الإرهاب الالكتروني: دراسة في إشكالات المفهوم والأبعاد

Electronic terrorism: a study of the conceptual and dimensional problematics

د. فريدة بن عمروش*
جامعة الجزائر 3 – University of Algiers 3
benamrouche.farida@univ-alger3.dz

تاريخ الاستلام: 2020/03/24 تاريخ القبول: 2020/09/29

الملخص

إن الثورة التكنولوجية والتطور التقني في عصرنا الحاضر أدى إلى تغيير شكل الحياة في العالم وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوما بعد يوم في شتى نواحي الحياة الاقتصادية والسياسية والاجتماعية. وقد أصبح الحاسوب الآلي أحد مقومات المؤسسات المالية و المرافق العامة والمجال التعليمي والأمني، إلا أنه لا يمكن التغاضي عن الاستخدامات السلبية لهذه التقنيات الحديثة، ومن مظاهر هذه الاستخدامات الإرهاب الالكتروني كشكل من أشكال الإرهاب الذي أصبح هاجسا يخيف العالم المعرض لهجمات الإرهابيين عبر الانترنت، الذين يمارسون نشاطهم الإجرامي من أي مكان في العالم و من وراء شاشاتهم الالكترونية، و هذه المخاطر تتفاقم يوما بعد يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الالكترونية ، و التي سببت أضرارا جسيمة على الأفراد و المنظمات و الدول، ولقد سعت العديد من الدول و المنظمات العالمية إلى اتخاذ التدابير و الإجراءات اللازمة لمواجهة الإرهاب الالكتروني، إلا أن هذه الجهود ما زالت غير كافية لمواجهة هذا السلاح الخطير.

الكلمات المفتاحية: الإرهاب، الإرهاب الالكتروني، الأنترنت، شبكات المعلومات، وسائل الاتصالات.

Abstract:

The world today is living an unprecedented knowledge and technological revolution, with the internet being the most prominent of these innovations, which imposed itself on a global level over the past few years, until it became a way of daily dealings and a pattern for the exchange of knowledge between the people of the developed world. The rapid propagation of this network made it one of the features of the modern era, so that some called it, the era of cognitive explosion or the era of information revolution, The technological revolution and development in the present era had many

*المؤلف المرسل: فريدة بن عمروش ، الإيميل:faridabenamrouche@yahoo.fr

positive impacts on the fields of education and security, however, the negative uses of these new technologies cannot be overlooked, such as electronic terrorism as a modern form of terrorism which threatens the world with the dangers of terrorist attacks through the internet and from behind the gauze of their electronic screens. These dangers are increasing day after day, because modern technology alone is incapable of protecting people from electronic terrorist attacks, which causes serious damages to individuals, organizations and nations, which led many countries and international organizations to take the necessary measures to face electronic terrorism, yet, these efforts are still not sufficient to confront this dangerous weapon.

Keywords : Terrorism, Cyber terrorism, The internet, information net work, Communication means.

مقدمة

تعد ظاهرة الإرهاب من أخطر الظواهر التي شهدها العالم، والتي ألمت بواقع العالم العربي والغربي من خلال تعدد الأحداث الإرهابية وتداعياتها، وما خلفته من آثار اقتصادية وسياسية واجتماعية، ولقد أصبحت مصطلحات مثل الإرهاب، الإرهاب الدولي الالكتروني، كلها تعبيرات كثيرة التداول الإعلامي، أثارت الكثير من الجدل حول أبعادها ومضامينها السياسية والإيديولوجية، وذلك نتيجة تداخل المواقف، واختلاف المصالح السياسية والاستراتيجية والاقتصادية بين الدول، فأصبح الإرهاب فعلا حديث الساعة لدى الشعوب على اختلاف مستوياتها، خاصة بعد أن عرفت التنظيمات الإرهابية زيادة قدراتها واتساع رقعتها وكثرة جرائمها، لتصبح أقوى في الوسائل وأوسع في المدى.

والجدير بالذكر أن العالم اليوم يشهد مجموعة من التحولات والتغيرات في شتى المجالات، ومن أبرز هذه التحولات ظهور الثورة التكنولوجية، والعولمة التي تهدف إلى جعل العالم قرية صغيرة على حد تعبير ماكلوهان، فكان لهذه التحولات أثر على مختلف المفاهيم وتطويرها إلى مفاهيم جديدة مواكبة للعصر، ومن أهم هذه المفاهيم مفهوم الإرهاب الإلكتروني كشكل من أشكال الإرهاب الذي يعتمد على استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات وذلك لنشر الرعب والخوف لتحقيق مآرب سياسية واقتصادية على الخصوص.

لقد أصبح الإرهاب الالكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت، الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الأفراد من العمليات الإرهابية الإلكترونية والتي سببت أضرار جسيمة على الأفراد والمنظمات والدول، ولقد سعت العديد من

الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الالكتروني، إلا أن هذه الجهود مازالت قليلة لمواجهة هذا السلاح الفتاك.

تأسيسا على ما سبق، تكمن مشكلة البحث في تفاقم ظاهرة الإرهاب الالكتروني وتعدد حجم خسائرها وأضرارها وانعكاساتها السلبية على المجتمعات والأمم، حيث أصبحت هاجسا مهددا لأمن المعلومات في كافة المجالات الحيوية، كما أضحت تشكل خطورة على الأمن القومي وعلى السلم الدولي بسبب استغلال مختلف مصادر المعلومات الالكترونية في النشاطات الإرهابية.

وعليه تصبو هذه الدراسة، إلى محاولة استكشاف وتحديد معالم وأبعاد ظاهرة الإرهاب المستحدثة، التي تعتمد على استغلال وسائل الاتصالات وشبكات المعلومات، وذلك من حيث تحديد مفهوم الجريمة الإرهابية المستحدثة، وبيان أسبابها، خصائصها، وأهدافها، ومن ثم إبراز أهم مظاهرها وأشكالها وكذلك تبيان كيفية مواجهتها والتصدي لها.

1- تساؤلات الدراسة :

تفرعت عن الإشكالية المطروحة التساؤلات التالية:

- ما هو الإرهاب الالكتروني وماهي أسبابه، خصائصه، والآثار المترتبة عنه؟
- فيما تتجلى مظاهر الإرهاب الالكتروني وما هي أ شكاله؟
- ما هي السبل والأساليب المعتمدة لدى الهيئات والمنظمات الدولية لمواجهة هذه الظاهرة بكل صورها وأشكالها؟

2-أهداف الدراسة: تسعى هذه الدراسة إلى تحقيق الأهداف التالية:

- ابراز واقع الإرهاب الالكتروني وأسبابه والآثار المترتبة عنه.
- عرض أشكال وأنماط الإرهاب الالكتروني.
- التعرف على أهم الوسائل والأساليب المعتمدة لدى الهيئات والمنظمات الدولية لمكافحة ظاهرة الإرهاب الالكتروني.

3-أهمية الدراسة:

تكتسب الدراسة أهميتها من أهمية التحديات الأمنية و التقنية و التكنولوجية و القانونية، المصاحبة لاستخدامات تقنية المعلومات و الحاسب الآلي و الأنترنت، كما تكمن أهميتها في خطورة هذه الظاهرة المستحدثة على البنيات التحتية لأنظمة تقنية المعلومات و الاتصالات، و تحديد طبيعة

الاختراقات و الهجومات المستمرة لكل المصالح في شتى المجالات، لهذا كان من الضروري تكاثف الجهود لإيجاد الطرق و السبل و الحلول العملية و العلمية لمواجهة هذه الظاهرة و الحد من ارتفاع معدلاتها و آثارها المؤكدة لدى الكثير من الدراسات على المستوى العالمي.

4-حدود الدراسة:

نظرا لكون الجريمة الالكترونية ظاهرة عالمية، اكتسحت العالم كله مخلفة بذلك آثارا متعددة على جميع الدول، فقد أثارت قلقا كبيرا لدى الهيئات والمنظمات الدولية، لهذا اتسعت حدود الدراسة لتشمل كل أبعاد الظاهرة.

5-المنهج المتبع في الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، وذلك من خلال وصف الظاهرة محل الدراسة، التعرف على سماتها الداخلية وتحديد ماهيتها، طبيعتها، أسبابها، اتجاهاتها، آثارها وتحليل العلاقة بين المتغيرات، والتعرف على أفضل الوسائل والسبل لمواجهتها وإيجاد الحلول لها.

6-إشكالات مفهوم الإرهاب الالكتروني:

يعترف الجميع بصعوبة إعطاء مفهوم محدد للإرهاب، نظرا لعدم وجود اتفاق موحد بين المختصين حول هذا المصطلح المعقد ذو الطبيعة المتغيرة، ويرجع ذلك حسب البعض لتداخل مفهوم الإرهاب مع مفاهيم أخرى، كالعنف السياسي أو الجريمة السياسية أو الجريمة المنظمة، كما أنه مفهوم ديناميكي متطور تختلف أشكاله ودوافعه، باختلاف الأماكن والفترات الزمنية، لذا تعددت وتباينت مفاهيم الإرهاب، تبعا لتفاوت منطلقات الباحثين في الموضوع، إلا أن العامل المشترك بينها جميعا هو أن العمل الإرهابي ضرب من أعمال العنف التي تستهدف كيان المجتمع.

يعرف جينافو فيتش الإرهاب بأنه: «الأفعال التي من طبيعتها أن تثير قلقا لدى شخص ما من شعور بالتهديد، أو هي الأعمال التي تؤدي إلى التخويف والرعب بأي قدر وبأي وسيلة» (عياد،2008، ص28).

وقد عرف بعض الفقهاء، الإرهاب الالكتروني بأنه: «العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان نفسه، بغير حق بشتى أنواعه وصور الإفساد في الأرض». (نواف، 2009، ص11).

إن ما يتميز به الإرهاب الالكتروني عن الإرهاب التقليدي بالطريقة المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبها عصر تقنية المعلومات أن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

ويشير الإرهاب الالكتروني إلى عنصرين أساسيين هما: الفضاء الافتراضي، أو العالم الالكتروني، وهو المكان الذي تعمل به أجهزة وبرامج الحاسوب والحواسيب المعلوماتية، كما تنتقل فيه المعلومات الإلكترونية، والإرهاب، وقد استفادت تلك المنظمات الإرهابية من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية، مما زاد من خطورتها، كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والشركات الاقتصادية الكبرى.

كانت بداية استخدام مصطلح الإرهاب الالكترونيCyber terrorism، في فترة الثمانينات على يد باري كولين Barry Colin، والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفا للإرهاب الالكتروني مقتضاه بأنه: «هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن لهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب». (cyberterrorism ،2019)، وعرفه جميس لويس James Lewiss، على أنه: «استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين» .(desforges,2011,p3)

أما دوروثي دينيغ Dorothy Denning، فترى أن الإرهاب الالكتروني هو: «الهجوم على الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمرا وتخريبيا لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب». (denning,2000, p 01).

كما يعرف "الإرهاب الالكتروني" بأنه: «هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الانتقام أو الابتزاز أو التأثير في الحكومات والشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، وبالتالي فلكي يُوصف شخصا ما بأنه إرهابيا على الإنترنت، وليس فقط محترفا، فلابد أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب» (شوقي، 2016)،فالإرهاب الالكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من

أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم،(Patrick, 2019)،كما يعتبره البعض على أنه عمل متعمد لتدمير أو تغيير البيانات أو تدفق المعلومات للدول بهدف الإضرار بها لأسباب سياسية دينية وعقائدية. (العاني،2013، ص80).

يتبين جليا مما سبق أن مفهوم الإرهاب الالكتروني ارتبط ظهوره بالتطور التكنولوجي لوسائل الإعلام والاتصال وبالأخص بعد ظهور الشبكة العنكبوتية (Internet) وكذا التطور الحاصل في مجال الصناعات الإلكترونية الحديثة، حيث تحتوي الإنترنت على عدد من شبكات الحاسب المترابط في أنحاء العالم ويحكم ترابطها ما يسمى بروتوكول تراسل الإنترنت (TCP/IP).

وقد بدأت الإنترنت بتاريخ 12 جانفي 1969 بالولايات المتحدة الأمريكية وكان يقتصر استعمالها على المجال العسكري، ثم في عام 1983 تحول استخدامها إلى المجال السلمي والمدني، وفي عام 1986 أنشأت خمسة مراكز كمبيوتر عملاقة وتم ربط شبكاتها وأصبحت بذلك مركز ازدهار الإنترنت. (عبد الرحمان،2014، ص98).

لم يفوت الإرهابيون فرصة استخدام الإنترنت للقيام بأعمالهم الإرهابية والترويج لأفكارهم وأيديولوجياتهم، سواء من خلال استخدامها في التنسيق بين أفراد الجماعات الإرهابية وجمع المعلومات وجذب المؤيدين، أو من خلال نشر صور الأعمال الإرهابية على صفحات الويب للدعاية وبث الرعب والخوف بين الناس واستعراض القوة، إلى جانب استغلال الهواتف النقالة المربوطة بالأقمار الصناعية في الاتصال فيما بينهم، بل سرعان ما استثمر الإرهابيون في ميدان التكنولوجيا والالكترونيات وحصلوا على قنابل وأسلحة ذات فاعلية قصوى. (موريس، وهو،1991، ص27).

وقد بلغ عدد المواقع الإلكترونية الإرهابية في عام 1998 أكثر من 4800 موقع وازداد سنة 2008م إلى خمسة آلاف موقع (هاشم سلطان،2019،ص 132)، وفي دراسة أعدها الدكتور" أحمد عظيمي بعنوان "الإرهاب الالكتروني : القاعدة نموذجا " أحصى ستة آلاف (6000) موقع الكتروني إرهابي، وأجرى دراسته على عينة من المواقع الإلكترونية الإرهابية ، بلغ عددها مئة (100) موقع، وعرف الإرهاب الالكتروني أيضا على أنه: « العنف الذي يمارس باستعمال تكنولوجيا الاتصال، سواء عن طريق الإنترنت، أو البث عبر الأقمار الصناعية أو الأقراص المضغوطة أو كاسيت الفيديو»، (زهراء، 2009، ص 3)، كما يرى "جون بول ناي" (Jean– Paul Ney) أن «الإرهاب الالكتروني يركز على مهاجمة مواقع الويب وخاصة أجهزة الكمبيوتر الاستراتيجية للعدو، وينطبق هذا المصطلح كذلك على المنظمات الإرهابية التي تستخدم الإنترنت لربط الاتصالات وعرض العمليات ». (Ney, 1999, p70).

يتبين جليا مما سبق، أن الإرهاب الالكتروني هو الهجوم الالكتروني على نظم المعلومات وأجهزة الحاسوب بتقنيات حديثة. لأسباب متعددة لتدمير البنية التحتية بهدف تخويف، ترهيب وإخضاع الحكومات والمدينين لهم.

7-أسباب الإرهاب الالكتروني

إن أسباب الإرهاب الالكتروني متعددة ومتنوعة ومتشابكة، وهي في نفس الوقت أسباب ظاهرة الإرهاب عموما باستثناء بعض جوانبها ومظاهرها، ونعرض هذه الأسباب على النحو التالي:

– ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق، حيث أن شبكات المعلومات مصممة بشكل مفتوح دون حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين، ويمكن للمنظمات الإرهابية استغلال الثغرات المتواجدة في الأنظمة الإلكترونية والشبكات المعلوماتية في التسلل إلى البنى المعلوماتية التحتية وممارسة العمليات التخريبية والإرهابية.

– عدم وضوح الهوية الرقمية للمستخدم، يجعل الفرصة سانحة للإرهابيين حيث يستطيع محترف الحاسوب أن يتخفى تحت شخصية وهمية ويشن بالتالي هجومه الالكتروني بعيدا عن مراقبة السلطات العامة. (كافي،2015، ص151).

– سهولة استخدام شبكة المعلومات وقلة التكلفة مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون الحاجة إلى مصادر تمويل، فشن هجوم إرهابي الكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة، وصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب الإرهاب الالكتروني، لأنها تساعد المجرم على الإفلات من العقوبة.

– صعوبة اكتشاف واثبات الجريمة الإرهابية خاصة في مجال جرائم الاختراق، مما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.

– غياب السيطرة والرقابة على الشبكات المعلوماتية ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى.(Weismann, 2004, pp2-6) .

8-خصائص الإرهاب الالكتروني

يتميز الإرهاب الالكتروني بعدد من الخصائص التي يختلف فيها عن بقية الجرائم وتحول دون اختلاطها بالإرهاب العادي، ويمكن إيجاز تلك الخصائص فيما يلي:

-الحاسب الآلي أداة لارتكاب الجرم، فلا يمكن إتيان أية جريمة على شبكة الإنترنت إلا وكان جهاز الكمبيوتر وسيلة ارتكابها بشكل أساسي.

-يُرتكب الإرهاب الالكتروني عبر شبكة الإنترنت، فهي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك، الشركات وحتى الأفراد العاديين.

- مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الإعلام الآلي، فحتى تقع جريمة الإنترنت يجب أن يكون الفاعل متمكنا من التقنية ومتمتعا بالدراية العالية لاستخدام الحاسب الآلي، فالكثير من الجرائم، اكتشف المحققون أن فاعليها من خبراء الإعلام الآلي. (الدليمي،2010، ص 83).

- يَحمل الإرهاب الالكتروني صفة العولمة والعالمية، فهو جريمة لا حدود جغرافية لها، حيث تقع جرائم الإنترنت متخطية حدود الدولة، التي ارتكب فيها، ويمكن أن تترتب آثارها عبر كافة دول العالم،- أي أن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

- يتسم الإرهاب الالكتروني بكونه جريمة إرهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق إقليمي محدود.

- صعوبة اكتشاف جرائم الإرهاب الالكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.

- صعوبة الإثبات في الإرهاب الالكتروني نظرا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره.

(عبد الرحيم،2008، ص50).

- يتميز الإرهاب الالكتروني بأنه يجري عادة بتعاون أكثر من شخص على ارتكابه.

- لا يترك الإرهاب الالكتروني أي دليل مادي بعد ارتكاب الجريمة، وهذا مما يصعب عملية العقاب واكتشاف الجريمة أساسا.

- سهولة إتلاف الأدلة في حال العثور على أي دليل يمكن إدانة الجاني وغيرها من الخصائص المستخدمة مع حداثة الوسائل الإلكترونية. (موسى،2015، ص 151).

9-أهداف الإرهاب الالكتروني

يهدف الإرهاب الالكتروني إلى تحقيق جملة من الأهداف غير المشروعة يمكن إبرازها في ضوء النقاط التالية:

-نشر الخوف والرعب بين الأشخاص والدول وتعريض سلامة المجتمع وأمنه للخطر.

-الإخلال بالأمن المعلوماتي وزعزعة الطمأنينة.

-تدمير البنى التحتية المعلوماتية والأضرار بوسائل الاتصالات وتقنية المعلومات.

-الدعاية والإعلان وإثارة الرأي العام.

-الاستيلاء على الأموال. (السويدان،2005، ص95)

10. وسائل الإرهاب الالكتروني

1.10. البريد الالكتروني:

يعتبر من أهم وأوسع الخدمات انتشارا عبر الشبكة العالمية، حيث يستخدم لأغراض مهنية وبحثية مختلفة، ومن شرائح اجتماعية ومهنية متباينة ومنهم الباحثين في التخصصات المختلفة، ومن أهم مميزاته أنه لا يحتاج إلى جهد كبير في إرسال واستقبال الرسائل بشكل سهل وسريع، كما يمكن إرسال رسالة إلى المئات من الجهات والأفراد الموزعين في مختلف مناطق العالم. (قنديلمي،2002، ص 226).

وعلى الرغم من أن البريد الالكتروني، أصبح أكثر الوسائل استخداما في مختلف القطاعات وخاصة الأعمال لكونه أكثر سهولة وأمنا وسرعة لإيصال الرسائل، إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الالكتروني من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم بل أن كثيرا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها. (ممدوح، حجية،2008، ص 59).

وكذلك يقوم الإرهابيون باستغلال البريد الالكتروني في نشر أفكارهم والترويج لها عبر المراسلات الإلكترونية.

كما يقوم الإرهابيون باختراق البريد الالكتروني للآخرين، وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها، في عملياتهم الإرهابية. (حجية،2008، ص19).

10. 2. إنشاء مواقع على الإنترنت:

يعرف الموقع بأنه: «مجموعة مصادر للمعلومات متضمنة في وثائق متمركزة في الحاسبات والشبكات حول العالم»، كما عرف أيضا بأنه: «مجموعة صفحات الكترونية مرتبطة مع بعضها البعض يمكن مشاهدتها والتفاعل معها عبر برامج حاسوبية تدعى المتصفحات كما

يمكن عرضها بواسطة الهواتف النقالة عبر تقنية نظام التطبيقات الكلاسيكية. (آل زيان، 2011، ص 19).

تعتبر شبكة (world vide web)،الأكثر غنى بالمعلومات في شبكة الإنترنت ويتجاوز عدد الحواسيب المزودة لشبكة الواب حاليا ،12000 حاسوب مزود، تملكها جامعات ودور نشر وشركات كبرى وغيرها، وتحتوي على صفحات من المعلومات تغطي مجالات شتى، وتتضمن عادة نصوصا وصورا ورسوما متحركة وأصوات وهي مبوبة بطريقة تسهل الوصول إليها، وتترابط بكل المعلومات التي تحتويها الشبكة حسب موضوعاتها بواسطة وصلات فائقة التشعب والترابط Hyper links والوصلات فائقة التشعيب والترابط ،وهي تسهل الوصول إلى كتلة من المعلومات بالنقر على كلمات ذات الوصلات العنكبوتية عادة ما تكون ملونة بلون مختلف أو يوضع تحتها خط لتمييزها. وقد يعني الانتقال من كتلة معلومات إلى أخرى بهذه الطريقة، التحول من حاسوب موجود في كندا إلى آخر في نيوزيلندا، بمجرد النقر بزر الموس. (Zatarian،noel،2000، p24) .

بهذا يتضح أن المعلومات والوثائق المتداولة عبر الإنترنت وبفضل الشبكة العنكبوتية بكل مكوناتها، تفضي إلى حرية وسهولة الوصول إلى المعلومة دون أية رقابة، لذلك عملت العديد من الدول على فرض الرقابة على الإنترنت مثل: السعودية، سوريا، أوكرانيا، الصين، فالمواقع الإلكترونية سهلت على المنظمات الإرهابية توسيع أنشطتهم لأبعد الحدود من خلال تبادل الآراء والأفكار والمعلومات، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، كما ساعدتهم أيضا على جمع أكبر عدد ممكن من الأنصار لترويج أفكارهم ومبادئهم من خلال هذه المواقع ومنتديات الحوار، وغرف الدردشة، فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فإن إنشاء مواقع على الإنترنت واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين أصبح ممكنا، بل نجد لبعض المنظمات الإرهابية آلاف المواقع، لضمان الانتشار الواسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها. (عطية،2014).

لهذا يقوم الإرهابيين بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات وكيفية اختراق وتدمير المواقع وطرق اختراق البريد الالكتروني وكيفية الدخول على المواقع المحجوبة وطريقة لنشر الفيروسات.

إن الإنترنت بمختلف وتعدد وتنوع تطبيقاتها، سهلت عملية تعلم طرق الإرهاب والإجرام من حيث تبادل الآراء والأفكار والمعلومات، كما وجد الإرهابيين ضالتهم في تلك الوسائل الرقمية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة المعلومات العالمية، وأصبحت المواقع من أبرز الوسائل المستخدمة في الإرهاب الالكتروني.

3.10. اختراق وتدمير المواقع :

يقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي(service–PC) أو مجموعة نظم مترابطة شبكيا (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

وتتم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ، ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي، أما تدمير المواقع فهو الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام إلي (Server–PC) أو مجموعة نظم مترابطة شبكيا (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

(عبد الله ،2019/05/01).

ومن الوسائل الناجحة لتدمير المواقع، ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف، للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدي عليه. (كافي، ص153).

أما عن أسباب تسهيل عملية تدمير المواقع ما يلي:

1–ضعف الكلمات السرية، فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسر وتحصين الكلمات السرية من المخترق.

2–عدم وضع برامج حماية كافية لحماية المواقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق للموقع.

3-استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر أو تستخدم برامج وأنظمة غير موثوقة أمنيا ولا يتم تحديثها باستمرار.

4-عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية. (عياد،2008، ص 112)، تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.

5- عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة فيه وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في السنوات الأخيرة ، وبعد عام 2002م من أكثر الأعوام اختراقا فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات (weimann,2004).

11-الإرهاب الالكتروني والعولمة:

لقد كان للعولمة والتغير التكنولوجي بالغ الأثر في تنشيط الأعمال الإرهابية وتمويلها، فقد أدت إلى تزايد حجم التحويلات المالية بصورة سريعة فبعد أن كان حجم الأموال التي تم تحويها حول العالم لا يتجاوز في عام2000 ما قيمته 119 مليار دولار أمريكي، تضاعف بعد ست سنوات إلى 225 مليار دولار في عام 2006 ووصل في عام 2012 إلى ما يقارب 500 مليار دولار وهو في تزايد مستمر مدعوما بالطفرة التكنولوجية في التجارة الدولية وتحويلات النقود بعد استحداث خدمة (M-payement) التي تستخدم الهواتف النقالة لنقل الأموال الكترونيا فضلا عن زيادة أهمية نقل وتخزين الأموال عبر كيفيات الكترونية كـ .(Cash.U) و(E-gold) وهو ما سهل وزاد من حجم التحويلات خاصة في الدول ذات الأنظمة المالية الهشة، ناهيك عما وفرته خدمة الإنترنت من وسائل اتصال مجانية في سهلت الاتصال بين عناصر الجماعات الإرهابية والترويج لفكرها وحتى التدريب على صناعة المواد المتفجرة من خلال إلقاء المحاضرات والتحضير لعمل العبوات الناسفة باستخدام المواقع التي تتيح نشر مقاطع الفيديو التي تحمل تلك المضامين والحصول على المعلومات عن المواقع المستهدفة بكبسة زر واحدة على أحد محركات البحث العملاقة في الإنترنت : (Google)و(Yahoo) وغيرها (عيسى،2009، ص 08) .

ومن هنا فقد شكلت هذه التسهيلات المتوفرة للجماعات الإرهابية عائقا كبيرا أمام تمويل جهود مكافحة الإرهاب الالكتروني من خلال ما يلي:

– مكنت التنظيمات الإرهابية من الظفر بكثير من مصادر التمويل التي تقوم عليها أعمالها الإرهابية المختلفة.

–حدت كثيرا من حجم التمويل الذي تحتاجه تلك التنظيمات للقيام بالمهام التي تعمل على تحقيقها.

–أشغلت الكثير من الدول بمسألة محاربة ومراقبة تلك الجماعات عبر استخدام التكنولوجيا المتطورة وما يتطلبه ذلك من المال والجهد والكوادر المتدربة.

–دفعت الكثير من الدول إلى إيقاف بعض المواقع على الإنترنت كمواقع التواصل الاجتماعي (الفيس بوك وتوتير واليوتيوب وغيرها) وبرامج الاتصال المجاني (الوتساب والفايبر والتاكو وغيرها)، التي تسهل تلك الأعمال مما سبب لها بعض الإشكالات في مجال حرية التعبير وحقوق الإنسان (الصياد،2002، ص 120).

وعلى الرغم من ذلك فإن التكنولوجيا الحديثة وإن عدت في جانب منها قيدا على تمويل جهود مكافحة الإرهاب الالكتروني، فإنها في الوقت ذاته سهلت الكثير من عمليات الرقابة الإلكترونية على أنشطة التنظيمات الإرهابية ويسرت التعرف على أماكن ومواقع تواجدهم عبر خدمة الـ(GPS)، وغيرها من الخدمات الإلكترونية الأخرى المتوفرة في الهواتف الجوالة، مما يقلص الكثير من الجهد الميداني الذي يمكن أن يبذل لولا توافر هذه الخدمات (دراسة أمريكية، 2019).

وعلى هذا الأساس، فإن الفائدة التي توفرها الخدمات الإلكترونية تفوق بكثير القيود والعقبات والمخاوف التي تتركها على تمويل جهود مكافحة الإرهاب الالكتروني، لهذا كان من الضروري الاستفادة من تلك الخدمات من خلال تأهيل كوادر متخصصة في هذا المجال وقلب المعادلة الإلكترونية لصالح جهود مكافحة الإرهاب الالكتروني والتضييق على التنظيمات الإرهابية لمنعها من التصرف بحرية وبالتالي الحد من أنشطتها الإجرامية.

12–خطورة الإرهاب الالكتروني

إن خطورة الإرهاب الالكتروني تزداد في الدول المتقدمة التي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية. مما يجعلها هدفا سهل المنال، فبدلا من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح، تدمير البنية المعلوماتية وتحقيق آثار تدميرها تفوق مثليتها، حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة وإنماء، أو اختراق النظام المصرفي وإلحاق الضرر

بأعمال البنوك وأسواق المال العالمية، ونظرا لارتباط المجتمعات العالمية فيما بينها ينظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية. فقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة. (قرار مجلس الأمن،2019).

كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في منزله أو في مكتبه أو في غرفته الفندقية وبعيدا عن أنظار السلطة والمجتمع.

وتجدر الإشارة إلى أن تدمير شبكة معلوماتية تقدر خسائرها اليومية بأضعاف مضاعفة لانهيار مبنى أو قصف منشآت أو تفجير جسر أو اختطاف طائرة، وعندما انقطع الكبل البحري الذي يربط أوربا بالمشرق الأوسط في نهاية شهر يناير عام 2007 وما أعقبه من انقطاع آخر للكبل القريب من ساحل دبي وخليج عمان، وقدرت الخسائر المتولدة من ذلك والتي لحقت بانقطاع الاتصالات والتعاملات الإلكترونية بمئات الملايين من الدولارات، ولا تزال الأسباب مجهولة من وراء ذلك الانقطاع المفاجئ.

13-طرق مكافحة الإرهاب الالكتروني

إن التقدم التقني الذي يشهده العالم اليوم له من الجوانب الايجابية ما لا يعد ولا يحصى، إلا أن جوانبه السلبية تكاد تكون مدمرة ما لم تكن هناك مقاومة لهذه السلبيات، فمن خلال شبكة الإنترنت يمكن معرفة كيفية صناعة التفجيرات وغسيل الأموال وصناعة القنبلة النووية وسرقة البطاقات الائتمانية ، ولقد أظهر تقرير لمركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على المؤسسات الأمنية في إجراءات معالجة المعلومات والبيانات الإلكترونية وتعاون ضحايا جرائم الكمبيوتر مع رجال الأمن إلى جانب الحاجة إلى التعاون الدولي المتبادل للبحث الجنائي والنظامي في مجال مكافحة جرائم الكمبيوتر أو الإرهاب الالكتروني.

ومن هذا المنطلق تسهر المنظمات العالمية على استخدام الرسائل العلمية الحديثة والطرق العلمية المدروسة واستنفاذ كل الطاقات في مجال مكافحة الإرهاب وذلك على النحو التالي:

– اعتماد المنهج العلمي في العمل الأمني، باتخاذ التخطيط العلمي أساسا للعمل الأمني، والتزام الأجهزة الأمنية بصيغ البحث العلمي واستثمار التكنولوجيا الحديثة، واستحداث مراكز البحوث

والدراسات الأمنية، ولعل أقدم دول العالم في استخدام منهج تحليلي للمعلومات باستخدام الحاسب الآلي هي الولايات المتحدة الأمريكية.

– تعاون أجهزة الأمن لتحقيق وملاحقة المجرمين في الجرائم الخطيرة عن طريق السرعة وتبادل المعلومات والخبرات بين أعضاء الجماعة الدولية من خلال التقنيات الحديثة.

– تحديث أجهزة ووسائل مكافحة الإرهاب بما يتلاءم مع تطور العمليات الإرهابية.

– تبادل المعلومات والخبرات والدراسات والأبحاث بين الدول أعضاء الجماعة الدولية في مجال مكافحة الإرهاب، ودعم مراكز الدراسات الأمنية لتتمكن من أداء رسالتها في الإعداد والتدريب للكوادر الأمنية المتخصصة.

– دعم عمليات التعاون والتنسيق الأمني المباشر مع وزارات وأجهزة الأمن في مجال تبادل المعلومات والبيانات المتابعة ومتابعة ورصد مراكز النشاط الإرهابي بالخارج واتصالاتها بالداخل.

– إتاحة المعلومات والبيانات الخاصة بالعناصر الإرهابية الهاربة للدول التي تقيم فيها بهدف ملاحظتها وضبطها وإقامة الأدلة المادية والقانونية على تورطها في الأنشطة وذلك باستخدام الوسائل التكنولوجية الحديثة.

– إتاحة استخدام الأجهزة الأمنية لتكنولوجيا التشويش على أجهزة الحاسب الآلي أو تعطيلها لمنع تداول المعلومات والبيانات الحيوية الخاصة بالإرهابيين.

– تبادل الخبرات المتعلقة بالتنظيمات الإرهابية.

– كشف أهداف التنظيمات الإرهابية والتوعية بأخطار الإرهاب عن طريق وسائل الإعلام.

– استخدام التقنيات الحديثة في عمليات التحري والتطبيق والكشف من أدلة الجريمة.

– المساهمة في إتاحة خدمات البلاغ الرقمي للجمهور ومتابعة البلاغ.

– عقد دورات تدريسية وندوات علمية في سبيل التقدم التكنولوجي والتفوق التقني للعاملين بمجال المكافحة.

خاتمة:

لقد أصبح الإرهاب الالكتروني هاجسا يخيف العالم الذي أصبح عرضه لهجمات الإرهابيين عبر الإنترنت، الذين يمارسون نشاطهم التخريبي من أي مكان في العالم وهذه المخاطر تتفاقم بمرور كل يوم ،لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية التي سببت أضرارا جسيمة على الأفراد والمنظمات الدولية، بالإضافة إلى ذلك فإن خطورة الإرهاب الالكتروني لا تقف عند ذلك ،لأن الخطوة الأمنية والمجتمعية تأخذ بعدا أخطر إذا أدركنا أن الجماعات المتطرفة كانت من أوائل الجماعات الفكرية التي دخلت العالم الالكتروني حتى قبل ظهور شبكة الإنترنت بسنوات.

وفي ضوء ما تقدم، ولمواجهة هذه الظاهرة الخطيرة على المجتمعات والأمم، ينبغي العمل على تفعيل المكافحة الوقائية التي تسبق وقوع الجريمة الإلكترونية، وذلك من خلال ما يلي:

- سن القوانين والأنظمة الخاصة التي تسد الثغرات المستغلة في ارتكاب الجرائم الإلكترونية.
- التأكيد على أهمية نشر القيم الإنسانية الفاضلة، وإشاعة روح التسامح والتعايش، وحث وسائل الإعلام على الامتناع عن نشر المواد الإعلامية الداعية للتطرف والعنف.
- الاهتمام بالدور الوقائي الذي يسبق وقوع جريمة الإرهاب الالكتروني، وذلك من خلال تفعيل دور المؤسسات التوعوية مثل المسجد، دور التعليم، ووسائل الاعلام، والتحذير من خطورة هذه الجرائم على الأسرة والمجتمع.
- إنشاء مدارس ومعاهد وأقسام في الجامعات، ومراكز بحثية تعنى بالأمن المعلوماتي وبتدريب كوادر، لمواكبة كل ما هو حديث في هذا المجال.
- عقد الاتفاقيات بين الدول بخصوص الجرائم الإلكترونية وقاية وعلاجا وتبادلا للمعلومات والأدلة.
- حث الدول على الانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.
- التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية الإلكترونية الواقعة في أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي.

-المصادر والمراجع :

1-مراجع باللغة العربية:

أحمد حسين السويدان (2005)، *الإرهاب الدولي في ظل المتغيرات الدولية*، بيروت: منشورات الجبلي الحقوقية.

أحمد عيسى، (2009)، *الإعلام، الإرهاب وحقوق الإنسان في عصر العولمة*، الإسكندرية: مركز الإسكندرية للكتاب.

أريك موريس والان هو، (1991)، *الإرهاب التهديد والرد عليه*، ترجمة أحمد حمدي محمود، مصر: الهيئة المصرية.

إسماعيل محمود عبد الرحمان، (2014)، *الإعلام والإرهاب والثقافة البديلة*، دار القاهرة: مكتبة الوفاء القانونية.

أيسر محمد عطية، (أيام02-04 -2014)، دور *الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهتها* ، ملتقى دولي، بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، جامعة القاهرة، مصر.

زهراء، (2009)، *6 آلاف موقع الكتروني تستغله القاعدة لنشر الوشايات الكتابية*، جريدة الشعب، يومية جزائرية، العدد 14916. 24 جوان.

سامي علي حامد عياد، (2008)، *استخدام تكنولوجيا المعلومات في مكافحة الإرهاب*، الإسكندرية: دار الفكر الجامعي.

عامر وهاب، خلف العاني، (2013)، *الإعلام ودوره في معالجة ظاهرة الإرهاب*، عمان: دار مكتبة الحامد للنشر والتوزيع.

عامر قنديلجي، (2002)، *البحث العلمي واستخدام مصادر المعلومات التقليدية والإلكترونية*، القاهرة: دار اليازوري العلمية للنشر والتوزيع.

عبد الرزاق محمد الدليمي، (2010)، *الدعاية والإرهاب*، عمان: دار جرير للنشر والتوزيع.

عبد العاطي أحمد الصياد، (2002)، *الإرهاب والعولمة*، الرياض: مركز الدراسات والبحوث الأكاديمية نايف العربية للعلوم الأمنية.

عدنان هاشم سلطان، (2008)، *صناعة الإرهاب*، مصر: المكتب المصري الحديث.

علي عبد الرحيم، (2008)، *الإعلام العربي وقضايا الإرهاب*، القاهرة: مركز محروسة للنشر والخدمات الصحفية والمعلومات.

مشيب ناصر محمد أل زيران، (2011)، *المواقع الإلكترونية ودورها في نشر الغلو الديني وطرق مواجهتها من وجهة نظر المختصين*، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض.

مصطفى محمد موسى، (2015)، *الإرهاب الالكتروني، دراسة قانونية أمنية، تقنية، اجتماعية*، الأردن: دار الإعصار للنشر والتوزيع.

مصطفى يوسف كافي، ماهر عودة، محمود عزت اللحام، (2015)، *الإعلام والإرهاب الالكتروني*، الأردن: دار الإعصار للنشر والتوزيع.

ناظم نواف إبراهيم، (2009)، *ظاهرة العنف السياسي في العراق المعاصر بعد الاحتلال الأمريكي*، أطروحة دكتوراه، معهد البحوث والدراسات العربية، القاهرة، مصر.

إيهاب شوقي، (2019)، *الإرهاب الالكتروني*: على www ,entv ,tv/new/show subject

عبد الرحمان بن عبد الله السند، (2019)، *وسائل الإرهاب الالكتروني وطرق مكافحتها*: من الموقع: .shamela.ws/browse /book

دراسة أمريكية متخصصة بشأن تجفيف منابع تمويل الإرهاب، منشور على شبكة الإنترنت على الرابط الاتي:www.ahewar.org/debat/show.art.asp .

قرار مجلس الأمن الأخير الرابط الآتي:www.aliragnet.net

2-المراجع باللغة الفرنسية:

Alex des forges, (2011), *cyber terrorisme: quel périmètre.* Fiche de l'irsem، n°11 décembre 2011.

DOROTHY E. Denning, (2000), *cyber terrorism, global dialogue*, Autun, 2000.N °11

File://C:Usens/sarra/Dowloads.

Gabriel Weismann,(2004), *cyberterrorism : how real the threat ?* united states institute of peace December 2004.

Jean Paul Ney,(1999), *terreurs virtuelles*, éditions Carnot, France 1999.

Patrick Chambet،,(2016), *cyber terrorisme*, http :www, chambet.com/ publications/ cyber terrorisme.

Vahe Zatarian, Emie Noël (2000), *cyber mondes où tu nous mènes grand frère*, édition, médecine, Genève, 2er édition, février, 2000.