدولية، هي إحدى نتائج الحرب السيبرية أو حرب الفضاء الإلكتروني، فكل حرب تقود إلى ظهور وسائل مضادة ومثل هذه التحالفات واحدة منها².

الظروف التي مر بها العالم العربي منذ ثورات الربيع العربي و قبلها غزو العراق، وما أعقب ذلك من استخدام التنظيمات الإرهابية المتطرفة مثل داعش للفضاء الإلكتروني في تجنيد عناصر من مواطني دول غربية، وجهت الانتباه إلى أهمية المجال الإلكتروني في حركة العلاقات الدولية والأمن والسلام العالميين، خاصة مع دوره في الحشد والتعبئة و التجنيد واستخدامه في نشر الأفكار المتطرفة. العالم

¹ عبد النور بن عنتر، نفس المرجع ص 60

² محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الاسكندرية ، طبعة

دولا وشعوب أصبح أمام تحد كبير، يتطلب تنسيقا إلكترونيا عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلا تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذا المشكلة وبخاصة الإنتربول لمواجهة كافة أشكال جرائم الإرهاب على الإنترنت¹

لقد تصدى العالم بأجمعه للإرهاب الإلكتروني ، وهبت دول العالم بعد التطور الهائل لتقنية المعلومات وسنت أنظمة لضبط التعاملات الالكترونية ، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الالكترونية ، ففى أمريكا عقاب بالسجن والغرامة ، مع جواز التجسس على البريد الإلكتروني ، وإن كان الإسلام يحرم اختراق الرسائل الإلكترونية إلا في حالات التجسس على المجرمين وكذا توالى العقوبات في كل دول العالم لتجرم الإرهاب الإلكتروني ، فلم تجد دولة صغيرة أو كبيرة لم تسن قانونا لمكافحة هذه الجريمة العصرية.

وهو الأمر الذي دعا 30 دولة إلى التوقيع على "الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت"، في بودابست، عام 2001، يمكننا تعريفه " بأنه "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. وبالتالي فلنكتفي بتهديد شخص ما بأنه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب". فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.²

2 - مكافحة الإرهاب الإلكتروني على المستوى الوطني

لقد قدمت بعض من الدول بما فيها الأردن والجزائر والسعودية بعضاً من التشريعات فيما يخص الارهاب الإلكتروني من خلال ان تعطيل سبل الاتصالات

¹ محمد سيد سلطان- قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية-2012. ص26

² محمد حسين منصور، مرجع سابق، ص267

³ راجع اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة جرائم المركبة عبر الانترنت

وأنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها أو تعطيل وسائل النقل أو الحاق ضرر بها كليا أو جزئيا يدخل في مفهوم المؤامرة التي يقصد بها ارتكاب عمل أو اعمال ارهابية .

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخارجاتها يعد سببا مهما 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 فيها.

من الأسباب أيضا غياب دور المنزل والمدرسة في الرقابة على الأطفال والشباب، مما يجعلهم يستخدم هذه التكنولوجيا استخداما خاطئا ، أو يتمادى الطالب في السلوك التقني السيئ ، ومن الأسباب التي أدت إلى ظهور الإرهاب عامة والإلكتروني خاصة : الغلو والتشدد في بعض أمور الدين .وربما بدا سبب الفراغ الذي يغلب على كثير من الشباب سببا رئيسا ، فبسبب الفراغ يلجأ الشباب إلى هذه التكنولوجيا ، وقد يقع في براثن الإرهابيين عن طريق مواقع التواصل الاجتماعي ، ومن الأسباب غير المباشرة الجهل بطريقة التصحيح الصحيحة في التعامل مع التكنولوجيا . كما أكدت ضرورة تعاون عدة جهات مع بعضها بعضا، بمعنى أن تسن الحكومة قوانين وعقوبات لمرتكبي الإرهاب الإلكتروني، ودعم الجهود التشريعية والأمنية، بالإضافة إلى ضرورة تصميم الشركات لبرامج حماية ضد تلك الجرائم التي ترتكب وتهدد أمن المجتمعات، إلى جانب أهمية دور الأفراد وحثهم على استخدام أنظمة الحماية والوقاية لكل الأضرار التي يمكن أن تلحق بأجهزتهم ومؤسساتهم، بمعنى دعم تنمية الوعي الإلكتروني.

3-حكم الترويج للإرهاب في التشريع الجزائري:

بالرجوع إلى الجزائر فدرجة خطورة القرصنة قليلة مقارنة بمثلتها من الدول، خاصة في مجال التجارة الإلكترونية التي لم تشرع بعد في استعمالها، إلا أنه يجب التأكيد على ضرورة التفكير من الآن في تنظيم هذه العملية وتحصين المواقع وتأمينها، من خلال التطبيق الصارم للإجراءات خاصة ما تعلق بقرصنة البرامج "حيث يبقى تطبيق عقوبات على المخالفين متفاوت رغم أن القانون يمنع أي نوع من القرصنة سواء كانت إلكترونية أو كلاسيكية.

إن التكتّم عن ظاهرة القرصنة وعدم التبليغ وتقديم شكاوي عن حالات القرصنة، خوفا من المشاكل التي قد يواجهها القائمون على الانترنت، يبقى عائقا أمام محاربة هذه الظاهرة، بإنشاء مركز وطني لمراقبة تدفق المعلومات والذي سيضبط أكثر تبادل المعلومات سيحيي المشتركين من أي قرصنة من خلال جمعه كل ممولي الانترنت، يؤمن المعلومات من خلال وضع نقطة التقاء بين مختلف الممولين لمراقبة المحتويات ومنع المواقع غير المرغوب فيها، سواء من قبل الممول أو من قبل الدولة التي لها الحق في الاطلاع على ما يجري عبر الشبكة العنكبوتية، خاصة أن الجزائر "تعتبر الوحيدة التي لها الحرية المطلقة في دخول المواقع واستعمالها.

خاصة في إطار برنامج الحكومة ستنضم الجزائر للدول المستعملة للدفع الالكتروني، الحكومة الالكترونية ومجتمع المعلوماتية الأمر الذي دفع بالجزائر إلى عرض مشروع قانون لحماية المعلومات ومشروع قانون آخر حول المعاملات الالكترونية. إن نجاح هذه المشاريع يتطلب حماية تبادل المعلومات وتأمينها، وأيضا سن قانون خاص بالتشفير، لأن القرصنة يبحثون عن الثغرات للمساس بالمواقع التي لم يسلم منها أشهر المواقع وأكثرها أمانا.

القرصنة الالكترونية، جريمة من الجرائم المنصوص عليها في المادة 394 من قانون العقوبات الذي يعتبرها مساسا بأنظمة المعالجة الآلية للمعطيات "وكل دخول إلى نظام معلوماتي وتغيير معطياته أو سرقتها أو تخريبها"، حيث تعالج هذه الجرائم المرتبطة بالتطور التكنولوجي كبقية الجرائم على مستوى الشرطة القضائية، التي تقوم بمعانة هذا النوع من الجرائم والبحث عن المجرمين وتقديمهم أمام العدالة، وذلك بالاعتماد على تقنيات تحقيق حديثة وتقنيين مختصين ومحققين تم تكوينهم في هذا المجال من خلال خمس دورات تكوينية تم تنظيمها منذ 2002.

وعلى هذا الأساس سنت الجزائر قانونا للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك في خطوة نحو ردع جرائم المعلوماتية، خاصة ما تعلق منها بتسخير الوسيلة التكنولوجية للترويج للإرهاب والدعاية، وبذلك تكون الحكومة قد أخذت أول خطوة نحو سد الفراغ القانوني الذي كان موجودا في

مكافحة الجريمة المعلوماتية. ويعد هذا القانون الذي يأتي في سياق مكافحة الإرهاب الإلكتروني بمثابة إطار قانوني مهم يحدد في بابه الأول تعريف وتحديد الجرائم المعلوماتية ثم ينتقل إلى إمكانية الحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات، حيث جاء في 19 مادة و6 فصول تؤكد في مجملها على احترام مبدأ المحافظة على سرية الاتصالات إلا في استثناءات حددها المشروع.

خاتمة

تأسيساً على ما سبق يمكن القول بأن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم، نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، مع توفير قدر كبير من السلامة والأمان للإرهابيين. لهذا فدور مصممي البرامج في ملاحقة هذا الإرهاب قبل وقوعه يعد بمثابة الإنذار؛ فإنه لا شك فيه أن مطوري تكنولوجيا المعلومات وخبراء الإنترنت مطالبون بملاحقة أنشطتهم التوسعية بأنشطة حماية وسد الثغرات، لحماية هذا الفضاء الحيوي من أن يصبح ساحة إرهاب دامية.

يجب تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الإلكترونية، وتوفير التقنيات اللازمة لمواجهتها، عبر تطوير أمن شبكات الحاسب باستخدام أنظمة التشفير المتقدمة والجدران النارية في الشبكات، وأنظمة اكتشاف المخترقين عالية الدقة، والبرامج المضادة للفيروسات كما وأن إنشاء إدارات لمكافحة "الإرهاب الإلكتروني" في أنظمة الأمن، خصوصاً في الدول التي تشهد تقدماً مطرداً في اعتمادها على تكنولوجيا المعلومات، أمر حيوي، خاصة وأن التطور الحاصل في هذا المجال يتسارع، والثغرات التكنولوجية فيه تتسع، وهو الأمر الذي يستلزم مواجهة كفاءة متخصصة للحد من احتمالات نجاح التهديدات الإرهابية في هذا المجال.